Linear Network Coding Over Rings – Part I: Scalar Codes and Commutative Alphabets

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

***Abstract*— Linear network coding over finite fields is a well-studied problem. We consider the more general setting of linear coding for directed acyclic networks with finite commutative ring alphabets. Our results imply that for scalar linear network coding over commutative rings, fields can always be used when the alphabet size is flexible, but other rings may be needed when the alphabet size is fixed. We prove that if a network has a scalar linear solution over some finite commutative ring, then the (unique) smallest such commutative ring is a field. We also show that fixed-size commutative rings are quasi-ordered, such that all the scalar linearly solvable networks over any given ring are also scalar linearly solvable over any higher-ordered ring. We study commutative rings that are maximal with respect to this quasi-order, as they may be considered the best commutative rings of a given size. We prove that a commutative ring is maximal if and only if some network is scalar linearly solvable over the ring, but not over any other commutative ring of the same size. Furthermore, we show that maximal commutative rings are direct products of certain fields specified by the integer partitions of the prime factor multiplicities of the ring's size. Finally, we prove that there is a unique maximal commutative ring of size m if and only if each prime factor of m has multiplicity in $\{1, 2, 3, 4, 6\}$. As consequences, 1) every finite field is such a maximal ring and 2) for each prime p, some network is scalar linearly solvable over a commutative ring of size p^k but not over the field of the same size if and only if $k \notin \{1, 2, 3, 4, 6\}$.**

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

I. Introduction

LINEAR coding over finite fields has been the cornerstone of a large portion of network coding research during the last decade. Scalar linear codes over fields consist of network out-edges carrying field elements which are linear combinations of their input field elements. It has been shown that scalar linear codes over finite fields are sufficient for multicast networks [25]. This means that whenever a multicast network is solvable, it must be scalar linearly solvable over some finite field. In contrast, the more general class of vector linear codes over fields has out-edges carrying linear combinations of input vectors of field elements, where the linear combination coefficients are matrices of field elements. Vector linear codes over finite fields (or even more generally, vector linear codes over rings or linear codes over modules) are known to not always be sufficient for non-multicast networks [8]. This means that solvable non-multicast networks may sometimes require non-linear codes to implement a solution, no matter what field or vector dimension is chosen. Even though linear network codes may be suboptimal for some networks, they have been attractive to study for two primary reasons:

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

(2) They may be mathematically tractable to analyze.

One of the most general forms of linear network coding uses codes over modules. Specifically, a module consists of an Abelian group $(G, \oplus)$, a ring R, and a scalar multiplication

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

that together satisfy certain properties. A linear network code over such a module consists of edge functions of the form

$$(C_1 \cdot x_1) \oplus \cdots \oplus (C_m \cdot x_m)$$

where the variables $x_1, \ldots, x_m$ are elements of G and represent input symbols to a network node, and the multiplier coefficients $C_1, \ldots, C_m$ are constant elements of R.[1] As an example, vector linear network coding occurs when R is the ring of $n \times n$ matrices over a finite field, G is the set of n-dimensional vectors over the same field, and $\cdot$ is matrix-vector multiplication over the field. As another example, if G is the additive group of the finite ring R and $\cdot$ is multiplication in R, then we get scalar linear coding over the ring alphabet R.

In this paper (i.e. Part I), we focus on the further special case where R is a commutative ring, and we make comparisons to the even more specialized (and more studied) case where R is a field. In a companion paper [5] (i.e. Part II), we study vector linear codes and non-commutative rings and specifically contrast the results with the results on scalar codes and commutative rings given in this present paper. Since the founding of network coding in 2000, network codes whose edge functions are linear over fixed finite field alphabets have been studied extensively (e.g. [9], [11], [13], [16], [18]–[25], [29], [31]–[34]). In contrast, very little is presently known about linear network coding over more general ring and module alphabets.

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

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

Communicated by P. Sadeghi, Associate Editor for Coding Techniques.

Digital Object Identifier 10.1109/TIT.2017.2697421

[1] Throughout this paper it will be assumed that rings always have multiplicative identities, as any reasonable linear network code over rings would require.

Since a field is a commutative ring that has inverses for all its non-zero elements, a linear network code over a ring may be implemented analogously to a linear code over a field, by performing multiplications and additions over the ring for each nontrivial edge function.[2] It is natural, then, to ask whether it is better in some sense to use linear coding over a finite field alphabet or over some other ring alphabet of the same size. Additionally, a finite field alphabet must have prime-power size, so linear codes over rings may be of value if non-power-of-prime alphabet sizes are required.

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

Many interesting questions regarding linear codes over rings exist: Which rings minimize the alphabet size needed for a scalar linear solution? What is the best ring alphabet of a given size to use for linear network coding? Are finite fields always the best choice? Can a network be scalar linearly solvable over a ring, even though it is not scalar linearly solvable over the field of the same size? Is the set of networks that are scalar linearly solvable over some field a proper subset of the set of networks that are scalar linearly solvable over some ring? For alphabets whose sizes are not powers of primes, over which rings (if any) are particular networks scalar linearly solvable? We address these and some other questions in this paper.

Two of our main results are:

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

(2) If a network has a scalar linear solution over a commutative ring that is not a field, then it also has a scalar linear solution over a field of strictly smaller size.

A. Network Model

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

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

In particular, we will consider codes over alphabets that have addition and multiplication operations, namely finite rings. If $\mathcal{A}$ is a ring alphabet, then a function

$$f : \mathcal{A}^m \longrightarrow \mathcal{A}$$

is *linear over* $\mathcal{A}$ if it can be written in the form

$$f(x_1, \ldots, x_m) = C_1 x_1 + \cdots + C_m x_m$$

where $C_1, \ldots, C_m$ are constant values in $\mathcal{A}$. A code is *scalar linear over* $\mathcal{A}$ if each edge function and each decoding function is linear over $\mathcal{A}$.

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

In contrast, in a *k-dimensional vector linear code over* $\mathcal{A}$, messages and edge symbols are k-dimensional vectors over $\mathcal{A}$ (i.e. the alphabet is $\mathcal{A}^k$), and edge functions are linear combinations of input vectors, using $k \times k$ matrices over $\mathcal{A}$ as coefficients. Scalar linear codes are a special case of vector linear codes where $k = 1$.

B. Related Work

Ahlswede *et al.* [1] introduced network coding in 2000 and showed that it is possible to increase the information throughput of a network by allowing nodes to transmit functions of their inputs, as opposed to simply relaying their inputs. Li *et al.* [25] showed that every solvable multicast network is scalar linearly solvable over every sufficiently large finite field, although it was shown in [8] that non-multicast networks may not have this property. More generally, it was recently shown in [4] that for each composite number m, there exists a network that is not linearly solvable over any module alphabet yet is non-linearly solvable over an alphabet of size m.

Networks were demonstrated by Riis [29], Rasala Lehman and Lehman [28], and in [10] that are solvable non-linearly but not scalar linearly over the same alphabet size. Effros *et al.* [14] showed that network coding and index coding are equivalent in a general setting, including with linear and non-linear codes. It is not currently known whether there exists an algorithm that determines if a network is solvable; however, determining whether a network is scalar linearly solvable over a particular field has been studied extensively.

Koetter and Médard [21] showed that for every network, there exists a finite collection of polynomials, such that for

[2] The most efficient implementation of ring arithmetic generally depends on the specific algebraic properties of the ring being used.

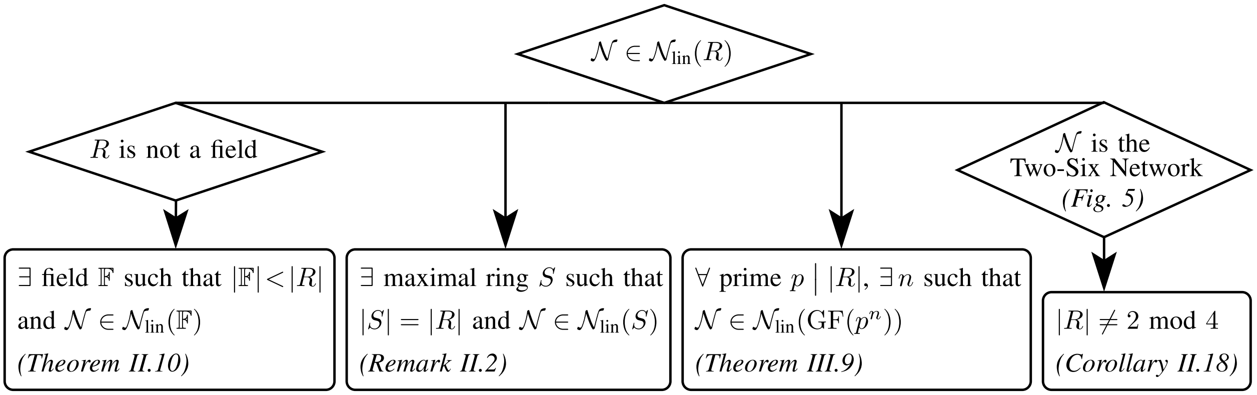
$\mathcal{N} \in \mathcal{N}_{\text{lin}}(R)$
R is not a field
$\mathcal{N}$ is the Two-Six Network *(Fig. 5)*
$\exists$ field $\mathbb{F}$ such that $|\mathbb{F}| < |R|$ and $\mathcal{N} \in \mathcal{N}_{\text{lin}}(\mathbb{F})$ *(Theorem II.10)*
$\exists$ maximal ring S such that $|S| = |R|$ and $\mathcal{N} \in \mathcal{N}_{\text{lin}}(S)$ *(Remark II.2)*
$\forall$ prime $p \mid |R|$, $\exists n$ such that $\mathcal{N} \in \mathcal{N}_{\text{lin}}(\text{GF}(p^n))$ *(Theorem III.9)*
$|R| \neq 2 \bmod 4$ *(Corollary II.18)*

Fig. 1. $\mathcal{N}$ denotes an arbitrary network, R denotes an arbitrary finite commutative ring, and $\mathcal{N}_{\text{lin}}(R)$ denotes the set of networks scalar linearly solvable over R. It follows from these results that finite fields minimize the alphabet size needed for a scalar linear solution over commutative rings, and the set of networks that are scalar linearly solvable over some commutative ring and the set of networks that are scalar linearly solvable over some field are equal.

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

The study of linear network codes over fields has led to efficient methods of constructing scalar linear solutions for networks that also minimize the field alphabet size. Ho *et al.* [18] described a random scalar linear coding technique where the probability that a code is a solution grows with the field size. Jaggi *et al.* [19] presented polynomial-time algorithms for designing scalar linear codes for multicast networks. Karimian *et al.* [20] showed there exists a class of non-multicast networks for which random scalar linear coding algorithms fail with high probability and presented a new approach to random scalar linear network coding for such networks. Lehman and Lehman [28] and Tavory *et al.* [34] independently showed that some solvable multicast networks asymptotically require finite field alphabets to be at least as large as twice the square root of the number of receiver nodes in order to achieve scalar linear solutions. Sun *et al.* [32] and Sun *et al.* [33] both demonstrated classes of multicast networks that are scalar linearly solvable over certain fields but not every larger field.

Médard *et al.* [27] showed that there can exist a network that is vector linearly solvable over some field but not scalar linearly solvable over any field. Sun *et al.* [31] demonstrated that, while vector linear codes can outperform scalar linear codes in terms yielding solutions for general networks, there can exist multicast networks that are not k-dimensional vector linearly solvable over GF(2) yet have scalar linear solutions over some field alphabet whose size is less than 2^k. Etzion and Wachter-Zeh [16] bounded the reduction in alphabet size needed for a vector linear solution to a multicast network as compared to a scalar linear solution. Ebrahimi and Fragouli [13] presented algorithms for constructing vector linear codes that achieve solutions not possible with scalar linear codes.

Convolutional network coding (e.g. [22], [23]) is a technique for linear coding for networks that may contain cycles, and the alphabets in such codes can be viewed as principal ideal domains (and more generally as discrete valuation rings), which are not necessarily finite. However, in this paper, we focus on acyclic networks and finite coding alphabets.

To our knowledge, outside of the context of the insufficiency of linear codes and convolutional coding, there has been little study of linear network codes over more general ring and module alphabets. In this paper and its companion, we consider such linear codes and compare them to the well-studied case of linear codes over fields.

C. Our Contributions

In this paper (i.e. Part I), we restrict attention to network coding alphabets that are finite rings with at least two elements and specifically focus on scalar linear codes over commutative rings with identity. Our main results show that for networks that use scalar linear codes over commutative rings, finite fields can always be used if the alphabet size is flexible, but if the alphabet size is fixed, then finite fields may not always be the best choice for every network. Figure 1 summarizes our main results for fixed networks, and Figure 2 summarizes our main results on the "best" commutative rings of a fixed size. We outline the remainder of the paper in what follows.

We prove (in Theorem II.10) that if a network has a scalar linear solution over some commutative ring, then the unique smallest-size commutative ring over which the network has a scalar linear solution is a field. Thus, for a given network, if the minimum alphabet size is desired for scalar linear network coding, it suffices to use finite fields. This result also shows that networks that are scalar linearly solvable over some commutative ring are also scalar linearly solvable over some field although not necessarily of the same size.

Section II introduces a "dominance" relation on finite rings, such that all networks that are scalar linearly solv-

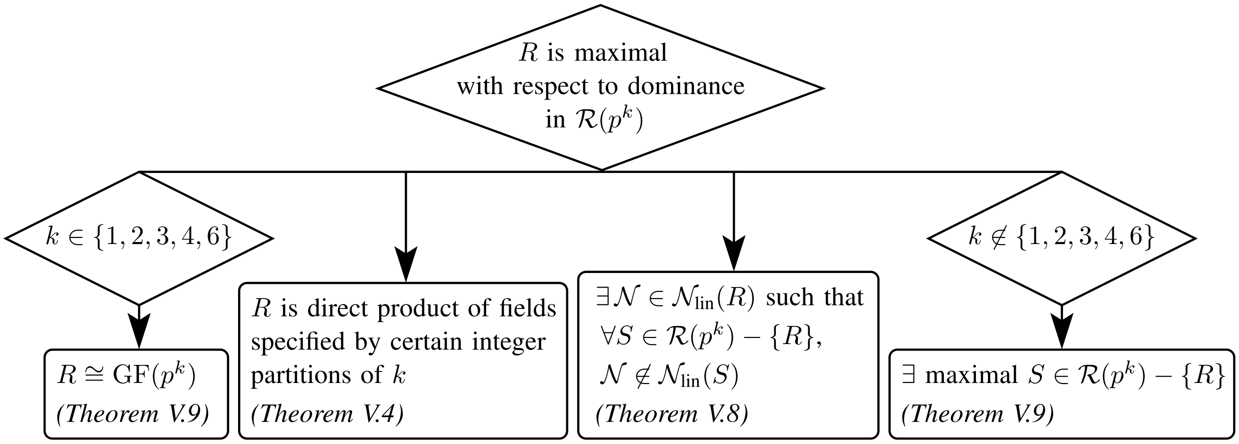
R is maximal with respect to dominance in $\mathcal{R}(p^k)$
$k \in \{1,2,3,4,6\}$
$k \notin \{1,2,3,4,6\}$
$R \cong \mathrm{GF}(p^k)$ *(Theorem V.9)*
R is direct product of fields specified by certain integer partitions of k *(Theorem V.4)*
$\exists \mathcal{N} \in \mathcal{N}_{\text{lin}}(R)$ such that $\forall S \in \mathcal{R}(p^k) - \{R\}$, $\mathcal{N} \notin \mathcal{N}_{\text{lin}}(S)$ *(Theorem V.8)*
$\exists$ maximal $S \in \mathcal{R}(p^k) - \{R\}$ *(Theorem V.9)*

Fig. 2. A ring S *is dominated by* a ring R if every network that is scalar linearly solvable over S is also scalar linearly solvable over R. This dominance induces a *quasi-order* on $\mathcal{R}(p^k)$, i.e. the set of commutative rings of size p^k. The rings which are *maximal* with respect to these quasi-orders are, in some sense, the best rings of a given size. The finite field GF(p^k) is always maximal *(Theorem II.16)*, but it follows from these results that, whenever $k = 5$ or $k \geq 7$, there are other maximal rings of size p^k. GF(8) × GF(4) is the smallest such maximal commutative ring *(Corollary V.10)*. In particular, it follows that there exist networks with scalar linear solutions over some ring of size p^k but not the field GF(p^k), whenever $k \notin \{1, 2, 3, 4, 6\}$. The maximal rings of size $p_1^{k_1} \cdots p_t^{k_t}$ (for distinct primes $p_1, \ldots, p_t$) are direct products of maximal rings of size $p_1^{k_1}, \ldots, p_t^{k_t}$ *(Remark V.5)*.

able over a given ring are also scalar linearly solvable over any ring that dominates the given ring. We show that this relation is a quasi-order on the set of commutative rings of a given size.[3] We also demonstrate (in Theorem II.19 and Corollary III.3) non-isomorphic commutative rings of the same size that are equivalent with respect to dominance, and we show (in Theorem II.20) that dominance is a total quasi-order of the commutative rings of size p^2.

Section II-D analyzes the scalar linear solvability of a class of multicast networks. We show (in Theorem II.16) that for every finite field, there exists a multicast network that is scalar linearly solvable over the field but is not scalar linearly solvable over any other commutative ring of the same size. This demonstrates that every finite field is maximal with respect to the dominance. We also show (in Corollary II.18) that there exists a solvable multicast network that is not scalar linearly solvable over any ring whose size is equal to 2 mod 4, which contrasts with the fact that every solvable multicast network is scalar linearly solvable over every sufficiently large field.

Section III compares various commutative rings with respect to dominance. We demonstrate (in Theorem III.8) that some network is scalar linearly solvable over a commutative ring of size 32 but is not scalar linearly solvable over any other commutative ring of size 32, including the field GF(32), and we later prove (in Corollary V.10) that 32 is the size of the smallest such commutative ring alphabet where this phenomenon can occur.

We prove (in Theorem III.9) that whenever a network is scalar linearly solvable over a commutative ring, the network must also be scalar linearly solvable over a field whose size divides the ring size. In fact, for each prime factor of the ring size, there is a corresponding such field whose characteristic equals the prime factor. As a consequence (in Corollary III.11), whenever a network is scalar linearly solvable over a ring whose size is a product of distinct primes (i.e. “square free”), the network must also be scalar linearly solvable over each finite field whose size is a prime factor of the ring size. However, we demonstrate (in Corollary III.12) that when the ring size is not square free, the particular ring may need to be examined in order to determine over which fields the network is scalar linearly solvable.

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

Section V connects the relations of ring dominance and partition division. We prove (in Theorem V.4) that, when restricting to commutative rings of a given size, the maximal commutative rings under dominance are precisely partitions rings where each partition is maximal under partition division. We prove (in Theorem V.8) that a finite commutative ring is maximal if and only if there exists a network that is scalar linearly solvable over the ring but is not scalar linearly solvable over any other commutative ring of the same size.

Finally, we prove (in Theorem V.9) that if p is prime, then the field GF(p^k) is the unique maximal commutative ring of size p^k whenever $k \in \{1, 2, 3, 4, 6\}$, but if $k = 5$ or $k \geq 7$, then there exist multiple maximal commutative rings of size p^k. This result is also generalized to commutative rings of non-power-of-prime sizes in Theorem V.9. Since there can exist more than one maximal ring of a given size, there are instances

[3] Although the relation is defined on all finite rings, a maximal ring will always refer to a commutative ring which is maximal with respect to the quasi-order on the set of commutative rings of a given size.

where scalar linear solutions cannot be obtained using finite field alphabets of a given size but can be achieved using other commutative rings of the same size.

Part II [5] studies similar network coding questions with emphasis on non-commutative rings and vector linear codes.

II. Ring Dominance

A *quasi-order*[4] $\preccurlyeq$ on a set A is a subset of $A \times A$ that is reflexive and transitive. We write $x \preccurlyeq y$ to indicate that the pair (x, y) is in the relation. Each quasi-order induces an equivalence relation on A defined by $x \equiv y$ if and only if $x \preccurlyeq y$ and $y \preccurlyeq x$. We denote the equivalence class of x by $[x]$. Any quasi-order naturally extends to a partial order on the equivalence classes by defining $[x] \preccurlyeq [y]$ if and only if $x \preccurlyeq y$. An element $x \in A$ is said to be *maximal* with respect to the quasi-order if for all $y \in A$, we have $y \preccurlyeq x$ whenever $x \preccurlyeq y$. The same definition of maximal applies with respect to the induced partial order on equivalence classes.

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

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

Definition II.1: For any two finite rings R and S, we say S *is dominated by* R (denoted $S \preceq R$) if every network that is scalar linearly solvable over S is also scalar linearly solvable over R.

Equivalently, $S \preceq R$ if and only if $\mathcal{N}_{\text{lin}}(S) \subseteq \mathcal{N}_{\text{lin}}(R)$. On the other hand, S is not dominated by R whenever there exists a network with a scalar linear solution over S but not over R.

For each $m \geq 2$, it can be verified that the relation $\preceq$ is a quasi-order on the set $\mathcal{R}(m)$. Throughout this paper, whenever we refer to a finite commutative ring as being *maximal*, we mean the ring is maximal with respect to the relation $\preceq$ on the set of commutative rings of the same size. Since $\mathcal{R}(m)$ is a finite set, every ring $R \in \mathcal{R}(m)$ is dominated by some maximal ring, so there must exist at least one maximal ring in $\mathcal{R}(m)$.

The induced equivalence relation on rings has the property that $R \equiv S$ if and only if $\mathcal{N}_{\text{lin}}(R) = \mathcal{N}_{\text{lin}}(S)$. It turns out that the exact same set of networks can sometimes be scalar linearly solvable over non-isomorphic rings of the same size (as illustrated later, in Theorem II.19 and Corollary III.3), which means that the quasi-order $\preceq$ is not anti-symmetric on $\mathcal{R}(m)$.

Intuitively, if a ring R dominates a ring S of the same size, it may be viewed as advantageous[5] to use R instead of S in a network coding implementation, since any network that is scalar linearly solvable over S is also scalar linearly solvable over R. If, additionally, $\mathcal{N}_{\text{lin}}(S) \subset \mathcal{N}_{\text{lin}}(R)$ then even more networks are scalar linearly solvable over R.

A maximal commutative ring R has the desirable property that, for any commutative ring S of the same size, the set of networks that are scalar linearly solvable over R cannot be a proper subset of the set of networks that are scalar linearly solvable over S. Thus, in this sense, maximal rings may be considered the "best" commutative rings to use for network coding, and non-maximal rings are always "worse" than some maximal ring of the same size.

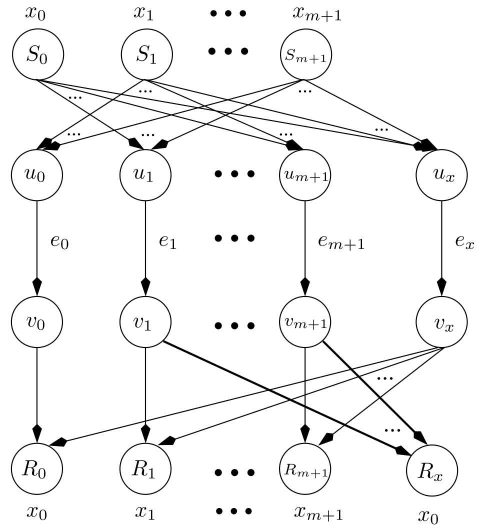

Fig. 3. The Char-m Network has source nodes $S_0, S_1, \ldots, S_{m+1}$ which generate the message $x_0, x_1, \ldots, x_{m+1}$, respectively. The node u_x has a single incoming edge from each source node, and the edge connecting nodes u_x and v_x carries the edge symbol e_x. For each $i = 0, 1, \ldots,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

Remark II.2: Every commutative ring of size m is dominated by a maximal commutative ring of size m, since $\mathcal{R}(m)$ is a finite quasi-order. Hence any network that is linearly solvable over some commutative ring of size m is linearly solvable over some maximal commutative ring of size m.

A. Fundamental Ring Comparisons

In this section, we prove results on ring dominance which will be used throughout the rest of the paper.

For each integer $m \geq 2$, the *Char-m Network* is given in Figure 3. This network was introduced as $\mathcal{N}_2(m, 1)$ (with a slight relabeling of sources) in [4] and is a generalization of the Fano Network. We use this class of networks to demonstrate some interesting properties of scalar linear codes over rings. The following lemma was shown in [4, Lemma IV.6] in a slightly more general form.

Lemma II.3: For each finite ring R and integer $m \geq 2$, the Char-m Network is scalar linearly solvable over R if and only if $\mathsf{char}(R) \mid m$.

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

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

[4] Also known as a *pre-order* (e.g. [30, Ch. 1]).

[5] There may be other advantages to using one ring over another, such as lower computational complexity arithmetic, ease of implementation, etc.

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

$$\begin{aligned} R_i : \quad & e_x - e_i = x_i \\ R_x : \quad & \sum_{i=1}^{m+1} e_i = x_0 + m \sum_{i=0}^{m+1} x_i \\ & \qquad = x_0 \quad \left[\text{from } \mathsf{char}(R) \;\middle|\; m\right]. \end{aligned}$$

On the other hand, if $\mathsf{char}(R) \nmid m$, then $m \neq 0$ in R, so this code is not a solution in this case, which agrees with Lemma II.3.

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

Corollary II.4: Let p and q be distinct primes, and let k and n be positive integers. No ring of size p^k is dominated by a ring of size q^n.

Proof: The characteristic of any ring of size p^k must divide p^k, so by taking $m = p^k$ in Lemma II.3, the Char-p^k Network is scalar linearly solvable over any ring of size p^k, but this network is not scalar linearly solvable over any ring of size q^n, since p and q are distinct primes. Hence, no ring of size p^k is dominated by a ring of size q^n. □

The following lemma is also shown in Part II Corollary I.7, where it follows from a more general result on linear codes over modules. However, we include the proof of Lemma II.5 in this paper for completeness.

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

Lemma II.5: Let R and S be finite rings. If $\phi : S \to R$ is a homomorphism, then S is dominated by R.

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

$$x_i = \sum_{j=1}^{n} B_{i,j}\, z_j$$

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

$$\begin{aligned} y &= \sum_{i=1}^{m} C_i\, x_i && (1) \\ &= \sum_{j=1}^{n} \left(\sum_{i=1}^{m} C_i\, B_{i,j} \right) z_j && (2) \end{aligned}$$

for some constants $C_1, \ldots, C_m \in S$. Then (1) describes y in terms of the inputs to the node, and (2) describes y in terms of the messages of the network.

Form a scalar linear code for $\mathcal{N}$ over R by replacing each coefficient C_i in (1) by $\phi(C_i)$. In other words, the coefficients in R that describe the linear combinations of the inputs at a node are the image under ϕ of the corresponding coefficients in S. We will now show that the coefficients in R that describe the linear combinations of the messages at a node are the image under ϕ of the corresponding coefficients in S.

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

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

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

$$\begin{aligned} y' &= \sum_{i=1}^{m} \phi(C_i)\, x'_i \\ &= \sum_{i=1}^{m} \phi(C_i) \sum_{j=1}^{n} \phi(B_{i,j})\, z'_j \\ &= \sum_{j=1}^{n} \sum_{i=1}^{m} \phi(C_i)\, \phi(B_{i,j})\, z'_j \\ &= \sum_{j=1}^{n} \phi\left(\sum_{i=1}^{m} C_i\, B_{i,j} \right) z'_j && (3) \end{aligned}$$

so the coefficients in R that describe the linear combinations of the messages at a node in (3) are the image under ϕ of the corresponding coefficients in S in (2).

If a decoding function in the linear solution over S produces the message z_l (i.e. $y = z_l$), then in (2)

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

Since ϕ is a homomorphism, $\phi(1) = 1$ and $\phi(0) = 0$, so the corresponding coefficients in (3) are

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

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

The following corollary is a special case of Lemma II.5 where S is a subring of R. A further special case, which will be used frequently throughout the rest of the paper, is when

$$R = \mathrm{GF}(p^k) \text{ and } S = \mathrm{GF}(p^m)$$

where p is prime and k, m are positive integers such that m divides k (e.g. see [3, Th. 2.3.1]). We also remark that for finite rings R_1 and R_2, the multiplicative identity of $R_1 \times R_2$ is in neither R_1 nor R_2, so while R_1 and R_2 are isomorphic to subsets of $R_1 \times R_2$ that are closed under addition and multiplication, neither is a subring of $R_1 \times R_2$.

Corollary II.6: If S is a subring of a finite commutative ring R, then S is dominated by R.

Proof: If S is a subring of R, then the identity mapping from S to R is an injective homomorphism, so by Lemma II.5, $S \preceq R$. □

In general, if a network is scalar linearly solvable over an alphabet $\mathcal{A}$, then it is also scalar linearly solvable over the alphabet $\mathcal{A}^k$, for any $k \geq 2$, by using a Cartesian product code.[6] In particular, if a network is scalar linearly solvable over the ring $\mathbf{Z}_n$, then it is also scalar linearly solvable over the direct product of rings

$$\mathbf{Z}_n^k = \underbrace{\mathbf{Z}_n \times \cdots \times \mathbf{Z}_n}_{k \text{ times}}.$$

Since $\mathbf{Z}_{n^k}$ is not isomorphic to the product ring $\mathbf{Z}_n^k$, it does not immediately follow that a network scalar linearly solvable over $\mathbf{Z}_n$ must also be scalar linearly solvable over $\mathbf{Z}_{n^k}$, and, in fact, the contrary is demonstrated below in Corollary II.7.

Corollary II.7: Let $m, n \geq 2$. The ring $\mathbf{Z}_m$ is dominated by the ring $\mathbf{Z}_n$ if and only if $n \bigm| m$.

Proof: Let $\phi : \mathbf{Z}_m \to \mathbf{Z}_n$ be defined such that $\phi(a)$ is the unique integer in $\{0, 1, \ldots, n-1\}$ satisfying

$$\phi(a) = a \bmod n.$$

If $n \bigm| m$, then ϕ is a surjective homomorphism, so by Lemma II.5 we have $\mathbf{Z}_m \preceq \mathbf{Z}_n$.

Conversely, if $n \nmid m$, then by Lemma II.3, the Char-m Network is scalar linearly solvable over $\mathbf{Z}_m$ but not $\mathbf{Z}_n$, since

$$\mathsf{char}(\mathbf{Z}_m) = m \bigm| m \quad \text{and} \quad \mathsf{char}(\mathbf{Z}_n) = n \nmid m$$

which implies $\mathbf{Z}_m$ is not dominated by $\mathbf{Z}_n$. □

If p is prime and $k \geq 2$, then by Corollary II.7, we have

$$\mathcal{N}_{\text{lin}}(\mathbf{Z}_{p^k}) \subset \mathcal{N}_{\text{lin}}(\mathbf{Z}_p).$$

In this sense, the larger ring alphabet $\mathbf{Z}_{p^k}$ is strictly "worse" than the smaller field alphabet $\mathbf{Z}_p$. This contrasts significantly with finite fields, where, generally speaking, larger field alphabets are "better" than smaller field alphabets. In particular, it follows from Corollary II.6 and Lemma II.15 that

$$\mathcal{N}_{\text{lin}}(\text{GF}(p)) \subset \mathcal{N}_{\text{lin}}(\text{GF}(p^k)).$$

B. Minimizing Alphabet Size

In this section, we prove our main result (Theorem II.10) on minimizing the alphabet size needed for a scalar linear solution over a commutative ring. The following lemma is a standard result of algebra related to ideals of rings which will be used to show Corollary II.9.

Lemma II.8 [12, Th. 7, p. 243]: If I is a two-sided ideal of ring R, then the mapping $\phi : R \to R/I$ given by $\phi(x) = x + I$ is a surjective homomorphism.

Corollary II.9 demonstrates that rings with large ideals are "bad" in the sense that they are always dominated by a smaller ring. Intuitively, rings without ideals should minimize the ring-size needed for a scalar linear solution. We formalize this notion in Theorem II.10.

Corollary II.9: If I is a proper ideal in a finite commutative ring R, then R is dominated by R/I.

Proof: The quotient ring R/I is finite and commutative. By Lemma II.8, there is a surjective homomorphism from R to R/I, so $R \preceq R/I$ by Lemma II.5. □

Theorem II.10 next demonstrates that when attempting to find a minimum size commutative ring over which a network is scalar linearly solvable, it suffices to restrict attention to finite field alphabets. In other words, if $\mathcal{N} \in \mathcal{N}_{\text{lin}}(R)$ for some commutative ring R, then there exists a field $\mathbb{F}$ such that

$$\mathcal{N} \in \mathcal{N}_{\text{lin}}(\mathbb{F}) \text{ and } \mathcal{N} \notin \mathcal{N}_{\text{lin}}(S)$$

whenever $S \in \mathcal{R}(n) - \{\mathbb{F}\}$ and $n \leq |\mathbb{F}|$.

Theorem II.10: If a network is scalar linearly solvable over a commutative ring, then the unique smallest such ring is a field.

Proof: Let $\mathcal{N}$ be a scalar linearly solvable network and let R be a smallest commutative ring over which $\mathcal{N}$ is scalar linearly solvable. Suppose R is not a finite field, and let I be a maximal ideal[7] of R. Since $\{0\}$ is an ideal in every ring, R must have at least one maximal (proper) ideal. Then R/I is a field (e.g. see [12, p. 254, Proposition 12]). By Lemma II.8, there is a surjective homomorphism from R to R/I, but R/I is a field and R is not, so the rings cannot be isomorphic. Therefore, $|R/I| < |R|$. By Corollary II.9, $R \preceq R/I$. Thus $\mathcal{N}$ must also be scalar linearly solvable over R/I, which contradicts the assumption that R is a smallest commutative ring over which $\mathcal{N}$ is scalar linearly solvable. □

C. Direct Products of Rings

Sun *et al.* [32] presented a class of multicast networks, called *Swirl Networks*, parameterized by an integer $\omega \geq 3$ that affects the number of independent messages generated by the source as well as the number of receivers and intermediate nodes. An interesting open question is for which p and k does there exist a multicast network that is scalar linearly solvable over some ring of size p^k but not over the field of the same size. Example II.11 demonstrates a particular Swirl Network is such a multicast network for $p = 2$ and $k = 13$.

Example II.11: It was shown in [32, p. 6185] that the Swirl Network with $\omega = 2^{13}$ is scalar linearly solvable over GF(2^9) *and* GF(2^4) *but not over* GF(2^{13})*. By using a Cartesian product code, this Swirl Network is scalar linearly solvable over the ring* GF$(2^9) \times$ GF(2^4).

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

Lemma II.12: A network is scalar linearly solvable over a finite direct product of finite rings if and only if the network is scalar linearly solvable over each ring in the product.

[6] In fact, the network is solvable over any alphabet of size $|\mathcal{A}|^k$ but linearity may not be preserved.

[7] Whenever we refer to a maximal ideal, we will always mean maximal with respect to set inclusion.

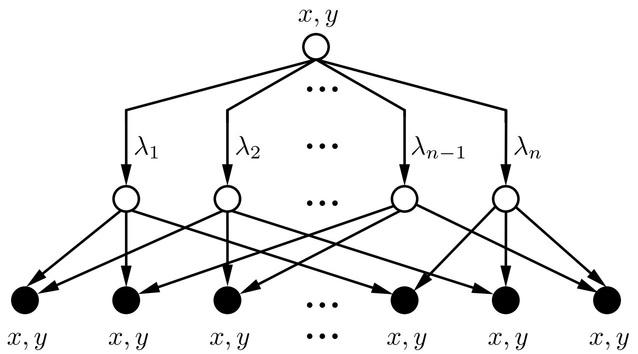

Fig. 4. The n-Choose-Two Network is parameterized by an integer $n \geq 2$. The network's name indicates the number of receivers.

Proof: Let $R_1, \ldots, R_m$ be finite rings. For each $j = 1, \ldots, m$, the projection mapping

$$\phi_j : R_1 \times \cdots \times R_m \to R_j$$

defined by $\phi_j(x_1, \ldots, x_m) = x_j$ is a surjective homomorphism, so by Lemma II.5,

$$R_1 \times \cdots \times R_m \preceq R_j$$

and thus any network that is scalar linearly solvable over the product ring $R_1 \times \cdots \times R_m$ is also scalar linearly solvable over each ring $R_1, \ldots, R_m$.

Conversely, any network that is scalar linearly solvable over each ring $R_1, \ldots, R_m$, is clearly scalar linearly solvable over the product ring $R_1 \times \cdots \times R_m$ by using a Cartesian product code of the scalar linear solutions over each $R_1, \ldots, R_m$. □

Lemma II.13 demonstrates that if each ring in a collection of rings dominates at least one ring in a second collection of rings, then the direct product of the rings in the first collection dominates the direct product of the rings in the second collection.

Lemma II.13: If each of the finite rings $S_1, \ldots, S_n$ is dominated by at least one of the finite rings $R_1, \ldots, R_m$, then $S_1 \times \cdots \times S_n$ is dominated by $R_1 \times \cdots \times R_m$.

Proof: Let $\mathcal{N}$ be a network that is scalar linearly solvable over $S_1 \times \cdots \times S_n$. Let $i \in \{1, \ldots, m\}$ and let j be such that $S_j \preceq R_i$. By Lemma II.12, $\mathcal{N}$ is scalar linearly solvable over S_j, so $\mathcal{N}$ is scalar linearly solvable over R_i. Thus by Lemma II.12, since i was chosen arbitrarily, $\mathcal{N}$ is also scalar linearly solvable over $R_1 \times \cdots \times R_m$. □

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

Remark II.14: For each finite ring R and all positive integers m, n, the direct product rings

$$\underbrace{R \times \cdots \times R}_{n \text{ times}} \text{ and } \underbrace{R \times \cdots \times R}_{m \text{ times}}$$

each dominate the other by Lemma II.13.

D. The n-Choose-Two Networks

Figure 4 shows a multicast network studied by Rasala Lehman and Lehman [28], which we call the *n-Choose-Two Network*. This network will be used to illustrate various facts in what follows. The network has two messages x and y, intermediate edge symbols $\lambda_1, \ldots, \lambda_n$, and $\binom{n}{2}$ receivers. Each receiver receives a unique pair of symbols (λ_i, λ_j), where $i < j$, and must decode both messages x and y.

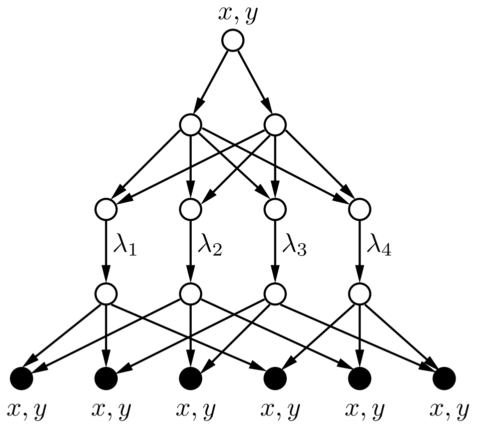

Fig. 5. The Two-Six Network is a multicast network studied in [10]. Each of the receivers gets a unique pair of edge symbols (λ_i, λ_j), where $i < j$. The network's name indicates the alphabet sizes over which the network is not solvable.

A variation of the 4-Choose-Two Network, called the *Two-Six Network*, is given in Figure 5. The Two-Six Network was used in [10] to show that a multicast network with a solution over a given alphabet size might not have a solution over all larger alphabet sizes.

The following lemma was shown in [28], and it characterizes the finite fields over which a scalar linear solution to the n-Choose-Two Network exists and gives an alphabet-size condition necessary for solvability.

Lemma II.15 [28, p. 144]: Let $\mathcal{A}$ be an alphabet and let $n \geq 3$.

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

The following theorem demonstrates that for each finite field, there exists a multicast network that is scalar linearly solvable over the field but is not scalar linearly solvable over any other commutative ring of the same size. Theorem II.16 additionally implies that GF(p^k) is not dominated by any other commutative ring of size p^k, which implies that GF(p^k) is maximal with respect to the quasi-order of commutative rings of size p^k.

Theorem II.16: For each prime p and positive integer k, the $(p^k + 1)$-Choose-Two Network is scalar linearly solvable over the field GF(p^k) *but not over any other commutative ring of size p^k.*

Proof: Lemma II.15 (b) implies that the (p^k+1)-Choose-Two Network is scalar linearly solvable over GF(p^k). On the other hand, if the (p^k+1)-Choose-Two Network network were scalar linearly solvable over a commutative ring R of size p^k that is not a field, then by Theorem II.10, it would also be scalar linearly solvable over some field whose size is less than p^k, which would contradict Lemma II.15. □

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

Theorem II.17: Let $m = p_1^{k_1} \cdots p_t^{k_t}$ denote the prime factorization of $m \geq 2$, and let $n \geq 3$. The n-Choose-Two Network is scalar linearly solvable over some ring of size m if and only if $p_i^{k_i} \geq n-1$ for each i.

Proof: Assume $p_i^{k_i} \geq n-1$. Then by Lemma II.15 (b), the n-Choose-Two Network is scalar linearly solvable over $\mathrm{GF}(p_i^{k_i})$. So by Lemma II.12, the n-Choose-Two Network is scalar linearly solvable over the product ring

$$\mathrm{GF}(p_1^{k_1}) \times \cdots \times \mathrm{GF}(p_t^{k_t})$$

which has cardinality m.

Conversely, suppose $m = p_1^{k_1} \cdots p_t^{k_t}$ and the n-Choose-Two Network is scalar linearly solvable over a ring R of size m. R is isomorphic to a direct product of rings of size $p_1^{k_1}, \ldots, p_t^{k_t}$ (e.g. see [26, p. 2]). For each $i = 1, \ldots, t$, let R_i be the ring of size $p_i^{k_i}$. Then by Lemma II.12, the n-Choose-Two Network is scalar linearly solvable over each of $R_1, \ldots, R_t$. Hence by Lemma II.15 (a), we must have $p_i^{k_i} \geq n-1$ for all i. □

Corollary II.18 gives conditions on the solvability and scalar linear solvability of the Two-Six Network. We use the fact that the Two-Six Network is equivalent in terms of solvability to the 4-Choose-Two Network.

Corollary II.18: For each $m \geq 2$, the Two-Six Network is:

(a) *Solvable over an alphabet of size m if and only if $m \notin \{2, 6\}$.*
(b) *Scalar linearly solvable over some ring of size m if and only if $m \neq 2$ mod 4.*
(c) *Scalar linearly solvable over all finite fields except* GF(2).

Proof: Part (a) is [10, Lemma V.3]. Parts (b) and (c) follow immediately from Theorem II.17 and Lemma II.15, respectively, when $n = 4$. □

The proof of Corollary II.18 (a) (i.e. [10, Lemma V.3]) made use of a theorem characterizing the orders for which orthogonal latin squares exist. Euler originally conjectured over 230 years ago that orthogonal latin squares existed for all orders not congruent to 2 mod 4. It turned out that Euler was incorrect, and it was shown in 1960 that orthogonal latin squares existed for all orders except 2 and 6. Interestingly, the Two-Six Network was shown in Corollary II.18 to be solvable for all alphabet sizes except 2 and 6 and scalar linearly solvable over some ring of every size that is not congruent to 2 mod 4.

Li *et al.* [25] showed that every solvable multicast network is scalar linearly solvable over every sufficiently large finite field. We observe that this property is not true for finite rings, as the Two-Six Network is a solvable multicast network and is not scalar linearly solvable over any ring whose size is 2 mod 4.

E. Rings of Size p^2

Remark II.14 demonstrated that it is possible for the exact same set of networks to be scalar linearly solvable over two rings of different sizes. The following theorem shows that, for each prime p, this is also possible for two rings of size p^2, i.e. it is possible to have two non-isomorphic commutative rings of size p^2, such that the rings are equivalent under dominance.

Theorem II.19: For each prime p, the rings $\mathrm{GF}(p)[x]/\langle x^2 \rangle$ and $\mathrm{GF}(p) \times \mathrm{GF}(p)$ are each dominated by the other but are not isomorphic.

Proof: The rings are clearly not isomorphic since the only element of $\mathrm{GF}(p) \times \mathrm{GF}(p)$ whose square is zero is zero itself, and in $\mathrm{GF}(p)[x]/\langle x^2 \rangle$, the squares of both zero and x are zero. The field $\mathrm{GF}(p)$ is a subring of $\mathrm{GF}(p)[x]/\langle x^2 \rangle$, so by Corollary II.6,

$$\mathrm{GF}(p) \preceq \mathrm{GF}(p)[x]/\langle x^2 \rangle.$$

On the other hand, the mapping $\phi : \mathrm{GF}(p)[x]/\langle x^2 \rangle \to \mathrm{GF}(p)$ given by $\phi(a + bx) = a$ is a surjective homomorphism, so by Lemma II.5,

$$\mathrm{GF}(p)[x]/\langle x^2 \rangle \preceq \mathrm{GF}(p).$$

Thus,

$$\mathrm{GF}(p) \equiv \mathrm{GF}(p)[x]/\langle x^2 \rangle$$

and by Lemma II.12, $\mathrm{GF}(p) \times \mathrm{GF}(p) \equiv \mathrm{GF}(p)$. □

In the proof of the previous theorem it is shown that

$$\mathrm{GF}(p) \equiv \mathrm{GF}(p)[x]/\langle x^2 \rangle$$

which is another interesting example of rings of different sizes being equivalent under dominance.

It is known [17, Th. 2, p. 250] that, for each prime p, the only four commutative rings of size p^2 are

$$\mathrm{GF}(p^2),\ \mathrm{GF}(p) \times \mathrm{GF}(p),\ \mathbf{Z}_{p^2},\ \text{and } \mathrm{GF}(p)[x]/\langle x^2 \rangle.$$

The following theorem describes a chain of dominances between these rings and shows that dominance is a total quasi-order of the commutative rings of size p^2.

Theorem II.20: For each prime p, the four commutative rings of size p^2 satisfy

$$\begin{aligned} \mathcal{N}_{lin}(\mathbf{Z}_{p^2}) &\subset \mathcal{N}_{lin}(\mathrm{GF}(p)[x]/\langle x^2 \rangle) \\ &= \mathcal{N}_{lin}(\mathrm{GF}(p) \times \mathrm{GF}(p)) \\ &\subset \mathcal{N}_{lin}(\mathrm{GF}(p^2)). \end{aligned}$$

Proof: The field $\mathrm{GF}(p)$ is a subring of the field $\mathrm{GF}(p^2)$, so by Corollary II.6, $\mathrm{GF}(p) \preceq \mathrm{GF}(p^2)$. This, along with the fact the (p^2+1)-Choose-Two Network is scalar linearly solvable over $\mathrm{GF}(p^2)$ but not $\mathrm{GF}(p)$ (via Lemma II.15), implies

$$\mathcal{N}_{\mathrm{lin}}(\mathrm{GF}(p)) \subset \mathcal{N}_{\mathrm{lin}}(\mathrm{GF}(p^2)).$$

By Theorem II.19 and Corollary II.7, we also have

$$\mathbf{Z}_{p^2} \preceq \mathrm{GF}(p) \equiv \mathrm{GF}(p) \times \mathrm{GF}(p) \equiv \mathrm{GF}(p)[x]/\langle x^2 \rangle.$$

Additionally, by Lemma II.3, the Char-p Network is scalar linearly solvable over $\mathrm{GF}(p)$ but not $\mathbf{Z}_{p^2}$, thus proving the claim. □

III. Finite Field Dominance

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

Lemma III.1 [9, Sec. VI, Example (7)]: For any primes $q_1, \ldots, q_s$ and any positive integers $m_1, \ldots, m_s$, there exists a non-multicast network that is scalar linearly solvable over the fields

$$\mathrm{GF}(q_1^{nm_1}),\ \ldots,\ \mathrm{GF}(q_s^{nm_s})$$

for all $n \geq 1$, but not over any other fields.

Note that the primes $q_1, \ldots, q_s$ in Lemma III.1 need not be distinct. The following lemma will enable us to demonstrate certain networks that are scalar linearly solvable over some ring of prime power size but not over the field of the same size. Lemma III.2 will also be used in some of the proofs in Section V.

Lemma III.2: Let $p_1, \ldots, p_r$ and $q_1, \ldots, q_s$ be primes, and let $k_1, \ldots, k_r$ and $m_1, \ldots, m_s$ be positive integers. The ring

$$\mathrm{GF}(q_1^{m_1}) \times \cdots \times \mathrm{GF}(q_s^{m_s})$$

is dominated by the ring

$$\mathrm{GF}(p_1^{k_1}) \times \cdots \times \mathrm{GF}(p_r^{k_r})$$

if and only if for each $i \in \{1, \ldots, r\}$ there exists $j \in \{1, \ldots, s\}$ such that $q_j = p_i$ and $m_j \mid k_i$.

Proof: If, for each i, there is a j such that $q_j = p_i$ and $m_j \mid k_i$, then $\mathrm{GF}(q_j^{m_j})$ is a subring of $\mathrm{GF}(p_i^{k_i})$ so by Corollary II.6,

$$\mathrm{GF}(q_j^{m_j}) \preceq \mathrm{GF}(p_i^{k_i})$$

and therefore, by Lemma II.13,

$$\mathrm{GF}(q_1^{m_1}) \times \cdots \times \mathrm{GF}(q_s^{m_s}) \preceq \mathrm{GF}(p_1^{k_1}) \times \cdots \times \mathrm{GF}(p_r^{k_r}).$$

To prove the converse, suppose to the contrary that there exists $i \in \{1, \ldots, r\}$ such that for all $j \in \{1, \ldots, s\}$, either $q_j \neq p_i$ or $m_j \nmid k_i$. By Lemma III.1, there exists a network $\mathcal{N}$ that is scalar linearly solvable precisely over those fields of size $q_j^{nm_j}$, where $j \in \{1, \ldots, s\}$ and $n \geq 1$. Taking $n = 1$ and applying Lemma II.12, implies that $\mathcal{N}$ is scalar linearly solvable over

$$\mathrm{GF}(q_1^{m_1}) \times \cdots \times \mathrm{GF}(q_s^{m_s}).$$

But $\mathcal{N}$ can not be scalar linearly solvable over $\mathrm{GF}(p_i^{k_i})$, since for all $j \in \{1, \ldots, s\}$, either $q_j \neq p_i$ or $m_j \nmid k_i$, so by Lemma II.12, $\mathcal{N}$ is not scalar linearly solvable over

$$\mathrm{GF}(p_1^{k_1}) \times \cdots \times \mathrm{GF}(p_r^{k_r}).$$

Thus,

$$\mathrm{GF}(q_1^{m_1}) \times \cdots \times \mathrm{GF}(q_s^{m_s}) \not\preceq \mathrm{GF}(p_1^{k_1}) \times \cdots \times \mathrm{GF}(p_r^{k_r}).$$

□

As in Theorem II.19, the following corollary demonstrates that two non-isomorphic commutative rings of the same size may be equivalent with respect to the dominance relation $\preceq$. In this case, the rings are both direct products of fields.

Corollary III.3: For each $k \geq 3$ and prime p, the rings

$$\mathrm{GF}(p^{k-1}) \times \mathrm{GF}(p) \text{ and } \mathrm{GF}(p^{k-2}) \times \mathrm{GF}(p) \times \mathrm{GF}(p)$$

each dominate the other.

Proof: The result follows from Lemma III.2 by taking $r = 2, s = 3$, $p_1 = p_2 = q_1 = q_2 = q_3 = p$, $k_1 = k - 1$, $m_1 = k - 2$, and $k_2 = m_2 = m_3 = 1$ to get

$$\mathrm{GF}(p^{k-2}) \times \mathrm{GF}(p) \times \mathrm{GF}(p) \preceq \mathrm{GF}(p^{k-1}) \times \mathrm{GF}(p)$$

and by taking $r = 3, s = 2$, $p_1 = p_2 = p_3 = q_1 = q_2 = p$, $k_1 = k - 2$, $m_1 = k - 1$, and $k_2 = k_3 = m_2 = 1$ to get

$$\mathrm{GF}(p^{k-1}) \times \mathrm{GF}(p) \preceq \mathrm{GF}(p^{k-2}) \times \mathrm{GF}(p) \times \mathrm{GF}(p).$$

□

Example III.4 next demonstrates a network that is scalar linearly solvable over a ring of size 32 but is not scalar linearly solvable over the field of size 32. It turns out that 32 is the smallest prime power alphabet size for which a network can have a scalar linear solution over a commutative ring but not over the field of the same size (see Corollary V.10).

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

Theorem II.16 and Examples II.11 and III.4 also demonstrate that dominance is not necessarily a total quasi-order of the commutative rings of a given size, as there can exist rings of the same size such that neither dominates the other.

A. Local Rings

A finite commutative ring is said to be *local* if it has a single maximal ideal (see [3, Definition 1.2.9]). Lemmas III.5 and III.6 are standard results from commutative ring theory.

Lemma III.5 [3, Th. 3.1.4]: Every finite commutative ring is a direct product of local rings.

Lemma III.6 [3, Th. 6.1.2 II]: If R is a finite commutative local ring with maximal ideal I, then there exists a prime p and positive integers k and m such that

(i) $|R| = p^k$

(ii) *R/I is a field of size p^m and m divides k.*

All finite fields are local rings, since their unique maximal ideal is the trivial ring $\{0\}$. The ring $\mathbf{Z}_n$ is local if and only if n is a prime power, since for any prime divisor p of n,

$$\langle p \rangle = \{ap \ : \ a \in \mathbf{Z}_n\}$$

is a maximal ideal of $\mathbf{Z}_n$. However, not every ring of prime power size is local. For example, GF(2) × GF(2) has distinct maximal ideals $\{(0, 0), (1, 0)\}$ and $\{(0, 0), (0, 1)\}$.

The following lemma connects the algebraic concept of local rings to the dominance relation of network coding.

Lemma III.7: Every finite commutative local ring is dominated by the finite field of the same size.

Proof: Let R be a finite commutative local ring with maximal ideal I. By Lemma III.6, there exist a prime p and positive integers k and m such that $|R| = p^k$, $m \mid k$, and

$$R/I \cong \mathrm{GF}(p^m). \tag{4}$$

Thus,

$$\begin{aligned} R &\preceq \mathrm{GF}(p^m) \quad \big[\text{from (4), Corollary II.9}\big] \\ &\preceq \mathrm{GF}(p^k) \quad \big[\text{from } m \mid k \text{, Lemma III.2}\big]. \end{aligned}$$

□

Example III.4 demonstrated that there exists a network that is scalar linearly solvable over the ring GF(8) × GF(4) but not over the field GF(32). The following theorem strengthens the result in Example III.4 by additionally showing the network is not even scalar linearly solvable over any other commutative ring of size 32. This contrasts with Theorem II.16, which demonstrates a network that is scalar linearly solvable over GF(32) but not over any other commutative ring of size 32.

Theorem III.8: There exists a network that is scalar linearly solvable over GF(8) × GF(4) *but not over any other commutative ring of size* 32.

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

By Lemmas III.5 and III.6 (i), every commutative ring R of size 32 satisfies exactly one of the following seven properties:

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

By Lemma III.7, any network that is scalar linearly solvable over a commutative local ring of size 32 is also scalar linearly solvable over GF(32). This eliminates case (a). Similarly, any network that is scalar linearly solvable over a local ring of size 2 is also scalar linearly solvable over GF(2). By Lemma II.12, any network that is scalar linearly solvable over a direct product ring is also scalar linearly solvable over every ring in the direct product. This eliminates cases (b),(d),(e),(f),(g). Thus if $\mathcal{N}$ is scalar linearly solvable over a commutative ring R of size 32, R must satisfy case (c).

Suppose S is a commutative local ring of size 8 with maximal ideal I. Then Lemma III.6 (ii) implies $S/I \cong \mathrm{GF}(2^m)$ for some $m \in \{1, 3\}$. If $m = 3$, then $S \cong \mathrm{GF}(8)$, and if $m = 1$, then by Corollary II.9, $S \preceq \mathrm{GF}(2)$. Similarly, a commutative local ring of size 4 is either isomorphic to GF(4) or is dominated by GF(2). Thus if $\mathcal{N}$ is scalar linearly solvable over a ring R satisfying case (c), then $R \cong \mathrm{GF}(8) \times \mathrm{GF}(4)$; otherwise, by Lemma II.12, a scalar linear solution over R would imply there exists a scalar linear solution over GF(2). Thus GF(8) × GF(4) is the only commutative ring of size 32 over which $\mathcal{N}$ is scalar linearly solvable. □

Theorem III.8 demonstrates that GF(8) × GF(4) is not dominated by any other commutative ring of size 32 (including GF(32)) and thus is maximal. On the other hand, Theorem II.16 demonstrates that GF(32) is not dominated by any other commutative ring of size 32 (including GF(8) × GF(4)) and thus is maximal. In Section V, we characterize all maximal rings, and we show that all maximal rings have the property that there exists some network that is scalar linearly solvable over the maximal ring but not over any other commutative ring of the same size, which agrees with Theorems III.8 and II.16.

The network in the previous theorem is clearly also scalar linearly solvable over the fields GF(8) and GF(4). So while GF(8) × GF(4) is the only commutative ring of size 32 that the network is scalar linearly solvable over, it is not the smallest commutative ring the network is scalar linearly solvable over. This fact agrees with Theorem II.10.

B. Non-Power-of-Prime Size Rings

Theorem II.10 demonstrated that scalar linear solutions over commutative rings induce scalar linear solutions over finite fields. For a network that is scalar linearly solvable over a given commutative ring it is natural to ask over which fields is the network also scalar linearly solvable. In this section, we partially answer this question.

Theorem III.9: Suppose a network is scalar linearly solvable over some commutative ring whose size is divisible by the prime p. Then the network is scalar linearly solvable over some finite field of characteristic p whose size divides the size of the ring.

Proof: Let the commutative ring be R. By Lemma III.5, there exist commutative local rings $R_1, \ldots, R_n$ such that

$$R \cong R_1 \times \cdots \times R_n.$$

So we have

$$|R| = |R_1| \cdots |R_n|$$

and since p divides $|R|$, there exists $j \in \{1, \ldots, n\}$ such that p divides $|R_j|$. By Lemma III.6 (i), this implies $|R_j| = p^m$ for some positive integer m. Therefore, by Lemma III.7,

$$R_j \preceq \mathrm{GF}(p^m).$$

Since $\mathcal{N}$ is scalar linearly solvable over R, by Lemma II.12, $\mathcal{N}$ must be scalar linearly solvable over R_j, and since $R_j \preceq \mathrm{GF}(p^m)$, $\mathcal{N}$ must also be scalar linearly solvable over $\mathrm{GF}(p^m)$. □

Theorem III.9 demonstrates that commutative rings of non-power-of-prime size are always dominated by some fields whose characteristics are the prime factors of the ring's size. Determining which fields dominate a particular ring appears to be a non-trivial problem, since it depends on the local decomposition of the ring. We address a select few cases.

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

Lemma III.10 [2, p. 457]: Let $p_1, \dots, p_n$ be distinct primes. The commutative ring $\mathrm{GF}(p_1) \times \cdots \times \mathrm{GF}(p_n)$ *is the only ring of size $p_1 \cdots p_n$.*

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

Corollary III.11: Let $p_1, \dots, p_n$ be distinct primes. If a network is scalar linearly solvable over a ring of size $p_1 \cdots p_n$, then the network is scalar linearly solvable over each of the fields $\mathrm{GF}(p_1), \dots, \mathrm{GF}(p_n)$.

Proof: By Lemma III.10, the only ring of size $p_1 \cdots p_n$ is $\mathrm{GF}(p_1) \times \cdots \times \mathrm{GF}(p_n)$. By Lemma II.12, any network that is scalar linearly solvable over this ring must also have a scalar linear solution over each of $\mathrm{GF}(p_1), \dots, \mathrm{GF}(p_n)$. □

In general, one cannot specify in Theorem III.9 which fields of characteristic p a particular network is scalar linearly solvable over without knowing the particular ring R. As an example, the following corollary illustrates that different networks that are scalar linearly solvable over different rings of size 12, may be scalar linearly solvable over different finite fields. Additionally, Corollary III.12 demonstrates that Corollary III.11 does not always hold when $p_1, \dots, p_n$ are non-distinct primes.

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

Proof: Part (i) follows from Lemma II.12 and the fact that the Two-Six Network is scalar linearly solvable over GF(4) and GF(3) but not over GF(2) (see Corollary II.18).

Part (ii) follows from Corollary II.7. □

IV. Integer Partitions

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

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

Definition IV.1: For each prime p, and each partition $\mathrm{A} = (a_1, \dots, a_r)$ of k, define the product ring

$$\mathrm{R}_{\mathrm{A},p} = \prod_{i=1}^{r} \mathrm{GF}(p^{a_i}).$$

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

$$R \cong \prod_{i=1}^{t} \mathrm{R}_{\mathrm{A}_i, p_i}.$$

We will refer to $\mathrm{A}_1, \dots, \mathrm{A}_t$ as the *partitions of* R.

As an example, if $m = 864 = 2^5 3^3$, then

$$R = \mathrm{GF}(2^2) \times \mathrm{GF}(2^2) \times \mathrm{GF}(2^1) \times \mathrm{GF}(3^2) \times \mathrm{GF}(3^1)$$

is a partition ring and the partitions of R are $A_1 = (2, 2, 1)$ and $A_2 = (2, 1)$. Another partition ring of size 864 is

$$R = \mathrm{GF}(2^4) \times \mathrm{GF}(2^1) \times \mathrm{GF}(3^3)$$

and the partitions of R are $A_1 = (4, 1)$ and $A_2 = (3)$. As another special case, any field $\mathrm{GF}(p^k)$ is a partition ring whose partition is (k).

In later proofs, we will encounter direct products of fields not given in terms of partitions; however, Lemma IV.2 demonstrates that each such direct product is, in fact, a partition ring.

Lemma IV.2: Every finite direct product of finite fields is a partition ring.

Proof: Suppose $q_1, \dots, q_s$ are (not necessarily distinct) prime numbers and $n_1, \dots, n_s$ are positive integers and define the product ring

$$R = \prod_{j=1}^{s} \mathrm{GF}(q_j^{n_j}).$$

Let $p_1^{k_1} \cdots p_t^{k_t}$ denote the prime factorization of the ring size $|R|$, so that

$$p_1^{k_1} \cdots p_t^{k_t} = q_1^{n_1} \cdots q_s^{n_s}.$$

For each $j \in \{1, \dots, s\}$, we have $q_j = p_i$ for some unique $i \in \{1, \dots, t\}$. Thus, for each $i = 1, \dots, t$, there exist positive integers r_i and $a_{i,1} \geq \cdots \geq a_{i,r_i}$ such that $\displaystyle\sum_{j=1}^{r_i} a_{i,j} = k_i$ and

$$\prod_{j=1}^{s} \mathrm{GF}(q_j^{n_j}) \cong \prod_{i=1}^{t} \prod_{j=1}^{r_i} \mathrm{GF}(p_i^{a_{i,j}}).$$

Let $\mathrm{A}_i = (a_{i,1}, \dots, a_{i,r_i})$. Then for each i, A_i is a partition of k_i, and we have

$$R \cong \prod_{i=1}^{t} \prod_{j=1}^{r_i} \mathrm{GF}(p_i^{a_{i,j}}) \cong \prod_{i=1}^{t} \mathrm{R}_{\mathrm{A}_i, p_i}.$$

□

A. Partition Division

Definition IV.3: Let A and B be partitions of k. We say that A *divides* B and write $\mathrm{A} \bigm| \mathrm{B}$ if for each element b of B, there exists an element a of A such that $a \bigm| b$. We call the relation "$\bigm|$" *partition division*.

For each positive integer k, it can be verified that the partition division relation is a quasi-order on the set $\Pi(k)$. Throughout this paper, whenever we refer to a partition of an integer as being *maximal*, we mean the partition is maximal with respect to the relation $\bigm|$ on the set of all partitions of the same integer. In particular, a partition B of k is maximal if and only if $\mathrm{A} \bigm| \mathrm{B}$ whenever $\mathrm{B} \bigm| \mathrm{A}$, for all partitions A of k.

Sometimes distinct partitions of the same integer each divide the other. For example, for each $k \geq 3$, the partitions

$$(k-1, 1) \text{ and } (k-2, 1, 1)$$

of k divide one another. Hence partition division is not anti-symmetric on $\Pi(k)$.

Lemma IV.4 demonstrates the connection between partition division and dominance of partition rings. Lemma IV.4 is a special case of Lemma III.2, where the direct products of finite fields are based on partition rings.

Lemma IV.4: Let $m \geq 2$ have prime factorization $m = p_1^{k_1} \cdots p_t^{k_t}$, and for each $i = 1, \ldots, t$, let A_i and B_i be partitions of k_i. Then

$$\mathrm{R}_{\mathrm{A}_1, p_1} \times \cdots \times \mathrm{R}_{\mathrm{A}_t, p_t}$$

is dominated by the ring

$$\mathrm{R}_{\mathrm{B}_1, p_1} \times \cdots \times \mathrm{R}_{\mathrm{B}_t, p_t}$$

if and only if A_i divides B_i for all i.

Proof: For each $i \in \{1, \ldots, t\}$, let $\mathrm{A}_i = (a_{i,1}, \ldots, a_{i,r_i})$ and $\mathrm{B}_i = (b_{i,1}, \ldots, b_{i,s_i})$. Then

$$\prod_{i=1}^{t} \mathrm{R}_{\mathrm{A}_i, p_i} \cong \prod_{i=1}^{t} \prod_{j=1}^{r_i} \mathrm{GF}(p_i^{a_{i,j}})$$

and

$$\prod_{i=1}^{t} \mathrm{R}_{\mathrm{B}_i, p_i} \cong \prod_{i=1}^{t} \prod_{j=1}^{s_i} \mathrm{GF}(p_i^{b_{i,j}}).$$

By Lemma III.2,

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

if and only if for each $i \in \{1, \ldots, t\}$ and each $j \in \{1, \ldots, r_i\}$, there exists $l \in \{1, \ldots, s_i\}$ such that $a_{i,l} \bigm| b_{i,j}$. However, the latter condition is precisely $\mathrm{A}_i \bigm| \mathrm{B}_i$ for all i. □

B. Maximal Partitions

The following lemma shows that if a partition divides a partition that is not shorter than it, then it also divides a partition which is shorter. This property will be used to characterize maximal partitions in Theorems IV.6 and IV.9.

Lemma IV.5: Let A *and* B *be different partitions of k. If $|\mathrm{A}| \leq |\mathrm{B}|$ and $\mathrm{A} \bigm| \mathrm{B}$, then there exists a partition* C *of k such that $|\mathrm{C}| < |\mathrm{A}|$ and $\mathrm{A} \bigm| \mathrm{C}$.*

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

- **Base case:** $|\mathrm{B}| - |\mathrm{A}| = 0$.
  If no element of A divides multiple elements of B, then, since $|\mathrm{A}| = |\mathrm{B}|$, each element of A must divide exactly one element of B. Then there exists a permutation σ of $\{1, \ldots, |\mathrm{A}|\}$ such that a_i divides $b_{\sigma(i)}$. Then

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

  which implies $a_i = b_{\sigma(i)}$ for all i. However, this contradicts the assumption that $\mathrm{A} \neq \mathrm{B}$.
  So we may assume there exists an element a of A that divides some distinct elements b_i, b_j of B. Let C be the partition B with elements b_i and b_j removed and replaced by $(b_i + b_j)$. Then C is a partition of k that is shorter than A, and since a divides $(b_i + b_j)$, we have $\mathrm{A} \bigm| \mathrm{C}$.
- **Induction step:** Assume true whenever $|\mathrm{B}| - |\mathrm{A}| < n$ (where $n \geq 1$).
  Suppose $|\mathrm{B}| - |\mathrm{A}| = n$.
  - ▶ Case: $n = 1$
    Since $|\mathrm{B}| > |\mathrm{A}|$ and $\mathrm{A} \bigm| \mathrm{B}$, there exists an element a of A that divides some distinct elements b_i, b_j of B. If there is a third distinct element b_l of B such that $a \bigm| b_l$, then let C be the partition B with elements b_i, b_j, and b_l removed and replaced by $(b_i + b_j + b_l)$. Then C is a partition of k that is shorter than A, and since a divides $(b_i + b_j + b_l)$, we have $\mathrm{A} \bigm| \mathrm{C}$.
    If there is no such third distinct element b_l, then modify B by removing the elements b_i and b_j and adding an element $(b_i + b_j)$. The new B is a partition of k that is the same length as A, and since a divides $(b_i + b_j)$, we have $\mathrm{A} \bigm| \mathrm{B}$. Since a divides both b_i and b_j, we have $a \neq b_i + b_j$, and since $(b_i + b_j)$ is the only element of B that a divides, the value a is not one of the elements of B. Hence $\mathrm{B} \neq \mathrm{A}$, which reduces to the base case $n = 0$.
  - ▶ Case: $n \geq 2$
    Since $|\mathrm{B}| > |\mathrm{A}|$ and $\mathrm{A} \bigm| \mathrm{B}$, there exists an element a of A that divides some distinct elements b_i, b_j of B. Modify the partition B by removing the elements b_i and b_j and adding the element $(b_i + b_j)$. The new B is a partition of k that is one shorter than before the modification, and since a divides $(b_i + b_j)$, we have $\mathrm{A} \bigm| \mathrm{B}$. This reduces to the case $|\mathrm{B}| - |\mathrm{A}| = n - 1$, which is true by the induction hypothesis.

□

Theorem IV.6: No maximal partition of k can divide any other partition of k.

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

Let A be a maximal partition of k such that A is of minimal length among the partitions in [A], and suppose $\mathrm{B} \in [\mathrm{A}] - \{\mathrm{A}\}$. Then $|\mathrm{A}| \leq |\mathrm{B}|$ and $\mathrm{A} \bigm| \mathrm{B}$, so by Lemma IV.5, there exists $\mathrm{C} \in \Pi(k)$ such that $|\mathrm{C}| < |\mathrm{A}|$ and $\mathrm{A} \bigm| \mathrm{C}$. Since [A] is maximal, we must have C $\mid$ A, which implies C ∈ [A], but this violates the minimum length of A in [A]. Thus, [A] = {A}. □

In theory, the maximal elements in a quasi-order could be equivalent to another maximal element, i.e. the corresponding equivalence class contains more than one element. However, Theorem IV.6 implies the maximal partitions of k are precisely the partitions of k that do not divide any other partition of k, i.e. each maximal partition is in a distinct equivalence class. This is a stronger maximality condition than the maximality induced by the quasi-order.

Lemma IV.7 demonstrates a property of maximal partitions that will be used in a later proof.

Lemma IV.7: No element of a maximal partition of k is divisible by a different element of the partition.

Proof: Let A $= (a_1, \ldots, a_r)$ be a partition of k. Assume there exist distinct $i, j \in \{1, \ldots, r\}$ such that a_i divides a_j. Then a_i divides $(a_i + a_j)$. Create a new partition B of k by removing the elements a_i and a_j of A and inserting a new element $(a_i + a_j)$. Then B ≠ A and A $\mid$ B, so by Theorem IV.6, A is not maximal. □

The converse of Lemma IV.7 does not necessarily hold. For example, the partition $(5, 3, 2)$ satisfies the latter condition of Lemma IV.7, but $(5, 3, 2) \mid (10)$, so $(5, 3, 2)$ is not maximal.

C. Maximal Partitions of Short Length

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

Remark IV.8: For each $k \geq 1$, the partition (k) is maximal since k does not divide any positive integer less than k.

Theorem IV.9 gives a complete characterization of the maximal partitions of length 2.

Theorem IV.9: Let k and m be positive integers such that $m \leq k/2$. The partition $(k-m, m)$ of k is maximal if and only if $m \nmid k$.

Proof: Assume $m \mid k$. Then $(k - m, m) \mid (k)$, so by Theorem IV.6, $(k - m, m)$ is not a maximal partition.

Now assume $m \nmid k$. Then $k \neq 2m$, so $m < k/2$, or equivalently $k - m > k/2$. Thus, $(k-m) \nmid k$, which means that $(k - m, m)$ does not divide (k). But (k) is the only partition of k shorter than the partition $(k - m, m)$, so by Lemma IV.5, the partition $(k - m, m)$ cannot divide any other partition of k that is at least as long as $(k - m, m)$. Thus $(k - m, m)$ is maximal. □

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

TABLE I

THE MAXIMAL PARTITIONS OF $k = 1, 2, \ldots, 30$ UNDER PARTITION DIVISION

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

Theorem IV.10: Let k be a positive integer. Then (k) is the unique maximal partition of k if and only if $k \in \{1, 2, 3, 4, 6\}$.

Proof: For each positive integer k, by Remark IV.8, (k) is a maximal partition. It is easily verified that the following are all the partitions of k, for $k \in \{1, 2, 3, 4, 6\}$:

$$\Pi(1) = \{(1)\}$$

$$\Pi(2) = \{(2), (1, 1)\}$$

$$\Pi(3) = \{(3), (2, 1), (1, 1, 1)\}$$

$$\Pi(4) = \{(4), (3, 1), (2, 2), (2, 1, 1), (1, 1, 1, 1)\}$$

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

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

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

$$\begin{aligned}\mathsf{gcd}\left(\frac{k-1}{2}, k\right) &= \mathsf{gcd}\left(\frac{k-1}{2}, k-2\left(\frac{k-1}{2}\right)\right)\\ &= \mathsf{gcd}\left(\frac{k-1}{2}, 1\right) = 1 < \frac{k-1}{2}\end{aligned}$$

so $\frac{k-1}{2} \nmid k$. Therefore $\left(\frac{k+1}{2}, \frac{k-1}{2}\right)$ is a maximal partition, by taking $m = \frac{k-1}{2}$ in Theorem IV.9.

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

$$\begin{aligned}\mathsf{gcd}\left(\frac{k}{2}-1, k\right) &= \mathsf{gcd}\left(\frac{k}{2}-1, k-2\left(\frac{k}{2}-1\right)\right)\\ &= \mathsf{gcd}\left(\frac{k}{2}-1, 2\right) \leq 2 < \frac{k}{2}-1\end{aligned}$$

so $\left(\frac{k}{2}-1\right) \nmid k$. Therefore $\left(\frac{k}{2}+1, \frac{k}{2}-1\right)$ is a maximal partition, by taking $m = \frac{k}{2}-1$ in Theorem IV.9.

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

V. Maximal Commutative Rings

In this section, we characterize the commutative rings which are maximal with respect to the quasi-order of commutative rings of a given size under dominance.

Corollary V.1: If each of a partition ring's integer partitions is maximal, then the ring is not dominated by any other partition ring of the same size.

Proof: Let $m = p_1^{k_1} \cdots p_t^{k_t}$ be the prime factorization of m. For each $i = 1, \ldots, t$, let $\mathrm{A}_i, \mathrm{B}_i \in \Pi(k_i)$ be such that A_i is maximal. Suppose

$$\prod_{i=1}^{t} \mathrm{R}_{\mathrm{A}_i, p_i} \preceq \prod_{i=1}^{t} \mathrm{R}_{\mathrm{B}_i, p_i}.$$

Then by Lemma IV.4, $\mathrm{A}_i \mid \mathrm{B}_i$ for all i. Since each A_i is maximal, by Theorem IV.6, $\mathrm{B}_i = \mathrm{A}_i$, for all i. Therefore

$$\prod_{i=1}^{t} \mathrm{R}_{\mathrm{B}_i, p_i} \cong \prod_{i=1}^{t} \mathrm{R}_{\mathrm{A}_i, p_i}.$$

□

Lemma V.2 extends Corollary V.1 to show that partition rings, where each partition is maximal, are not dominated by any other (not necessarily partition) commutative ring of the same size.

Lemma V.2: If each of a partition ring's integer partitions is maximal, then the ring is not dominated by any other commutative ring of the same size.

Proof: Let $m = p_1^{k_1} \cdots p_t^{k_t}$ be the prime factorization of the size of the ring

$$R = \prod_{i=1}^{t} \mathrm{R}_{\mathrm{A}_i, p_i}$$

where for each $i = 1, \ldots, t$, the partition $\mathrm{A}_i = (a_{i,1}, \ldots, a_{i,r_i})$ of k_i is maximal. Suppose R is dominated by a commutative ring S of size m. We will show that R and S are isomorphic rings.

By Lemma III.5, S can be written as a direct product of commutative local rings, and by Lemma III.6 (i), the size of each such local ring has to be a power of one of the prime factors $p_1, \ldots, p_t$ of m. Specifically, for each $i = 1, \ldots, t$, there exist local rings $L_{i,1}, \ldots, L_{i,s_i}$ such that each $|L_{i,j}|$ is a power of p_i and

$$S \cong \prod_{i=1}^{t} \prod_{j=1}^{s_i} L_{i,j}. \tag{5}$$

For each $i = 1, \ldots, t$ and $j = 1, \ldots, s_i$, Lemma III.7 impies that $L_{i,j} \preceq \mathrm{GF}(|L_{i,j}|)$. Then,

$$\begin{aligned}\prod_{i=1}^{t} \mathrm{R}_{\mathrm{A}_i, p_i} &\preceq \prod_{i=1}^{t} \prod_{j=1}^{s_i} L_{i,j} \quad [\text{from } R \preceq S,\ (5)]\\ &\preceq \prod_{i=1}^{t} \prod_{j=1}^{s_i} \mathrm{GF}(|L_{i,j}|) \quad [\text{from Lemma II.13}] \end{aligned} \tag{6}$$

and the right-hand-side of (6) is a partition ring of size m, by Lemma IV.2.

Since each A_i is maximal, by Corollary V.1 and (6), we have

$$\begin{aligned}\prod_{i=1}^{t} \prod_{j=1}^{s_i} \mathrm{GF}(|L_{i,j}|) &\cong \prod_{i=1}^{t} \mathrm{R}_{\mathrm{A}_i, p_i}\\ &\cong \prod_{i=1}^{t} \prod_{j=1}^{r_i} \mathrm{GF}(p_i^{a_{i,j}}). \end{aligned} \tag{7}$$

Therefore for each $i = 1, \ldots, t$, we have $s_i = r_i$, and by (7), without loss of generality, we may assume $|L_{i,j}| = p_i^{a_{i,j}}$, for all $j = 1, \ldots, r_i$.

For each $i = 1, \ldots, t$ and $j = 1, \ldots, r_i$, let $I_{i,j}$ be the maximal ideal of the local ring $L_{i,j}$. Then, by Lemma III.6 (ii), for each i and j, there exists a positive integer $b_{i,j}$ such that $b_{i,j} \mid a_{i,j}$ and

$$\mathrm{GF}(p_i^{b_{i,j}}) \cong L_{i,j}/I_{i,j}.$$

Corollary II.9 then implies

$$L_{i,j} \preceq \mathrm{GF}(p_i^{b_{i,j}}) \quad (i = 1, \ldots, t \text{ and } j = 1, \ldots, r_i) \tag{8}$$

and therefore

$$\begin{aligned}R &\cong \prod_{i=1}^{t} \prod_{j=1}^{r_i} \mathrm{GF}(p_i^{a_{i,j}})\\ &\preceq \prod_{i=1}^{t} \prod_{j=1}^{r_i} L_{i,j} \quad [\text{from } R \preceq S,\ (5)]\\ &\preceq \prod_{i=1}^{t} \prod_{j=1}^{r_i} \mathrm{GF}(p_i^{b_{i,j}}) \quad [\text{from (8), Lemma II.13}]. \end{aligned} \tag{9}$$

Lemma III.2 and (9) imply that for each $i \in \{1, \ldots, t\}$ and $j \in \{1, \ldots, r_i\}$, there exists $l \in \{1, \ldots, r_i\}$ such that $a_{i,l} \mid b_{i,j}$. We also have $b_{i,j} \mid a_{i,j}$, so $a_{i,l} \mid a_{i,j}$. Since A_i is maximal, by Lemma IV.7, this implies $l = j$. Thus $b_{i,j} = a_{i,j}$, for all $i \in \{1, \ldots, t\}$ and $j \in \{1, \ldots, r_i\}$, and therefore

$$L_{i,j}/I_{i,j} \cong \mathrm{GF}(p_i^{a_{i,j}})$$

for all i, j. However, we also have $|L_{i,j}| = p_i^{a_{i,j}}$ for all i, j. So it must be the case that $|I_{i,j}| = 1$, and

$$L_{i,j} \cong \mathrm{GF}(p_i^{a_{i,j}}) \quad (i = 1, \dots, t \text{ and } j = 1, \dots, r_i). \tag{10}$$

Thus,

$$\begin{aligned} S &\cong \prod_{i=1}^{t} \prod_{j=1}^{r_i} \mathrm{GF}(p_i^{a_{i,j}}) \quad \text{[from (5), (10)]} \\ &\cong \prod_{i=1}^{t} \mathrm{R}_{\mathrm{A}_i, p_i} \cong R. \end{aligned}$$

□

Lemmas V.2 and V.3 will be used in the proof of Theorem V.4 to show that the maximal commutative rings with respect to dominance are precisely partition rings where each partition is maximal.

Lemma V.3: Every finite commutative ring is dominated by some partition ring of the same size, all of whose partitions are maximal.

Proof: Let R be a finite commutative ring. By Lemma III.5, there exist commutative local rings $R_1, R_2, \dots, R_n$ such that

$$R \cong \prod_{j=1}^{n} R_j. \tag{11}$$

By Lemma III.7, for each $j = 1, \dots, n$, we have

$$R_j \preceq \mathrm{GF}(|R_j|)$$

so by Lemma II.13, we have

$$\prod_{j=1}^{n} R_j \preceq \prod_{j=1}^{n} \mathrm{GF}(|R_j|). \tag{12}$$

Let $m = p_1^{k_1} \cdots p_t^{k_t}$ denote the prime factorization of m. Then by Lemma IV.2, for each $i = 1, \dots, t$, there exists a partition B_i of k_i such that

$$\prod_{i=1}^{t} \mathrm{R}_{\mathrm{B}_i, p_i} \cong \prod_{j=1}^{n} \mathrm{GF}(|R_j|). \tag{13}$$

Since $\Pi(k_i)$ is a finite quasi-ordered set under partition division, for each $i = 1, \dots, t$, there exists maximal $\mathrm{A}_i \in \Pi(k_i)$ such that $\mathrm{B}_i \bigm| \mathrm{A}_i$. So we have

$$\begin{aligned} R &\cong \prod_{j=1}^{n} R_j \quad \text{[from (11)]} \\ &\preceq \prod_{j=1}^{n} \mathrm{GF}(|R_j|) \quad \text{[from (12)]} \\ &\cong \prod_{i=1}^{t} \mathrm{R}_{\mathrm{B}_i, p_i} \quad \text{[from (13)]} \\ &\preceq \prod_{i=1}^{t} \mathrm{R}_{\mathrm{A}_i, p_i} \quad \text{[from Lemma IV.4]}. \end{aligned}$$

□

The following theorem characterizes maximal commutative rings.

Theorem V.4: A finite commutative ring is maximal if and only if it is a partition ring, each of whose integer partitions is maximal.

Proof: If R is a partition ring such that each of its partitions is maximal, then by Lemma V.2, no other commutative ring of the same size dominates R. Thus, R is maximal.

Conversely, assume commutative ring R is maximal. By Lemma V.3, R is dominated by a partition ring S of the same size where each of its partitions is maximal. Since R is maximal, this implies $S \preceq R$. However, by Lemma V.2, this implies $S \cong R$. Thus, R is a partition ring such that each of its partitions is maximal. □

Remark V.5: Since the maximal rings of a given size are partition rings where each integer partition is maximal, the maximal rings of non-power-of-prime size are direct products of maximal rings of prime-power sizes.

Corollary V.6: Let $m \geq 2$ have prime factorization $m = p_1^{k_1} \cdots p_t^{k_t}$. Then $\mathrm{GF}(p_1^{k_1}) \times \cdots \times \mathrm{GF}(p_t^{k_t})$ is a maximal ring of size m.

Proof: This follows from Theorem V.4 and Remark IV.8. □

It was shown in Theorem II.19 and Corollary III.3 that non-isomorphic rings can be equivalent under dominance; however, Corollary V.7 demonstrates that such equivalent rings cannot be maximal.

Corollary V.7: No maximal commutative ring is dominated by any other commutative ring of the same size.

Proof: This follows immediately from Theorem V.4 and Lemma V.2 □

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

Theorem II.16 demonstrated that for each finite field, there exists a multicast network that is scalar linearly solvable over the field but not over any other commutative ring of the same size, and Theorem III.8 demonstrated a network that is scalar linearly solvable over GF(8) × GF(4) but not over any other commutative ring of size 32. The following theorem shows a similar property for every maximal commutative ring and provides an alternate characterization of maximal commutative rings than in Theorem V.4.

Theorem V.8: A finite commutative ring is maximal if and only if there exists a network that is scalar linearly solvable over the ring but not over any other commutative ring of the same size.

Proof: Let R be a maximal commutative ring of size m. By Corollary V.7, R is not dominated by any other commutative ring of size m, so for each ring S of size m that is not isomorphic to R, there exists a network $\mathcal{N}_S$ that is scalar linearly solvable over R but not S. Then the disjoint union of networks

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

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

$$\bigcup_{\substack{S\in\mathcal{R}(m)\\ S\not\cong R}} \mathcal{N}_S$$

is not scalar linearly solvable over S.

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

An interesting open problem related to Theorem V.8 is to characterize rings with the property that there exists a multicast network that is scalar linearly solvable over the ring but not over any other commutative ring of the same size. We showed (in Theorem II.16) that such a multicast network exists for every finite field, and we showed (in Example II.11) that there exists a multicast network that is scalar linearly solvable over a ring of size 2^{13} but not the field $\mathrm{GF}(2^{13})$.

A. Multiple Maximal Rings of a Given Size

Theorem V.9 demonstrates that in some cases, there is only one maximal commutative ring of a given size. If R is the only maximal ring of a given size, then by Lemma V.3, any network with a scalar linear solution over some commutative ring of size $|R|$ also has a scalar linear solution over R. Alternatively, since the set of commutative rings of size $|R|$ is finite and quasi-ordered under dominance, each ring $S \in \mathcal{R}(|R|)$ is dominated by some maximal ring, and if R is the only maximal ring of size $|R|$, then S is dominated by R. In this case, R can be thought of as the "best" commutative ring of size $|R|$, in terms of scalar linear solvability.

However, by Theorem V.8, for each maximal ring, there exists a network which is scalar linearly solvable over the maximal ring but not over any other commutative ring of the same size. When there are multiple maximal rings of a given size, not every network with a scalar linear solution over some commutative ring of this size is scalar linearly solvable over every maximal ring. Thus there is no "best" commutative ring of this size.

Theorem V.9: Let $m \geq 2$ have prime factorization $m = p_1^{k_1} \cdots p_t^{k_t}$. Then $\mathrm{GF}(p_1^{k_t}) \times \cdots \times \mathrm{GF}(p_t^{k_t})$ is the only maximal ring of size m if and only if $\{k_1, \dots, k_t\} \subseteq \{1, 2, 3, 4, 6\}$.

Proof: By Corollary V.6,

$$\mathrm{GF}(p_1^{k_t}) \times \cdots \times \mathrm{GF}(p_t^{k_t})$$

is a maximal ring. Assume $k_i \in \{1, 2, 3, 4, 6\}$ for all i. Then by Theorem IV.10, (k_i) is the only maximal partition of k_i for all i. Thus, by Theorem V.4,

$$\mathrm{GF}(p_1^{k_t}) \times \cdots \times \mathrm{GF}(p_t^{k_t})$$

is the only maximal ring of size m.

Conversely, assume there exists j such that $k_j = 5$ or $k_j \geq 7$. Then by Theorem IV.10, there exists a maximal partition B_j of k_j such that $\mathrm{B}_j \neq (k_j)$. Then by Theorem V.4,

$$\mathrm{R}_{\mathrm{B}_j, p_j} \times \prod_{\substack{i=1\\ i\neq j}}^{t} \mathrm{GF}(p_i^{k_i})$$

and

$$\mathrm{GF}(p_1^{k_t}) \times \cdots \times \mathrm{GF}(p_t^{k_t})$$

are distinct maximal rings of size m. □

The bound in the following corollary can be achieved with equality, as illustrated in Example III.4.

Corollary V.10: If a network is not scalar linearly solvable over a given finite field but is scalar linearly solvable over some commutative ring of the same size, then the size of the field is at least 32.

Proof: It follows from Theorem V.9 that for each $k \in \{1, 2, 3, 4, 6\}$ and prime p, any network that is scalar linearly solvable over some commutative ring of size p^k must also be scalar linearly solvable over the field $\mathrm{GF}(p^k)$. The claim follows from the fact $p = 2$ and $k = 5$ yield the minimum p^k that does not satisfy this condition. □

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

Example V.11: For each integer $k \geq 1$ and prime p, $\mathrm{GF}(p^k)$ is a maximal ring. The following are the other maximal commutative rings of size p^k for all $k \leq 12$:

$$\begin{array}{ll}
p^5: & \mathrm{GF}(p^3) \times \mathrm{GF}(p^2)\\
p^7: & \mathrm{GF}(p^5) \times \mathrm{GF}(p^2) \textit{ and } \mathrm{GF}(p^4) \times \mathrm{GF}(p^3)\\
p^8: & \mathrm{GF}(p^5) \times \mathrm{GF}(p^3)\\
p^9: & \mathrm{GF}(p^7) \times \mathrm{GF}(p^2) \textit{ and } \mathrm{GF}(p^5) \times \mathrm{GF}(p^4)\\
p^{10}: & \mathrm{GF}(p^7) \times \mathrm{GF}(p^3) \textit{ and } \mathrm{GF}(p^6) \times \mathrm{GF}(p^4)\\
p^{11}: & \mathrm{GF}(p^9) \times \mathrm{GF}(p^2),\ \mathrm{GF}(p^8) \times \mathrm{GF}(p^3),\\
 & \mathrm{GF}(p^7) \times \mathrm{GF}(p^4),\ \textit{and } \mathrm{GF}(p^6) \times \mathrm{GF}(p^5)\\
p^{12}: & \mathrm{GF}(p^7) \times \mathrm{GF}(p^5).
\end{array}$$

$\mathrm{GF}(8) \times \mathrm{GF}(4)$ is the smallest prime-power size maximal commutative ring that is not a finite field, and

$$\mathrm{GF}(128) \times \mathrm{GF}(64) \times \mathrm{GF}(16)$$

has size 2^{17} and is the smallest known[8] *prime-power size maximal commutative ring consisting of a direct product of more than two fields.*

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

$$\begin{array}{l}
\mathrm{GF}(2^7) \times \mathrm{GF}(3^5) \times \mathrm{GF}(5^2)\\
\mathrm{GF}(2^5) \times \mathrm{GF}(2^2) \times \mathrm{GF}(3^5) \times \mathrm{GF}(5^2)\\
\mathrm{GF}(2^4) \times \mathrm{GF}(2^3) \times \mathrm{GF}(3^5) \times \mathrm{GF}(5^2)\\
\mathrm{GF}(2^7) \times \mathrm{GF}(3^3) \times \mathrm{GF}(3^2) \times \mathrm{GF}(5^2)\\
\mathrm{GF}(2^5) \times \mathrm{GF}(2^2) \times \mathrm{GF}(3^3) \times \mathrm{GF}(3^2) \times \mathrm{GF}(5^2)\\
\mathrm{GF}(2^4) \times \mathrm{GF}(2^3) \times \mathrm{GF}(3^3) \times \mathrm{GF}(3^2) \times \mathrm{GF}(5^2).
\end{array}$$

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

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

VI. Open Questions

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

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

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] V. G. Antipkin and V. P. Elizarov, "Rings of order p^3," *Siberian Math. J.*, vol. 23, no. 4, pp. 457–464, 1982.

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

[4] 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.

[5] 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.

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

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

[8] 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.

[9] R. Dougherty, C. Freiling, and K. Zeger, "Linear network codes and systems of polynomial equations," *IEEE Trans. Inf. Theory*, vol. 54, no. 5, pp. 2303–2316, May 2008.

[10] R. Dougherty, C. Freiling, and K. Zeger, "Linearity and solvability in multicast networks," *IEEE Trans. Inf. Theory*, vol. 50, no. 10, pp. 2243–2256, Oct. 2004.

[11] 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.

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

[13] 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.

[14] M. Effros, S. El Rouayheb, and M. Langberg, "An equivalence between network coding and index coding," *IEEE Trans. Inf. Theory*, vol. 61, no. 5, pp. 2478–2487, May 2015.

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

[16] T. Etzion and A. Wachter-Zeh. (May 13, 2016). "Vector network coding based on subspace codes outperforms scalar linear network coding." [Online]. Available: https://arxiv.org/abs/1512.06352

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

[18] 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.

[19] 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.

[20] P. Karimian, R. R. Borujeny, and M. Ardakani, "On network coding for funnel networks," *IEEE Commun. Lett.*, vol. 19, no. 11, pp. 1897–1900, Nov. 2015.

[21] R. Koetter and M. Médard, "An algebraic approach to network coding," *IEEE/ACM Trans. Netw.*, vol. 11, no. 5, pp. 782–795, Oct. 2003.

[22] S.-Y. R. Li and R. W. Yeung, "On convolutional network coding," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2006, pp. 1743–1747.

[23] S.-Y. R. Li and Q. Sun, "Network coding theory via commutative algebra," *IEEE Trans. Inf. Theory*, vol. 57, no. 1, pp. 403–415, Jan. 2011.

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

[25] 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.

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

[27] 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.

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

[29] S. Riis, "Linear versus non-linear Boolean functions in network flow," in *Proc. Conf. Inf. Sci. Syst. (CISS)*, Princeton, NJ, USA, Mar. 2004.

[30] J. Roitman, *Introduction to Modern Set Theory*. Richmond, VA, USA: Virginia Commonwealth Univ. Mathematics, 2011.

[31] Q. Sun, X. Yangy, 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.

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

[33] Q. 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.

[34] A. Tavory, M. Feder, and D. Ron, "Bounds on linear codes for network multicast," in *Proc. Electron. Colloq. Comput. Complex. (ECCC)*, vol. 33. 2003, pp. 1–9.

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

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