Network Coding Using Unital Modules over Rings

Shweta Agrawal and Sriram Vishwanath
Laboratory of Informatics, Networks and Communication (LINC),
Department of Electrical and Computer Engineering,
The University of Texas at Austin, Austin TX 78712.
e-mail: {sagrawal,sriram}@ece.utexas.edu.

***Abstract*— The traditional notion of network coding is that of the output being linear combinations of incoming vectors at each node in the network. This simple but powerful strategy has been proved to possess multiple properties, from both a throughput and a robustness/security perspective. This paper seeks to take this strategy from the realm of vector spaces to (unital free) modules over rings for two reasons: a. modules are more general algebraic entities than vector spaces, allowing for a larger set of options in picking code constructions and thus allowing for a wider range of possibilities and tradeoffs among parameters that govern network coding. b. Properties such as non-commutativity and non-invertibility (no-inverse element) of elements in the underlying ring *may* permit the network designer to control the amount of information available at nodes in the network, both on the data and the structure (topology) of the network itself.**

This paper's main focus is to show that using modules based on rings (with identity) does not cause a loss in throughput, i.e., that with or without inverse elements and commutativity, the network-coding strategy achieves the cut-set bound in unicast and multicast networks. The task of exploiting the more general structure of such a coding scheme (for security or robustness purposes) is left to a later document.

I. Introduction

Network coding has emerged as a new paradigm and platform on which we can construct and design networks [1]. Granting each node the ability to mix information flows impacts the design of each component of the entire protocol stack [2], [3], [4] of the network. Although this mixing can in general be non-linear, the primary focus of much of network coding research has been on linear transformations over vectors spaces [9], [6], [5], as linear coding has proved sufficient for attaining the cutset bound in multicast networks [7].

Linear coding unfortunately, is not sufficient to achieve the cutset bound for more general network configurations [8]. This is one among several reasons to study extensions of network coding theory to other (perhaps more general) algebraic structures.

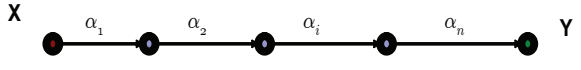


Fig. 1. Network Tomography: Non-commutative vs. Commutative Algebras

In this paper, we initiate the study of network coding as a problem of transformations on modules over rings. As vector spaces are special cases of modules and a multitude of coding strategies exist in the linear domain alone, it is immediate that the number of constructions and coding strategies to pick from in the domain of network codes over rings is larger. Our aim here is to show the existence of strategies that do not reduce, in essence, to a linear coding strategy over finite fields. We are therefore interested in strategies that involve (possibly non-commutative) ring elements with or without inverses. Although the exact quantitative benefits of network coding over rings need careful investigation, here are some intuitive applications of the idea:

1) Separating multiple flows in the network: Among the difficulties in network coding are determining the set of nodes at which to permit mixing of flows and the subsequent separation of flows in the network. In the finite field framework, given an element $a \in F$ where F is a finite field, the set $ker(a) = x \in F | a \cdot x = 0$ (sometimes called the kernel of element a) is the (trivial) singleton set 0. In rings, however, each element may have a non-trivial kernel, which for matrix rings is referred to as the "null space" of the matrix. This allows for flows to be separated using scalar multiplication only, and in particular, it does not require that an intermediate node be able to partially decode incoming flows.
2) Structural information about the network (tomography): The disadvantage of commutativity among field elements in traditional linear network coding over finite fields is that even if the destination knew the coefficients being used by intermediate nodes in the network, it may not always be able determine the nodes' placement in the network. This is illustrated in the linear network case in Figure 1. In the figure $\mathbf{Y} = \prod_{i=1}^{n} \alpha_i \mathbf{X}$. If α_i are chosen to be non-commutative ring elements instead of field elements in the encoding process, it may be possible to distinguish the ordering of the nodes and thus determine limited location information. If there is a change in topology (i.e., two of the nodes switch positions) a clever selection of non-commutative ring elements again allows for this to be detected at the destination.

The algebraic formulation for network coding using mod-

ules over rings is primarily performed for unicast networks in this paper. This is because proofs for the multicast case turn out to be relatively straightforward generalizations of the techniques for unicast, and therefore are left out for brevity. Multi-source settings are not considered in this paper.

The rest of the paper is organized as follows. The next section introduces the algebraic formulation and basic coding strategy. Section III, introduces and proves the main results in the paper. Section V concludes the paper and discusses future directions.

II. Network Coding: Algebraic Formulation

In this section, we introduce an algebraic formulation for network coding very similar to the one discussed in [9]. Let G be directed acyclic graph that forms a delay-free communication network. Given any labeling on the vertices in the graph $\{1, \ldots, m\}$, let node i have inputs X_{i_j} and outputs Y_{i_k}. Our interest is in a "linear-like" relationship of the form:

$$Y_{i_k} = \sum_j \alpha_{kj} X_{i_j} \quad \forall \quad k$$

where α_{kj} are coefficients drawn from a ring with identity. X_{i_j} and Y_{i_k} themselves are modeled as the direct sum[1]. By [10], both X_{i_j} and Y_{i_k} for all i, j, k in the network are elements of free unital modules. Although the formulation is "linear-like", the elements that form the transformation from input(s) to output(s) may not have inverses in the ring and may not commute with other elements.

In the same spirit as [9], we can define a transfer function for this network. Let $|C|$ be the size of the min-cut of this network. Since each path in the graph is of finite length and there are finitely many paths from source to destination in this network, one can find a $|C| \times |C|$ matrix $\mathbf{M}$ that represents the network as:

$$\mathbf{O} = \mathbf{MI}$$

where $\mathbf{I}$ and $\mathbf{O}$ are $|C| \times 1$ input and output "vectors" whose elements are from the ring under consideration. We already know that if the elements that form the matrix $\mathbf{M}$ (and $\mathbf{I}$ and $\mathbf{O}$) are drawn from a finite field, then the symbolic determinant of $\mathbf{M}$ is non-zero and that a substitution technique can be found to find a linear network coding strategy that achieves capacity [9]. Our goal is to find a similar substitution this matrix with ring elements.

A. Encoding and Decoding: Requirements and Decoupling

For the candidate ring to be used for encoding, we must have, at minimum:

1) Finite-ness: The ring from which we draw components of vectors and coefficients must be finite, as ultimate we desire to map the elements of the ring to vectors over F_2.
2) Closure: This is part of the definition of rings. This is essential for the same reason as in (1) above.
3) Identity: The ring must contain an identity to allow for the encoding process to be reversed.

In network coding over finite fields, a natural decoding mechanism (and analysis) is based on the invertibility of the transfer function matrix. Inverting a matrix over a ring R requires certain elements of the matrix to have inverses in R, which cannot be guaranteed in an arbitrary ring. Division rings have inverses, but Wedderburn's "Little" Theorem [10, Theorem 13.1] asserts that if R is a finite division ring, then R is a field. Thus, considering division rings for encoding and decoding does not allow for network coding to be generalized. To get around this problem, we decouple encoding and decoding. For encoding, we consider a finite ring R, and for decoding, we use the division ring D generated by R. In general, this division ring will be infinite in size. This is however not an issue for transmission or reception at any node in the network, as the encoding at every node in the network happens within the finite ring R. Thus, for the rest of this paper, we will always assume that the decoding occurs in the division ring generated by the ring.

III. Network Coding over Commutative and Noncommutative Rings

A. Commutative Rings

Given the formulation in Section II , we can state the theorem for unicast transmission using commutative rings as follows:

Main Theorem: Given a directed acyclic graph G, there exists a network code using free modules over a finite commutative ring R as long as the size of R is large enough.

Proof: Note that the notion of determinant used for matrices over fields extends to matrices over commutative rings [11]. This is because the determinant is only a polynomial function of the elements of the transfer matrix, and does not require the notion of inverse to be defined. Similarly, the notion of row (and column independence) extends to commutative rings. Thus, if the multinomial corresponding to the determinant has a non-zero evaluation, the transfer matrix is invertible *in the division ring generated by* R. Thus, if we can find a ring large enough to allow a non-zero determinant for $\mathbf{M}$, we have the desired network code.

A polynomial of degree n over a division ring generated by a commutative ring can have at most n zeroes [10, Theorem 16.4]. Thus, if the maximum degree of the multinomial corresponding to the determinant of $\mathbf{M}$ is d, a commutative ring with identity with more than d non-zero elements will allow for a network code that is invertible. This concludes the proof.

Note that, like network coding over finite fields, the (only) constraint on the commutative ring is on its size. In the case of non-commutative rings, neither the proof technique nor the constraints are this succinct.

[1] direct sum of a ring is loosely defined as a "tuple" of ring elements. For a formal definition, see [10]

B. Non-commutative Rings

In the case of a non-commutative ring R, there is no standard notion of determinant of a matrix comprised of entries from R. For the case where all the coefficients are picked from the center of the ring, the proof technique is identical to that in Subsection III-A. In this section, we study the case where coefficients are drawn from outside the center and therefore do not commute with each other.

The notion of quasi-determinant for a matrix over R was defined in [12] by Gel'fand and Retakh, and is the key tool we use for the noncommutative scenario. For an $n \times n$ matrix $\mathbf{M}^n$ let $\mathbf{M}^k, k \leq n$ denote the kth leading principal submatrix and let $m^k_{i,j}$ denote the $(i,j)th$ element of $\mathbf{M}^k$. Let $\mathbf{M}^k_{/p,/q}$ denote the $k-1 \times k-1$ submatrix of $\mathbf{M}^k$ with the pth row and the qth column removed. Let $\mathbf{M}^k_{r,/s}$ be the rth row of $\mathbf{M}^k$ with the sth element removed and let $(\mathbf{M}^k)^T_{s,/r}$ be the sth column of $\mathbf{M}^k$ with the rth element removed.

For the matrix $\mathbf{M}^k$, [12] defines k^2 quasi-determinants $A^k_{i,j}, 1 \leq i \leq k, 1 \leq j \leq k$ as follows:

$$A^k_{i,j} \triangleq m^k_{i,j} - \mathbf{M}^k_{i,/j}(\mathbf{M}^k_{/i,/j})^{-1}(\mathbf{M}^k)^T_{j,/i}$$

Note that if the inverse of $\mathbf{M}^k$ (denoted $(\mathbf{M}^k)^{-1}$) was defined, then

$$(A^k_{i,j})^{-1} = (\mathbf{M}^k)^{-1}_{i,j}$$

in the division ring generated by the ring R. For the matrix $\mathbf{M}^n$ to be invertible over R (or in other words, to have left linearly independent rows and right linearly independent columns), it is sufficient that for any p, there exists a q such that $A_{p,q}$ is non zero [12, Proposition 1]. This can be recursively reduced to the following statement:

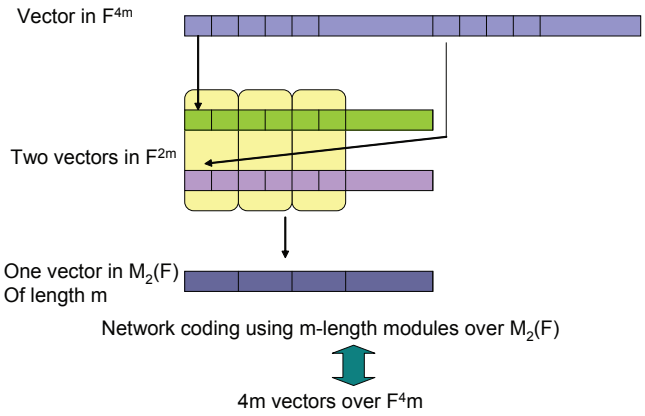
Corollary:[12] For every $1 \leq k \leq n$, if $A^k_{1,1}$ is non-zero, then $\mathbf{M}^k$ is invertible.

Thus, instead of one polynomial as in the finite field case, we now have n functions of the entries of $\mathbf{M}_n$, none of which are polynomials. This makes it much harder to solve, but the recursive nature of the corollary above would suggest an inductive construction. Given a general (not left nor right) polynomial, *if* we can find a nonzero assignment for it over an infinite noncommutative division ring, then we can recursively construct a solution as described below:

1) For $k = 1$, we obtain a polynomial, say P. For this polynomial P, we want to find a substitution that makes it non-zero. Note that this is a general multinomial over the ring R. *Assume* we can find a nonzero assignment for P over R.
2) Assume that for $k-1$ a substitution exists such that $\mathbf{M}^{k-1}$ is invertible. To ensure that $\mathbf{M}^k$ is invertible, we must ensure that $A^k_{1,1}$ is non-zero. Note that with the given choice of substitutions for $\mathbf{M}^{k-1}$, $\mathbf{M}^k$ is a polynomial over the division ring, and it is a general polynomial that is non-zero in the symbolic form. Thus, in the (infinite) division ring, we hope that there exist substitutions for this polynomial such that the polynomial is non-zero.
3) Repeat this process until $k = n$. The ring R is the smallest ring that contains all the n substitutions made above.

Thus, the construction is contingent upon finding substitutions from R for a given general polynomial so that it evaluates to a nonzero value. There is in general no guarantee that the ring R above will be finite. If R is finite, then we can use binary coding, otherwise we will have to use the reals. It turns out however, that we can construct network codes over perhaps the most intuitive framework for network coding over rings- the matrix ring. We provide a concrete example of the matrix ring next.

IV. Matrix Rings



A special class of non-commutative rings of interest is the family of matrix rings. Matrix rings over finite fields (denoted $M_n(F)$, where F is the finite field and the matrices in the ring have size $n \times n$) are particularly attractive as the coding scheme for them (and the mapping from ring elements to bits) is quite intuitive and the generalization from linear networks codes is straightforward.

For simplicity, we deal with $M_2(F)$ in this section, a set of 2×2 matrices over a finite field F. Note that this is a finite ring and not a division ring as every element does not have an inverse. The *encoding* process treats each packet (consisting of $4m$ elements of the finite field F) as a vector of length m formed from elements of $M_2(F)$. This is done as follows: if $v_1^{4m} \in F^{4m}$ denotes the packet as a row-vector over F, the encoding process transforms it into a matrix of the form

$$\begin{bmatrix} v_1^{2m} \\ v_{2m+1}^{4m} \end{bmatrix} = w_1^m$$

where w_1^m is a m-length vector over $M_2(F)$. In this setting, each symbol $w_1^m \in M_2(F)$ carries 4 times the amount of information as $v_1^m \in F$. After encoding, the vector w_1^m is transmitted across the network, network coding is done by matrix multiplication at intermediate nodes and

the output vector, say z_1^m is re-converted into a length $4m$ vector over F at the receiver.

The net transfer function in this case can also be represented as a $m \times m$ matrix over the ring $M_2(F)$. However, it is also equivalently a $2m \times 2m$ matrix over the field F. Thus, equivalently in terms of fields, the encoding process can be seen as the use of the same $2m \times 2m$ transfer matrix for two sub-packets of the original $4m$ length packet - v_1^{2m} and v_{2m+1}^{4m}. If this transfer function is invertible, then both of these sub-packets can be received successfully at the destination. We can easily ensure this using the principles detailed for linear coding over finite fields in [9] by picking a field large enough to ensure the resulting matrix is invertible.

Thus, network coding using modules that are based on matrix rings over fields seems like a special case of regular linear network coding over finite fields. It is however, an interesting case as constraining the two sub-packets of the packet to have the same transfer matrix grants us the non-commutativity property of the network code, while it does not reduce network capacity.

V. Conclusions and Future Directions

In this paper, we present a formulation that allows for network coding to be performed using free unital modules over rings. Intuitively, this can be viewed as replacing the scalars in linear network coding with vectors, and vectors in linear network coding with "vectors" of vectors, and thus, in a loose sense, performing network coding in higher dimensions. We find sufficiency conditions on commutative rings such that network coding achieves unicast capacity. The generalization of this to multicast capacity is relatively straightforward and thus not discussed in the paper. An inductive methodology is presented for designing network codes in non-commutative rings. Two possible applications of these codes are identified: in network tomography and in separating flows in the network.

Future directions include: a) application of these codes in studying multi-source multi-destination networks and b) in developing identity and topology maintenance algorithms that use network coding as their main framework.

References

[1] Network Coding Homepage, visit http://www.ifp.uiuc.edu/ koetter/NWC/ and the bibliography therein.

[2] Ning Cai and Raymond W. Yeung, Network Coding and Error Correction, ITW2002 Bangalore http://personal.ie.cuhk.edu.hk/ pwkwok4/Yeung/3.pdf

[3] T. Ho, B. Leong, R. Koetter, M. Médard, M. Effros, and D. R. Karger, Byzantine Modification Detection in Multicast Networks using Randomized Network Coding, IEEE International Symposium on Information Theory (ISIT 2004), June 27th-July 2nd, Chicago.

[4] S. Sarkar, L. Tassiulas, A framework for routing and congestion control for multicast information flows, IEEE Transactions on Information Theory, Volume: 48 Issue: 10, pp 2690-2708, Oct. 2002

[5] S. Jaggi, M. Effros T. C. Ho, M. Médard, "On Linear Network Coding", In Proc. 42nd Annual Allerton Conference on Communication, Control, and Computing, September-October 2004.

[6] S. -Y. Li, N. Cai, R. Yeung, On Theory of Linear Network Coding, ISIT 2005.

[7] T. Ho, R. Koetter, M. Medard, D. Karger and M. Effros, The Benefits of Coding over Routing in a Randomized Setting, ISIT 2003

[8] R. Dougherty, C. Freiling, and K. Zeger, Insufficiency of Linear Coding in Network Information Flow, IEEE Transactions on Information Theory, 2005.

[9] R. Koetter, M. Médard, An Algebraic Approach to Network Coding, Transactions on Networking, October 2003

[10] T.Y. Lam, "A First Course in Non-Commutative Rings", Springer-Verlag, New York, 1991.

[11] P.M. Cohn, "An introduction to Ring Theory", Springer, London, 2000.

[12] I.M. Gel'fand and V.S. Retakh, "Determinants of Matrices over Noncommutative Rings", Funct. Anal. Appl. 25 (1991), no. 2, 91-102.

[13] B.V. Zabavskii, "On noncommutative rings with elementary divisors", Ukrainian Mathematical Journal, Vol. 42, No. 6, June, 1990.

[14] T. M. Cover and J. A. Thomas, "Elements of Information Theory", New York: Wiley, 1991.