Achievable Rate Regions for Network Coding

Randall Dougherty, Chris Freiling, and Kenneth Zeger, *Fellow, IEEE*

***Abstract*— Determining the achievable rate region for networks using routing, linear coding, or nonlinear coding is thought to be a difficult task in general, and few are known. We describe the achievable rate regions for four interesting networks (completely for three and partially for the fourth). In addition to the known matrix-computation method for proving outer bounds for linear coding, we present a new method that yields actual characteristic-dependent linear rank inequalities from which the desired bounds follow immediately.**

***Index Terms*— Shannon capacity, routing, entropy, information theory.**

I. Introduction

IN THIS paper, a *network* is a directed acyclic multigraph $G = (V, E)$, some of whose nodes are information sources or receivers (see [22]). Associated with the sources are m generated *messages*, where the i^{th} source message is assumed to be a vector of k_i arbitrary elements of a fixed finite alphabet, $\mathcal{A}$, of size at least 2. At any node in the network, each out-edge carries a vector of n alphabet symbols which is a function (called an *edge function*) of the vectors of symbols carried on the in-edges to the node, and of the node's message vectors if it is a source. Each network edge is allowed to be used at most once (i.e. at most n symbols can travel across each edge). It is assumed that every network edge is reachable by some source message. Associated with each receiver are one or more *demands*; each demand is a network message. Each receiver has *decoding functions* which map the receiver's inputs to vectors of symbols in an attempt to produce the messages demanded at the receiver. The goal is for each receiver to deduce its demanded messages from its in-edges and source messages by having information propagate from the sources through the network.

A $(k_1, \ldots, k_m, n)$ *fractional code* is a collection of edge functions, one for each edge in the network, and decoding functions, one for each demand of each node in the network. A $(k_1, \ldots, k_m, n)$ *fractional solution* is a $(k_1, \ldots, k_m, n)$ fractional code which results in every receiver being able to compute its demands via its decoding functions, for all possible assignments of length-k_i vectors over the alphabet to the i^{th} source message, for all i.

Special codes of interest include *linear codes*, where the edge functions and decoding functions are linear, and *routing codes*, where the edge functions and decoding functions simply copy specified input components to output components.[1] Special networks of interest include *multicast* networks, where there is only one source node and every receiver demands all of the source messages, and *multiple-unicast* networks, where each network message is generated by exactly one source node and is demanded by exactly one receiver node.

For each i, the ratio k_i/n can be thought of as the rate at which source i injects data into the network. If a network has a $(k_1, \ldots, k_m, n)$ fractional solution over some alphabet, then we say that $(k_1/n, \ldots, k_m/n)$ is an *achievable rate vector*, and we define the *achievable rate region* of the network as the following convex hull[2]

$$S = \mathrm{CHULL}(\{\mathbf{r} \in \mathbf{Q}^m : \mathbf{r} \text{ is an achievable rate vector}\})$$

where $\mathbf{Q}$ is the set of all rational numbers. Every vector in the achievable rate region can be effectively achieved by time-sharing between two achievable points (since it is a convex combination of those achievable points).

Determining the achievable rate region of an arbitrary network appears to be a formidable task. Alternatively, certain scalar quantities that reveal information about the achievable rates are typically studied. For any $(k_1, \ldots, k_m, n)$ fractional solution, we call the scalar quantity

$$\frac{1}{m}\left(\frac{k_1}{n} + \cdots + \frac{k_m}{n}\right)$$

an *achievable average rate* of the network. We define the *average coding capacity* of a network to be the supremum of all achievable average rates, namely

$$\mathcal{C}^{\text{average}} = \sup\left\{\frac{1}{m}\sum_{i=1}^{m} r_i : (r_1, \ldots, r_m) \in S\right\}.$$

Similarly, for any $(k_1, \ldots, k_m, n)$ fractional solution, we call the scalar quantity

$$\min\left(\frac{k_1}{n}, \ldots, \frac{k_m}{n}\right)$$

Manuscript received November 19, 2013; revised October 5, 2014; accepted January 12, 2015. Date of publication February 13, 2015; date of current version April 17, 2015. This work was supported in part by the Directorate for Computer and Information Science and Engineering, in part by the Institute for Defense Analyses, and in part by the U.S. National Science Foundation.

R. Dougherty is with the Center for Communications Research, San Diego, CA 92121 USA (e-mail: rdough@ccrwest.org).

C. Freiling is with the Department of Mathematics, California State University, San Bernardino, CA 92407 USA (e-mail: cfreilin@csusb.edu).

K. Zeger is with the Department of Electrical and Computer Engineering, University of California at San Diego, La Jolla, CA 92093 USA (e-mail: zeger@ucsd.edu).

Communicated by Y. Liang, Associate Editor for Shannon Theory.

Digital Object Identifier 10.1109/TIT.2015.2403315

[1] If an edge function for an out-edge of a node depends only on the symbols of a single in-edge of that node, then, without loss of generality, we assume that the out-edge simply carries the same vector of symbols (i.e. routes the vector) as the in-edge it depends on.

[2] There is some variation in the definition and terminology in the literature. Some authors use the term "capacity region" or "rate region". Alternative definitions of the region have been defined as the topological closure of S or without the convex hull.

an *achievable uniform rate* of the network. We define the *uniform coding capacity* of a network to be the supremum of all achievable uniform rates, namely

$$\mathcal{C}^{\text{uniform}} = \sup\{\min(r_1, \ldots, r_m) : (r_1, \ldots, r_m) \in S\}.$$

Note that for any $\mathbf{r} \in S$ and $\mathbf{r}' \in \mathbf{R}^m$, if each component of $\mathbf{r}'$ is nonnegative, rational, and less than or equal to the corresponding component of $\mathbf{r}$, then $\mathbf{r}' \in S$. In particular, if $(r_1, \ldots, r_m) \in S$ and

$$r_i = \min_{1 \le j \le m} r_j$$

then $(r_i, r_i, \ldots, r_i) \in S$, which implies

$$\mathcal{C}^{\text{uniform}} = \sup\{r_i : (r_1, \ldots, r_m) \in S, \quad r_1 = \cdots = r_m\}.$$

In other words, all messages can be restricted to having the same dimension $k_1 = \cdots = k_m$ when considering $\mathcal{C}^{\text{uniform}}$. Also, note that

$$\mathcal{C}^{\text{uniform}} \le \mathcal{C}^{\text{average}}.$$

The quantities $\mathcal{C}^{\text{average}}$ and $\mathcal{C}^{\text{uniform}}$ are attained by points on the boundary of S. It is known that not every network has a uniform coding capacity which is an achievable uniform rate [7].

If a network's edge functions are restricted to purely routing functions, then we write the capacities as $\mathcal{C}^{\text{average}}_{\text{routing}}$ and $\mathcal{C}^{\text{uniform}}_{\text{routing}}$, and refer to them as the *average routing capacity* and *uniform routing capacity*, respectively. Likewise, for solutions using only linear edge functions, we write $\mathcal{C}^{\text{average}}_{\text{linear}}$ and $\mathcal{C}^{\text{uniform}}_{\text{linear}}$ and refer to them as the *average linear capacity* and *uniform linear capacity*, respectively.

Given random variables $x_1, \ldots, x_i$ and $y_1, \ldots, y_j$, we write

$$x_1, \ldots, x_i \longrightarrow y_1, \ldots, y_j$$

to mean that $y_1, \ldots, y_j$ are deterministic functions of $x_1, \ldots, x_i$. We say that $x_1, \ldots, x_i$ *yield* $y_1, \ldots, y_j$.

In this paper, we study four specific networks, namely the Generalized Butterfly network, the Fano network, the non-Fano network, and the Vámos network. The last three of these networks were shown to be matroidal in [8] and various capacities of these networks have been computed. However, the full achievable rate regions of these networks have not been previously determined, to the best of our knowledge. These particular networks were chosen to demonstrate that a wide variety of techniques can be useful for determining these achievable rate regions. Some other work on achievable rates and capacities has been done in [5], [15], and [21]. We note that the derivations presented in this paper were often quite challenging, even though in hindsight they may appear neat and concise. We hope that some intuition can be learned from the derivations present herein.

The Generalized Butterfly network (studied in Section II and illustrated in Figure 1) has the same topology as the usual Butterfly network [2], but instead of one source at each of nodes v_1 and v_2, there are two sources at each of these nodes. For each of the source nodes, one of its source messages is demanded by receiver v_5 and the other by receiver v_6. The usual Butterfly network is the special case when messages a and d do not exist (or are just not demanded by any receiver). A large majority of network coding publications mention in some context the Butterfly network, so it plays an important role in the field.

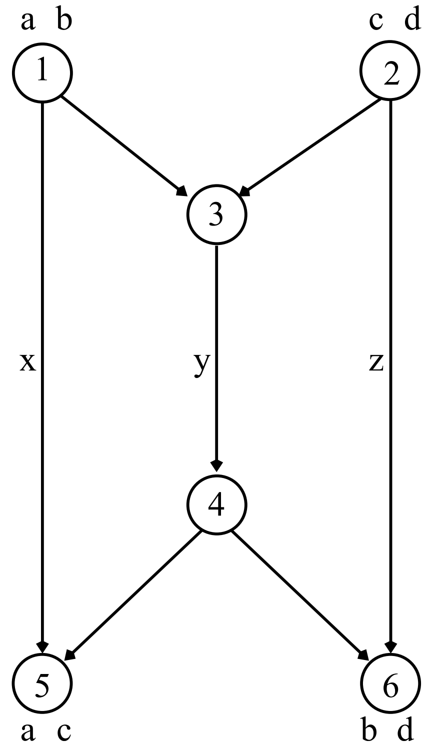

Fig. 1. The Generalized Butterfly network. Source node v_1 generates messages a and b, and source node v_2 generates messages c and d. Receiver node v_5 demands messages a and c, and receiver node v_6 demands messages b and d. The symbol vectors carried on edges $e_{1,5}$, $e_{3,4}$, and $e_{2,6}$ are denoted x, y, and z, respectively.

The Fano network (studied in Section III and illustrated in Figure 2) and the non-Fano network (studied in Section V and illustrated in Figure 6) were used in [7] as components of a larger network to demonstrate the unachievability of network coding capacity. Specifically, in [7] the Fano network was shown to be solvable if and only if the alphabet size is a power of 2 and the non-Fano network was shown to be solvable if and only if the alphabet size is odd. In [9], the Fano and non-Fano networks were used to build a solvable multicast network whose reverse (i.e. all edge directions change, and sources and receivers exchange roles) was not solvable, in contrast to the case of linear solvability, where reversals of linearly solvable multicast networks were previously known to be linearly solvable [16], [17], [20]. In [6], the Fano and non-Fano networks were used to construct a network which disproved a previously published conjecture asserting that all solvable networks are vector linearly solvable over some finite field and some vector dimension.

The Vámos network (studied in Section VII and illustrated in Figure 10) was used in [8] to demonstrate that non-Shannon-type information inequalities could yield upper bounds on network coding capacity which are tighter than the tightest possible bound theoretically achievable using only Shannon-type information inequalities. Here we completely determine the routing and linear rate regions for the Vámos network, but only give partial results for the non-linear rate region (which indicate that it could be quite complicated).

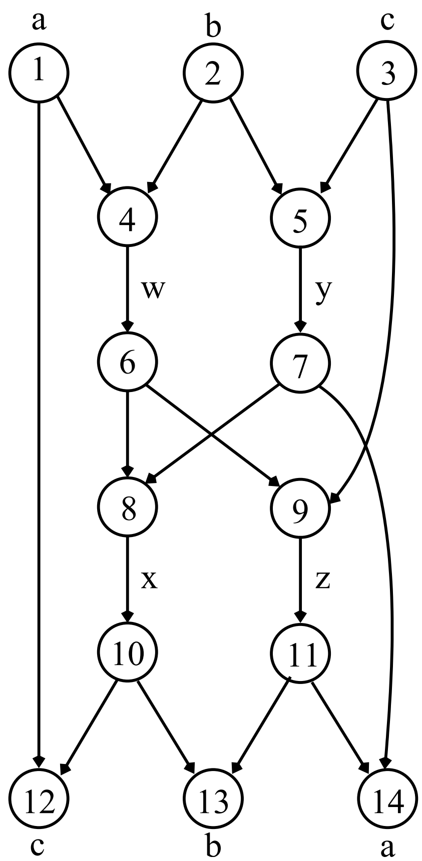

Fig. 2. The Fano network. Source nodes v_1, v_2, and v_3 generate messages a, b, and c, respectively. Receiver nodes v_{12}, v_{13}, and v_{14} demand messages c, b, and a, respectively. The symbol vectors carried on edges $e_{4,6}$, $e_{8,10}$, $e_{5,7}$, $e_{9,11}$ are labeled as w, x, y, and z, respectively.

Finally, we present a new method for proving bounds on achievable rate regions for linear coding, which actually produces explicit linear rank inequalities which directly imply the desired bounds.

II. Generalized Butterfly Network

Theorem 1: The achievable rate regions for either linear or non-linear coding are the same for the Generalized Butterfly network and are equal to the closed polytope in $\mathbf{R}^4$ *whose faces lie on the* 9 *planes:*

$$\begin{aligned} r_a &= 0\\ r_b &= 0\\ r_c &= 0\\ r_d &= 0\\ r_b &= 1\\ r_c &= 1\\ r_a + r_b + r_c &= 2\\ r_b + r_c + r_d &= 2\\ r_a + r_b + r_c + r_d &= 3 \end{aligned}$$

and whose vertices are the 14 *points:*

$$\begin{array}{llll} (0,0,0,0) & (0,0,0,2) & (2,0,0,0) & (0,1,0,0)\\ (0,0,1,0) & (2,0,0,1) & (1,0,0,2) & (0,0,1,1)\\ (1,1,0,0) & (1,0,1,1) & (1,1,0,1) & (0,1,1,0)\\ (0,1,0,1) & (1,0,1,0). & & \end{array}$$

Furthermore, the coding capacity and linear coding capacity are given by:

$$\begin{aligned} \mathcal{C}^{\text{uniform}} &= \mathcal{C}^{\text{uniform}}_{\text{linear}} = 2/3\\ \mathcal{C}^{\text{average}} &= \mathcal{C}^{\text{average}}_{\text{linear}} = 3/4. \end{aligned}$$

Proof: Consider a network solution over an alphabet $\mathcal{A}$ and denote the source message dimensions by k_a, k_b, k_c, and k_d, and the edge dimensions by n. Let each source be a random variable whose components are independent and uniformly distributed over $\mathcal{A}$. Then the solution must satisfy the following inequalities:

$$\begin{aligned} k_a &\geq 0 && (1)\\ k_b &\geq 0 && (2)\\ k_c &\geq 0 && (3)\\ k_d &\geq 0 && (4)\\ k_b &= H(b) = H(y|a,c,d) \leq n && (5)\\ k_c &= H(c) = H(y|a,b,d) \leq n && (6)\\ k_a + k_b + k_c &= H(a,b,c) = H(x,y|d) &&\\ &\leq H(x,y) \leq 2n && (7)\\ k_b + k_c + k_d &= H(b,c,d) = H(y,z|a) &&\\ &\leq H(y,z) \leq 2n && (8)\\ k_a + k_b + k_c + k_d &= H(a,b,c,d) = H(x,y,z) &&\\ &\leq 3n. && (9) \end{aligned}$$

(1)–(4) are trivial; (5) follows because

$$c, d, y \longrightarrow y, z \longrightarrow b, d$$

(at node v_6), and therefore $a, c, d, y \longrightarrow a, b, c, d$ and thus $H(a, b, c, d) = H(a, c, d, y)$; similarly for (6); (7) follows because $x, y \longrightarrow a, c$ (at node v_5), $c, d, y \longrightarrow b, d$ (at node v_6), and therefore

$$d, x, y \longrightarrow a, c, d, y \longrightarrow a, b, c, d$$

and thus $H(a, b, c, d) = H(d, x, y)$; similarly for (8); (9) follows because $x, y, z \longrightarrow a, b, c, d$ (at nodes v_5 and v_6). Dividing each inequality in (1)–(9) by n gives the 9 bounding hyperplanes stated in the theorem.

Let

$$\begin{aligned} r_a &= k_a/n\\ r_b &= k_b/n\\ r_c &= k_c/n\\ r_d &= k_d/n \end{aligned}$$

and let $\mathcal{P}$ denote the polytope in $\mathbf{R}^4$ consisting of all 4-tuples (r_a, r_b, r_c, r_d) satisfying (1)–(9). Then (1)–(4) and (9) ensure that $\mathcal{P}$ is bounded. One can easily calculate that each point in $\mathbf{R}^4$ that satisfies some independent set of four of the inequalities (1)–(9) with equality and also satisfies the remaining five inequalities must be one of the 14 points stated in the theorem. Now we show that all 14 such points do indeed lie in the achievable rate region, and therefore their convex hull equals the achievable rate region. The following 5 points are achieved by taking $n = 1$ with the following codes over any field (where, if $k_a = 2$, the two components of a are denoted a_1 and a_2):

$$\begin{array}{ll}(2,0,0,1): & x = a_1, \quad y = a_2, \quad z = d \\ (1,0,0,2): & x = a, \quad y = d_1, \quad z = d_2 \\ (1,0,1,1): & x = a, \quad y = c, \quad z = d \\ (1,1,0,1): & x = a, \quad y = b, \quad z = d \\ (0,1,1,0): & x = b, \quad y = b + c, \quad z = c\end{array}$$

and the remaining 9 points are achieved by fixing certain messages to be 0.

Since the above codes are all linear, the achievable rate regions for linear and non-linear codes are the same.

By (9), we have $\mathcal{C}^{\text{average}} \leq 3/4$, and this upper bound is achievable by routing using the code given above for the point $(2, 0, 0, 1)$, namely taking $x = a_1$, $y = a_2$, and $z = d$. By (8), we have $\mathcal{C}^{\text{uniform}} \leq 2/3$; since

$$(2/3)(1,1,1,1) = (1/3)(1,0,1,1) + (1/3)(1,1,0,1) + (1/3)(0,1,1,0)$$

the upper bound of $2/3$ is achievable by a convex combination of the linear codes given above for the points $(1, 0, 1, 1)$, $(1, 1, 0, 1)$, and $(0, 1, 1, 0)$, as follows. Take $k = 2$ and $n = 3$ and use the (linear) code determined by:

$$\begin{aligned} x &= (a_1, a_2, b_2) \\ y &= (c_1, b_1, b_2 + c_2) \\ z &= (d_1, d_2, c_2). \end{aligned}$$

■

Theorem 2: The achievable rate region for routing for the Generalized Butterfly network is the closed polytope in $\mathbf{R}^4$ *bounded by the* 9 *planes in Theorem 1 together with the plane*

$$r_b + r_c = 1$$

and whose vertices are the 13 *points:*

(0, 0, 0, 0)	(0, 0, 0, 2)	(2, 0, 0, 0)	(0, 1, 0, 0)
(0, 1, 0, 1)	(0, 0, 1, 0)	(2, 0, 0, 1)	(1, 0, 0, 2)
(0, 0, 1, 1)	(1, 0, 1, 0)	(1, 1, 0, 0)	(1, 0, 1, 1)
(1, 1, 0, 1).			

Furthermore, the routing capacities are given by:

$$\begin{aligned} \mathcal{C}^{\text{uniform}}_{\text{routing}} &= 1/2 \\ \mathcal{C}^{\text{average}}_{\text{routing}} &= 3/4. \end{aligned}$$

Proof: With routing, in addition to the inequalities (1)–(9), a solution must also satisfy

$$k_b + k_c \leq n \tag{10}$$

since all of the components of messages b and c must be carried by the edge labeled y. One can show that each point in $\mathbf{R}^4$ that satisfies with equality some independent set of four of the inequalities (1)–(9) and (10) and also satisfies the remaining six inequalities must be one of the 13 points stated in this theorem (i.e. 13 of the 14 points stated in Theorem 1 by excluding the point $(0, 1, 1, 0)$). The proof of Theorem 1 showed that all vertices of $\mathcal{P}$ except $(0, 1, 1, 0)$ were achievable using routing.

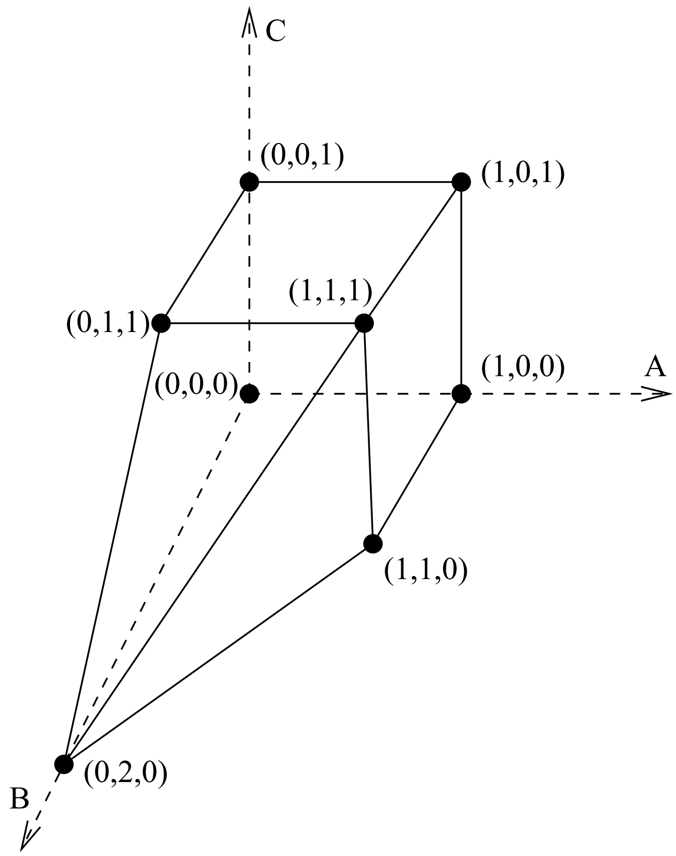

Fig. 3. The achievable coding rate region for the Fano network is a 7-sided polyhedron with 8 vertices.

By (10), we have $\mathcal{C}^{\text{uniform}}_{\text{routing}} \leq 1/2$, and this upper bound is achievable, for example, by taking a convex combination of codes that achieve $(1, 0, 1, 0)$ and $(0, 1, 0, 1)$, as follows. Take $k = 1$ and $n = 2$ and use the routing code determined by:

$$\begin{aligned} x &= (0, a) \\ y &= (b, c) \\ z &= (d, 0). \end{aligned}$$

The capacity $\mathcal{C}^{\text{average}}_{\text{routing}} = 3/4$ follows immediately from the proof of Theorem 1. ■

III. Fano Network

Theorem 3: The achievable rate regions for either linear coding over any finite field alphabet of even characteristic or non-linear coding are the same for the Fano network and are equal to the closed polyhedron in $\mathbf{R}^3$ *whose faces lie on the* 7 *planes (see Figure 3):*

$$\begin{aligned} r_a &= 0 \\ r_b &= 0 \\ r_c &= 0 \\ r_a &= 1 \\ r_c &= 1 \\ r_b + r_c &= 2 \\ r_a + r_b &= 2 \end{aligned}$$

and whose vertices are the 8 *points:*

$$(0,0,0) \quad (0,0,1) \quad (1,0,0) \quad (0,2,0)$$
$$(0,1,1) \quad (1,0,1) \quad (1,1,0) \quad (1,1,1).$$

Proof: Consider a network solution over an alphabet $\mathcal{A}$ and denote the source message dimensions by k_a, k_b, and k_c, and the edge dimensions by n. Let each source be a random variable whose components are independent and uniformly distributed over $\mathcal{A}$. Then the solution must satisfy the following inequalities:

$$k_a \geq 0 \tag{11}$$
$$k_b \geq 0 \tag{12}$$
$$k_c \geq 0 \tag{13}$$
$$k_a = H(a) = H(z|b,c) \leq H(z) \leq n \tag{14}$$
$$k_c = H(c) = H(y|a,b) \leq H(y) \leq n \tag{15}$$
$$k_b + k_c = H(b,c) = H(x,z|a) \leq H(x,z) \leq 2n \tag{16}$$
$$k_a + k_b = H(a,b) = H(x,z|c) \leq H(x,z) \leq 2n. \tag{17}$$

(11)–(13) are trivial; (14) follows because

$$z, b, c \longrightarrow z, y \longrightarrow a$$

(at node v_{14}), so $z,\ b,\ c \longrightarrow a,\ b,\ c$ and thus $H(z,b,c) = H(a,b,c)$; (15) follows because

$$a, b, y \longrightarrow a, w, y \longrightarrow a, x \longrightarrow c$$

(at node v_{12}), so $a,\ b,\ y \longrightarrow a,\ b,\ c$ and thus $H(a,b,y) = H(a,b,c)$; (16) follows because

$$a, x, z \longrightarrow a, b, c$$

(at nodes v_{12} and v_{13}) and thus $H(a,x,z) = H(a,b,x)$; (17) follows from: $x, z \longrightarrow b$ (at node v_{13}), $b, c \longrightarrow y$ (at node v_5),

$$x, z, c \longrightarrow z, b, c \longrightarrow y, z, b, c \longrightarrow a, b, c$$

so $H(x,z,c) = H(a,b,c)$. Dividing each inequality in (11)–(17) by n gives the 7 bounding planes stated in the theorem.

Let $r_a = k_a/n$, $r_b = k_b/n$, and $r_c = k_c/n$, and let $\mathcal{P}$ denote the polygon in $\mathbf{R}^3$ consisting of all 3-tuples (r_a, r_b, r_c) satisfying (11)–(17). Then $\mathcal{P}$ is bounded by (11)–(17). One can easily calculate that each point in $\mathbf{R}^3$ that satisfies some set of three of the inequalities (11)–(17) with equality and also satisfies the remaining four inequalities must be one of the 8 points stated in the theorem. Now we show that all 8 such points do indeed lie in $\mathcal{P}$. The following 5 points are seen to lie in $\mathcal{P}$ by taking $n = 1$ and the following codes over any even-characteristic finite field

$$(0,1,1): \quad x = y = c, \quad w = z = b$$
$$(1,0,1): \quad x = y = c, \quad w = z = a$$
$$(1,1,0): \quad x = y = b, \quad w = z = a$$
$$(0,2,0): \quad x = y = b_1, \quad w = z = b_2$$
$$(1,1,1): \quad w = a+b, \quad y = b+c, \quad x = a+c, \quad z = a+b+c$$

and the remaining 3 points are achieved by fixing certain messages to be 0 (note that the codes for $(0,1,1)$, $(1,0,1)$, and $(1,1,0)$ can be obtained from the linear code for $(1,1,1)$ but we gave routing solutions for them here).

Since the above codes are all linear, the achievable rate regions for linear and non-linear codes are the same. ■

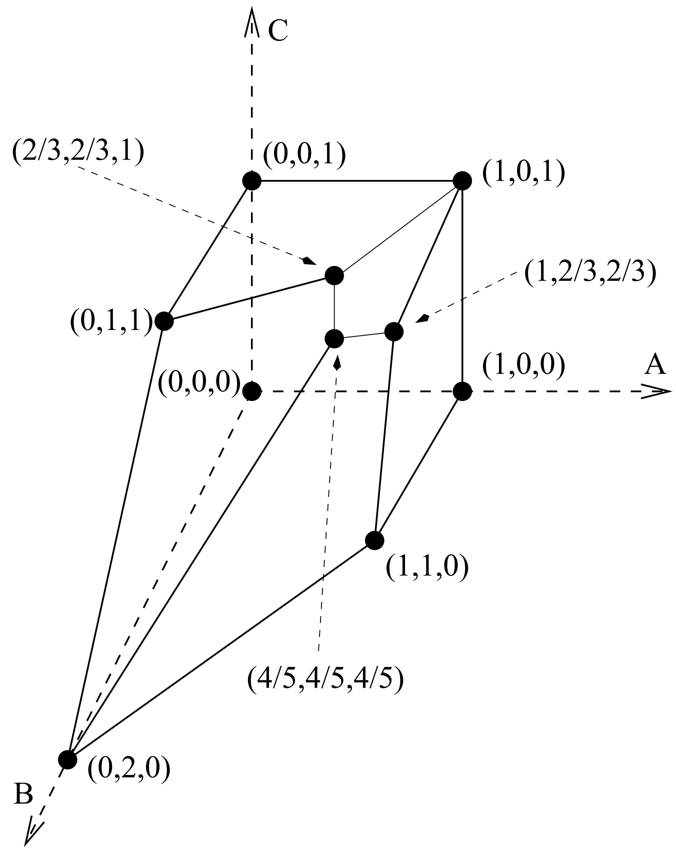

Fig. 4. The achievable linear coding rate region over even-characteristic finite fields for the Fano network is a 8-sided polyhedron with 8 vertices.

It was shown in [6] that for the Fano network, $\mathcal{C}^{\text{average}} = \mathcal{C}^{\text{uniform}} = 1$ and $\mathcal{C}^{\text{uniform}}_{\text{linear}} = 1$ for all even-characteristic fields and $\mathcal{C}^{\text{uniform}}_{\text{linear}} = 4/5$ for all odd-characteristic fields. The calculation of $\mathcal{C}^{\text{uniform}}_{\text{linear}} = 4/5$ in [6] required a rather involved computation. We now extend that computation to give the following theorem.

Theorem 4: The achievable rate region for linear coding over any finite field alphabet of odd characteristic for the Fano network is equal to the closed polyhedron in $\mathbf{R}^3$ *whose faces lie on the* 8 *planes (see Figure 4):*

$$r_a = 0$$
$$r_b = 0$$
$$r_c = 0$$
$$r_a = 1$$
$$r_c = 1$$
$$r_a + 2r_b + 2r_c = 4$$
$$2r_a + r_b + 2r_c = 4$$
$$2r_a + 2r_b + r_c = 4$$

and whose vertices are the 10 *points:*

$$(0,0,0) \quad (0,0,1) \quad (1,0,0) \quad (0,2,0)$$
$$(0,1,1) \quad (1,0,1) \quad (1,1,0)$$
$$(2/3,2/3,1) \quad (1,2/3,2/3) \quad (4/5,4/5,4/5).$$

Proof: In addition to satisfying the conditions (11)–(17), the solution must satisfy the following inequalities:

$$k_a + 2k_b + 2k_c \leq 4n \quad (18)$$
$$2k_a + k_b + 2k_c \leq 4n \quad (19)$$
$$2k_a + 2k_b + k_c \leq 4n. \quad (20)$$

The proofs of these inequalities are given in Section IV, and an alternate proof of (19) is given in Section VIII-A.

A straightforward argument as in previous theorems shows that the vertices of the (bounded) region specified by inequalities (11)–(15) and (18)–(20) (inequalities (16) and (17) are now redundant) are the ten vertices listed in the theorem. For the first seven of these, the codes given in Theorem 3 work here as well; the remaining points are attained by the following three codes (the last of which was given in [6]):

$$\begin{aligned}
(1, 2/3, 2/3):\quad & n = 3,\\
& w = (a_1 + b_1, a_2 + b_2, a_3)\\
& x = (a_1 - c_1, a_2 - c_2, a_2 + b_2)\\
& y = (b_1 + c_1, b_2 + c_2, b_1)\\
& z = (a_1 + b_1 - c_1, a_2 + b_2 + c_2, a_3)\\
(2/3, 2/3, 1):\quad & n = 3,\\
& w = (a_1 + b_1, a_2 + b_2, b_2)\\
& x = (a_1 - c_1, a_2 - c_2, c_3)\\
& y = (b_1 + c_1, b_2 + c_2, c_3)\\
& z = (a_1 + b_1 - c_1, a_2 - b_2 - c_2, c_1)\\
(4/5, 4/5, 4/5):\quad & n = 5,\\
& w = (a_1 + b_1, a_2 + b_2, a_3 + b_3, a_4 + b_4, b_1 + b_4)\\
& x = (c_1 + a_1, c_2 + a_2, c_3 - a_3, c_4 - a_4, a_3 + b_3)\\
& y = (c_1 - b_1, c_2 - b_2, c_3 + b_3, c_4 + b_4, b_2)\\
& z = (a_1 + b_1 + c_1, a_2 + b_2 + c_2, a_3 + b_3 + c_3, a_4 + b_4 + c_4, b_1 + b_4 + c_4).
\end{aligned}$$

■

Theorem 5: The achievable rate region for routing for the Fano network is the closed polyhedron in $\mathbf{R}^3$ whose faces lie on the 6 planes (see Figure 5):

$$r_a = 0$$
$$r_b = 0$$
$$r_c = 0$$
$$r_a = 1$$
$$r_c = 1$$
$$r_a + r_b + r_c = 2$$

and whose vertices are the 7 points:

$$(0, 0, 0) \quad (0, 0, 1) \quad (1, 0, 0) \quad (0, 2, 0)$$
$$(0, 1, 1) \quad (1, 0, 1) \quad (1, 1, 0).$$

Proof: With routing, in addition to the inequalities (11)–(17), a solution must also satisfy

$$k_a + k_b + k_c \leq 2n \quad (21)$$

since all of the components of messages a, b, and c must be carried by the edges labeled x and z. One can easily check that

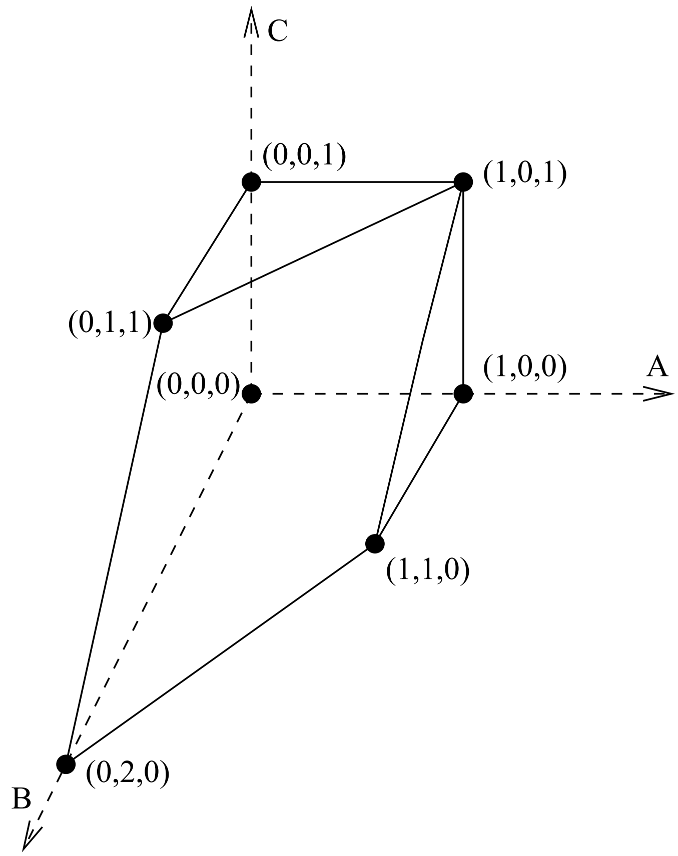

Fig. 5. The achievable routing rate region for the Fano network is a 6-sided polyhedron with 7 vertices.

the extreme points of the new region with the inequality (21) added are the 7 points stated in this theorem (i.e., the points stated in Theorem 3 excluding the point (1, 1, 1)); see figure 5. The proof of Theorem 3 showed that all vertices of $\mathcal{P}$ other than (1, 1, 1) were achievable using routing. ■

IV. Proofs of Remaining Bounds for the Fano Network

For the case of linear coding over a finite field of odd characteristic, we want to prove the bounds:

$$k_a + 2k_b + 2k_c \leq 4n \quad (22)$$
$$2k_a + k_b + 2k_c \leq 4n \quad (23)$$
$$2k_a + 2k_b + k_c \leq 4n. \quad (24)$$

We will do this by following and extending the arguments from [6, Sec. IV], with minor modifications needed because we now have separate source message dimensions k_a, k_b, k_c instead of a single message dimension k.

These arguments are built up step-by-step, starting from a proof that (in this case) the network is not scalar-linear solvable over a field of odd characteristic. This is extended to a proof that the network is not vector-linear solvable (with $k_a = k_b = k_c = n$) over such a field; arguments involving division of scalar network coefficients turn into arguments involving matrices, so, as in [6, Sec. II], one first has to show that the relevant matrices are invertible.

When one proceeds to the case where the k's can differ from n, the matrices are no longer completely invertible; one has to extract as large a part of them as possible that is invertible. Constructing the achievable rate region becomes an iterative process. Given the bounds produced so far, one determines the extreme points (corners) of the resulting region and tries to find linear network codes attaining these points; if such an attempt fails, the reason for that failure can lead to an improvement in the matrix argument and hence a new bounding inequality. The iteration continues until, it is hoped, success is attained because all of the current extreme points have been achieved. Here we will just give the final result of that iteration.

We already have the bounds $k_a \le n$ and $k_c \le n$ (but we do *not* necessarily have $k_b \le n$). Therefore, we can think of the length-n symbol vectors w and z (referred to in [6] as $e_{13,17}$ and $e_{22,30}$) as coming in two parts, one of length k_a and one of length $\delta_a = n - k_a$. Similarly, we can think of the symbol vectors x and y (referred to in [6] as $e_{21,29}$ and $e_{14,18}$) as coming in two parts, one of length k_c and one of length $\delta_c = n - k_c$. In order to consider what happens to these parts separately, we decompose each of the transition matrices M_i from [6] in the form

$$M_i = \begin{bmatrix} R_i & S_i \\ T_i & U_i \end{bmatrix}$$

where the submatrices R_i, S_i, T_i, U_i are of appropriate sizes (or are omitted altogether if appropriate). For instance, for $i = 2$ we have that R_2 is $k_a \times k_b$, T_2 is $\delta_a \times k_b$, and S_2 and U_2 are omitted; for $i = 5$ we have that R_5 is $k_c \times k_a$, S_5 is $k_c \times \delta_a$, T_5 is $\delta_c \times k_a$, and U_5 is $\delta_c \times \delta_a$.

We can now follow the arguments in [6, pp. 2752–2755] and verify that they apply in this new context with no further changes. In particular, the following formulas from [6, pp. 2754–2755] still hold:

$$\begin{aligned}&(U_7 + T_8 S_5)T_2 b + T_8 R_5 R_2 b,\ T_3 b \\ &\qquad \longrightarrow (I + R_8 R_5)R_2 b + (S_7 + R_8 S_5)T_2 b \end{aligned} \tag{25}$$

and

$$\begin{aligned}&T_5 a + T_5 R_2 b + U_5 T_2 b + U_6 T_3 b, \\ &\quad a + R_2 b + S_7 T_2 b - R_8 R_5 a,\ U_7 T_2 b - T_8 R_5 a \longrightarrow b. \end{aligned} \tag{26}$$

Since the field has odd characteristic, we can let

$$a' = a + 2^{-1} R_2 b$$

and then rewrite (26) in the following form:

$$\begin{aligned}&T_5 a' + 2^{-1} T_5 R_2 b + U_5 T_2 b + U_6 T_3 b, \\ &(I - R_8 R_5)a' + 2^{-1}((I + R_8 R_5)R_2 b \\ &\qquad + (S_7 + R_8 S_5)T_2 b + (S_7 - R_8 S_5)T_2 b), \\ &\qquad U_7 T_2 b + 2^{-1} T_8 R_5 R_2 b - T_8 R_5 a' \longrightarrow b. \end{aligned} \tag{27}$$

Note that a' has k_a independent components and is independent of b, just like a is, because $a', b \longrightarrow a, b$.

The three vectors on the left-hand side of (26) have respective dimensions δ_c, k_a, and δ_a; these add up to $2n - k_c$. From these vectors we can compute all of b by (26), and then we can also reconstruct some information about a, namely $(I - R_8 R_5)a$ from the second of the three vectors and $T_8 R_5 a$ from the third vector. (We can also get $T_5 a$ from the first vector, but this will not be used below.) This gives a total of

$$k_b + \mathsf{rank}\left(\begin{bmatrix} I - R_8 R_5 \\ T_8 R_5 \end{bmatrix}\right)$$

independent components reconstructed from these three vectors, so we must have

$$k_b + \mathsf{rank}\left(\begin{bmatrix} I - R_8 R_5 \\ T_8 R_5 \end{bmatrix}\right) \le 2n - k_c. \tag{28}$$

Now, using (25), we see that

$$T_2 b, T_3 b, T_8 R_5 R_2 b \longrightarrow (I + R_8 R_5)R_2 b. \tag{29}$$

But we can add $(I + R_8 R_5)R_2 b$ and $(I - R_8 R_5)R_2 b$ to get $2R_2 b$, which yields $R_2 b$ because the field has odd characteristic. And (26) implies

$$a, T_2 b, T_3 b, R_2 b \longrightarrow a, b. \tag{30}$$

Putting these together, we get

$$a, T_2 b, T_3 b, \begin{bmatrix} I - R_8 R_5 \\ T_8 R_5 \end{bmatrix} R_2 b \longrightarrow a, b.$$

Now, using (28) and the known sizes of the vectors a, $T_2 b$, and $T_3 b$, we get the inequality

$$k_a + n - k_a + n - k_c + 2n - k_c - k_b \ge k_a + k_b,$$

which reduces to (22).

Using (25) and (27) together, we get

$$\begin{aligned} a',\quad T_2 b,\quad T_3 b,\quad T_8 R_5 R_2 b,\quad T_5 R_2 b, &\longrightarrow a', b \\ &\longrightarrow a, b, \end{aligned}$$

yielding the inequality

$$k_a + n - k_a + n - k_c + n - k_a + n - k_c \ge k_a + k_b,$$

which is (23).

For the remaining inequality (24), we will use the following fact: if M is a $k \times k$ matrix and N is an $r \times k$ matrix, then

$$\begin{aligned}\mathsf{rank}\left(\begin{bmatrix} M \\ N \end{bmatrix}\right) + \mathsf{rank}\left(\begin{bmatrix} M - I \\ N \end{bmatrix}\right) + \mathsf{rank}\left(\begin{bmatrix} M + I \\ N \end{bmatrix}\right) \\ \ge 2k + \mathsf{rank}(N). \end{aligned} \tag{31}$$

Since $1 \ne -1$ in a field of odd characteristic, (31) is a special case of:

Lemma 1: If M is a $k \times k$ matrix and N is an $r \times k$ matrix, and the scalars $\lambda_1, \ldots, \lambda_t$ are distinct, then

$$\sum_{i=1}^{t} \mathsf{rank}\left(\begin{bmatrix} M - \lambda_i I \\ N \end{bmatrix}\right) \ge (t-1)k + \mathsf{rank}(N). \tag{32}$$

We thank Nghi Nguyen for supplying the following clean proof of this result.

Proof: Let E_i be the null space of $M - \lambda_i I$, and let E be the null space of N. Then

$$\mathsf{rank}\left(\begin{bmatrix} M - \lambda_i I \\ N \end{bmatrix}\right) = k - \dim(E_i \cap E)$$

and

$$\mathsf{rank}(N) = k - \dim(E).$$

So (32) is equivalent to

$$tk - \sum_i \dim(E_i \cap E) \geq tk - \dim(E)$$

and hence to

$$\sum_i \dim(E_i \cap E) \leq \dim(E),$$

and the latter inequality is true because the subspaces $(E_i \cap E)$ are linearly independent in E. (If $\mathbf{v} \in E$ is the sum of vectors $\mathbf{v}_i \in E_i \cap E$ for $1 \leq i \leq t$, then we can recover the vectors $\mathbf{v}_i$ from $\mathbf{v}$ using formulas such as

$$(\lambda_1 - \lambda_2)\ldots(\lambda_1 - \lambda_t)\mathbf{v}_1 = (M - \lambda_2 I)\ldots(M - \lambda_t I)\mathbf{v}.)$$

■

Now, we have

$$\mathsf{rank}\left(\begin{bmatrix} R_8 R_5 - I \\ T_8 R_5 \end{bmatrix}\right) \leq 2n - k_c - k_b$$

from (28). Since

$$\begin{bmatrix} R_8 R_5 \\ T_8 R_5 \end{bmatrix} = \begin{bmatrix} R_8 \\ T_8 \end{bmatrix} R_5,$$

we have

$$\mathsf{rank}\left(\begin{bmatrix} R_8 R_5 \\ T_8 R_5 \end{bmatrix}\right) \leq \mathsf{rank}(R_5) \leq k_c.$$

Now, as stated in [6, p. 2756], we can find a matrix Q such that

$$\mathsf{rank}\left(\begin{bmatrix} I + R_8 R_5 \\ T_8 R_5 \\ Q \end{bmatrix}\right) = k_a \tag{33}$$

and

$$\mathsf{rank}(Q) = k_a - \mathsf{rank}\left(\begin{bmatrix} I + R_8 R_5 \\ T_8 R_5 \end{bmatrix}\right),$$

so

$$\mathsf{rank}\left(\begin{bmatrix} I + R_8 R_5 \\ T_8 R_5 \end{bmatrix}\right) = k_a - \mathsf{rank}(Q).$$

Substituting these facts into (31) gives

$$2n - k_c - k_b + k_c + k_a - \mathsf{rank}(Q) \geq 2k_a + \mathsf{rank}(T_8 R_5). \tag{34}$$

But (33) implies that

$$\begin{bmatrix} I + R_8 R_5 \\ T_8 R_5 \\ Q \end{bmatrix} R_2 b \longrightarrow R_2 b; \tag{35}$$

combining this with (29) and (30) yields

$$T_2 b,\ T_3 b,\ T_8 R_5 R_2 b,\ Q R_2 b \longrightarrow b.$$

Using this with the bound on $\mathsf{rank}(T_8 R_5)$ obtained from (34), we get

$$n - k_a + n - k_c + 2n - k_a - k_b - \mathsf{rank}(Q) + \mathsf{rank}(Q) \geq k_b,$$

which reduces to the desired inequality (24).

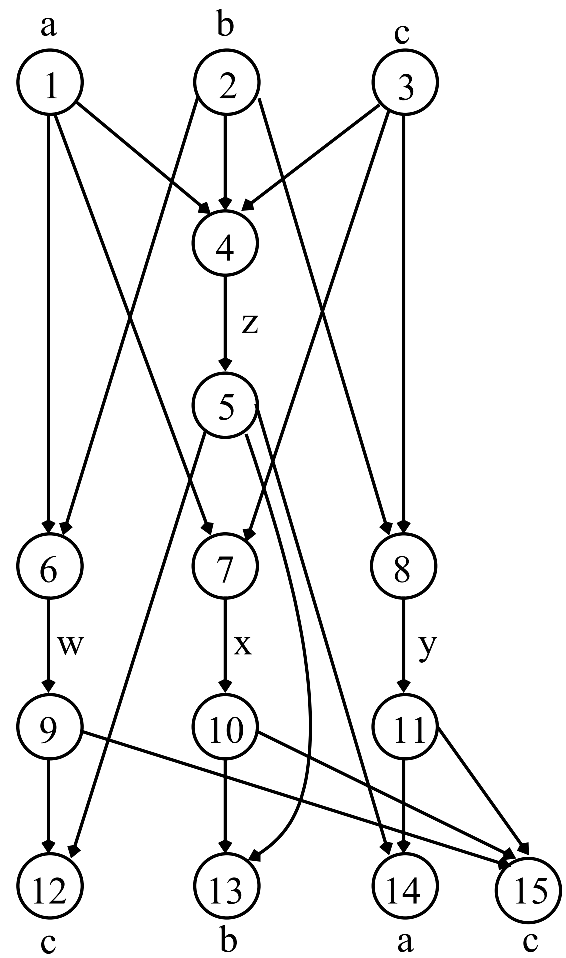

Fig. 6. The non-Fano network. Source nodes v_1, v_2, and v_3 generate messages a, b, and c, respectively. Receiver nodes v_{12}, v_{13}, v_{14}, and v_{15} demand messages c, b, a, and c, respectively. The symbol vectors carried on edges $e_{6,9}$, $e_{7,10}$, $e_{8,11}$, $e_{4,5}$ are labeled as w, x, y, and z, respectively.

V. Non-Fano Network

Theorem 6: The achievable rate region for either linear coding over any finite field alphabet of odd characteristic or non-linear coding are the same for the non-Fano network and are equal to the closed cube in $\mathbf{R}^3$ *whose faces lie on the* 6 *planes (see Figure 7):*

$$r_a = 0$$
$$r_b = 0$$
$$r_c = 0$$
$$r_a = 1$$
$$r_b = 1$$
$$r_c = 1$$

and whose vertices are the 8 *points:*

$$(0,0,0) \quad (0,0,1) \quad (1,0,0) \quad (0,1,0)$$
$$(0,1,1) \quad (1,0,1) \quad (1,1,0) \quad (1,1,1).$$

Proof: Consider a network solution over an alphabet $\mathcal{A}$ and denote the source message dimensions by k_a, k_b, and k_c, and the edge dimensions by n. Let each source be a random variable whose components are independent and uniformly

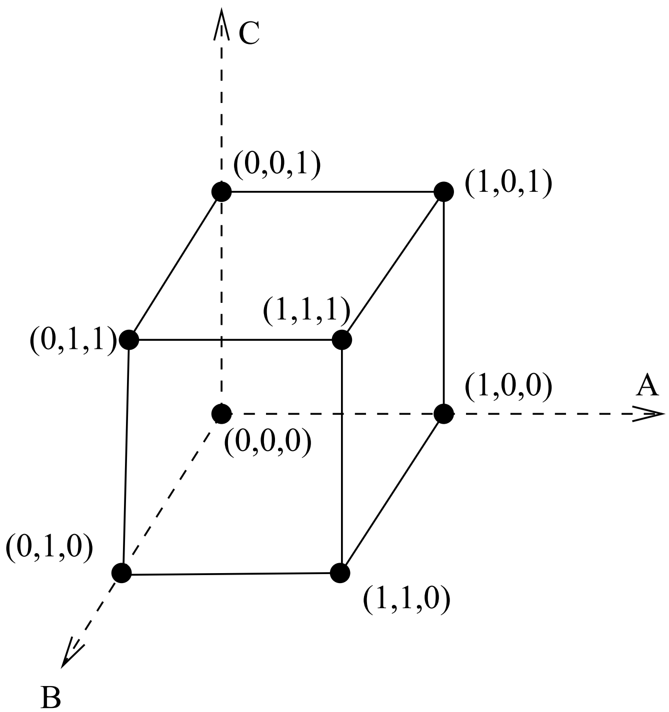

Fig. 7. The achievable coding rate region for the Fano network is a cube in $\mathbf{R}^3$.

distributed over $\mathcal{A}$. Then the solution must satisfy the following inequalities:

$$k_a \geq 0 \tag{36}$$
$$k_b \geq 0 \tag{37}$$
$$k_c \geq 0 \tag{38}$$
$$k_a = H(a) = H(z|b,c) \leq H(z) \leq n \tag{39}$$
$$k_b = H(b) = H(z|a,c) \leq H(z) \leq n \tag{40}$$
$$k_c = H(c) = H(z|a,b) \leq H(z) \leq n. \tag{41}$$

(36)–(38) are trivial; (39) follows because

$$z, b, c \longrightarrow z, y \longrightarrow a$$

(at node v_{14}), so $z,\ b,\ c \longrightarrow a,\ b,\ c$ and thus $H(a,b,c) = H(z,b,c)$. (40) follows because

$$z, a, c \longrightarrow z, x \longrightarrow b$$

(at node v_{13}), so $z,\ a,\ c \longrightarrow a,\ b,\ c$ and thus $H(a,b,c) = H(z,a,c)$. (41) follows because

$$z, a, b \longrightarrow z, w \longrightarrow c$$

(at node v_{12}), so $z, a, b \longrightarrow a, b, c$ and thus $H(a,b,c) = H(z,a,b)$. Dividing each inequality in (36)–(41) by n gives the 8 bounding planes stated in the theorem.

Let $r_a = k_a/n$, $r_b = k_b/n$, and $r_c = k_c/n$, and let $\mathcal{P}$ denote the polyhedron in $\mathbf{R}^3$ consisting of all 3-tuples (r_a, r_b, r_c) satisfying (36)–(41). Then $\mathcal{P}$ is simply the unit cube shown in Figure 7, and its extreme points are the 8 points stated in the theorem. To show that the 8 points lie in the achievable rate region, let $n = k_a = k_b = k_c = 1$ and use the following linear code for $(1, 1, 1)$ over any odd-characteristic finite field:

$$w = a + b, \quad y = b + c, \quad x = a + c, \quad z = a + b + c$$

where node v_{15} can recover its demand via

$$c = (w - y + x) \cdot 2^{-1}.$$

The other 7 points are obtained by setting certain messages to 0 in the code for $(1, 1, 1)$. Since the above codes are all linear, the achievable rate regions for linear and non-linear codes are the same. ■

Theorem 7: The achievable rate region for linear coding over any finite field alphabet of even characteristic for the non-Fano network is equal to the closed polyhedron in $\mathbf{R}^3$ *whose faces lie on the 7 planes (see Figure 8):*

$$\begin{aligned} r_a &= 0 \\ r_b &= 0 \\ r_c &= 0 \\ r_a &= 1 \\ r_b &= 1 \\ r_c &= 1 \\ r_a + r_b + r_c &= 5/2 \end{aligned}$$

and whose vertices are the 10 *points:*

$$\begin{array}{llll} (0,0,0) & (0,0,1) & (1,0,0) & (0,1,0) \\ (0,1,1) & (1,0,1) & (1,1,0) & \\ (1,1,1/2) & (1,1/2,1) & (1/2,1,1). & \end{array}$$

Proof: The six inequalities from Theorem 6 still apply here; the proof that the additional inequality

$$2k_a + 2k_b + 2k_c \leq 5n \tag{42}$$

must also hold in the case of even-characteristic finite fields is given in Section VI (and another proof is given in Section VIII-B).

The new inequality (42) cuts down the achievable rate region to the polyhedron shown in Figure 8, whose extreme points are the 10 points listed in the theorem. The point $(1, 1, 1/2)$ is achieved by the following code with $n = k_a = k_b = 2$ and $k_c = 1$, which works over any finite field:

$$\begin{aligned} w &= (a_1, b_1) \\ y &= (b_1 + c, b_2) \\ x &= (a_1 + c, a_2) \\ z &= (a_1 + b_1 + c, a_2 + b_2). \end{aligned}$$

The other two new extreme points are achieved by permuting the variables in the above code. ■

Note that both the uniform capacity and average capacity are $5/6$ for the non-Fano network, for any even-characteristic finite field.

Theorem 8: The achievable rate region for routing for the non-Fano network is the closed tetrahedron in $\mathbf{R}^3$ *whose faces*

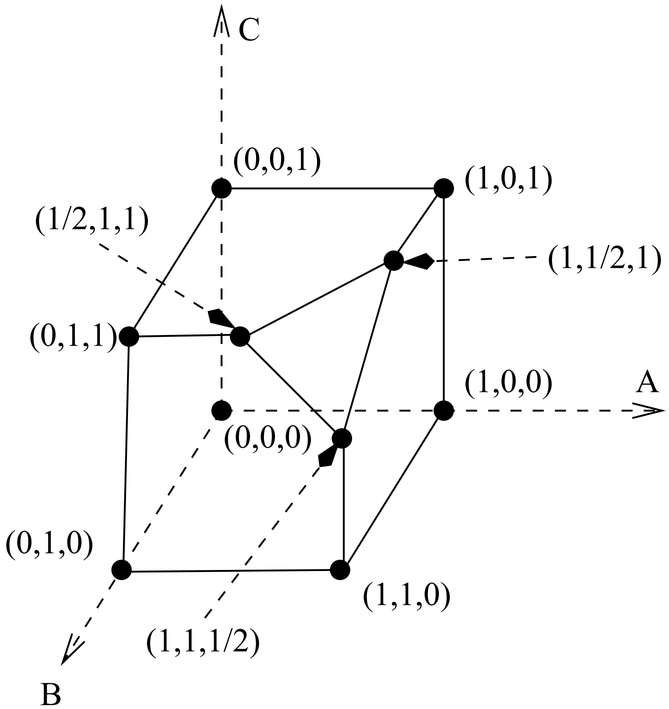

Fig. 8. The achievable linear coding rate region over even-characteristic finite fields for the non-Fano network is a 7-sided polyhedron with 10 vertices.

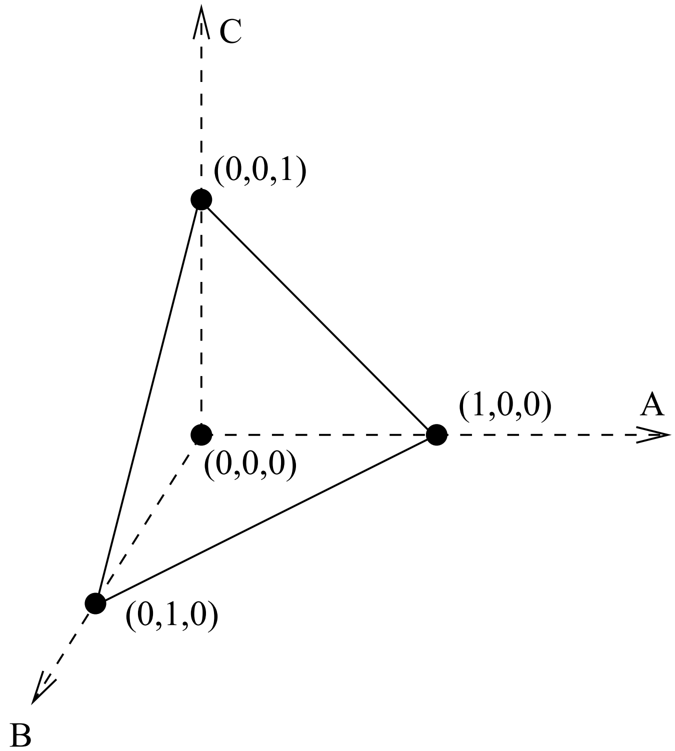

Fig. 9. The achievable routing rate region for the Fano network is a tetrahedron in $\mathbf{R}^3$.

lie on the 4 *planes (see Figure 9):*

$$r_a = 0$$
$$r_b = 0$$
$$r_c = 0$$
$$r_a + r_b + r_c = 1$$

and whose vertices are the 4 *points:*

$$(0, 0, 0),\ (0, 0, 1),\ (1, 0, 0),\ (0, 1, 0).$$

Proof: In addition to satisfying (36)–(41), a routing solution must also satisfy

$$k_a + k_b + k_c \le n \tag{43}$$

since the edge labeled z must carry all 3 messages a, b, and c. The inequality (43) makes the inequalities (39)–(41) redundant, and, in fact, the vertices of the polygon determined by (36)–(38) and (43) are the 4 listed in the theorem. These are achievable using the following routing codes:

$$(0, 0, 1):\quad y = z = c$$
$$(1, 0, 0):\quad z = a$$
$$(0, 1, 0):\quad z = b.$$

■

VI. Proof of Remaining Bound for the Non-Fano Network

For the case of linear coding over a finite field of characteristic 2, we want to prove the bound:

$$2k_a + 2k_b + 2k_c \le 5n \tag{44}$$

We will again do this by following the arguments from [6, Sec. IV], with minor modifications. (Those arguments were for a different network which was two copies of the non-Fano network with one demand node merged, but a number of them concentrated on just the left half of that network and hence will be directly applicable to the non-Fano network.) The ideas behind the proof are basically the same as in Section IV, although the specific linear algebra techniques that ended up being needed were somewhat different.

The matrices M_1 through M_{15} will be the same as they are in [6, pp. 2756–2757]; they label a part of the network there which is identical to the non-Fano network. Again here, instead of one value $\delta = n - k$ we have three values

$$\delta_a = n - k_a$$
$$\delta_b = n - k_b$$
$$\delta_c = n - k_c.$$

When we talk about thinking of an edge vector as one part of length k followed by one part of length $n - k$, we will use $k = k_c$ here; so, for instance, R_7 is a $k_c \times k_a$ matrix, while R_9 is $k_c \times k_c$.

Now follow the argument from [6, pp. 2756–2757] as written, except that L is just the five vectors

$$M_3a + M_4c,$$
$$M_5b + M_6c,$$
$$Q_{13}(M_7a + M_9c),$$
$$Q_{15}(M_8b + M_9c),$$
$$Q_{10}(M_1a + M_2b)$$

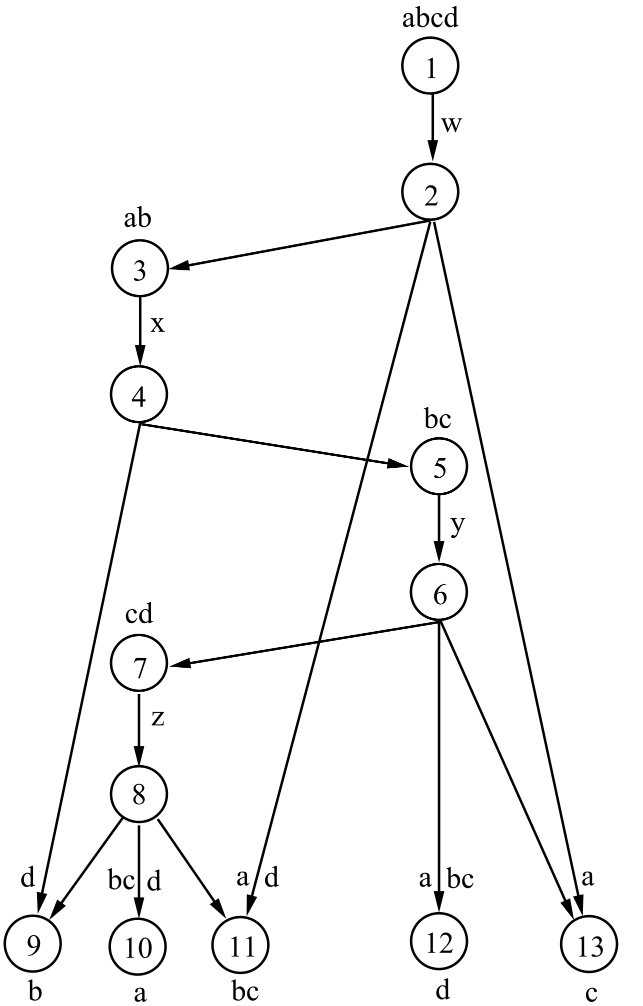

Fig. 10. The Vámos network. A message variable a, b, c, or d labeled above a node indicates an in-edge (not shown) from the source node (not shown) generating the message. Demand variables are labeled below the receivers v_9–v_{13} demanding them. The edges $e_{1,2}$, $e_{3,4}$, $e_{5,6}$, and $e_{7,8}$ are denoted by w, x, y, and z, respectively.

without any "corresponding five objects" from the other side. The same argument then yields $L \longrightarrow a, b, c$. Since $M_{15}M_7 = I_{k_a}$, we have $\mathsf{rank}(M_{15}) \geq k_a$ and hence $\mathsf{rank}(Q_{15}) \leq \delta_a$; similarly, $\mathsf{rank}(Q_{13}) \leq \delta_b$. Therefore, following the computation in [6, p. 2757], we find that L has only

$$n + n + [\delta_a + \delta_b - (k_c - \alpha)] + [n - \alpha] = 2n + \delta_a + \delta_b + \delta_c$$

independent entries. Therefore,

$$2n + \delta_a + \delta_b + \delta_c \geq k_a + k_b + k_c,$$

so

$$2k_a + 2k_b + 2k_c \leq 5n.$$

VII. Vámos Network

Theorem 9: The achievable rate region for routing for the Vámos network is the polytope in $\mathbf{R}^4$ whose faces lie on the 6 planes:

$$\begin{aligned} r_a &= 0 \\ r_b &= 0 \\ r_c &= 0 \\ r_d &= 0 \\ 2r_a + r_b + 2r_d &= 2 \\ r_a + r_b + r_c + 2r_d &= 2 \end{aligned}$$

and whose vertices are the points

$$\begin{array}{ccc} (0,0,0,0) & (1,0,0,0) & (0,0,0,1) \\ (1,0,1,0) & (0,2,0,0) & (0,0,2,0) \end{array}$$

Proof: The first 4 planes are trivial.

Now, notice that in a routing solution, y must carry all of a and d in order to meet the demands at nodes v_{10} and v_{12}, respectively. Thus, x must carry all of a and d too. Also, x and y together must carry all of b in order to meet the demand at node v_9. In summary, x and y together must carry at least 2 copies of a, 2 copies of d, and one copy of b. This implies

$$2k_a + k_b + 2k_d \leq 2n$$

and therefore

$$2r_a + r_b + 2r_d \leq 2.$$

Similarly, w must carry all of d in order to meet the demand at node v_{12}, and w and y together must carry all of b and c in order to meet the demands at nodes v_{11} and v_{13}. Since y must carry all of a and d, we conclude that w and y together must carry at least one copy of a, one copy of b, one copy of c, and two copies of d. This implies

$$k_a + k_b + k_c + 2k_d \leq 2n$$

and therefore

$$r_a + r_b + r_c + 2r_d \leq 2.$$

It is easy to check that the vertices of the polytope bounded by the 6 planes listed in the theorem are the 6 vertices listed in the theorem. Each of the 6 vertices can be achieved as follows:

(0000) trivially;
(1000) with $x = y = z = a$;
(0001) with $w = x = y = z = d$;
(1010) with $w = c$ and $x = y = z = a$;
(0200) with $w = x = b_1$ and $y = z = b_2$;
(0020) with $w = x = c_1$ and $y = z = c_2$.

■

The following theorem uses only Shannon-type information inequalities to obtain a polytopal outer bound in $\mathbf{R}^4$ to the achievable rate region.

Theorem 10: The achievable rate region for the Vámos network lies inside the polytope in $\mathbf{R}^4$ whose faces lie on *the* 9 *planes:*

$$
\begin{aligned}
r_a &= 0\\
r_b &= 0\\
r_c &= 0\\
r_d &= 0\\
r_a &= 1\\
r_d &= 1\\
r_b + r_c &= 2\\
r_a + r_b &= 2\\
r_c + r_d &= 2
\end{aligned}
$$

and whose vertices are the points:

$$
\begin{array}{cccc}
(0,2,0,1) & (0,2,0,0) & (1,1,1,0) & (1,1,0,0)\\
(1,1,0,1) & (1,0,0,1) & (0,0,0,1) & (0,0,0,0)\\
(1,0,0,0) & (1,0,1,1) & (0,0,1,1) & (0,1,1,1)\\
(1,0,2,0) & (0,0,2,0) & (1,1,1,1). &
\end{array}
$$

Proof: Consider a network solution over an alphabet $\mathcal{A}$ and denote the source message dimensions by k_a, k_b, k_c, and k_d, and the edge dimensions by n. Let each source be a random variable whose components are independent and uniformly distributed over $\mathcal{A}$. Then the solution must satisfy the following inequalities:

$$k_a \geq 0 \tag{45}$$
$$k_b \geq 0 \tag{46}$$
$$k_c \geq 0 \tag{47}$$
$$k_d \geq 0 \tag{48}$$
$$k_a = H(a) \leq H(z|b,c,d) \leq n \tag{49}$$
$$k_d = H(d) \leq H(y|a,b,c) \leq n \tag{50}$$
$$\begin{aligned} k_b + k_c &= H(b,c) \leq H(w,z|a,d)\\ &\leq H(w,z) \leq 2n \end{aligned} \tag{51}$$
$$\begin{aligned} k_a + k_b &= H(a,b) \leq H(x,z|c,d)\\ &\leq H(y,z) \leq 2n \end{aligned} \tag{52}$$
$$\begin{aligned} k_c + k_d &= H(c,d) \leq H(w,y|a,b)\\ &\leq H(w,y) \leq 2n. \end{aligned} \tag{53}$$

(45)–(48) are trivial; (49) follows because $b,c,d,z \longrightarrow a$; (50) follows because $a,b,c,y \longrightarrow d$; (51) follows because $a,d,w,z \longrightarrow b,c$; (52) follows because $x,z,c,d \longrightarrow a,b$; (53) follows because $w,y,a,b \longrightarrow c,d$; Dividing each inequality in (45)–(53) by n gives the 9 bounding hyperplanes stated in the theorem.

Let

$$
\begin{aligned}
r_a &= k_a/n\\
r_b &= k_b/n\\
r_c &= k_c/n\\
r_d &= k_d/n
\end{aligned}
$$

and let $\mathcal{P}$ denote the polytope in $\mathbf{R}^4$ consisting of all 4-tuples (r_a, r_b, r_c, r_d) satisfying (1)–(9). Then (45)–(48) and (52)–(53) ensure that $\mathcal{P}$ is bounded. One can easily calculate that each point in $\mathbf{R}^4$ that satisfies some independent set of four of the inequalities (45)–(53) with equality and also satisfies the remaining five inequalities must be one of the 15 points stated in the theorem. ■

For further bounds, we use the following result from [10]:

Suppose that A, B, C, and D are random variables and we have an information inequality of the form

$$
\begin{aligned}
a_1 I(A;B) \leq{}& a_2 I(A;B|C) + a_3 I(A;C|B) + a_4 I(B;C|A)\\
&+ a_5 I(A;B|D) + a_6 I(A;D|B) + a_7 I(B;D|A)\\
&+ a_8 I(C;D) + a_9 I(C;D|A) + a_{10} I(C;D|B).
\end{aligned} \tag{54}
$$

Then we get the following bound on the Vámos message and edge entropies:

$$
\begin{aligned}
&(a_2 + a_3 + a_4)H(a) + (a_2 + a_3 + a_8 + a_9 + a_{10})H(b)\\
&\quad + (a_5 + a_7 + a_8 + a_9 + a_{10})H(c)\\
&\quad + (a_5 + a_6 + a_7)H(d)\\
&\quad + (a_2 - a_1 - a_7)I(c;y)\\
&\quad + (a_4 + a_7 - a_{10})I(b;x)\\
&\leq (a_5 + a_6 + a_7 + a_8 + a_9 + a_{10})H(w)\\
&\quad + (a_2 + a_3 + a_4 + a_7)H(x)\\
&\quad + (-a_1 + a_2 + a_5 + a_9)H(y)\\
&\quad + (a_3 + a_8 + a_{10})H(z).
\end{aligned} \tag{55}
$$

And by the same argument, if (54) is a linear rank inequality (for a particular characteristic), then (55) holds for any linear (for that characteristic) fractional code for the Vámos network.

If the inequalities

$$
\begin{aligned}
a_2 &\geq a_1 + a_7\\
a_4 + a_7 &\geq a_{10}
\end{aligned} \tag{56}
$$

are satisfied, then the inequality (55) directly leads to a Vámos achievable rate region bound, by neglecting the (nonnegative) terms involving $I(c;y)$ and $I(b;x)$. Specifically, in this case, by substituting

$$
\begin{aligned}
H(a) &= k_a\\
H(b) &= k_b\\
H(c) &= k_c\\
H(d) &= k_d\\
H(w) &= H(x) = H(y) = H(z) = n
\end{aligned}
$$

into (55), we obtain

$$
\begin{aligned}
&k_a(a_2 + a_3 + a_4) + k_b(a_2 + a_3 + a_8 + a_9 + a_{10})\\
&\quad + k_c(a_5 + a_7 + a_8 + a_9 + a_{10})\\
&\quad + k_d(a_5 + a_6 + a_7)\\
&\leq n(-a_1 + 2a_2 + 2a_3 + a_4 + 2a_5\\
&\quad + a_6 + 2a_7 + 2a_8 + 2a_9 + 2a_{10}).
\end{aligned} \tag{57}
$$

Theorem 11: The achievable rate region for linear coding over any finite field alphabet for the Vámos network is the polytope in $\mathbf{R}^4$ *whose faces lie on the* 10 *planes:*

$$\begin{aligned} r_a &= 0 \\ r_b &= 0 \\ r_c &= 0 \\ r_d &= 0 \\ r_a &= 1 \\ r_d &= 1 \\ r_b + r_c &= 2 \\ r_a + r_b &= 2 \\ r_c + r_d &= 2 \\ r_a + 2r_b + 2r_c + r_d &= 5 \end{aligned}$$

and whose vertices are the points

$$\begin{array}{llll} (0,0,2,0) & (0,0,1,1) & (1,0,1,1) & (1,0,0,0) \\ (0,0,0,0) & (0,0,0,1) & (1,0,0,1) & (1,1,0,1) \\ (1,1,0,0) & (0,2,0,0) & (1,1,1/2,1) & (1,1/2,1,1) \\ (0,2,0,1) & (1,1,1,0) & (0,1,1,1) & (1,0,2,0). \end{array}$$

Proof: The first nine bounding planes come from Theorem 10. The tenth bounding plane is shown by letting (54) be the Ingleton inequality [14], which can be written in the form

$$I(A;B) \le I(A;B|C) + I(A;B|D) + I(C;D)$$

and which is a linear rank inequality for all characteristics, to get the Vámos linear rate region bound

$$H(a) + 2H(b) + 2H(c) + H(d) \le 2H(w) + H(x) + H(y) + H(z)$$

from (55).

The proof that the extreme points of the polytope bounded by these planes are the 16 points listed above is left as an exercise for the reader's computer (we used `cddlib` [11]).

Here are linear codes over an arbitrary field) achieving six of the extreme points:

$$\begin{aligned} (1,1,1,0):\quad & n = 1, \\ & w = a + c \\ & x = a \\ & y = z = a + b \\ (0,1,1,1):\quad & n = 1, \\ & w = x = b + d \\ & y = b + c + d \\ & z = c \\ (1,0,2,0):\quad & n = 1, \\ & w = c_1 \\ & x = a \\ & y = z = a + c_2 \\ (0,2,0,1):\quad & n = 1, \\ & w = x = b_1 + d \\ & y = z = b_2 + d \\ (1,1,1/2,1):\quad & n = 2, \\ & w = (b_2 + d_1, c + d_2) \\ & x = (a_1 + d_1, a_2 + b_2 + c + d_2) \\ & y = (a_1 + b_1 + d_1, a_2 + d_2) \\ & z = (a_1 + b_1, a_2 + c) \\ (1,1/2,1,1):\quad & n = 2, \\ & w = (c_1 + d_1, b + d_2) \\ & x = (a_1 + c_1 + d_1, a_2 + d_2) \\ & y = (a_1 + d_1, a_2 + b + c_2 + d_2) \\ & z = (a_1 + c_2, a_2 + b) \end{aligned}$$

The remaining 10 points are achieved by fixing certain messages to be 0. ■

The following theorem uses the non-Shannon-type Zhang-Yeung information inequality to obtain an additional outer bound in $\mathbf{R}^4$ to the achievable rate region.

Theorem 12: The achievable rate region for non-linear coding for the Vámos network is bounded by the inequalities:

$$4r_a + 4r_b + 2r_c + r_d \le 10 \quad (58)$$
$$2r_a + 2r_b + 4r_c + 4r_d \le 11 \quad (59)$$
$$r_a + 2r_b + 4r_c + 5r_d \le 11 \quad (60)$$
$$5r_a + 6r_b + 6r_c + 5r_d \le 20. \quad (61)$$

Proof: If we let (54) be the Zhang-Yeung inequality [23], which can be written in the form

$$I(A;B) \le 2I(A;B|C) + I(A;C|B) + I(B;C|A) + I(A;B|D) + I(C;D), \quad (62)$$

then we get the Vámos network bound

$$4H(a) + 4H(b) + 2H(c) + H(d) + I(c;y) \le 2H(w) + 4H(x) + 2H(y) + 2H(z) \quad (63)$$

from (55). This immediately gives the inequality (58) (we can simply discard the $I(c;y)$ term).

Also, we can let (54) be (62) with variables C and D interchanged; then the result from (55) is

$$H(a) + 2H(b) + 4H(c) + 4H(d) - I(c;y) + I(b;y) \le 5H(w) + 2H(x) + 2H(y) + H(z). \quad (64)$$

This does not directly give a rate region bound, because the term $-I(c;y)$ cannot be simply discarded. However, if we add (63) and (64), we get an inequality that yields (61); if we add to (64) the inequality

$$H(a) + I(c;y) \le H(y)$$

(which, as noted in [10], holds in the Vámos network because $b, c, d, y \longrightarrow a$), we get (59); and if we add to (64) the inequality

$$H(d) + I(c;y) \le H(y)$$

(which, as noted in [10], holds in the Vámos network because $a, b, c, y \longrightarrow d$), we get (60). ■

Many additional non-Shannon-type information inequalities are given in [10]. These can be used as above to give additional bounds on the achievable rate region for non-linear coding for the Vámos network. In fact, the inequalities from [10] using at most four copy variables with at most three copy steps yield 158 independent constraints on this achievable rate region. (Note: inequalities (58)–(61) are superseded by these new inequalities.) One of these is used in [10] to show that the uniform coding capacity of the Vámos network is at most $19/21$.

Since there are infinitely many information inequalities on four random variables [18], it is quite possible that the achievable rate region for non-linear coding for the Vámos network is not a polytope. On the other hand, this rate region could be quite simple; to date, no fractional solution is known for the Vámos network which lies outside the achievable rate region for linear coding.

VIII. New Linear Rank Inequalities From Networks

We now give a new method for producing bounds on achievable rate regions for linear coding. Unlike the previous method using matrix algebra, this method actually produces explicit linear rank inequalities (perhaps only true for some characteristics) which directly imply the bounds in question. However, it is not clear yet that this new method can produce all results obtained from the matrix algebra method. We will use the method to prove one of the three bounds needed for the Fano network, and a weaker version of the bound needed for the non-Fano network; we hope to find further refinements of the method later which will yield all four of these bounds.

In particular, we produce an explicit linear rank inequality valid only for odd-characteristic fields, and another linear rank inequality valid only for even-characteristic fields. Such inequalities have also been produced by Blasiak, Kleinberg, and Lubetzky [3] (also by use of the Fano and non-Fano matroids), but those inequalities do not directly give bounds for the networks here.

Unlike the matrix computation method, which concentrates on the matrices specifying how information moves forward through the network, the new method concentrates on inverse functions specifying how the information on each edge was produced from the information on its predecessor edges. (One can think of the edge as carrying some linear functions of the original message components; then the information on this edge can be thought of as the vector space spanned by these functions, as a subspace of the space of all linear functions of the message components.) If the network conditions are satisfied, then the information can be traced back from the receiver node to the source nodes using these functions; one will be able to give arguments that some of these functions are invertible, just as one gave arguments that some of the matrices were invertible or full-rank. But now we will go farther, by saying that even if the network conditions do not quite hold, the reasoning about invertibility of the functions will still work on a subspace of the domain of the functions; the extent to which the reasoning does not work (i.e., the codimension of this subspace) is the same as the extent to which the network condition fails (which can also be measured in terms of dimensions of subspaces). The result will be that we can produce an unconditional (but perhaps dependent on characteristic) linear rank inequality which, in combination with the network conditions, will directly imply the desired rate region bound.

We start by giving some basic results in linear algebra.

If A is a subspace of a finite-dimensional vector space V, then we denote the codimension of A in V by

$$\mathsf{codim}_V(A) = \mathsf{dim}(V) - \mathsf{dim}(A).$$

Linear rank inequalities are closely related to information inequalities. In fact, in order to describe linear rank inequalities we will borrow notation from information theory to use in the context of linear algebra in the following manner.

Suppose A and B are subspaces of a given vector space V, and let $\langle A, B\rangle$ denote the span of $A \cup B$. We will let $H(A)$ denote the rank of A, and let $H(A, B)$ denote the rank of $\langle A, B\rangle$. The meaning of conditional entropy notation with subspace dimensions then follows from

$$H(A|B) = H(A, B) - H(B)$$

that is, $H(A|B)$ denotes the excess rank of subspace A over that of subspace $A \cap B$, or equivalently, the codimension of $A \cap B$ in A. Similarly, the mutual information

$$I(A; B) = H(A) - H(A|B)$$

when applied to subspaces A and B, gives the dimension of the intersection $A \cap B$.

Lemma 2: For any subspaces $A_1, \dots, A_m$ of finite-dimensional vector space V,

$$\mathsf{codim}_V\left(\bigcap_{i=1}^{m} A_i\right) \le \sum_{i=1}^{m} \mathsf{codim}_V(A_i).$$

Lemma 3: Let A and B be finite-dimensional vector spaces, let $f : A \to B$ be a linear function, and let B' be a subspace of B. Then

$$\mathsf{codim}_A\left(f^{-1}(B')\right) \le \mathsf{codim}_B\left(B'\right).$$

Proof: Let $S = f^{-1}(B')$ and let T be a subspace of A such that $S + T = A$ and $S \cap T = \{0\}$. Let $g : T \to B$ be a linear function such that $g = f$ on T. Then we have

$$\begin{aligned} &\mathsf{codim}_A(S) \\ &= \mathsf{dim}(T) && [\text{from } S + T = A \text{ and } S \cap T = \{0\}] \\ &= \mathsf{dim}(g(T)) + \mathsf{nullity}(g) \\ &= \mathsf{dim}(g(T)) && [\text{from } g^{-1}(\{0\}) = \{0\}] \\ &\le \mathsf{codim}_B\left(B'\right). && [\text{from } B' \cap g(T) = \{0\}] \end{aligned}$$

■

Lemma 4: Let $A_1, \dots, A_k, B$ be subspaces of a finite-dimensional vector space V. There exist linear functions $f_i : B \to A_i$ (for $i = 1, \dots, k$) such that $f_1 + \cdots + f_k = I$ on a subspace of B of codimension $H(B|A_1, \dots, A_k)$ in B.

Proof: The subspace is

$$W = (A_1 + \cdots + A_k) \cap B.$$

For each w_j in a basis for W, choose $x_{i,j} \in A_i$ for $i = 1, \ldots, k$ such that

$$w_j = x_{1,j} + \cdots + x_{k,j}.$$

Define linear maps $g_i : W \to A_i$ for $i = 1, \ldots, k$ so that $g_i(w_j) = x_{i,j}$ for all i and j; then extend each g_i arbitrarily to a linear map $f_i : B \to A_i$. We have

$$\begin{aligned} H(B|A_1, \ldots, A_k) &= \mathrm{dim}(B) - \mathrm{dim}(B \cap (A_1 + \cdots + A_k)) \\ &= \mathrm{dim}(B) - \mathrm{dim}(W). \end{aligned}$$

■

Lemma 5: Let A, B, C be subspaces of a finite-dimensional vector space V, and let $f : A \to B$ and $g : A \to C$ be linear functions such that $f + g = 0$ on A. Then $f = g = 0$ on a subspace of A of codimension at most $I(B; C)$ in A.

Proof: For all $u \in A$, $g(u) \in B$ so $f(u) = -g(u) \in B$ and therefore f maps A into $B \cap C$. Thus,

$$\mathrm{dim}(A) - \mathrm{nullity}(f) = \mathrm{rank}(f) \le \mathrm{dim}(B \cap C) = I(B; C)$$

so the kernel of f has codimension at most $I(B; C)$ in A. ■

Lemma 6: Let $A, B_1, \ldots, B_k$ be subspaces of a finite-dimensional vector space V, and let $f_i : A \to B_i$ be linear functions such that $f_1 + \cdots + f_k = 0$ on A. Then $f_1 = \cdots = f_k = 0$ on a subspace of A of codimension at most

$$H(B_1) + \cdots + H(B_k) - H(B_1, \ldots, B_k)$$

in A.

Proof: Use induction on k. The claim is trivially true for $k = 1$, and is true for $k = 2$ by Lemma 5. Let us assume it is true up to $k - 1$ for $k \ge 3$. Apply Lemma 5 with

$$\begin{aligned} B &= B_k \\ C &= B_1 + \cdots + B_{k-1} \\ f &= f_k \\ g &= f_1 + \cdots + f_{k-1} \end{aligned}$$

to get $f_1 + \cdots + f_{k-1} = f_k = 0$ on a subspace S of A satisfying

$$\mathrm{codim}_A(S) \le H(B_1, \ldots, B_{k-1}) + H(B_k) - H(B_1, \ldots, B_k).$$

By the induction hypothesis, $f_1 = \cdots = f_{k-1} = 0$ on a subspace S' of S satisfying

$$\mathrm{codim}_S(S') \le H(B_1) + \cdots + H(B_{k-1}) - H(B_1, \ldots, B_{k-1}).$$

Adding these two inequalities gives us the desired result for subspace S'. ■

A. A Linear Rank Inequality From the Fano Network

Theorem 13: Let A, B, C, D, W, X, Y, Z be subspaces of a finite-dimensional vector space V over a scalar field of odd characteristic. Then, the following linear rank inequality holds:

$$\begin{aligned} 2H(A) &+ H(B) + 2H(C) \\ &\le H(W) + H(X) + H(Y) + H(Z) \\ &\quad + 2H(A|Z, Y) + H(B|X, Z) + 2H(C|A, X) \\ &\quad + 3H(X|W, Y) + 3H(Z|W, C) \\ &\quad + 5H(W|A, B) + 5H(Y|B, C) \\ &\quad + 5(H(A) + H(B) + H(C) - H(A, B, C)). \qquad (65) \end{aligned}$$

Proof: See the Appendix. ■

In the context of the Fano network, all of the compound terms at the end of inequality (65) are zero, so this inequality directly implies inequality (19).

By replacing W with $W \cap (A + B + C + X + Y + Z)$ and similarly for X, Y, and Z, one can improve the inequality to a balanced form where $H(W)$ becomes $I(W; A, B, C, X, Y, Z)$, $H(W|A, B)$ becomes $I(W; C, X, Y, Z|A, B)$, and similarly for X, Y, and Z.

Theorem 14: The linear rank inequality in Theorem 13 holds for any scalar field if $\mathrm{dim}(V) \le 2$, but may not hold if the scalar field has characteristic 2 and $\mathrm{dim}(V) \ge 3$.

Proof: See the Appendix. ■

B. A Linear Rank Inequality From the Non-Fano Network

Theorem 15: Let A, B, C, W, X, Y, Z be subspaces of a finite-dimensional vector space V over a scalar field of even characteristic. Then, the following linear rank inequality holds:

$$\begin{aligned} 2H(A) &+ 3H(B) + 2H(C) \\ &\le H(W) + H(X) + H(Y) + 3H(Z) \\ &\quad + 2H(A|Y, Z) + 3H(B|X, Z) + H(C|W, Z) \\ &\quad + 2H(W|A, B) + 4H(X|A, C) + 3H(Y|B, C) \\ &\quad + 6H(Z|A, B, C) + H(C|W, X, Y) \\ &\quad + 7(H(A) + H(B) + H(C) - H(A, B, C)). \qquad (66) \end{aligned}$$

Proof: See the Appendix. ■

In the context of the non-Fano network, all of the compound terms at the end of inequality (66) are zero, so this inequality directly implies the inequality

$$2k_a + 3k_b + 2k_c \le 6n, \qquad (67)$$

which is a weaker version of inequality (42).

Theorem 16: The linear rank inequality in Theorem 15 holds for any scalar field if $\mathrm{dim}(V) \le 2$, but may not hold if the scalar field has odd characteristic and $\mathrm{dim}(V) \ge 3$.

Proof: In $V = GF(p)^3$ for any odd prime p, define the following subspaces of V:

$$A = \langle(1, 0, 0)\rangle$$
$$B = \langle(0, 1, 0)\rangle$$
$$C = \langle(0, 0, 1)\rangle$$
$$W = \langle(1, 1, 0)\rangle$$
$$X = \langle(1, 0, 1)\rangle$$
$$Y = \langle(0, 1, 1)\rangle$$
$$Z = \langle(1, 1, 1)\rangle.$$

It is easily verified that the inequality in Theorem 15 is not satisfied in this case.

To show that the inequality indeed holds if $\mathsf{dim}(V) \le 2$, one can again show that the inequality becomes a Shannon inequality under the assumption that $H(A) = 0$, or under the assumption $H(B|A) = 0$, or under the assumption $H(C|A, B) = 0$. If all three of these assumptions fail, then we must have

$$\mathsf{dim}(V) \ge H(A, B, C) > H(A, B) > H(A) > 0 \tag{68}$$

and hence $\mathsf{dim}(V) \ge 3$. Or one can give a case-by-case direct argument. ∎

IX. Conclusion

We have determined the exact complete achievable (routing, linear, and non-linear) rate regions for the Generalized Butterfly, Fano, and non-Fano networks, as well as the routing and linear rate regions for the Vámos network. Bounds are given for the non-linear rate region for the Vámos network. A new method was presented using linear rank inequalities to obtain rate region bounds.

Both the older method using matrix computations and the new method using inverse functions are, as yet, incomplete methods for determining linear achievable rate regions. For the example networks given here, the matrix computation method eventually yielded a full solution, but new ideas needed to be found for each new network, and it is not clear that the method will succeed in all cases. The inverse function method has not yet reached even that level of development; it needs further refinements simply to duplicate the results from the matrix method. And presently the solution-finding phase (verifying that the corners of the current putative achievable rate region are indeed achievable) is largely a trial-and-error process, although guided by properties deduced during the proof of the currently-known bounding planes. So there is substantial further work to be done in order to make these methods automatically applicable to more general networks.

Appendix

Proof of Theorem 13: We will use the Fano network in Figure 2, derived in [8], from the Fano matroid, to help guide the proof. By Lemma 4, there exist linear functions

$$\begin{array}{ll} f_1 : W \to A & f_2 : W \to B \\ f_3 : Y \to B & f_4 : Y \to C \\ f_5 : X \to W & f_6 : X \to Y \\ f_7 : Z \to W & f_8 : Z \to C \\ f_9 : C \to A & f_{10} : C \to X \\ f_{11} : B \to X & f_{12} : B \to Z \\ f_{13} : A \to Z & f_{14} : A \to Y \end{array}$$

such that

$$f_1 + f_2 = I \text{ on a subspace } W' \text{ of } W \text{ with } \mathsf{codim}_W(W') \le H(W|A, B) \tag{A.1}$$
$$f_3 + f_4 = I \text{ on a subspace } Y' \text{ of } Y \text{ with } \mathsf{codim}_Y(Y') \le H(Y|B, C) \tag{A.2}$$
$$f_5 + f_6 = I \text{ on a subspace } X' \text{ of } X \text{ with } \mathsf{codim}_X(X') \le H(X|W, Y)$$
$$f_7 + f_8 = I \text{ on a subspace } Z' \text{ of } Z \text{ with } \mathsf{codim}_Z(Z') \le H(Z|W, C) \tag{A.3}$$
$$f_9 + f_{10} = I \text{ on a subspace } C' \text{ of } C \text{ with } \mathsf{codim}_C(C') \le H(C|A, X)$$
$$f_{11} + f_{12} = I \text{ on a subspace } B' \text{ of } B \text{ with } \mathsf{codim}_B(B') \le H(B|X, Z)$$
$$f_{13} + f_{14} = I \text{ on a subspace } A' \text{ of } A \text{ with } \mathsf{codim}_A(A') \le H(A|Z, Y). \tag{A.4}$$

Combining these, we get maps

$$f_1 f_7 f_{13} : A \to A \tag{A.5}$$
$$f_2 f_7 f_{13} + f_3 f_{14} : A \to B \tag{A.6}$$
$$f_8 f_{13} + f_4 f_{14} : A \to C. \tag{A.7}$$

Note that

$$f_1 f_7 f_{13} + f_2 f_7 f_{13} = f_7 f_{13} \quad \text{on the subspace } f_{13}^{-1} f_7^{-1}(W') \text{ of } A$$
$$f_7 f_{13} + f_8 f_{13} = f_{13} \quad \text{on the subspace } f_{13}^{-1}(Z') \text{ of } A$$
$$f_3 f_{14} + f_4 f_{14} = f_{14} \quad \text{on the subspace } f_{14}^{-1}(Y') \text{ of } A$$

so the sum of the functions in (A.5)–(A.7) is equal to I on the subspace

$$A'' \doteq A' \cap f_{13}^{-1}(Z') \cap f_{13}^{-1} f_7^{-1}(W') \cap f_{14}^{-1}(Y')$$

and we get

$$\begin{aligned} &\mathsf{codim}_A(A'') \\ &\le \mathsf{codim}_A(A') + \mathsf{codim}_A\left(f_{13}^{-1}(Z')\right) \\ &\quad + \mathsf{codim}_A\left(f_{13}^{-1} f_7^{-1}(W')\right) + \mathsf{codim}_A\left(f_{14}^{-1}(Y')\right) \\ &\hspace{6cm} \text{[from Lemma 2]} \\ &\le \mathsf{codim}_A(A') + \mathsf{codim}_Z(Z') + \mathsf{codim}_W(W') + \mathsf{codim}_Y(Y') \\ &\hspace{6cm} \text{[from Lemma 3]} \\ &\le H(A|Z, Y) + H(Z|W, C) + H(W|A, B) + H(Y|B, C) \\ &\hspace{4cm} \text{[from (A.1), (A.2), (A.3), (A.4)].} \end{aligned}$$

Applying Lemma 6 to

$$f_1 f_7 f_{13} - I$$
$$f_2 f_7 f_{13} + f_3 f_{14}$$
$$f_8 f_{13} + f_4 f_{14}$$

we get a subspace $\bar{A}$ of A'' such that

$$\begin{aligned} &\mathrm{codim}_A(\bar{A}) \\ &= \mathrm{codim}_A(A'') + \mathrm{codim}_{A''}(\bar{A}) \le \Delta_A && \text{(A.8)} \\ &\doteq H(A|Z,Y) + H(Z|W,C) + H(W|A,B) + H(Y|B,C) \\ &\quad + H(A) + H(B) + H(C) - H(A,B,C) && \text{(A.9)} \end{aligned}$$

on which

$$\begin{aligned} f_1 f_7 f_{13} &= I && \text{(A.10)} \\ f_2 f_7 f_{13} + f_3 f_{14} &= 0 \\ f_8 f_{13} + f_4 f_{14} &= 0. \end{aligned}$$

Similarly, we get a subspace $\bar{C}$ of C such that

$$\begin{aligned} &\mathrm{codim}_C(\bar{C}) \\ &\le \Delta_C && \text{(A.11)} \\ &\doteq H(C|A,X) + H(X|W,Y) + H(W|A,B) + H(Y|B,C) \\ &\quad + H(A) + H(B) + H(C) - H(A,B,C) && \text{(A.12)} \end{aligned}$$

on which

$$\begin{aligned} f_4 f_6 f_{10} &= I && \text{(A.13)} \\ f_2 f_5 f_{10} + f_3 f_6 f_{10} &= 0 \\ f_9 + f_1 f_5 f_{10} &= 0 \end{aligned}$$

and a subspace $\bar{B}$ of B such that

$$\begin{aligned} &\mathrm{codim}_B(\bar{B}) \\ &\le \Delta_B && \text{(A.14)} \\ &\doteq H(B|X,Z) + H(X|W,Y) + H(Z|W,C) + H(W|A,B) \\ &\quad + H(Y|B,C) + H(A) + H(B) + H(C) - H(A,B,C) \\ &&& \text{(A.15)} \end{aligned}$$

on which

$$\begin{aligned} f_2 f_5 f_{11} + f_2 f_7 f_{12} + f_3 f_6 f_{11} &= I \\ f_1 f_5 f_{11} + f_1 f_7 f_{12} &= 0 \\ f_4 f_6 f_{11} + f_8 + f_{12} &= 0. \end{aligned}$$

Note: There is only one $H(W|A,B)$ in (A.15) because we can write

$$f_i f_5 f_{11} + f_i f_7 f_{12} = f_i(f_5 f_{11} + f_7 f_{12})$$

for $i = 1, 2$.

Let us define the following subspaces of B:

$$\begin{aligned} S_1 &= \{u \in B : f_{11} u \in f_{10}\bar{C}\} \\ S_2 &= \{u \in B : f_{12} u \in f_{13}\bar{A}\} \\ S_3 &= \{u \in B : f_5 f_{11} u \in f_7 f_{13}\bar{A}\} \\ S_4 &= \{u \in B : f_{14} f_1 f_7 f_{12} u \in f_6 f_{10}\bar{C}\} \\ S &= \bar{B} \cap S_1 \cap S_2 \cap S_3 \cap S_4. && \text{(A.16)} \end{aligned}$$

Then we have the following:

$$\begin{aligned} \mathrm{codim}_B(S_1) &\le \mathrm{codim}_X(f_{10}\bar{C}) && \text{[from Lemma 3]} \\ &= \dim(X) - \dim(\bar{C}) \\ &&& \text{[from (A.13)} \longrightarrow f_{10} \text{ injective]} \\ &= \mathrm{codim}_C(\bar{C}) + H(X) - H(C) \\ &\le \Delta_C + H(X) - H(C) && \text{[from (A.11)]} \\ &&& \text{(A.17)} \end{aligned}$$

$$\begin{aligned} \mathrm{codim}_B(S_2) &\le \mathrm{codim}_Z(f_{13}\bar{A}) && \text{[from Lemma 3]} \\ &= \dim(Z) - \dim(\bar{A}) \\ &&& \text{[from (A.10)} \longrightarrow f_{13} \text{ injective]} \\ &= \mathrm{codim}_A(\bar{A}) + H(Z) - H(A) \\ &\le \Delta_A + H(Z) - H(A) && \text{[from (A.8)]} \\ &&& \text{(A.18)} \end{aligned}$$

$$\begin{aligned} \mathrm{codim}_B(S_3) &\le \mathrm{codim}_W(f_7 f_{13}\bar{A}) && \text{[from Lemma 3]} \\ &= \dim(W) - \dim(\bar{A}) \\ &&& \text{[from (A.10)} \longrightarrow f_7, f_{13} \text{ injective]} \\ &= \mathrm{codim}_A(\bar{A}) + H(W) - H(A) \\ &\le \Delta_A + H(W) - H(A) && \text{[from (A.8)]} \\ &&& \text{(A.19)} \end{aligned}$$

$$\begin{aligned} \mathrm{codim}_Y(S_4) &\le \mathrm{codim}_Y(f_6 f_{10}\bar{A}) && \text{[from Lemma 3]} \\ &= \dim(Y) - \dim(\bar{C}) \\ &&& \text{[from (A.13)} \longrightarrow f_6, f_{10} \text{ injective]} \\ &= \mathrm{codim}_C(\bar{C}) + H(Y) - H(C) \\ &\le \Delta_C + H(Y) - H(C). && \text{[from (A.11)]} \\ &&& \text{(A.20)} \end{aligned}$$

Suppose $t \in S$. Then,

$$\begin{aligned} &f_2 f_5 f_{11} t + f_2 f_7 f_{12} t \\ &\quad = f_2 f_7 f_{13} f_1 f_5 f_{11} t + f_2 f_7 f_{12} t \\ &\qquad \text{[we have } f_5 f_{11} t = f_7 f_{13} u \text{ for some } u \in \bar{A}, \\ &\qquad \text{and } f_7 f_{13} f_1 f_7 f_{13} u = f_7 f_{13} u \text{ since } f_1 f_7 f_{13} u = u] \\ &\quad = f_2 f_7 f_{13} f_1 f_5 f_{11} t + f_2 f_7 f_{13} f_1 f_7 f_{12} t \\ &&& \text{[since } f_{12} t \in f_{13}\bar{A}] \\ &\quad = f_2 f_7 f_{13}(f_1 f_5 f_{11} + f_1 f_7 f_{12}) t \\ &\quad = 0 && \text{(A.21)} \\ &&& \text{[since } t \in \bar{B}] \end{aligned}$$

$$\begin{aligned} &f_2 f_5 f_{11} t + f_3 f_6 f_{11} t \\ &\quad = f_2 f_5 f_{10} f_4 f_6 f_{11} t + f_3 f_6 f_{10} f_4 f_6 f_{11} t \\ &&& \text{[since } f_{11} t \in f_{10}\bar{C}] \\ &\quad = (f_2 f_5 f_{10} t + f_3 f_6 f_{10}) f_4 f_6 f_{11} t \\ &\quad = 0 && \text{(A.22)} \\ &&& \text{[since } f_{11} t \in f_{10}\bar{C} \text{ and hence} \\ &&& f_4 f_6 f_{11} t \in f_4 f_6 f_{10}\bar{C} = \bar{C}] \end{aligned}$$

$$\begin{aligned}
&f_2 f_7 f_{12} t + f_3 f_6 f_{11} t \\
&\quad = f_2 f_7 f_{12} t + f_3 f_6 f_{10} f_4 f_6 f_{11} t \\
&\quad = f_2 f_7 f_{12} t - f_3 f_6 f_{10} f_8 f_{12} t \\
&\quad = f_2 f_7 f_{12} t - f_3 f_6 f_{10} f_8 f_{13} f_1 f_7 f_{12} t \\
&\quad = f_2 f_7 f_{12} t + f_3 f_6 f_{10} f_4 f_{14} f_1 f_7 f_{12} t \\
&\quad = f_2 f_7 f_{12} t + f_3 f_{14} f_1 f_7 f_{12} t \\
&\quad = f_2 f_7 f_{13} f_1 f_7 f_{12} t + f_3 f_{14} f_1 f_7 f_{12} t \\
&\quad = (f_2 f_7 f_{13} + f_3 f_{14}) f_1 f_7 f_{12} t \\
&\quad = 0. \qquad \text{(A.23)}
\end{aligned}$$

We therefore obtain

$$\begin{aligned}
2t &= 2(f_2 f_5 f_{11} t + f_2 f_7 f_{12} t + f_3 f_6 f_{11} t) \\
&= (f_2 f_5 f_{11} t + f_2 f_7 f_{12} t) + (f_2 f_5 f_{11} t + f_3 f_6 f_{11} t) \\
&\quad + (f_2 f_7 f_{12} t + f_3 f_6 f_{11} t) \\
&= 0 + 0 + 0 = 0. \qquad \text{[from (A.21), (A.22), (A.23)]}
\end{aligned}$$

Since the field has odd characteristic, we must have $t = 0$. Thus, $S = \{0\}$, and therefore

$$\begin{aligned}
H(B) &= \mathrm{codim}_B(S) \\
&\leq \mathrm{codim}_B(\bar{B}) + \sum_{i=1}^{4} \mathrm{codim}_B(S_i) \\
&\qquad \text{[from (A.16), Lemma 2]} \\
&\leq \Delta_B + 2\Delta_A + 2\Delta_C \\
&\quad + H(W) + H(X) + H(Y) + H(Z) \\
&\quad - 2H(A) - 2H(C). \quad \text{[from (A.14), (A.17)–(A.20)]}
\end{aligned}$$

The result then follows from (A.9), (A.12), and (A.15). ■

Proof of Theorem 14: In $V = GF(2)^3$, define the following subspaces of V:

$$\begin{aligned}
A &= \langle (1,0,0) \rangle \\
B &= \langle (0,1,0) \rangle \\
C &= \langle (0,0,1) \rangle \\
W &= \langle (1,1,0) \rangle \\
X &= \langle (1,0,1) \rangle \\
Y &= \langle (0,1,1) \rangle \\
Z &= \langle (1,1,1) \rangle.
\end{aligned}$$

It is easily verified that the inequality in Theorem 13 is not satisfied in this case.

Next we show the inequality indeed holds if $\mathrm{dim}(V) \leq 2$. One way to do this is to show (using software such as Xitip [19]) that the inequality becomes a Shannon inequality under the assumption that $H(A) = 0$, or under the assumption $H(B|A) = 0$, or under the assumption $H(C|A, B) = 0$. If all three of these assumptions fail, then we must have

$$\mathrm{dim}(V) \geq H(A, B, C) > H(A, B) > H(A) > 0 \qquad \text{(A.24)}$$

and hence $\mathrm{dim}(V) \geq 3$.

Or one can give a direct argument by cases. Assume to the contrary that there exist subspaces A, B, C, W, X, Y, Z of vector space V such that

$$\begin{aligned}
&2H(A) + H(B) + 2H(C) \\
&\quad > H(W) + H(X) + H(Y) + H(Z) \\
&\qquad + 2H(A|Z, Y) + H(B|X, Z) + 2H(C|A, X) \\
&\qquad + 3H(X|W, Y) + 3H(Z|W, C) \\
&\qquad + 5H(W|A, B) + 5H(Y|B, C) \\
&\qquad + 5(H(A) + H(B) + H(C) - H(A, B, C)). \qquad \text{(A.25)}
\end{aligned}$$

Let

$$\begin{aligned}
Q &= (H(A), H(B), H(C), H(A, B, C)) \\
R &= H(A) + H(B) + H(C) - H(A, B, C).
\end{aligned}$$

Let LHS and RHS denote the left and right sides of inequality (A.25). We will obtain contradictions for all the possible values of Q.

Case (i): $\mathrm{dim}(V) = 1$

All entropies are 0 or 1. Since LHS ≤ 5, at most one of $H(A), H(B), H(C)$ can equal 1, for otherwise $R \geq 1$ would imply RHS ≥ 5.

- **(1001):** LHS $= 2$ implies $H(A|Z, Y) = 0$ which implies $H(Z) = 1$ or $H(Y) = 1$. Also, we must have $H(Z|W, C) = H(Y|B, C) = 0$, the latter implying $H(Y) = 0$. So we must have $H(Z) = 1$ which in turn implies $H(W) = 1$ and therefore RHS ≥ 2.
- **(0101):** LHS $= 1$ implies $H(B|X, Z) = 0$ which implies $H(X) = 1$ or $H(Z) = 1$, and therefore RHS ≥ 1.
- **(0011):** $LHS = 2$ implies $H(C|A, X) = 0$ and $H(X|W, Y) = 0$, which imply $H(X) = 1$, which implies $H(W) = 1$ or $H(Y) = 1$ and therefore RHS ≥ 2.

Case (ii): $\mathrm{dim}(V) = 2$

All entropies are 0, 1, or 2. LHS ≤ 10 implies RHS ≤ 9, and therefore $R \leq 1$. LHS ≥ 1 implies $H(A, B, C) > 0$ and therefore $H(A, B, C) \in \{1, 2\}$.

- **(1011):** LHS ≤ 4 and $R = 1$ imply RHS ≥ 5.
- **(1101):** Same.
- **(0111):** Same.
- **(2001):** Same.
- **(0201):** Same.
- **(0021):** Same.
- **(2012):** LHS $= 6$. $R = 1$ implies RHS ≥ 5 which implies $H(A|Z, Y) = 0$ which implies $H(Z, Y) \geq 1$ and therefore RHS ≥ 6.
- **(1022):** Same.
- **(1112):** LHS $= 5$. $R = 1$ implies RHS ≥ 5.
- **(0122):** Same.
- **(2102):** Same.
- **(0212):** LHS $= 4$. $R = 1$ implies RHS ≥ 5.
- **(1202):** Same.
- **(1001):** LHS $= 2$ implies $H(A|Z, Y) = 0$ which implies $H(Z) = 1$ or $H(Y) = 1$. If $H(Z) = 1$, then $H(Z|W, C) = 0$ which would imply $H(W) = 1$ and therefore RHS ≥ 2. If $H(Y) = 1$, then $H(Z|W, C) = 1$ which would imply RHS ≥ 5.

- **(0101):** LHS $= 1$ implies $H(X) = H(Z) = 0$ which implies $H(B|X, Z) = 1$ and therefore RHS ≥ 1.
- **(0011):** LHS $= 2$ implies $H(C|A, X) = 0$ which implies $H(X) = 1$. Also, $H(X|W, Y) = 0$ implies $H(W, Y) \geq 1$ and therefore RHS ≥ 2.
- **(0202):** $LHS = 2$ implies $H(X) + H(Z) \leq 1$ which implies $H(B|X, Z) \geq 1$ which implies $H(B|X, Z) = 1$ which implies $H(X, Z) = 1$ which implies $H(X) + H(Z) = 1$ and therefore RHS ≥ 2.
- **(0022):** LHS $= 4$ implies $H(W|A, B) = 0$ which implies $H(W) = 0$. Also, $H(C|A, X) \leq 1$ implies $H(X) \geq 1$ which implies $H(X|W, Y) = 0$ which implies $H(Y) \geq H(X)$. Thus, $H(C|A, X) = 0$ which implies $X = C$ which implies $H(Y) \geq H(C) = 2$ and therefore RHS ≥ 4.
- **(2002):** LHS $= 4$ implies $H(Y|B, C) = 0$ which implies $H(Y) = 0$. Also, $H(A|Z, Y) \leq 1$ which implies $H(Z) \geq 1$. Additionally, $H(Z|W, C) = 0$ which implies $H(W) \geq H(Z)$ which implies $H(A|Z, Y) = 0$ which implies $H(Z) = 2$ and therefore RHS ≥ 4.
- **(1102):** $H(A, B, C) = 2$ implies that $A \neq B$. LHS $= 3$ implies $H(A|Z, Y) = 0$ or $H(B|X, Z) = 0$. If $H(B|X, Z) = 0$, then $H(X)+H(Z) \geq 1$ which implies RHS ≥ 1 and therefore $H(A|Z, Y) = 0$. So it suffices to assume $H(A|Z, Y) = 0$. We have $H(Y|B, C) = 0$ which implies Y is a subspace of B, which implies $H(Z) \geq 1$. Thus, $H(Z|W, C) = 0$ which implies $H(W) \geq 1$, so RHS ≥ 2. Hence, $H(B|X, Z) = 0$ and $H(X) = 0$ which imply $Z = B$ and therefore $H(A|Z, Y) \neq 0$.
- **(0112):** $H(A, B, C) = 2$ implies $B \neq C$. LHS $= 3$ implies $H(B|X, Z) = 0$ or $H(C|A, X) = 0$. If $H(B|X, Z) = 0$, then $H(X) + H(Z) \geq 1$ which implies RHS ≥ 1 and therefore $H(C|A, X) = 0$. So it suffices to assume $H(C|A, X) = 0$. Thus we have $H(X) \geq 1$. Also, $H(X|W, Y) = 0$ which implies $H(W) + H(Y) \geq H(X)$ and so RHS ≥ 2. Thus, $H(X) = 1$ which implies $X = C$, and therefore $H(W) = 1$ or $H(Y) = 1$. Since $H(W|A, B) = 0$, W is a subspace of B and therefore $Y = C$. Finally, $H(B|X, Z) = 0$ which implies $H(Z) \geq 1$ and therefore RHS ≥ 3.
- **(1012):** $H(A, B, C) = 2$ implies $A \neq C$. LHS $= 4$ implies $H(A|Z, Y) = 0$ or $H(C|A, X) = 0$.
  Case (1): Suppose $H(C|A, X) = 0$. Then $H(X) \geq 1$ and $X \neq A$ which imply RHS ≥ 1. Thus, $H(X|W, Y) = 0$ which implies $H(W) + H(Y) \geq H(X)$, which implies RHS ≥ 2 and therefore $H(A|Z, Y) = 0$. We have $H(W|A, B) = 0$ which implies W is a subspace of A, which implies $H(Y) \geq 1$ and $Y \neq A$. Also, $H(Y|B, C) = 0$ which implies $Y = C$ and therefore $H(Z) \geq 1$ and $Z \neq C$. Finally, $H(Z|W, C) = 0$ which implies $H(W) \geq 1$ and therefore RHS ≥ 4.
  Case (2): Suppose $H(A|Z, Y) = 0$. We know $H(Y|B, C) = 0$, which implies Y is a subspace of C which implies $H(Z) \geq 1$ and $Z \neq C$ and therefore RHS ≥ 1. Thus, $H(Z|W, C) = 0$ which implies $H(W) \geq 1$ which implies RHS ≥ 2. So, $H(C|A, X) = 0$ which implies $H(X) \geq 1$ and $X \neq A$ and therefore RHS ≥ 3. Also, $H(W|A, B) = 0$ which implies $W = A$. Finally, $H(X|W, Y) = 0$ which implies $H(Y) \geq 1$ and therefore RHS ≥ 4. ■

Proof of Theorem 15: We will use the non-Fano network in Figure 6, derived in [8], from the non-Fano matroid, to help guide the proof. By Lemma 4, there exist linear functions

$$
\begin{array}{lll}
f_1 : W \to A & f_2 : W \to B & \\
f_3 : X \to A & f_4 : X \to C & \\
f_5 : Y \to B & f_6 : Y \to C & \\
f_7 : Z \to A & f_8 : Z \to B & f_9 : Z \to C \\
f_{10} : C \to W & f_{11} : C \to Z & \\
f_{12} : B \to X & f_{13} : B \to Z & \\
f_{14} : A \to Y & f_{15} : A \to Z & \\
f_{16} : C \to W & f_{17} : C \to X & f_{18} : C \to Y
\end{array}
$$

such that

$$
\begin{aligned}
f_1 + f_2 &= I \text{ on a subspace } W' \text{ of } W \text{ with} \\
&\quad \mathsf{codim}_W(W') \leq H(W|A, B) \qquad \text{(A.26)} \\
f_3 + f_4 &= I \text{ on a subspace } X' \text{ of } X \text{ with} \\
&\quad \mathsf{codim}_X(X') \leq H(X|A, C) \qquad \text{(A.27)} \\
f_5 + f_6 &= I \text{ on a subspace } Y' \text{ of } Y \text{ with} \\
&\quad \mathsf{codim}_Y(Y') \leq H(Y|B, C) \qquad \text{(A.28)} \\
f_7 + f_8 + f_9 &= I \text{ on a subspace } Z' \text{ of } Z \text{ with} \\
&\quad \mathsf{codim}_Z(Z') \leq H(Z|A, B, C) \qquad \text{(A.29)} \\
f_{10} + f_{11} &= I \text{ on a subspace } C' \text{ of } C \text{ with} \\
&\quad \mathsf{codim}_C(C') \leq H(C|W, Z) \qquad \text{(A.30)} \\
f_{12} + f_{13} &= I \text{ on a subspace } B' \text{ of } B \text{ with} \\
&\quad \mathsf{codim}_B(B') \leq H(B|X, Z) \qquad \text{(A.31)} \\
f_{14} + f_{15} &= I \text{ on a subspace } A' \text{ of } A \text{ with} \\
&\quad \mathsf{codim}_A(A') \leq H(A|Y, Z) \qquad \text{(A.32)} \\
f_{16} + f_{17} + f_{18} &= I \text{ on a subspace } C'' \text{ of } C \text{ with} \\
&\quad \mathsf{codim}_C(C'') \leq H(C|W, X, Y). \qquad \text{(A.33)}
\end{aligned}
$$

Combining these, we get maps

$$
\begin{aligned}
f_7 f_{15} &: A \to A \qquad \text{(A.34)} \\
f_5 f_{14} + f_8 f_{15} &: A \to B \qquad \text{(A.35)} \\
f_6 f_{14} + f_9 f_{15} &: A \to C. \qquad \text{(A.36)}
\end{aligned}
$$

Note that

$$
\begin{aligned}
f_5 f_{14} + f_6 f_{14} &= f_{14} \text{ on the subspace } f_{14}^{-1}(Y') \text{ of } A \\
f_7 f_{15} + f_8 f_{15} + f_9 f_{15} &= f_{15} \text{ on the subspace } f_{15}^{-1}(Z') \text{ of } A
\end{aligned}
$$

so the sum of the functions in (A.34)–(A.36) is equal to I on the subspace

$$
A'' \doteq A' \cap f_{14}^{-1}(Y') \cap f_{15}^{-1}(Z')
$$

and we get

$$\begin{aligned}\mathrm{codim}_A(A'') &\le \mathrm{codim}_A(A') + \mathrm{codim}_A\left(f_{14}^{-1}(Y')\right)\\ &\quad + \mathrm{codim}_A\left(f_{15}^{-1}(Z')\right) \qquad \text{[from Lemma 2]}\\ &\le \mathrm{codim}_A(A') + \mathrm{codim}_Y(Y') + \mathrm{codim}_Z(Z')\\ &\qquad \text{[from Lemma 3]}\\ &\le H(A|Y,Z) + H(Y|B,C) + H(Z|A,B,C).\\ &\qquad \text{[from (A.28), (A.29), (A.32)]}\end{aligned}$$

Applying Lemma 6 to

$$f_7 f_{15} - I$$
$$f_5 f_{14} + f_8 f_{15}$$
$$f_6 f_{14} + f_9 f_{15}$$

we get a subspace $\bar{A}$ of A'' such that

$$\begin{aligned}\mathrm{codim}_A(\bar{A}) &= \mathrm{codim}_A(A'') + \mathrm{codim}_{A''}(\bar{A})\\ &\le \Delta_A \qquad \text{(A.37)}\\ &\doteq H(A|Y,Z) + H(Y|B,C) + H(Z|A,B,C)\\ &\quad + H(A) + H(B) + H(C) - H(A,B,C) \qquad \text{(A.38)}\end{aligned}$$

on which

$$f_7 f_{15} = I \qquad \text{(A.39)}$$
$$f_5 f_{14} + f_8 f_{15} = 0 \qquad \text{(A.40)}$$
$$f_6 f_{14} + f_9 f_{15} = 0. \qquad \text{(A.41)}$$

Similarly, we get a subspace $\bar{B}$ of B such that

$$\begin{aligned}\mathrm{codim}_B(\bar{B}) &\le \Delta_B \qquad \text{(A.42)}\\ &\doteq H(B|X,Z) + H(X|A,C) + H(Z|A,B,C)\\ &\quad + H(A) + H(B) + H(C) - H(A,B,C) \qquad \text{(A.43)}\end{aligned}$$

on which

$$f_8 f_{13} = I \qquad \text{(A.44)}$$
$$f_3 f_{12} + f_7 f_{13} = 0 \qquad \text{(A.45)}$$
$$f_4 f_{12} + f_9 f_{13} = 0 \qquad \text{(A.46)}$$

and a subspace $\bar{C}$ of C such that

$$\begin{aligned}\mathrm{codim}_C(\bar{C}) &\le \Delta_C \qquad \text{(A.47)}\\ &\doteq H(C|W,Z) + H(W|A,B) + H(Z|A,B,C)\\ &\quad + H(A) + H(B) + H(C) - H(A,B,C) \qquad \text{(A.48)}\end{aligned}$$

on which

$$f_9 f_{11} = I \qquad \text{(A.49)}$$
$$f_1 f_{10} + f_7 f_{11} = 0 \qquad \text{(A.50)}$$
$$f_2 f_{10} + f_8 f_{11} = 0 \qquad \text{(A.51)}$$

and a subspace $\hat{C}$ of C such that

$$\begin{aligned}\mathrm{codim}_C(\hat{C}) &\le \hat{\Delta}_C \qquad \text{(A.52)}\\ &\doteq H(C|W,X,Y) + H(W|A,B)\\ &\quad + H(X|A,C) + H(Y|B,C)\\ &\quad + H(A) + H(B) + H(C) - H(A,B,C) \qquad \text{(A.53)}\end{aligned}$$

on which

$$f_4 f_{17} + f_6 f_{18} = I \qquad \text{(A.54)}$$
$$f_1 f_{16} + f_3 f_{17} = 0 \qquad \text{(A.55)}$$
$$f_2 f_{16} + f_5 f_{18} = 0. \qquad \text{(A.56)}$$

Define the following subspaces of Z:

$$A^* = f_{15}(\bar{A})$$
$$B^* = f_{13}(\bar{B})$$
$$C^* = f_{11}(\bar{C}).$$

By (A.39), the restriction maps

$$f_{15}|\bar{A} : \bar{A} \to A^*$$
$$f_7|A^* : A^* \to \bar{A}$$

are inverses of each other, and hence are injective. Similarly, by (A.44), $f_8|B^*$ is the inverse of $f_{13}|\bar{B}$ and, by by (A.49), $f_9|C^*$ is the inverse of $f_{11}|\bar{C}$, so these are all injective. In particular,

$$\dim(A^*) = \dim(\bar{A}) \qquad \text{(A.57)}$$
$$\dim(B^*) = \dim(\bar{B}) \qquad \text{(A.58)}$$
$$\dim(C^*) = \dim(\bar{C}). \qquad \text{(A.59)}$$

Now let

$$A^{**} = f_7(A^* \cap B^*) \subseteq \bar{A}.$$

Then f_{15} is injective on A^{**} and

$$f_{15}(A^{**}) = A^* \cap B^*$$

so $f_8 f_{15}$ is injective on A^{**}. But

$$f_5 f_{14} + f_8 f_{15} = 0$$

on $\bar{A}$, so $f_5 f_{14}$ is injective on A^{**}, and hence so is f_{14}. This gives

$$\dim(f_{14}A^{**}) = \dim(A^{**}) = \dim(A^* \cap B^*). \qquad \text{(A.60)}$$

Similarly, let

$$B^{**} = f_8(A^* \cap B^*) \subseteq \bar{B};$$

then $f_7 f_{13}$ is injective on B^{**} and

$$f_3 f_{12} + f_7 f_{13} = 0$$

on B^{**}, so f_{12} is injective on B^{**} and

$$\dim(f_{12}B^{**}) = \dim(B^{**}) = \dim(A^* \cap B^*). \qquad \text{(A.61)}$$

And let

$$C^{**} = f_9(B^* \cap C^*) \subseteq \bar{C};$$

then $f_8 f_{11}$ is injective on C^{**} and

$$f_2 f_{10} + f_8 f_{11} = 0$$

on C^{**}, so f_{10} is injective on C^{**} and

$$\mathsf{dim}(f_{10}C^{**}) = \mathsf{dim}(C^{**}) = \mathsf{dim}(B^* \cap C^*). \quad \text{(A.62)}$$

Let us define the following subspaces of C:

$$\begin{aligned} S_1 &= \{u \in C : f_{16}u \in f_{10}C^{**}\} \\ S_2 &= \{u \in C : f_{17}u \in f_{12}B^{**}\} \\ S_3 &= \{u \in C : f_{18}u \in f_{14}A^{**}\} \\ S &= \hat{C} \cap S_1 \cap S_2 \cap S_3. \end{aligned} \quad \text{(A.63)}$$

Then we have the following:

$$\begin{aligned} &\mathsf{codim}_C(S_1) \\ &\le \mathsf{codim}_W\big(f_{10}C^{**}\big) && \text{[from Lemma 3]} \\ &= \mathsf{dim}(W) - \mathsf{dim}(B^* \cap C^*) && \text{[from (A.62)]} \\ &= \mathsf{codim}_Z\big(B^* \cap C^*\big) + \mathsf{dim}(W) - \mathsf{dim}(Z) \\ &\le \mathsf{codim}_Z\big(B^*\big) + \mathsf{codim}_Z\big(C^*\big) + \mathsf{dim}(W) - \mathsf{dim}(Z) \\ &&& \text{[from Lemma 2]} \\ &= \mathsf{codim}_B\big(\bar{B}\big) + \mathsf{codim}_C\big(\bar{C}\big) + \mathsf{dim}(W) + \mathsf{dim}(Z) \\ &\quad -\mathsf{dim}(B) - \mathsf{dim}(C) && \text{[from (A.58), (A.59)]} \\ &\le \Delta_B + \Delta_C + H(W) + H(Z) - H(B) - H(C) \\ &&& \text{[from (A.42), (A.47)]} \end{aligned} \quad \text{(A.64)}$$

$$\begin{aligned} &\mathsf{codim}_C(S_2) \\ &\le \mathsf{codim}_X\big(f_{12}B^{**}\big) && \text{[from Lemma 3]} \\ &= \mathsf{dim}(X) - \mathsf{dim}(A^* \cap B^*) && \text{[from (A.61)]} \\ &= \mathsf{codim}_Z\big(A^* \cap B^*\big) + \mathsf{dim}(X) - \mathsf{dim}(Z) \\ &\le \mathsf{codim}_Z\big(A^*\big) + \mathsf{codim}_Z\big(B^*\big) + \mathsf{dim}(X) - \mathsf{dim}(Z) \\ &&& \text{[from Lemma 2]} \\ &= \mathsf{codim}_A\big(\bar{A}\big) + \mathsf{codim}_B\big(\bar{B}\big) + \mathsf{dim}(X) + \mathsf{dim}(Z) \\ &\quad -\mathsf{dim}(A) - \mathsf{dim}(B) && \text{[from (A.57), (A.58)]} \\ &\le \Delta_A + \Delta_B + H(X) + H(Z) - H(A) - H(B) \\ &&& \text{[from (A.37), (A.42)]} \end{aligned} \quad \text{(A.65)}$$

$$\begin{aligned} &\mathsf{codim}_C(S_3) \\ &\le \mathsf{codim}_Y\big(f_{14}A^{**}\big) && \text{[from Lemma 3]} \\ &= \mathsf{dim}(Y) - \mathsf{dim}(A^* \cap B^*) && \text{[from (A.60)]} \\ &= \mathsf{codim}_Z\big(A^* \cap B^*\big) + \mathsf{dim}(Y) - \mathsf{dim}(Z) \\ &\le \mathsf{codim}_Z\big(A^*\big) + \mathsf{codim}_Z\big(B^*\big) + \mathsf{dim}(Y) - \mathsf{dim}(Z) \\ &&& \text{[from Lemma 2]} \\ &= \mathsf{codim}_A\big(\bar{A}\big) + \mathsf{codim}_B\big(\bar{B}\big) + \mathsf{dim}(Y) + \mathsf{dim}(Z) \\ &\quad -\mathsf{dim}(A) - \mathsf{dim}(B) && \text{[from (A.57), (A.58)]} \\ &\le \Delta_A + \Delta_B + H(Y) + H(Z) - H(A) - H(B). \\ &&& \text{[from (A.37), (A.42)]} \end{aligned} \quad \text{(A.66)}$$

Suppose $t \in S$. Then there exist

$$\begin{aligned} a &\in A^{**} \\ b &\in B^{**} \\ c &\in C^{**} \end{aligned}$$

such that

$$\begin{aligned} f_{14}a &= f_{18}t \\ f_{12}b &= f_{17}t \\ f_{10}c &= f_{16}t. \end{aligned}$$

Since $t \in \hat{C}$, we have from ((A.54))–((A.56)) that

$$\begin{aligned} f_1 f_{16}t + f_3 f_{17}t &= 0 \\ f_2 f_{16}t + f_5 f_{18}t &= 0 \\ f_4 f_{17}t + f_6 f_{18}t &= t \end{aligned}$$

which gives

$$f_1 f_{10}c + f_3 f_{12}b = 0 \quad \text{(A.67)}$$
$$f_2 f_{10}c + f_5 f_{14}a = 0 \quad \text{(A.68)}$$
$$f_4 f_{12}b + f_6 f_{14}a = t. \quad \text{(A.69)}$$

But we also have

$$f_5 f_{14}a + f_8 f_{15}a = 0 \quad \text{[from (A.40)]} \quad \text{(A.70)}$$
$$f_6 f_{14}a + f_9 f_{15}a = 0 \quad \text{[from (A.41)]} \quad \text{(A.71)}$$
$$f_3 f_{12}b + f_7 f_{13}b = 0 \quad \text{[from (A.45)]} \quad \text{(A.72)}$$
$$f_4 f_{12}b + f_9 f_{13}b = 0 \quad \text{[from (A.46)]} \quad \text{(A.73)}$$
$$f_1 f_{10}c + f_7 f_{11}c = 0 \quad \text{[from (A.50)]} \quad \text{(A.74)}$$
$$f_2 f_{10}c + f_8 f_{11}c = 0 \quad \text{[from (A.51)]} \quad \text{(A.75)}$$

so

$$f_7 f_{11}c + f_7 f_{13}b = 0 \quad \text{[from (A.67), (A.72), (A.74)]} \quad \text{(A.76)}$$
$$f_8 f_{11}c + f_8 f_{15}a = 0 \quad \text{[from (A.68), (A.70) (A.75)]} \quad \text{(A.77)}$$
$$f_9 f_{13}b + f_9 f_{15}a = -t. \quad \text{[from (A.69), (A.71), (A.73)]} \quad \text{(A.78)}$$

Since $f_{11}c$ and $f_{15}a$ are both in B^*, and f_8 is injective on B^*, we get from (A.77) that $f_{11}c = -f_{15}a$. This implies that $f_{11}c$ is also in A^*, and since $f_{13}b \in A^*$ and f_7 is injective on A^*, we get from (A.76) that $f_{11}c = -f_{13}b$ and hence $f_{15}a = f_{13}b$.

Hence, since the field has characteristic 2, we have

$$\begin{aligned} t &= -(f_9 f_{13}b + f_9 f_{15}a) \\ &= -(f_9 f_{13}b + f_9 f_{13}b) \\ &= 0. \end{aligned}$$

Since the choice of t was arbitrary, this implies $S = \{0\}$, and therefore

$$\begin{aligned} H(C) &= \mathsf{codim}_C(S) \\ &\le \mathsf{codim}_C\left(\hat{C}\right) + \sum_{i=1}^{3} \mathsf{codim}_C(S_i) \\ &\qquad\qquad \text{[from (A.63), Lemma 2]} \\ &\le \hat{\Delta}_C + 2\Delta_A + 3\Delta_B + \Delta_C + H(W) + H(X) \\ &\quad + H(Y) + 3H(Z) - 2H(A) - 3H(B) - H(C) \\ &\qquad\qquad \text{[from (A.52), (A.64), (A.65), (A.66)].} \end{aligned}$$

The result then follows from (A.38), (A.43), (A.48), and (A.53). ■

REFERENCES

[1] M. Adler, N. J. A. Harvey, K. Jain, R. D. Kleinberg, and A. R. Lehman, "On the capacity of information networks," in *Proc. ACM-SIAM Symp. Discrete Algorithms (SODA)*, Miami, FL, USA, Jan. 2006, pp. 2345–2364.

[2] 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.

[3] A. Blasiak, R. Kleinberg, and E. Lubetzky. (2011). "Lexicographic products and the power of non-linear network coding." [Online]. Available: http://arxiv.org/abs/1108.2489

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

[5] T. H. Chan and A. Grant. (2012). "Network coding capacity regions via entropy functions." [Online]. Available: http://arxiv.org/abs/1201.1062

[6] 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.

[7] R. Dougherty, C. Freiling, and K. Zeger, "Unachievability of network coding capacity," *IEEE Trans. Inf. Theory*, vol. 52, no. 6, pp. 2365–2372, Jun. 2006.

[8] 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.

[9] R. Dougherty and K. Zeger, "Nonreversibility and equivalent constructions of multiple-unicast networks," *IEEE Trans. Inf. Theory*, vol. 52, no. 11, pp. 5067–5077, Nov. 2006.

[10] R. Dougherty, C. Freiling, and K. Zeger. (2011). "Non-Shannon information inequalities in four random variables." [Online]. Available: http://arxiv.org/abs/1104.3602

[11] K. Fukuda. *cdd and cddplus Homepage*. [Online]. Available: http://www.cs.mcgill.ca/~fukuda/soft/cdd_home/cdd.html, accessed Aug. 25, 2005.

[12] N. J. Harvey, R. D. Kleinberg, and A. R. Lehman, "Comparing network coding with multicommodity flow for the k-pairs communication problem," Lab. Comput. Sci., Massachusetts Inst. Technol., Cambridge, MA, USA, Tech. Rep. 964, Sep. 2004. [Online]. Available: http://theory.csail.mit.edu/~nickh/Publications/Publications.html

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

[14] A. W. Ingleton, "Representation of matroids," in *Combinatorial Mathematics and Its Applications*, D. J. A. Welsh, Ed. London, U.K.: Academic, 1971, pp. 149–167.

[15] A. Kim. (Mar. 2011). "On network coding capacity—Matroidal networks and network capacity regions." [Online]. Available: http://arxiv.org/abs/1103.0358

[16] R. Koetter, "A duality principle in network coding," presented at the Workshop Algebraic Coding Theory Inf. Theory Center Discrete Math. Theoretical Comput. Sci. (DIMACS), Piscataway, NJ, USA, Dec. 2003.

[17] R. Koetter, M. Effros, T. Ho, and M. Médard, "Network codes as codes on graphs," presented at the 38th Annu. Conf. Inf. Sci. Syst. (CISS), 2004. [Online]. Available: http://www.comm.csl.uiuc.edu/~koetter/publications/paper7.pdf

[18] F. Matúš, "Infinitely many information inequalities," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Nice, France, Jun. 2007, pp. 41–44.

[19] R. Pulikkoonattu, E. Perron, and S. Diggavi. *Xitip (Information Theoretic Inequality Prover)*. [Online]. Available: http://xitip.epfl.ch, accessed 2014.

[20] S. Riis. (May 2005). *Reversible and Irreversible Information Networks*. [Online]. Available: http://www.dcs.qmul.ac.uk/~smriis

[21] X. Yan, R. W. Yeung, and Z. Zhang, "The capacity region for multi-source multi-sink network coding," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Nice, France, Jun. 2007, pp. 116–120.

[22] R. W. Yeung, *A First Course in Information Theory*. Norwell, MA, USA: Kluwer, 2002.

[23] Z. Zhang and R. W. Yeung, "On characterization of entropy function via information inequalities," *IEEE Trans. Inf. Theory*, vol. 44, no. 4, pp. 1440–1452, Jul. 1998.

Randall Dougherty was born in 1961. He received the A.B. and Ph.D. degrees in mathematics from the University of California (Berkeley) in 1981 and 1985, respectively. After postdoctoral work at Caltech and UCLA, he joined the mathematics faculty of The Ohio State University in 1989, becoming an Associate Professor in 1992 and a Professor in 1998. In 2000 he left Ohio State to work for the software company LizardTech in Seattle; in 2002 he started to work full time at the Center for Communications Research (CCR) in La Jolla, California. He also spent shorter periods working as a consultant in various organizations, such as CCR and the Los Alamos National Laboratory. He is a three-time International Mathematical Olympiad medalist and a three-time Putnam Fellow. He received an NSF Presidential Young Investigator Award in 1991 and a Sloan Research Fellowship in 1992. His mathematical research interests range from foundations (logic and set theory) to other pure mathematics (real analysis, group theory, combinatorics) to applied work (numerical methods, network design, computational geometry, etc.).

Chris Freiling was born in 1954, received his Ph.D. from UCLA under the direction of Donald Martin. He has been on the faculty at California State University at San Bernardino since 1983, interrupted by two visiting appointments at UCLA. His mathematical interests include Foundations and Real Analysis. He is the recipient of the 2003 Andy Award in Real Analysis.

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.