Insufficiency of Linear Coding in Network Information Flow

Randall Dougherty
Center for Communications Research
4320 Westerra Court
San Diego, CA 92121-1969
Email: rdough@ccrwest.org

Christopher Freiling
Department of Mathematics
California State University
5500 University Parkway
San Bernardino, CA 92407-2397
Email: cfreilin@csusb.edu

Kenneth Zeger
Dept. of Electrical and Computer Eng.
University of California, San Diego
La Jolla, CA 92093-0407
Email: zeger@ucsd.edu

Abstract— **It is known that every solvable multicast network has a scalar linear solution over a sufficiently large finite field alphabet. It is also known that this result does not generalize to arbitrary networks. There are several examples in the literature of solvable networks with no scalar linear solution over any finite field. However, each example has a linear solution for some vector dimension greater than one. It has been conjectured that every solvable network has a linear solution over some finite field alphabet and some vector dimension. We provide a counterexample to this conjecture. We also show that if a network has no linear solution over any finite field, then it has no linear solution over any finite commutative ring with identity. Our counterexample network has no linear solution even in the more general algebraic context of modules, which includes as special cases all finite rings and Abelian groups. Furthermore, we show that the network coding capacity of this network is strictly greater than the maximum linear coding capacity over any finite field (exactly 10% greater), so the network is not even asymptotically linearly solvable. It follows that, even for more general versions of linearity such as convolutional coding, filter-bank coding, or linear time sharing, the network has no linear solution.**

I. Introduction

In this paper, a *network* is a directed acyclic multigraph, some of whose nodes are sources or sinks. Associated with the sources are *messages* and associated with the sinks are *demands*. The demands at each sink are a subset of all the messages of all the sources. Each directed edge (u, v) in a network carries information from node u to node v. The goal is for each sink to deduce its demanded messages from its in-edges by having information propagate from the sources through the network.

A network's messages are assumed to be arbitrary elements of a fixed finite alphabet. At any node in the network, each out-edge carries an alphabet symbol which is a function (called an *edge function*) of the symbols carried on the in-edges to the node, or a function of the node's messages if it is a source. Also, each sink has *demand functions* for each of its demands, which attempt to deduce the node's demands from its inputs. A network *code* is a collection of edge functions, one for each edge in the network, and demand functions, one for each demand of each node in the network. A *solution* (sometimes called a scalar solution) is a code which results in every sink being able to deduce its demands from its demand functions, and a network that has a solution is called *solvable*. It is known [1] that for some networks, coding can achieve solutions that are otherwise unachievable using only routing.

For a network code using vector transmission, the out-edge of each node carries a vector of alphabet symbols which is a function of the vectors carried on the in-edges to the node, or a function of the node's message vectors if it is a source. Also, each source has a vector of messages and each sink demands a subset of all the source vector messages. All edge vectors are assumed to have the same dimension n and all message vectors are assumed to have the same dimension k. For general k and n, a code that allows the sink nodes to deduce their demands is called a (k, n) *fractional coding solution*.

For a network alphabet with an algebraic structure (e.g. a field), a fractional coding solution is said to be *linear* if all edge functions and all demand functions are linear combinations of their vector inputs, where the coefficients are matrices over the alphabet.

The *coding capacity of a network with respect to an alphabet $\mathcal{A}$ and a class $\mathcal{C}$ of network codes* is

$$\sup\{k/n : \exists\ (k, n) \text{ fractional coding solution in } \mathcal{C} \text{ over } \mathcal{A}\}.$$

If $\mathcal{C}$ consists of all network codes, then we simply refer to the above quantity as the *coding capacity* of the network with respect to $\mathcal{A}$. The *linear coding capacity* is the coding capacity when $\mathcal{C}$ consists of all fractional linear codes. Whereas the coding capacity of a network is known to be independent of the alphabet size [2], the linear coding capacity of a network does in general depend on the alphabet size chosen (e.g. see Theorems 4.1 and 4.2). We say that a class of network codes is *sufficient* over a class of alphabets if every solvable network has a solution in the class of codes over some member of the alphabet class. For a given alphabet and a class of codes, a network is *asymptotically solvable* if its coding capacity is at least 1. We say that a class of network codes is *asymptotically sufficient* over a class of alphabets if every solvable network is asymptotically solvable in the class of codes over some member of the alphabet class.

Li, Yeung, and Cai [6] showed that any solvable multicast network has a scalar linear solution over a sufficiently large finite field alphabet. Riis [8] noted in particular that every solvable multicast network has a linear solution over $GF(2)$ in some vector dimension.

Rasala Lehman and Lehman [5] gave a collection of networks which are solvable, but which have no scalar linear solution over any finite field alphabet. Médard, Effros, Ho, and Karger [7] pointed out that the networks in [5] have linear solutions (based purely on routing) over every finite field in two dimensions. Similarly, it was noted in [7] that a certain network given by Koetter has no scalar linear solution but does have a linear (routing) solution in two dimensions.

It is clear that linear codes in dimensions two and higher are more powerful than scalar linear codes. In fact, Médard, Effros, Ho, and Karger stated in [7]: "We conjecture that linear coding under its most general definition is sufficient for network coding in systems with arbitrary demands." Jaggi, Effros, Ho, and Médard [4] stated that the "most general possible linear codes" are filter bank network codes, a generalization of convolutional codes. It is also stated in [4] that in [7] "it is conjectured that [linear codes] are asymptotically optimal".

We disprove the conjecture in [7] for vector linear coding over the general class of R-modules, which includes as special cases finite fields, commutative rings with identity, and Abelian groups. Thus, the result is not restricted to alphabet cardinalities which are powers of primes, nor to linearity with respect to only a finite field. In addition, we show that linear coding (over finite fields) is not sufficient even asymptotically using fractional coding, as the ratio of message dimensions to edge dimensions approaches one. From this, we deduce that even convolutional or filter-bank linear coding is not sufficient for network coding, thus disproving the full form of the conjecture in [7], given the characterization of "most general possible linear codes" from [4].

Due to space limitations, all proofs are omitted from this extended abstract.[1]

II. Insufficiency of Network Linear Codes over Finite Fields

Denote by $\mathcal{N}_3$ the network shown in Figure 1. Denote by $\mathcal{N}_1$ the left one-third of $\mathcal{N}_3$ (i.e. consisting of nodes $n_1 - n_6$, n_{13}, n_{14}, n_{17}, n_{18}, n_{21}, n_{22}, n_{29}, n_{30}, n_{37}, n_{38}, n_{39}). Denote by $\mathcal{N}_2$ the right two-thirds of $\mathcal{N}_3$ (i.e. consisting of nodes $n_1 - n_3$, $n_7 - n_{12}$, n_{15}, n_{16}, n_{19}, n_{20}, $n_{23} - n_{28}$, $n_{31} - n_{36}$, $n_{40} - n_{46}$).

Lemma 2.1: The network $\mathcal{N}_1$ has a scalar linear solution over any ring with characteristic two, but has no linear solution for any vector dimension over a finite field with odd characteristic. Also, the coding capacity of $\mathcal{N}_1$ is 1.

Lemma 2.2: The network $\mathcal{N}_2$ has a scalar linear solution over any ring where 2 is a unit, but has no linear solution for any vector dimension over a finite field with characteristic two. Also, the coding capacity of $\mathcal{N}_2$ is 1.

Theorem 2.3: Network $\mathcal{N}_3$ is solvable but has no linear solution over any finite field and any vector dimension.

A solution to $\mathcal{N}_3$ is shown in Fig. 1 over an alphabet of size 4. The symbols $+$ and $-$ indicate addition and subtraction in the ring $\mathbf{Z}_4$ of integers modulo 4, the symbol $\oplus$ indicates addition in the ring $\mathbf{Z}_2 \oplus \mathbf{Z}_2$ (i.e. bitwise xor), and $t(x)$ indicates the result of exchanging the order of the bits in a 2-bit binary word x. We represent the elements of the alphabet either as members of $\mathbf{Z}_4$ when using $+$ or $-$, or as elements of $\mathbf{Z}_2 \oplus \mathbf{Z}_2$ (i.e. 2-bit binary words) when using $\oplus$ or $t()$. Note that the functions $+$ and $-$ are linear over $\mathbf{Z}_4$ but not over $GF(4)$ or $\mathbf{Z}_2 \oplus \mathbf{Z}_2$, the function $\oplus$ is linear over $\mathbf{Z}_2 \oplus \mathbf{Z}_2$ and $GF(4)$ but not over $\mathbf{Z}_4$, and the function $t()$ is not linear over any of these.

Corollary 2.4: The coding capacity of the network $\mathcal{N}_3$ is 1.

III. Insufficiency of Network Linear Codes over Rings and Modules

Whereas finite fields are uniquely characterized up to isomorphism by their cardinality, the same is not true of rings. Such rings exist for every cardinality and often in many different forms. For a given finite alphabet, the linearity of a network code can be considered with respect to any commutative ring with identity whose cardinality is the same as that of the alphabet. The lack of inverses in a ring does not prevent the use of linear network codes. In fact, consideration of rings increases the variety of codes to choose from and also allows linear codes over arbitrary alphabet sizes, instead of only powers of primes.

Theorem 3.1: If a network does not have a linear solution over any finite field in k dimensions, then it does not have a linear solution over any finite commutative ring with identity in k dimensions.

Corollary 3.2: There exists a solvable network such that for every vector dimension there is no linear solution over any finite commutative ring with identity.

We can talk about linearity in even more generality than the above, if we are willing to separate the set of coefficients allowed in linear functions from the set of inputs to the linear functions (the set of messages). For example, it makes sense to talk about linear functions over any Abelian group G if we restrict the coefficients of those functions to be integers, because ng makes sense for any integer n and any element g of G. Or we can let the set of coefficients be any field F and let the message set be any vector space over F.

If we generalize the definition of vector space to use a ring R instead of a field F, we get what are called R-modules. For any ring R, an *R-module* (or, more specifically, a *left R-module*) is an Abelian group G together with an action of R on G (i.e., a mapping from $R \times G$ to G), denoted here by concatenation: rg is the result of ring element r acting on group element g. This action must satisfy the analogues of the usual vector space laws: for any $r, s \in R$ and $g, h \in G$, we have $(rs)g = r(sg)$, $(r+s)g = rg + sg$, $r(g+h) = rg + rh$, and $0g = 0$ (the first 0 here is the ring zero and the second 0 is the group zero). If R is a ring with identity I, then we also require that $Ig = g$ for all $g \in G$.

[1] Reference [3] is a full length version of this paper, complete with proofs, and is available on-line at http://code.ucsd.edu/zeger/pubs.html .

This generalizes the two previous examples; any Abelian group is a $\mathbf{Z}$-module under the obvious action of the integers $\mathbf{Z}$ on the group by repeated addition, and any vector space over a field F is an F-module.

The notions of scalar linear solution and (vector) linear solution for a network now easily generalize to the context of an R-module G. For a scalar R-linear solution over G, the set of messages to select from is G, and each edge function or decoding function must be an R-linear function (i.e., one of the form $f(x_1, \ldots, x_j) = r_1x_1 + \ldots + r_jx_j$ where $r_1, \ldots, r_j$ are fixed elements of R). For an R-linear solution of vector dimension k, the set of messages is G^k and the edge and decoding functions are such that each component of the output vector is a fixed R-linear combination of the components of the input vectors.

Any ring R is itself an R-module acting on itself by left multiplication, so module linearity includes ring linearity as a special case.

Note that if R is a ring and G is an R-module, then $M_k(R)$, the set of $k \times k$ matrices over R with matrix addition and multiplication defined in the usual way, is a ring (with identity if R has an identity) and G^k is an $M_k(R)$-module, and any k-dimensional R-linear solution over G becomes a scalar $M_k(R)$-linear solution over G^k. So, in this very general context, (vector) linear solvability gives no more generality than scalar linear solvability (on a larger module).

Theorem 3.3: There exists a solvable network that does not have an R-linear solution over G for any ring R, any finite R-module G with more than one element, and any vector dimension.

Since any ring R is itself an R-module, we get:

Corollary 3.4: Corollary 3.2 remains true if "finite commutative ring with identity" is replaced with "finite ring with more than one element."

IV. Asymptotic Insufficiency of Network Linear Codes over Finite Fields

Theorem 4.1: The linear coding capacity of network $\mathcal{N}_1$ is $4/5$ over any odd-characteristic finite field and is 1 over any even-characteristic finite field.

Theorem 4.2: The linear coding capacity of the network $\mathcal{N}_2$ is $10/11$ over any even-characteristic finite field and is 1 over any odd-characteristic finite field.

The next corollary follows immediately from Theorems 4.1 and 4.2, and together with Corollary 2.4 shows that the coding capacity of $\mathcal{N}_3$ (i.e., 1) is exactly 10% greater than the maximum linear coding capacity (i.e., $10/11$) over any finite field.

Corollary 4.3: The linear coding capacity of the network $\mathcal{N}_3$ is $10/11$ over any even-characteristic finite field and is $4/5$ over any odd-characteristic finite field.

From this and Corollary 2.4, we get:

Corollary 4.4: There exists a solvable network which is not asymptotically linearly solvable with respect to any finite-field alphabet. In other words, linear network codes are asymptotically insufficient over finite fields.

Asymptotic insufficiency allows us to deduce results about the extended linear coding methods known as convolutional coding and filter-bank network coding (see [4] for the definitions). This is because of the following simple result which appears to be well-known (it is just a variant of Lemma 8 from [4]):

Proposition 4.5: For any finite field alphabet, if a network is solvable by means of convolutional coding or filter-bank coding, then it is asymptotically linearly solvable.

Corollary 4.6: There exists a solvable network which is not solvable by means of convolutional coding or filter-bank coding over any finite field alphabet.

Acknowledgment

This work was supported by the Institute for Defense Analyses, the National Science Foundation, and Ericsson.

References

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

[2] J. Cannons, R. Dougherty, C. Freiling, and K. Zeger, "Network routing capacity," *IEEE/ACM Transactions on Networking*, (submitted October 16, 2004).

[3] R. Dougherty, C. Freiling, and K. Zeger, "Insufficiency of linear coding in network information flow," *IEEE Transactions on Information Theory* vol. 51, no. 8, August 2005 (to appear).

[4] S. Jaggi, M. Effros, T. Ho, and M. Médard, "On linear network coding", *42st Annual Allerton Conference on Communication Control and Computing*, Monticello, Illinois, October 2004.

[5] A. Rasala Lehman and E. Lehman, "Complexity classification of network information flow problems", *41st Annual Allerton Conference on Communication Control and Computing*, Monticello, Illinois, October 2003.

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

[7] M. Médard, M. Effros, T. Ho, D. Karger, "On coding for non-multicast networks", *41st Annual Allerton Conference on Communication Control and Computing*, Monticello, Illinois, October 2003.

[8] S. Riis, "Linear versus non-linear boolean functions in network flow", *38th Annual Conference on Information Sciences and Systems (CISS)*, Princeton, NJ, March 2004.

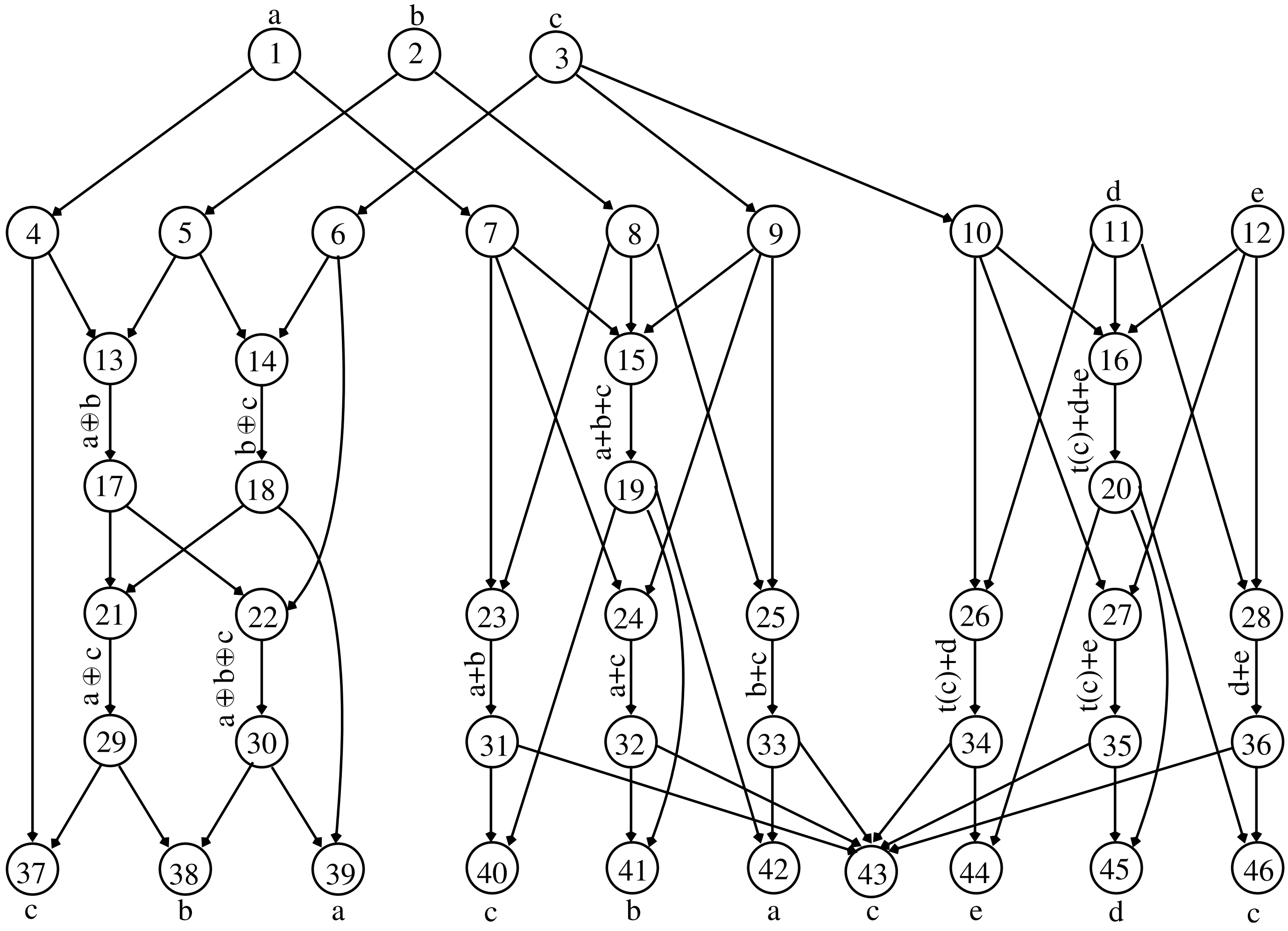

Fig. 1. The network $\mathcal{N}_3$ has sources $n_1, n_2, n_3, n_{11}, n_{12}$ with messages a, b, c, d, e respectively. Sinks n_{37} through n_{46} each demand one of the messages, as indicated. Some edges are labeled to illustrate a nonlinear solution over an alphabet of size 4 (used in Theorem 2.3).