

A Local Perspective on the Edge Removal Problem

Fei Wei
University at Buffalo
feiwei@buffalo.edu

Michael Langberg
University at Buffalo
mikel@buffalo.edu

Michelle Effros
California Institute of Technology
effros@caltech.edu

Abstract—The edge removal problem studies the loss in network coding rates that results when a network communication edge is removed from a given network. It is known, for example, that in networks restricted to linear coding schemes and networks restricted to Abelian group codes, removing an edge e^* with capacity R_{e^*} reduces the achievable rate on each source by no more than R_{e^*} . In this work, we seek to uncover larger families of encoding functions for which the edge removal statement holds. We take a *local* perspective: instead of requiring that all network encoding functions satisfy certain restrictions (e.g., linearity), we limit only the function carried on the removed edge e^* . Our central results give sufficient conditions on the function carried by edge e^* in the code used to achieve a particular rate vector under which we can demonstrate the achievability of a related rate vector once e^* is removed.

I. INTRODUCTION

The *edge removal problem* (see, for example, [1]–[10]) studies the impact on communication rate of removing a network communication edge e^* with capacity R_{e^*} from a given network coding network. (Detailed definitions of the statement above and those that follow appear in Section II.) In a number of special cases, including networks with co-located sources, networks with a super-source node, networks where the removed edge is connected to a terminal node, networks restricted to linear coding schemes, and networks restricted to Abelian group codes [1]–[3], [8], it is known that removing an edge e^* with capacity R_{e^*} from a given network reduces the achievable rate on each source by no more than the edge capacity R_{e^*} . When the loss in each source’s rate for each source that results from an edge removal is bounded by the capacity of the edge removed, we say that the network satisfies an *edge removal statement*.

Whether the edge removal statement holds universally for any network coding instance and any family of encoding functions remains an intriguing open question with connections to a variety of different network information theoretic problems. For example, the edge removal problem lends insight on the relationship between index coding and network coding instances [4], the reducibility of multiple-multicast network coding to 2-unicast network coding [6], [11], the entropic region characterization of network coding instances [7], [12], [13], other upper bounds on network coding capacity [5], and the notion of strong converses in network communication [9], [10]. These rich connections shed light on the significance of the edge-removal problem and its solution.

In this work, we continue the line of study from [2], [5], [8], seeking to find larger families of encoding functions for which

an edge removal statement holds. We here introduce a new *local* perspective, observing that when considering the impact of removing a given edge e^* from a network, it sometimes suffices to consider only the function carried by edge e^* , rather than considering the encoding functions for all network edges. For example, while [2] shows the edge removal statement is satisfied on networks restricted to linear coding schemes, we show, for a given coding scheme, that an edge removal statement is true on all edges e^* that carry linear functions of the source inputs even if other edges in the network carry non-linear functions of those inputs.¹ More precisely, we study a *local edge removal statement*: Given any network coding instance that has a solution achieving rate vector \mathbf{R} , if the function carried on a given edge e^* satisfies certain conditions (e.g., linearity), removing e^* from the network reduces the achievable rate on each source by no more than the capacity of e^* . Our work seeks to understand for which functions carried on edge e^* the local edge removal statement holds.

The remainder of this paper is organized as follows. In Section II, we present our model and the definitions used throughout this work. In Theorem 1 of Section III, we present a sufficient condition for the function carried by edge e^* that implies our local edge removal statement. As the local edge removal statement can imply the (original) edge removal statement studied, e.g., in [2], [8], our sufficient condition unifies and generalizes the previous results of [2], [8] on linear and Abelian group network codes.

In Section IV, we define a broad class of functions that generalize linear functions. We call these *component-wise-linear* (CWL) functions. We study CWL functions and show that such functions satisfy the sufficient condition of Theorem 1. Thus, for a given code, the local edge removal statement holds on e^* if the function carried by e^* is CWL. We then expand this result to certain functions that are *piece-wise* CWL.

In Section V, we study the possibility of proving the original edge removal statement (studied, e.g., in [1]–[10]) through the local lens of CWL functions. Namely, we ask the following question: *Given a network coding instance, a network edge e^* , and a network coding scheme, can the scheme be modified so that (a) the function carried on edge e^* is CWL, and (b) there is no compromise on the communication rate?* In other words, we ask if one can always modify a network coding scheme to preserve communication and guarantee that “locally” (on a given edge e^*) the function is CWL,

¹We note that this extension is implicit in the proofs appearing in [2].

whereas elsewhere, functions may be arbitrary. An affirmative answer to this question would imply the original edge removal statement for any network coding instance, while a negative answer would not necessarily have any implications on edge removal. As any instance for which linear encoding functions are optimal satisfies the conditions of the question above, we study instances for which linear encoding functions are sub-optimal. While we do not resolve the question in this work, we prove that such code modifications are possible for the network coding instances and solutions presented in [14]–[16] for which linear coding is known to be sub-optimal, implying that edge removal holds for these solutions. We note that our question is not resolved on the network instance given in [17] for which, as above, linear network coding is suboptimal.

Finally, we conclude in Section VI. The proofs of several of our claims appear in the Appendix.

II. MODEL AND DEFINITIONS

Throughout the paper, we denote the size of a finite set \mathcal{S} by $|\mathcal{S}|$. For any positive integer k , we denote the set $\{1, \dots, k\}$ by $[k]$. We use bold letters to denote vectors, for example $\mathbf{R} = (R_1, \dots, R_{|\mathcal{S}|})$ is a vector of dimension $|\mathcal{S}|$ and R_i is the i^{th} element of vector \mathbf{R} .

A network instance $\mathcal{I} = (\mathcal{N}, \mathcal{S}, \mathcal{T}, \mathcal{M})$ of the network coding problem includes a directed acyclic error-free network $\mathcal{N} = G(\mathcal{V}, \mathcal{E})$ with nodes (also referred to as vertices) \mathcal{V} and edges $\mathcal{E} \subset \mathcal{V} \times \mathcal{V}$. Each edge $e = (v_1, v_2) \in \mathcal{E}$ represents an error-free channel from node v_1 to node v_2 . We use $R_e > 0$ to denote the channel capacity of edge e . For each node $v \in \mathcal{V}$, $\text{In}(v) = \{(v_1, v) : (v_1, v) \in \mathcal{E}\}$ and $\text{Out}(v) = \{(v, v_1) : (v, v_1) \in \mathcal{E}\}$ denote the set of incoming and outgoing edges of node v respectively. The sets $\mathcal{S} \subseteq \mathcal{V}$ and $\mathcal{T} \subseteq \mathcal{V}$ denote the set of source nodes and the set of terminal nodes respectively. Without loss of generality, each source $s \in \mathcal{S}$ has no incoming edges and each terminal $t \in \mathcal{T}$ has no outgoing edges, which implies $\mathcal{S} \cap \mathcal{T} = \emptyset$. For convenience of notation, at times, we denote nodes in the source set \mathcal{S} by integers $i \in \{1, 2, \dots, |\mathcal{S}|\}$. Finally, $|\mathcal{S}| \times |\mathcal{T}|$ binary matrix $\mathcal{M} = [m_{st}]$ describes the network demands, with $m_{st} = 1$ if and only if source $s \in \mathcal{S}$ is requested by terminal $t \in \mathcal{T}$.

Consider an instance $\mathcal{I} = (\mathcal{N}, \mathcal{S}, \mathcal{T}, \mathcal{M})$ of the network coding problem. A network code of blocklength n and rate vector $\mathbf{R} = (R_i)_{i \in \mathcal{S}}$ on \mathcal{I} is defined by a set of random variables $\{X_f : f \in \mathcal{S} \cup \mathcal{E}\}$ as follows.

Each source $i \in \mathcal{S}$ independently generates source message X_i uniformly distributed on the support set $\mathcal{X}_i = [2^{nR_i}]$. Each edge $e \in \mathcal{E}$ carries edge message X_e with support set $\mathcal{X}_e = [2^{nR_e}]$. For any set $A \subseteq \mathcal{E}$, we use X_A to represent the vector of messages on the edges in A , giving $X_A = (X_e)_{e \in A}$. The local encoding function $\phi_{le} : \prod_{f \in \text{In}(u)} \mathcal{X}_f \mapsto \mathcal{X}_e$ for edge $e = (u, v) \in \mathcal{E}$ takes as its input the vector $X_{\text{In}(u)}$ of messages (i.e., random variables) associated with incoming edges $\text{In}(u)$. The edge message X_e equals the evaluation of ϕ_{le} on its input, giving $X_e = \phi_{le}(X_{\text{In}(u)})$. Notice that this relationship implies $H(X_e | X_{\text{In}(u)}) = 0$, for all $e = (u, v) \in \mathcal{E}$. Edges that

leave source node $s \in \mathcal{S}$ have corresponding local encoding functions that take the source information X_s as input.

The global encoding function may be defined inductively from the local encoding functions, see e.g. [18]. For any edge $e = (u, v) \in \mathcal{E}$, edge message X_e is uniquely determined by source message vector $X_{\mathcal{S}} = (X_i)_{i \in \mathcal{S}}$ via the global encoding functions $\phi_{ge} : \prod_{i \in \mathcal{S}} \mathcal{X}_i \mapsto \mathcal{X}_e$, giving $X_e = \phi_{le}(X_{\text{In}(u)}) = \phi_{ge}(X_{\mathcal{S}})$.

For any terminal node $t \in \mathcal{T}$, the received message $X_{\text{In}(t)}$ equals the evaluation of the global encoding functions ϕ_{ge} on $e \in \text{In}(t)$; thus $H(X_{\text{In}(t)} | X_{\mathcal{S}}) = 0$. The decoding function $\phi_t : \prod_{e \in \text{In}(t)} \mathcal{X}_e \mapsto \hat{\mathcal{X}}_t$ takes as input received message $X_{\text{In}(t)}$ and emits the reconstruction \hat{X}_t of the demanded source messages, giving $\hat{X}_t = \phi_t(X_{\text{In}(t)})$.

An instance \mathcal{I} is said to be $(\epsilon, \mathbf{R}, n)$ -feasible if and only if there exists a network code $\{X_f : f \in \mathcal{S} \cup \mathcal{E}\}$ (with corresponding encoding/decoding functions) of blocklength n , that satisfies the following properties:

- 1) Uniform and independent sources: $H(X_{\mathcal{S}}) = \sum_{i \in \mathcal{S}} H(X_i) = \sum_{i \in \mathcal{S}} \log |\mathcal{X}_i|$.
- 2) Source rate: $H(X_i) \geq nR_i, \forall i \in \mathcal{S}$.
- 3) Edge capacity: $\mathcal{X}_e = [2^{nR_e}], \forall e \in \mathcal{E}$.
- 4) Encoding: $H(X_e | X_{\text{In}(u)}) = 0, \forall e = (u, v) \in \mathcal{E}$.
- 5) Decoding: for each terminal $t \in \mathcal{T}$, $\Pr(\hat{X}_t = X_t) > 1 - \epsilon$, here, the probability is taken with respect to the distribution on the source random variables $X_{\mathcal{S}}$.

Statement 1 (Local edge removal statement). *Let $\mathcal{I} = (\mathcal{N}, \mathcal{S}, \mathcal{T}, \mathcal{M})$ be a network coding instance. Suppose that \mathcal{I} is $(\epsilon, \mathbf{R}, n)$ -feasible. Consider a modified instance $\mathcal{I}' = (\mathcal{N}', \mathcal{S}, \mathcal{T}, \mathcal{M})$ obtained by removing an edge e^* with capacity R_{e^*} from \mathcal{N} . If \mathcal{I}' is $(\epsilon, \mathbf{R} - R_{e^*} \cdot \mathbf{1}, n)$ -feasible, we say that the local edge removal statement holds on \mathcal{I} for edge e^* and parameters $(\epsilon, \mathbf{R}, n)$. If the local edge removal statement holds in this setting for all edges in \mathcal{N} and all settings of $(\epsilon, \mathbf{R}, n)$ for which \mathcal{I} is $(\epsilon, \mathbf{R}, n)$ -feasible, we say that the edge removal statement holds on \mathcal{I} . Here $\mathbf{R} - R_{e^*} \cdot \mathbf{1} = ((R_1 - R_{e^*})^+, \dots, (R_{|\mathcal{S}|} - R_{e^*})^+)$ where $(R - R_{e^*})^+ = \max\{0, R - R_{e^*}\}$.*

III. A SUFFICIENT CONDITION FOR LOCAL EDGE REMOVAL

In what follows, we present our sufficient condition for local edge removal. Roughly speaking, we show that the local edge removal statement holds on \mathcal{I} for a given edge e^* in \mathcal{I} and parameters $(\epsilon, \mathbf{R}, n)$ if there exists an $(\epsilon, \mathbf{R}, n)$ -feasible code $\{X_f : f \in \mathcal{S} \cup \mathcal{E}\}$ for \mathcal{I} and an auxiliary random variable Y that is a deterministic function f_Y of $X_{\mathcal{S}}$ such that:

- (A) X_{e^*} is a deterministic function of Y .
- (B) Conditioned on Y the sources are independent.
- (C) There exists a value y' of Y such that (a) the (source) pre-image of y' under function f_Y is “relatively large”, and (b) the pre-image captures the error statistics of the network code.

Note that as Y is a deterministic function of $X_{\mathcal{S}}$, the random variable Y induces a partition of the set $\mathcal{X}_{\mathcal{S}}$. Requirements

(A) – (C) are formalized in the theorem below using the following notation. Given an $(\epsilon, \mathbf{R}, n)$ network code, we say x_S is “good” if x_S is decoded correctly by all terminals; otherwise x_S is “bad.” We define the set of all good elements in \mathcal{X}_S as $\mathcal{X}_S^G = \{x_S : x_S \text{ is good}\}$ and the set of bad elements as $\mathcal{X}_S^B = \mathcal{X}_S \setminus \mathcal{X}_S^G$. With these definitions, $\epsilon = \frac{|\mathcal{X}_S^B|}{|\mathcal{X}_S|} = \frac{|\mathcal{X}_S^B|}{|\mathcal{X}_S^G| + |\mathcal{X}_S^B|}$ by the assumed uniform distribution on \mathcal{X}_S . We also express the partition induced by y as $A(y) = \{x_S \in \mathcal{X}_S : f_Y(x_S) = y\}$, $A^G(y) = \{x_S \in \mathcal{X}_S^G : f_Y(x_S) = y\}$, $A^B(y) = A(y) \setminus A^G(y)$ and $A_i(y) = \{x_i : \exists x_S \in A(y), x_i = x_S(i)\}$ for any $i \in \mathcal{S}$.

Theorem 1. *Let $\mathcal{I} = (\mathcal{N}, \mathcal{S}, \mathcal{T}, \mathcal{M})$ be a network coding instance that is $(\epsilon, \mathbf{R}, n)$ -feasible with a corresponding network code $\{X_f : f \in \mathcal{S} \cup \mathcal{E}\}$. The local edge removal statement holds on \mathcal{I} for edge e^* in \mathcal{I} and parameters $(\epsilon, \mathbf{R}, n)$ if there exists a random variable Y (with support \mathcal{Y}) which is a deterministic function of X_S such that*

- (A) $H(X_{e^*}|Y) = 0$. (Therefore, there exists a function g_Y s.t. $X_{e^*} = g_Y(Y)$.)
- (B) $H(X_S|Y) = \sum_{i \in \mathcal{S}} H(X_i|Y)$.
- (C) There exists $y' \in \mathcal{Y}$ s.t. $|A_i(y')| \geq |\mathcal{X}_i|/|\mathcal{X}_{e^*}|$ for every $i \in \mathcal{S}$ and $|A^B(y')| \leq \epsilon|A(y')|$.

Proof. By assumption (A), $X_{e^*} = g_Y(Y)$ for some deterministic function g_Y . Fix any $y' \in \mathcal{Y}$ that satisfies condition (C) of the theorem, let $x_{e^*} = g_Y(y')$. Fixing $Y = y'$, we design a new network code for the network instance \mathcal{I}' obtained by removing edge e^* from instance \mathcal{I} . The new network code is the restriction of the original code to $A(y')$.

We first define the source random variable X'_S with alphabet $\mathcal{X}'_S = A(y')$ and probability mass function (pmf) $\Pr(X'_S = x'_S) = \Pr(X_S = x_S|Y = y') = \frac{1}{|A(y')|}$. Under this pmf, $H(X'_S) = H(X_S|Y = y') = \log |A(y')|$. We define the random variable X'_i with alphabet $\mathcal{X}'_i = A_i(y')$, and pmf $\Pr(X'_i = x'_i) = \sum_{x'_S \in \mathcal{X}'_S : x'_S(i) = x'_i} \Pr(X'_S = x'_S) = \Pr(X_i = x'_i|Y = y')$, similarly, $H(X'_i) = H(X_i|Y = y')$.

For any $e \in \mathcal{E}$, let X'_e be a random variable with alphabet $\mathcal{X}'_e = \{x_e \in \mathcal{X}_e : \exists x_S \in \mathcal{X}'_S, x_e = \phi_{g_e}(x_S)\}$ and pmf $\Pr(X'_e = x'_e) = \Pr(X_e = x'_e|Y = y')$. Note that

$$|\mathcal{X}'_e| \leq |\mathcal{X}_e|. \quad (1)$$

We now show that $\{X'_f : f \in \mathcal{S} \cup \mathcal{E}\}$ is a network code over instance \mathcal{I}' .

1) *Uniform and independent sources:* We show independence first. By definition, we have

$$H(X_S|Y) = \sum_{y \in \mathcal{Y}} \Pr(Y = y) H(X_S|Y = y) \quad (2)$$

and

$$\begin{aligned} \sum_{i \in \mathcal{S}} H(X_i|Y) &= \sum_{i \in \mathcal{S}} \sum_{y \in \mathcal{Y}} \Pr(Y = y) H(X_i|Y = y) \\ &= \sum_{y \in \mathcal{Y}} \Pr(Y = y) \sum_{i \in \mathcal{S}} H(X_i|Y = y) \end{aligned} \quad (3)$$

Combining (2), (3) and condition (B) of the theorem gives

$$\sum_{y \in \mathcal{Y}} \Pr(Y = y) H(X_S|Y = y) = \sum_{y \in \mathcal{Y}} \Pr(Y = y) \sum_{i \in \mathcal{S}} H(X_i|Y = y). \quad (4)$$

For any $y \in \mathcal{Y}$, $H(X_S|Y = y) \leq \sum_{i \in \mathcal{S}} H(X_i|Y = y)$; therefore, (4) implies

$$H(X_S|Y = y) = \sum_{i \in \mathcal{S}} H(X_i|Y = y) \quad (5)$$

for each $y \in \mathcal{Y}$. Setting $Y = y'$, we conclude that $\{X'_i : i \in \mathcal{S}\}$ are independent.

Now we show that $\{X'_i : i \in \mathcal{S}\}$ are uniform. By our definitions, for any $x_S = (x_i)_{i \in \mathcal{S}} \in A(y')$, we have $x_i \in A_i(y')$ for all $i \in \mathcal{S}$, but not necessarily vice versa. Thus, $|A(y')| \leq \prod_{i \in \mathcal{S}} |A_i(y')|$. Suppose that there exists a tuple $x_S = (x_i)_{i \in \mathcal{S}}$ such that $x_i \in A_i(y')$ for all $i \in \mathcal{S}$ but $x_S \notin A(y')$, namely, $|A(y')| < \prod_{i \in \mathcal{S}} |A_i(y')|$. That is, $\Pr(X_S = x_S|Y = y') = 0$ and $\Pr(X_i = x_i|Y = y') \neq 0$ for all $i \in \mathcal{S}$. Accordingly $\Pr(X_S = x_S|Y = y') \neq \prod_{i \in \mathcal{S}} \Pr(X_i = x_i|Y = y')$ which contradicts the independence of $\{X'_i : i \in \mathcal{S}\}$. Thus $|A(y')| = \prod_{i \in \mathcal{S}} |A_i(y')|$. If there exists $i \in \mathcal{S}$ such that X'_i is not uniform, then $H(X'_S) = \log |A(y')| = \sum_{i \in \mathcal{S}} \log |A_i(y')| > \sum_{i \in \mathcal{S}} H(X'_i)$ which is a contradiction to the independence of $\{X'_i : i \in \mathcal{S}\}$.

2) *No information on edge e^* :* By condition (A), $X_{e^*} = g_Y(Y)$. Thus, the value on e^* is fixed over X'_S , which means we can use this code when the edge e^* is removed from the network.

3) *Encoding:* By the definition of a network code, $H(X_e|X_{\text{In}(u)}) = 0$ for every $e = (u, v) \in \mathcal{E}$. For the same edge $e = (u, v)$ in instance \mathcal{I}' , $H(X'_e, X'_{\text{In}(u)}) = H(X_e, X_{\text{In}(u)}|Y = y') = H(X_{\text{In}(u)}|Y = y') = H(X'_{\text{In}(u)})$. Thus $H(X'_e|X'_{\text{In}(u)}) = 0$ and $\{X'_f : f \in \mathcal{S} \cup \mathcal{E}\}$ is a network code.

4) *Decoding:* By our definitions, the decoding error is $|A^B(y')|/|A(y')|$ which by condition (C) of the theorem is at most ϵ .

5) *Impact on source rate:* By our definitions and by source uniformity, we have $nR'_i = \log |\mathcal{X}'_i| = \log |A_i(y')|$, $nR_i = \log |\mathcal{X}_i|$, and $nR_{e^*} = \log |\mathcal{X}_{e^*}|$. By condition (C) of the theorem, for each $i \in \mathcal{S}$ we have $R'_i \geq R_i - R_{e^*}$.

6) *Edge capacity limit:* By the definition of the new edge messages and (1), we have $2^{nR'_e} = |\mathcal{X}'_e| \leq |\mathcal{X}_e| = 2^{nR_e}$, accordingly $R'_e \leq R_e$ for any $e \in \mathcal{E}$ and the edge capacity limit is satisfied. \square

Corollary 1 follows directly from the proof of Theorem 1.

Corollary 1. *Let \mathcal{I} be a network coding instance that is $(\epsilon, \mathbf{R}, n)$ -feasible with a corresponding network code. The local edge removal statement holds on \mathcal{I} for edge e^* in \mathcal{I} and parameters $(\epsilon, \mathbf{R}, n)$ if there exists a subset $\mathcal{X}'_S \subseteq \mathcal{X}_S$ such that $\mathcal{X}'_S = \prod_{i \in \mathcal{S}} \mathcal{X}'_i$ for $\mathcal{X}'_i \subseteq \mathcal{X}_i$, with 1) X_{e^*} is constant conditioned on X'_S , 2) $|\mathcal{X}'_i| \geq \frac{|\mathcal{X}_i|}{|\mathcal{X}_{e^*}|}$ and 3) $|\mathcal{X}'_S \cap \mathcal{X}_S^G| \geq (1 - \epsilon)|\mathcal{X}'_S|$.*

Corollary 2 addresses Abelian group network codes which reproves Theorem 3 of [8] using the methodology of Theorem 1. The proof is given in Appendix.

Corollary 2. *Let \mathcal{I} be a network coding instance which is $(\epsilon, \mathbf{R}, n)$ -feasible for $\epsilon < \frac{1}{2}$ with a corresponding Abelian group network code $\{X_f : f \in \mathcal{S} \cup \mathcal{E}\}$. The edge removal statement holds on instance \mathcal{I} .*

Corollary 3 claims that the local edge removal statement holds on an edge e^* if the edge random variable X_{e^*} satisfies certain conditions. We may notice that here we only consider $\epsilon = 0$. The detailed discussion and proof are given in Appendix.

Corollary 3. *Let \mathcal{I} be a network coding instance which is $(0, \mathbf{R}, n)$ -feasible with a corresponding network code $\{X_f : f \in \mathcal{S} \cup \mathcal{E}\}$. The local edge removal statement holds on instance \mathcal{I} , edge e^* , and parameters $(0, \mathbf{R}, n)$ if $H(X_S | X_{e^*}) = \sum_{i \in \mathcal{S}} H(X_i | X_{e^*})$.*

IV. CWL FUNCTIONS

In this work we consider the following special family of encoding functions.

Definition 1 (Coordinate-wise linear). *For any $e \in \mathcal{E}$, a global encoding function $\phi_{ge} : (\mathcal{X}_1, \dots, \mathcal{X}_{|\mathcal{S}|}) \mapsto \mathcal{X}_e$ is called coordinate-wise linear (CWL) if and only if there exist finite groups $\{G_f : f \in \mathcal{S} \cup \{e\}\}$, with group operation “ $\overset{f}{\circ}$ ” defined on G_f , where $G_f = \mathcal{X}_f$ for $f \in \mathcal{S}$ and $G_e = \text{support}(\phi_{ge}) \subseteq \mathcal{X}_e$ is the support of ϕ_{ge} , such that ϕ_{ge} is a homomorphism from $G_S = \prod_{i \in \mathcal{S}} G_i$ to G_e . Namely, for every $(x_1, \dots, x_{|\mathcal{S}|})$ and $(x'_1, \dots, x'_{|\mathcal{S}|})$ we have $\phi_{ge}(x_1 \overset{1}{\circ} x'_1, \dots, x_{|\mathcal{S}|} \overset{|\mathcal{S}|}{\circ} x'_{|\mathcal{S}|}) = \phi_{ge}(x_1, \dots, x_{|\mathcal{S}|}) \overset{e}{\circ} \phi_{ge}(x'_1, \dots, x'_{|\mathcal{S}|})$.*

In the context of CWL functions, for any $f \in \mathcal{S} \cup \{e\}$, we denote the identity elements of G_f as \mathbf{i}_f . For any $\alpha \subseteq \mathcal{S}$, we define $x_\alpha = (x_i)_{i \in \alpha}$ and $G_\alpha = \prod_{i \in \alpha} G_i$. We denote the source message vector $(\mathbf{i}_1, \dots, x_i, \dots, \mathbf{i}_{|\mathcal{S}|})$ (with x_i in the i th coordinate and identity elements on all other coordinates) as $(x_i, \mathbf{i}_{\mathcal{S} \setminus i})$. In addition, we define $x_S \overset{1}{\circ} x'_S = (x_1 \overset{1}{\circ} x'_1), \dots, (x_{|\mathcal{S}|} \overset{|\mathcal{S}|}{\circ} x'_{|\mathcal{S}|})$ and sometimes omit the label on the operation “ \circ ”. We define $\ker \phi_{ge} = \{x_S \in G_S : \phi_{ge}(x_S) = \mathbf{i}_e\}$ and $A(x_e) = \{x_S \in G_S : \phi_{ge}(x_S) = x_e\}$.

Remark: It is important to understand the relationship between CWL encoding functions and group characterizable encoding functions (see, for example, [15]). In group characterizable encoding functions as in CWL functions, the random variables involved are characterized by a collection of groups. However, the characterization differs in that, in group characterizable functions the support of the variables involved are associated with certain co-sets of the corresponding groups while in CWL functions they are associated with the group elements themselves. Nevertheless, CWL functions are a special case of group characterizable functions (see the Appendix for a detailed proof). We note that while [8] proves the edge removal statement for Abelian group codes, the

CWL functions assumed here do not necessarily correspond to Abelian groups.

A. CWL functions satisfy Theorem 1

We now show that CWL functions satisfy the local sufficient condition specified by Theorem 1. Our proof conceptually follows ideas appearing in [2], which addresses edge removal in the context of linear codes.

Theorem 2. *Let \mathcal{I} be $(\epsilon, \mathbf{R}, n)$ -feasible with a corresponding network code $\{X_f : f \in \mathcal{S} \cup \mathcal{E}\}$. The local edge removal statement holds on \mathcal{I} for edge e^* and parameters $(\epsilon, \mathbf{R}, n)$ if the global encoding function ϕ_{ge^*} on edge $e^* \in \mathcal{E}$ is CWL.*

Proof of Theorem 2. Let $\{G_f : f \in \mathcal{S} \cup e^*\}$ be the groups corresponding to ϕ_{ge^*} . Using ϕ_{ge^*} , we define a random variable Y and show that Y satisfies the conditions of Theorem 1. For each i , we start by partitioning the set G_i into subsets. The number of subsets n_i in our partition of G_i determines $\mathcal{Y}_i = [n_i]$. The support set \mathcal{Y} of Y is set to $\prod_{i \in \mathcal{S}} \mathcal{Y}_i$. For each i , consider the equivalence relation $x_i \overset{i}{\sim} x'_i$ in which two elements of G_i are equivalent if and only if $\phi_{ge^*}(x_i, \mathbf{i}_{\mathcal{S} \setminus i}) = \phi_{ge^*}(x'_i, \mathbf{i}_{\mathcal{S} \setminus i})$. Each G_i is partitioned according the equivalence relation $\overset{i}{\sim}$. Denote the partition of G_i by sets $A_i(1), \dots, A_i(n_i)$. Now, $Y = Y_S$ is defined using a deterministic function f_Y of X_S that maps each $(x_1, \dots, x_{|\mathcal{S}|})$ to the corresponding $y_S = (y_1, \dots, y_{|\mathcal{S}|})$ for which $x_i \in A_i(y_i)$. The pre-image $A(y_S)$ of y_S under mapping f_Y is the product set $\prod_{i \in \mathcal{S}} A_i(y_i)$ of \mathcal{X}_S .

Notice that for any $x_S = (x_1, \dots, x_{|\mathcal{S}|})$, $x'_S = (x'_1, \dots, x'_{|\mathcal{S}|})$ in the pre-image $A(y_S)$ of $y_S = (y_1, \dots, y_{|\mathcal{S}|})$ it holds that $\phi_{ge^*}(x_S) = \phi_{ge^*}(x'_S)$. This follows from the fact that ϕ_{ge^*} is CWL. Namely, $\phi_{ge^*}(x_1, \dots, x_{|\mathcal{S}|}) = \phi_{ge^*}(x_1, \mathbf{i}_{\mathcal{S}-1}) \overset{1}{\circ} \dots \overset{|\mathcal{S}|}{\circ} \phi_{ge^*}(x_{|\mathcal{S}|}, \mathbf{i}_{\mathcal{S}-|\mathcal{S}|}) = \phi_{ge^*}(x'_1, \mathbf{i}_{\mathcal{S}-1}) \overset{1}{\circ} \dots \overset{|\mathcal{S}|}{\circ} \phi_{ge^*}(x'_{|\mathcal{S}|}, \mathbf{i}_{\mathcal{S}-|\mathcal{S}|}) = \phi_{ge^*}(x'_1, \dots, x'_{|\mathcal{S}|})$. Thus, for any $y_S = (y_1, \dots, y_{|\mathcal{S}|})$, the value of X_{e^*} conditioned on y_S is fixed. This in turn implies condition (A) in Theorem 1.

By our definition of Y , for every y_S , the pre-image $A(y_S)$ of f_Y is the product set $\prod_{i \in \mathcal{S}} A_i(y_i)$ of \mathcal{X}_S . This implies that $H(X_S | Y = y_S) = \sum_{i \in \mathcal{S}} H(X_i | Y = y_S)$, which in turn implies condition (B) in Theorem 1.

Before studying condition (C) in Theorem 1 we present the following technical lemma.

Lemma 1. *For any $i \in \mathcal{S}$ and for any $y_i, \bar{y}_i \in \mathcal{Y}_i$ it holds that $|A_i(y_i)| = |A_i(\bar{y}_i)|$.*

Proof. Let $y_i \in \mathcal{Y}_i$ and fix $\bar{y}_i \in \mathcal{Y}_i$ to be such that $\phi_{ge^*}(\delta_i, \mathbf{i}_{\mathcal{S} \setminus i}) = \mathbf{i}_{e^*}$ for all $\delta_i \in A_i(\bar{y}_i)$. As y_i is any element of \mathcal{Y}_i , it suffices to show that $|A_i(y_i)| = |A_i(\bar{y}_i)|$. Fix any $x_i \in A_i(y_i)$ and let $x_{e^*} = \phi_{ge^*}(x_i, \mathbf{i}_{\mathcal{S} \setminus i})$. As function ϕ_{ge^*} is CWL, for any $\delta_i \in A_i(\bar{y}_i)$ we have $\phi_{ge^*}(x_i \overset{i}{\circ} \delta_i, \mathbf{i}_{\mathcal{S} \setminus i}) = \phi_{ge^*}(x_i, \mathbf{i}_{\mathcal{S} \setminus i}) \overset{i}{\circ} \phi_{ge^*}(\delta_i, \mathbf{i}_{\mathcal{S} \setminus i}) = x_{e^*} \overset{i}{\circ} \mathbf{i}_{e^*} = x_{e^*}$. Thus, $x_i \overset{i}{\circ} \delta_i \in A_i(y_i)$, implying that $|A_i(y_i)| \geq |A_i(\bar{y}_i)|$.

Fix any $x_i \in A_i(y_i)$. By the discussion above, for any $\delta_i \in A_i(\bar{y}_i)$ we have $x_i \overset{i}{\circ} \delta_i \in A_i(y_i)$. If $|A_i(y_i)| > |A_i(\bar{y}_i)|$, there exists $x'_i \in A_i(y_i)$ such that $x'_i \neq x_i \overset{i}{\circ} \delta_i$ for any $\delta_i \in A_i(\bar{y}_i)$.

In other words, there exists $x'_i = x_i \circ \delta'_i \in A_i(y_i)$ and $\delta'_i \in G_i \setminus A_i(\bar{y}_i)$.

Then we have $x_{e^*} = \phi_{ge^*}(x_i \circ \delta'_i, \mathbf{i}_{S \setminus i}) = \phi_{ge^*}(x_i, \mathbf{i}_{S \setminus i}) \circ \phi_{ge^*}(\delta'_i, \mathbf{i}_{S \setminus i}) = x_{e^*} \circ \phi_{ge^*}(\delta'_i, \mathbf{i}_{S \setminus i}) \neq x_{e^*}$ which gives a contradiction. Accordingly, for any $y_i \in \mathcal{Y}_i$, $|A_i(y_i)| = |A_i(\bar{y}_i)|$. \square

Lemma 1 implies that for all $y_S \in \mathcal{Y}$ the size of the set $A(y_S)$ is identical. By the assumption of the theorem, there exist at least $(1 - \epsilon)|G_S|$ “good” elements in G_S . Thus, by an averaging argument, there exists some $y' = y'_S \in \mathcal{Y}$ such that

$$\frac{|A^G(y')|}{|A(y')|} \geq (1 - \epsilon). \quad (6)$$

Here $A^G(y') = \{x_S \in A(y') : x_S \text{ is good}\}$. Equation (6) satisfies the second part of condition (C) in Theorem 1. For the first part of condition (C), our definitions imply $|\mathcal{Y}_i| \leq |G_{e^*}|$. In addition, $\cup_{y_i \in \mathcal{Y}_i} A_i(y_i) = G_i$. Thus, by Lemma 1, $|A_i(y')| \geq |G_i|/|G_{e^*}|$. Here, for $y' = (y'_1, \dots, y'_S)$, $A_i(y') = A_i(y'_i)$. This suffices to prove our assertion. \square

B. Piece-wise CWL

Definition 2 (Piece-wise CWL). *For any $e \in \mathcal{E}$, a global encoding function ϕ_{ge} is called K -piece-wise CWL if and only if there exists a set of CWL functions $\{\phi_{ge}^{(k)} : k \in [K]\}$, all over groups $\{G_i : i \in \mathcal{S}\}$ and G_e , and a partition $\{S^{(k)} : k \in [K]\}$ of $\prod_{i \in \mathcal{S}} G_i$ such that $\phi_{ge}(x_1, \dots, x_{|\mathcal{S}|}) = \phi_{ge}^{(k)}(x_1, \dots, x_{|\mathcal{S}|})$ if and only if $(x_1, \dots, x_{|\mathcal{S}|}) \in S^{(k)}$.*

We now study piece-wise CWL function in the context of edge-removal. We show below that a certain structured class of piece-wise CWL functions implies a slightly relaxed local edge-removal statement. The theorem is limited to the 0-error setting. We discuss this limitation and give the proof in the Appendix.

Theorem 3. *Let $\mathcal{I} = (\mathcal{N}, \mathcal{S}, \mathcal{T}, \mathcal{M})$ be a network coding instance which is $(0, \mathbf{R}, n)$ -feasible with a corresponding network code that has a global encoding function ϕ_{ge^*} on a given edge e^* which is K -piece-wise CWL. Let $\mathcal{I}' = (\mathcal{N}', \mathcal{S}, \mathcal{T}, \mathcal{M})$ be a new instance obtained by removing the edge e^* from the network \mathcal{N} . If for every $k \in [K]$, the sub-domain $S^{(k)}$ of $\phi_{ge^*}^{(k)}$ equals a product space $\prod_{i \in \mathcal{S}} S_i^{(k)}$, then \mathcal{I}' is $(0, \mathbf{R}', n)$ -feasible, where $\mathbf{R}' = (R'_i)_{i \in \mathcal{S}}$ and $R'_i \geq R_i - R_{e^*} - (\log K)/n$.*

V. ON PROVING THE EDGE-REMOVAL STATEMENT THROUGH THE LOCAL LENS OF CWL FUNCTIONS

In this section we explore the possibility of proving the edge-removal statement through the local lens of CWL functions. Namely, we observe, via Theorem 2, that the following CWL statement, if true, implies the edge-removal statement.

Statement 2 (CWL statement). *Let \mathcal{I} be $(\epsilon, \mathbf{R}, n)$ -feasible. Let e^* be an edge in \mathcal{I} . Then there exists an $(\epsilon, \mathbf{R}, n)$ coding scheme for \mathcal{I} whose global encoding function on e^* is CWL.*

For any instance \mathcal{I} for which linear encoding functions are optimal, the CWL statement (Statement 2) above clearly holds.

We thus turn to study the validity of the CWL statement on instances for which linear encoding functions are sub-optimal. For all previous works that we are aware of that present network coding instances that are $(\epsilon, \mathbf{R}, n)$ -feasible with non linear codes but not $(\epsilon, \mathbf{R}, n)$ -feasible with linear codes, we ask whether the CWL statement is true or not. Specifically, we ask if for any given edge e^* the non-linear $(\epsilon, \mathbf{R}, n)$ -feasible network code presented in these works can be modified to give an $(\epsilon, \mathbf{R}, n)$ -feasible scheme in which the encoding on edge e^* is CWL, implying that the CWL statement holds for the instance and rate vector under study. In the case studies from [14]–[16] we are able to modify the non-linear coding scheme appropriately, thus supporting the CWL statement. However we are not able to prove (or disprove) the same for the instance given in [17]. Details appear in the Appendix. Whether the CWL statement holds for all network coding instances (implying that the edge-removal statement holds) is left open in this work.

VI. CONCLUSION

In this work, we study the edge removal problem by taking a local perspective in which we focus solely on the function carried on the removed edge. Through our local perspective, we generalize (and unify) previous results by giving a sufficient condition that captures a broad range of settings including that of CWL and certain piece-wise CWL functions. We study the possibility in proving the edge-removal statement by modifying general coding solutions to have CWL encoding functions on a given edge e^* . Whether any network code can be modified as above remains open in this work, as does the correctness of the edge-removal statement.

ACKNOWLEDGMENT

Work supported in part by NSF grants CCF-1526771, CCF-1527524 and CCF-1817241.

REFERENCES

- [1] T. Ho, M. Effros, and S. Jalali, “On equivalence between network topologies,” in *IEEE Allerton Conference on Communication, Control, and Computing*, 2010, pp. 391–398.
- [2] S. Jalali, M. Effros, and T. Ho, “On the impact of a single edge on the network coding capacity,” in *IEEE Information Theory and Applications Workshop*, 2011, pp. 1–5.
- [3] M. Langberg and M. Effros, “Network coding: Is zero error always possible?” in *IEEE Allerton Conference on Communication, Control, and Computing*, 2011, pp. 1478–1485.
- [4] M. F. Wong, M. Langberg, and M. Effros, “On a capacity equivalence between network and index coding and the edge removal problem,” in *IEEE International Symposium on Information Theory (ISIT)*, 2013, pp. 972–976.
- [5] E. J. Lee, M. Langberg, and M. Effros, “Outer bounds and a functional study of the edge removal problem,” in *IEEE Information Theory Workshop*, 2013, pp. 1–5.
- [6] M. F. Wong, M. Effros, and M. Langberg, “On an equivalence of the reduction of k-unicast to 2-unicast capacity and the edge removal property,” in *IEEE International Symposium on Information Theory (ISIT)*, 2015, pp. 371–375.
- [7] —, “On tightness of an entropic region outer bound for network coding and the edge removal property,” in *IEEE International Symposium on Information Theory (ISIT)*, 2016, pp. 1769–1773.
- [8] F. Wei and M. Langberg, “The effect of removing a network communication edge: group network codes,” in *IEEE Allerton Conference on Communication, Control, and Computing*, 2017.

- [9] W. Gu, "On achievable rate regions for source coding over networks," Ph.D. dissertation, California Institute of Technology, 2009.
- [10] O. Kosut and J. Kliewer, "On the relationship between edge removal and strong converses," in *IEEE International Symposium on Information Theory (ISIT)*, 2016, pp. 1779–1783.
- [11] S. Kamath, N. David, and C.-C. Wang, "Two-unicast is hard," in *IEEE International Symposium on Information Theory (ISIT)*, 2014, pp. 2147–2151.
- [12] T. H. Chan and A. Grant, "Network coding capacity regions via entropy functions," *IEEE Transactions on Information Theory*, vol. 60, no. 9, pp. 5347–5374, 2014.
- [13] W. Kim, M. Langberg, and M. Effros, "A characterization of the capacity region for network coding with dependent sources," in *IEEE International Symposium on Information Theory (ISIT)*, 2016, pp. 1764–1768.
- [14] R. Dougherty, C. Freiling, and K. Zeger, "Insufficiency of linear coding in network information flow," *IEEE Transactions on Information Theory*, vol. 51, no. 8, pp. 2745–2759, 2005.
- [15] T. Chan and A. Grant, "Dualities between entropy functions and network codes," *IEEE Transactions on Information Theory*, vol. 54, no. 10, pp. 4470–4487, 2008.
- [16] J. Connelly and K. Zeger, "A class of non-linearly solvable networks," *IEEE Transactions on Information Theory*, vol. 63, no. 1, pp. 201–229, 2017.
- [17] A. Blasiak, R. Kleinberg, and E. Lubetzky, "Lexicographic products and the power of non-linear network coding," in *IEEE 52nd Annual Symposium on Foundations of Computer Science (FOCS)*, 2011, pp. 609–618.
- [18] R. W. Yeung, *Information theory and network coding*. Springer Science & Business Media, 2008.
- [19] J. Gallian, *Contemporary abstract algebra*. Cengage Learning, 2016.

APPENDIX

I. PROOF OF COROLLARY 2

We apply the model and definitions from [8].

Proof of Corollary 2. We show that for any edge $e^* \in \mathcal{E}$ there exists a random variable Y which satisfies all three conditions in Theorem 1, which implies that the edge removal statement holds on \mathcal{I} . By Theorem 4 proven later in the Appendix, for $\epsilon < \frac{1}{2}$, any network instance \mathcal{I} which is $(\epsilon, \mathbf{R}, n)$ -feasible by a group network code is also $(0, \mathbf{R}, n)$ -feasible. Thus, without loss of generality, in the following discussion let $\epsilon = 0$. For any edge $e^* \in \mathcal{E}$, the global encoding function ϕ_{ge^*} is Abelian group characterizable such that the edge message X_{e^*} and source messages $\{X_i : i \in \mathcal{S}\}$ can be characterized by a finite Abelian group G with subgroups G_{e^*} and $\{G_i : i \in \mathcal{S}\}$, respectively. Without loss of generality (see [8]) we assume $G_{\mathcal{S}} = \bigcap_{i \in \mathcal{S}} G_i = \{\mathbf{i}\}$, here \mathbf{i} is the identity element of G . Using ϕ_{ge^*} we define a random variable Y and show that Y satisfies the conditions in Theorem 1.

Let $H_i = \bigcap_{j \in \mathcal{S} \setminus i} G_j$, by the proof of Theorem 3 in [8], $G' = \prod_{i \in \mathcal{S}} (G_{e^*} \cap H_i) \subseteq G_{e^*}$ is an Abelian group. We define Y as the random variable characterized by G' . X_{e^*} is a deterministic function of Y (as $G' \subseteq G_{e^*}$). Thus condition (A) of Theorem 1 holds.

By the definition of group characterizable random variables (see [8]),

$$\begin{aligned} H(X_{\mathcal{S}}|Y) &= H(X_{\mathcal{S}}, Y) - H(Y) \\ &= \log \frac{|G|}{|G' \cap G_{\mathcal{S}}|} - \log \frac{|G|}{|G'|} \\ &= \log |G'|. \end{aligned} \quad (7)$$

Similarly for any $i \in \mathcal{S}$,

$$\begin{aligned} H(X_i|Y) &= H(X_i, Y) - H(Y) \\ &= \log \frac{|G|}{|G' \cap G_i|} - \log \frac{|G|}{|G'|} \\ &= \log \frac{|G'|}{|G' \cap G_i|}. \end{aligned} \quad (8)$$

By (27), (31) in [8] and (7), (8), we have $H(X_{\mathcal{S}}|Y) = \sum_{i \in \mathcal{S}} H(X_i|Y)$ which satisfies condition (B) of Theorem 1.

By our settings of group codes, $X_{\mathcal{S}}$ is characterized by the trivial subgroup $\{\mathbf{i}\}$ ($G_{\mathcal{S}} = \{\mathbf{i}\}$). Note that \mathcal{Y} is the set of cosets of G' in G . The function f_Y takes as input $x_{\mathcal{S}} \in G$ (a coset of \mathbf{i}) and outputs y , the coset of G' which contains $x_{\mathcal{S}}$. Such that, $A(y) = y$ and $A_i(y)$ is the set of cosets of $G' \cap G_i$ contained in $A(y)$. By Lagrange's Theorem we have $|A_i(y)| = \frac{|G'|}{|G' \cap G_i|}$, $|\mathcal{X}_i| = \frac{|G|}{|G_i|}$ and $|\mathcal{X}_{e^*}| = \frac{|G|}{|G_{e^*}|}$. By the proof of Theorem 3 in [8], we have

$$\log \frac{|G'|}{|G_i \cap G'|} \geq \log \frac{|G_{e^*}|}{|G_i|}.$$

Accordingly, $|A_i(y)| \geq |\mathcal{X}_i|/|\mathcal{X}_{e^*}|$. Since here $\epsilon = 0$, condition (C) of Theorem 1 holds.

We have shown that for a network instance \mathcal{I} which is $(\epsilon, \mathbf{R}, n)$ -feasible by Abelian group network codes, the local edge removal statement holds on every edge e^* in \mathcal{I} which implies the edge removal statement on \mathcal{I} . \square

II. PROOF OF COROLLARY 3

Here we prove that the local edge removal statement holds on edge e^* when the edge random variable on e^* satisfies certain conditions. The proof of Corollary 3 is limited to the 0-error case. Roughly speaking, our proof does not naturally extend to the ϵ -error case due to our use of an averaging argument on $A(x'_{e^*})$. To prove Corollary 3 for ϵ -error one could need the averaging argument to preserve error, which is not necessarily the case.

Proof of Corollary 3. Here we replace the random variable Y with X_{e^*} , since X_{e^*} is a function of itself, the function f_Y in the definition of $A(Y)$ and $A_i(Y)$ is the global encoding function ϕ_{ge^*} . Let $A(x_{e^*}) = \{x_{\mathcal{S}} : x_{e^*} = \phi_{ge^*}(x_{\mathcal{S}})\}$, $A_i(x_{e^*}) = \{x_i \in \mathcal{X}_i : \exists x_{\mathcal{S}} \in A(x_{e^*}), x_{\mathcal{S}}(i) = x_i\}$. Here $x_{\mathcal{S}}(i)$ denotes the i th entry of vector $x_{\mathcal{S}}$.

Set $Y = X_{e^*}$, Condition (A) and (B) in Theorem 1 hold immediately. By an averaging argument, there exists $x'_{e^*} \in \mathcal{X}_{e^*}$ such that $|A(x'_{e^*})| \geq |\mathcal{X}_{\mathcal{S}}|/|\mathcal{X}_{e^*}|$. By definitions and the proof of Theorem 1, we have $|A(x'_{e^*})| = \prod_{i \in \mathcal{S}} |A_i(x'_{e^*})|$ and $|\mathcal{X}_{\mathcal{S}}| = \prod_{i \in \mathcal{S}} |\mathcal{X}_i|$, such that $|A_i(x'_{e^*})| \geq |\mathcal{X}_i|/|\mathcal{X}_{e^*}|$ for any $i \in \mathcal{S}$. Combined with the fact that $\epsilon = 0$, the condition (C) in Theorem 1 holds, which suffice to prove our assertion. \square

III. A CLAIM REGARDING CWL FUNCTIONS

Claim 1. *Let \mathcal{I} be a network coding instance. For edge $e \in \mathcal{E}$, if the global encoding function ϕ_{ge} on e is CWL, then it is group characterizable (but not necessarily Abelian group characterizable).*

Proof. Recall that for CWL functions the alphabet of each source $i \in \mathcal{S}$ is a group G_i and the edge message alphabet is a group G_e . Define $G' = G_1 \times \dots \times G_{|\mathcal{S}|}$ and $G'_i = G_1 \times \dots \times \{\mathbf{i}_i\} \times \dots \times G_{|\mathcal{S}|}$ for any $i \in \mathcal{S}$. Also, for $\alpha \subseteq \mathcal{S}$, let $G'_\alpha = \bigcap_{i \in \alpha} G'_i = \prod_{i \in \mathcal{S} \setminus \alpha} G_i \times \prod_{i \in \alpha} \{\mathbf{i}_i\}$. By [19], we know that $\{G'_\alpha : \alpha \subseteq \mathcal{S}\}$ are subgroups of G' . In what follows we use “.”, “o” to denote the binary group operations on G' , G_e , respectively.

Here, and in what follows all products of the form $\prod_{i \in \alpha} g_i$ for $\alpha \subseteq \mathcal{S}$ are ordered by the natural ordering of $\mathcal{S} = \{1, \dots, |\mathcal{S}|\}$.

With the definition of group homomorphism ϕ_{g_e} in Section IV, we define $G'_e = \phi_{g_e}^{-1}(\mathbf{i}_e)$. We first show that G'_e is a subgroup of G' . For any $a, b \in G'_e$, $\phi_{g_e}(a \cdot b) = \phi_{g_e}(a) \circ \phi_{g_e}(b) = \mathbf{i}_e$. Thus, G'_e is closed. Let $\mathbf{i}' = (\mathbf{i}_i)_{i \in \mathcal{S}} \in G'$. For any $a \in G'_e$ we have $\phi_{g_e}(a) = \phi_{g_e}(\mathbf{i}' \cdot a) = \phi_{g_e}(a \cdot \mathbf{i}') = \mathbf{i}_e \circ \phi_{g_e}(\mathbf{i}') = \mathbf{i}_e$, therefore $\mathbf{i}' \in G'_e$ and G'_e has an identity element. Let $b \in G'$ and b^{-1} be the inverse of b in G' . By our definitions, $\phi_{g_e}(\mathbf{i}') = \phi_{g_e}(b \cdot b^{-1}) = \phi_{g_e}(b) \circ \phi_{g_e}(b^{-1}) = \mathbf{i}_e \circ \phi_{g_e}(b^{-1}) = \mathbf{i}_e$ which implies $\phi_{g_e}(b^{-1}) = \mathbf{i}_e$, $b^{-1} \in G'_e$, and G'_e has inverse elements. Thus G'_e is a subgroup of G' .

Lemma 2. *Let ϕ_{g_e} be a group homomorphism from G to G_e , $|\phi_{g_e}^{-1}(g_e)| = |\phi_{g'_e}^{-1}(g'_e)|$ for any $g_e \neq g'_e \in G_e$. And $\{\phi_{g_e}^{-1}(g_e) : g_e \in G_e\}$ are cosets of G'_e .*

Proof. For any $g_e \neq g'_e \in G_e$, let $g \in \phi_{g_e}^{-1}(g_e)$ and $g' \in \phi_{g'_e}^{-1}(g'_e)$. Let $\delta \in G$ satisfy $g \cdot \delta = g'$, then $\phi_{g_e}(g \cdot \delta) = \phi_{g_e}(g) \circ \phi_{g_e}(\delta) = g'_e$, which implies $\phi_{g_e}(\delta) = g_e^{-1} \circ g'_e$. Now, for any $g'' \in \phi_{g_e}^{-1}(g_e)$, as $\phi_{g_e}(g'' \cdot \delta) = \phi_{g_e}(g'') \circ \phi_{g_e}(\delta) = g_e \circ g_e^{-1} \circ g'_e = g'_e$, we have $g'' \cdot \delta \in \phi_{g'_e}^{-1}(g'_e)$, such that $\{g'' \cdot \delta : g'' \in \phi_{g_e}^{-1}(g_e)\} \subseteq \phi_{g'_e}^{-1}(g'_e)$. Since $|\{g'' \cdot \delta : g'' \in \phi_{g_e}^{-1}(g_e)\}| = |\phi_{g_e}^{-1}(g_e)|$, we have $|\phi_{g_e}^{-1}(g_e)| \leq |\phi_{g'_e}^{-1}(g'_e)|$. Similarly, $|\phi_{g'_e}^{-1}(g'_e)| \geq |\phi_{g_e}^{-1}(g_e)|$, thus $|\phi_{g_e}^{-1}(g_e)| = |\phi_{g'_e}^{-1}(g'_e)|$. Since we have $|G_e|$ preimages sets, we have $|\phi_{g_e}^{-1}(g_e)| = \frac{|G'|}{|G_e|}$ for any $g_e \in G_e$.

Let $g \in \phi_{g_e}^{-1}(g_e)$, let $gG'_e = \{g \cdot g'_e : g'_e \in G'_e\}$. For any $g' \in gG'_e$, $\phi_{g_e}(g') = \phi_{g_e}(g) \circ \mathbf{i}_e = g_e$. Thus $gG'_e \subseteq \phi_{g_e}^{-1}(g_e)$. By Lagrange's Theorem, we have $|gG'_e| = \frac{|G'|}{|G_e|} = |\phi_{g_e}^{-1}(g_e)|$, such that $gG'_e = \phi_{g_e}^{-1}(g_e)$. In other words, for any $g_e \in G_e$, $\phi_{g_e}^{-1}(g_e)$ is a coset of G'_e with

$$|\phi_{g_e}^{-1}(g_e)| = |G'_e|. \quad (9)$$

□

To show that $\{G'_\alpha : \alpha \subseteq \mathcal{S} \cup \{e\}\}$ is a group characterization of ϕ_{g_e} , we need to show that $H(X_\alpha) = \log \frac{|G'|}{|G'_\alpha|}$ for any $\alpha \subseteq \mathcal{S} \cup \{e\}$. Here $G'_\alpha = \bigcap_{f \in \alpha} G'_f$.

For any $\alpha \subseteq \mathcal{S}$, recall that $G_\alpha = \prod_{f \in \alpha} G_f$ and in what follows we denote $\bar{\alpha} = \mathcal{S} \setminus \alpha$, $\mathbf{i}_\alpha = (\mathbf{i}_i)_{i \in \alpha}$. By our definitions $G_{\bar{\alpha}} = \prod_{i \in \mathcal{S} \setminus \alpha} G_i$ and $G' = G_\alpha \times G_{\bar{\alpha}}$.

By our definitions, we have $|G_\alpha| |G'_\alpha| = |G'|$ implying that

$$H(X_\alpha) = \log |G_\alpha| = \log \frac{|G'|}{|G'_\alpha|}.$$

In addition $|G'_e| = \frac{|G'|}{|G_e|}$ implying that

$$H(X_e) = \log |G_e| = \log \frac{|G'|}{|G'_e|}. \quad (10)$$

We now show that $X_{\alpha, e}$ is group characterizable, where $\alpha \subseteq \mathcal{S}$. We first prove that

$$\begin{aligned} H(X_\alpha | X_e) &= \sum_{g_e \in G_e} \Pr(X_e = g_e) H(X_\alpha | X_e = g_e) \\ &\stackrel{(a)}{=} H(X_\alpha | X_e = \mathbf{i}_e) \\ &\stackrel{(b)}{=} \log \frac{|\phi_{g_e}^{-1}(\mathbf{i}_e)|}{|\phi_{g_e}^{-1}(\mathbf{i}_e) \cap \{\mathbf{i}_\alpha \times G_{\bar{\alpha}}\}|} \\ &\stackrel{(c)}{=} \log \frac{|G'_e|}{|G'_e \cap G'_\alpha|}. \end{aligned} \quad (11)$$

By the uniformity of source random variables and by (9), we have

$$\begin{aligned} \Pr(X_e = g_e) &= \sum_{g_S \in \phi_{g_e}^{-1}(g_e)} \Pr(X_S = g_S) \\ &= \frac{|G'_e|}{|G'|} = \frac{1}{|G_e|} \end{aligned} \quad (12)$$

for any $g_e \in G_e$.

Let $\mathcal{Y}_i = \{g_e \in G_e : g_e = \phi_{g_e}(g_i, \mathbf{i}_{\mathcal{S} \setminus i}), g_i \in G_i\}$. For any $g_e \in \mathcal{Y}_i$, we define $A_i(g_e) = \{g_i \in G_i : \phi_{g_e}(g_i, \mathbf{i}_{\mathcal{S} \setminus i}) = g_e\}$ which is a subset of G_i . We partition G_i into subsets $\{A_i(g_e) : g_e \in \mathcal{Y}_i\}$. By Lemma 1, for any $g'_{e,i} \neq g''_{e,i} \in \mathcal{Y}_i$, we have $|A_i(g'_{e,i})| = |A_i(g''_{e,i})|$. For any $\alpha \subseteq \mathcal{S}$, let

$$\mathcal{Y}_\alpha = \left\{ \prod_{i \in \alpha} g_{e,i} : g_{e,i} \in \mathcal{Y}_i, i \in \alpha \right\}.$$

Note that $\mathcal{Y}_\alpha \subseteq G_e$. For any $g_{e,\alpha} \in \mathcal{Y}_\alpha$, we define

$$A_\alpha(g_{e,\alpha}) = \left\{ \prod_{i \in \alpha} A_i(g_{e,i}) : \prod_{i \in \alpha} g_{e,i} = g_{e,\alpha} \right\}.$$

As $A_i(g_{e,i}) \subset G_i$ for each $i \in \alpha$, $A_\alpha(g_{e,\alpha})$ is a subset of $G_\alpha = \prod_{i \in \alpha} G_i$.

Lemma 3. *For any $\alpha \subseteq \mathcal{S}$ and $g_{e,\alpha} \in \mathcal{Y}_\alpha$, we have $g_{e,\alpha}^{-1} \in \mathcal{Y}_\alpha$.*

Proof. As $\phi_{g_e}(\mathbf{i}_S) = \phi_{g_e}(\mathbf{i}_S \cdot \mathbf{i}_S) = \phi_{g_e}(\mathbf{i}_S) \circ \phi_{g_e}(\mathbf{i}_S)$, we have

$$\phi_{g_e}(\mathbf{i}_S) = \mathbf{i}_e. \quad (13)$$

Let $g_{e,\alpha} \in \mathcal{Y}_\alpha$ and $g_\alpha \in G_\alpha$, such that $\phi_{g_e}(g_\alpha, \mathbf{i}_{\bar{\alpha}}) = g_{e,\alpha}$. By our definition $g_\alpha = (g_i)_{i \in \alpha}$, define $g_\alpha^{-1} = (g_i^{-1})_{i \in \alpha}$ where $g_i \in G_i$. We have

$$\begin{aligned} \phi_{g_e}(\mathbf{i}_S) &= \phi_{g_e}(g_\alpha \cdot g_\alpha^{-1}, \mathbf{i}_{\bar{\alpha}}) \\ &= \phi_{g_e}(g_\alpha, \mathbf{i}_{\bar{\alpha}}) \circ \phi_{g_e}(g_\alpha^{-1}, \mathbf{i}_{\bar{\alpha}}) \\ &= g_{e,\alpha} \circ \phi_{g_e}(g_\alpha^{-1}, \mathbf{i}_{\bar{\alpha}}). \end{aligned}$$

Thus $\phi_{g_e}(g_\alpha^{-1}, \mathbf{i}_{\bar{\alpha}}) = \prod_{i \in \alpha} \phi_{g_e}(g_i^{-1}, \mathbf{i}_{\mathcal{S} \setminus i}) = g_{e,\alpha}^{-1}$ implying $g_{e,\alpha}^{-1} \in \mathcal{Y}_\alpha$. □

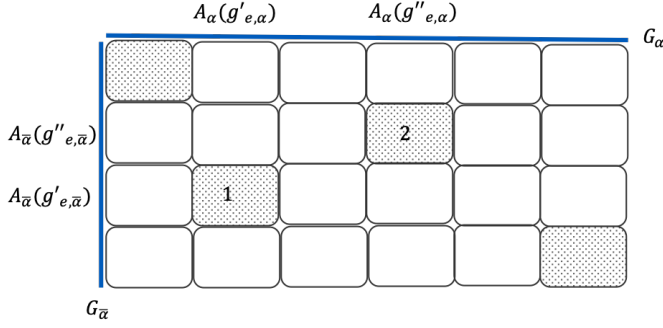


Fig. 1. An example depicting the proof of Lemma 4. The dark blocks represent the set $\phi_{g_e}^{-1}(g_e)$. Block 1 represents $A_\alpha(g'_{e,\alpha}) \times A_{\bar{\alpha}}(g'_{e,\bar{\alpha}})$ and Block 2 represents $A_\alpha(g''_{e,\alpha}) \times A_{\bar{\alpha}}(g''_{e,\bar{\alpha}})$.

Let $g'_{e,\alpha} \neq g''_{e,\alpha} \in \mathcal{Y}_\alpha$. By Lemma 3 we have $g'_{e,\alpha} \in \mathcal{Y}_\alpha$. Let $g'_\alpha, g''_\alpha \in G_\alpha$, such that $\phi_{g_e}(g'_\alpha, \mathbf{i}_\alpha) = g'_{e,\alpha}$ and $\phi_{g_e}(g''_\alpha, \mathbf{i}_\alpha) = g''_{e,\alpha}$. Define $\delta = g'_\alpha \cdot g''_\alpha$, such that

$$\phi_{g_e}(\delta, \mathbf{i}_\alpha) = \phi_{g_e}(g'_\alpha, \mathbf{i}_\alpha) \circ \phi_{g_e}(g''_\alpha, \mathbf{i}_\alpha) = g'_{e,\alpha} \circ g''_{e,\alpha}.$$

Let $g_\alpha \in A_\alpha(g'_{e,\alpha})$. As $\phi_{g_e}(g_\alpha \cdot \delta, \mathbf{i}_\alpha) = \phi_{g_e}(g_\alpha, \mathbf{i}_\alpha) \circ \phi_{g_e}(\delta, \mathbf{i}_\alpha) = g'_{e,\alpha} \circ g'_{e,\alpha} \circ g''_{e,\alpha} = g''_{e,\alpha}$, we have $\{g_\alpha \cdot \delta : g_\alpha \in G_\alpha\} \subseteq A_\alpha(g''_{e,\alpha})$. As $|A_\alpha(g'_{e,\alpha})| = |\{g_\alpha \cdot \delta : g_\alpha \in A_\alpha(g'_{e,\alpha})\}|$, we have $|A_\alpha(g'_{e,\alpha})| \leq |A_\alpha(g''_{e,\alpha})|$. Similarly, we can prove $|A_\alpha(g'_{e,\alpha})| \geq |A_\alpha(g''_{e,\alpha})|$. Thus, for $\alpha \subseteq \mathcal{S}$,

$$|A_\alpha(g'_{e,\alpha})| = |A_\alpha(g''_{e,\alpha})| \quad (14)$$

for any $g'_{e,\alpha} \neq g''_{e,\alpha} \in \mathcal{Y}_\alpha$.

By the definitions above, we can partition G' into cells. Namely, for any $\alpha \subseteq \mathcal{S}$ and $\bar{\alpha} = \mathcal{S} \setminus \alpha$, each cell is a subset $A_\alpha(g_{e,\alpha}) \times A_{\bar{\alpha}}(g_{e,\bar{\alpha}})$, where $g_{e,\alpha} \in \mathcal{Y}_\alpha$ and $g_{e,\bar{\alpha}} \in \mathcal{Y}_{\bar{\alpha}}$.

Lemma 4. *Let $g_e \in G_e$. Let $A_\alpha(g'_{e,\alpha}) \times A_{\bar{\alpha}}(g'_{e,\bar{\alpha}})$ and $A_\alpha(g''_{e,\alpha}) \times A_{\bar{\alpha}}(g''_{e,\bar{\alpha}})$ be two disjoint cells in $\phi_{g_e}^{-1}(g_e)$. Let $g'_{e,\alpha}, g''_{e,\alpha} \in \mathcal{Y}_\alpha$, $g'_{e,\bar{\alpha}}, g''_{e,\bar{\alpha}} \in \mathcal{Y}_{\bar{\alpha}}$, such that $(g'_{e,\alpha}, g'_{e,\bar{\alpha}}) \neq (g''_{e,\alpha}, g''_{e,\bar{\alpha}})$ and $g'_{e,\alpha} \circ g'_{e,\bar{\alpha}} = g''_{e,\alpha} \circ g''_{e,\bar{\alpha}} = g_e$. We have that $g'_{e,\alpha} \neq g''_{e,\alpha}$ and $g'_{e,\bar{\alpha}} \neq g''_{e,\bar{\alpha}}$.*

Proof. The proof is depicted in Figure 1.

Assume $g'_{e,\alpha} = g''_{e,\alpha}$, as $g'_{e,\alpha} \circ g'_{e,\bar{\alpha}} = g''_{e,\alpha} \circ g''_{e,\bar{\alpha}} = g_e$, we have $g'_{e,\bar{\alpha}} = g''_{e,\bar{\alpha}}$. This contradicts the assumption that $(g'_{e,\alpha}, g'_{e,\bar{\alpha}}) \neq (g''_{e,\alpha}, g''_{e,\bar{\alpha}})$. \square

We now show that for any cell $A_\alpha(g_{e,\alpha}) \times A_{\bar{\alpha}}(g_{e,\bar{\alpha}})$,

$$\begin{aligned} |A_{\bar{\alpha}}(g_{e,\bar{\alpha}})| &\stackrel{(a)}{=} |A_{\bar{\alpha}}(\mathbf{i}_e)| \\ &\stackrel{(b)}{=} |\phi_{g_e}^{-1}(\mathbf{i}_e) \cap \{\mathbf{i}_\alpha \times G_{\bar{\alpha}}\}|. \end{aligned} \quad (15)$$

By (13) we have $\phi_{g_e}(\mathbf{i}_i, \mathbf{i}_{\mathcal{S} \setminus i}) = \mathbf{i}_e$. As $\mathbf{i}_i \in G_i$, by the definition of \mathcal{Y}_i , we know that $\mathbf{i}_e \in \mathcal{Y}_i$. With the definition of \mathcal{Y}_α , we have $\prod_{i \in \alpha} \mathbf{i}_e = \mathbf{i}_e \in \mathcal{Y}_\alpha$. By (14), equation (a) of (15) holds. With our definitions, for any $g_e \in G_e$, we have

$$\phi_{g_e}^{-1}(g_e) = \{A_\alpha(g_{e,\alpha}) \times A_{\bar{\alpha}}(g_{e,\bar{\alpha}}) : g_{e,\alpha} \circ g_{e,\bar{\alpha}} = g_e\}. \quad (16)$$

As $\mathbf{i}_e \in \mathcal{Y}_\alpha$ for any $\alpha \subseteq \mathcal{S}$ and as $\mathbf{i}_e \circ \mathbf{i}_e = \mathbf{i}_e$, by (16) we have $A_\alpha(\mathbf{i}_e) \times A_{\bar{\alpha}}(\mathbf{i}_e) \subset \phi_{g_e}^{-1}(\mathbf{i}_e)$. By Lemma 4, $A_\alpha(\mathbf{i}_e) \times$

$A_{\bar{\alpha}}(\mathbf{i}_e)$ is the only cell in $\phi_{g_e}^{-1}(\mathbf{i}_e)$ with $g_{e,\alpha} = \mathbf{i}_e \in \mathcal{Y}_\alpha$ or $g_{e,\bar{\alpha}} = \mathbf{i}_e \in \mathcal{Y}_{\bar{\alpha}}$. The size of $A_{\bar{\alpha}}(\mathbf{i}_e)$ is exactly the projection of the cell $A_\alpha(\mathbf{i}_e) \times A_{\bar{\alpha}}(\mathbf{i}_e)$ onto $G_{\bar{\alpha}}$. Which by Lemma 4 is exactly the intersection of $(\mathbf{i}_\alpha \times G_{\bar{\alpha}})$ and $\phi_{g_e}^{-1}(\mathbf{i}_e)$. Namely, $|A_{\bar{\alpha}}(\mathbf{i}_e)| = |\phi_{g_e}^{-1}(\mathbf{i}_e) \cap \{\mathbf{i}_\alpha \times G_{\bar{\alpha}}\}| = |\phi_{g_e}^{-1}(\mathbf{i}_e) \cap \{\mathbf{i}_\alpha \times G_{\bar{\alpha}}\}|$, and the equation (b) of (15) holds.

The projection of $\phi_{g_e}^{-1}(g_e)$ on G_α is defined as $G_\alpha(g_e) = \{g_\alpha : \exists (g_\alpha, g_{\bar{\alpha}}) \in \phi_{g_e}^{-1}(g_e), g_{\bar{\alpha}} \in G_{\bar{\alpha}}\}$. By (9), (15) and (16),

$$|G_\alpha(g_e)| = \frac{|\phi_{g_e}^{-1}(g_e)|}{|A_{\bar{\alpha}}(\mathbf{i}_e)|} = \frac{|\phi_{g_e}^{-1}(\mathbf{i}_e)|}{|\phi_{g_e}^{-1}(\mathbf{i}_e) \cap \{\mathbf{i}_\alpha \times G_{\bar{\alpha}}\}|}.$$

Conditioning on $X_e = g_e$, as X_α is uniformly distributed over $G_\alpha(g_e)$, for any $g_e \in G_e$ we have

$$\Pr(X_\alpha = g_\alpha | X_e = g_e) = \frac{1}{|G_\alpha(g_e)|} = \frac{|\phi_{g_e}^{-1}(\mathbf{i}_e) \cap \{\mathbf{i}_\alpha \times G_{\bar{\alpha}}\}|}{|\phi_{g_e}^{-1}(\mathbf{i}_e)|}$$

for $g_\alpha \in G_\alpha(g_e)$ and $\Pr(X_\alpha = g_\alpha | X_e = g_e) = 0$ for $g_\alpha \in G_\alpha \setminus G_\alpha(g_e)$. Namely,

$$H(X_\alpha | X_e = g_e) = \log \frac{|\phi_{g_e}^{-1}(\mathbf{i}_e)|}{|\phi_{g_e}^{-1}(\mathbf{i}_e) \cap \{\mathbf{i}_\alpha \times G_{\bar{\alpha}}\}|} \quad (17)$$

for any $g_e \in G_e$. Accordingly, with (12) and (17), equation (a) of (11) holds and with (17) equation (b) of (11) holds. By our definition of G'_e and G'_α , equation (c) of (11) holds. Thus, by (10) and (11)

$$H(X_e) + H(X_\alpha | X_e) = \log \frac{|G'|}{|G'_e \cap G'_\alpha|} = H(X_e, X_\alpha).$$

We conclude that the group G' with subgroups $\{G'_f : f \in \mathcal{S} \cup \{e\}\}$ is a group characterization of random variables $\{X_f : f \in \mathcal{S} \cup \{e\}\}$. Accordingly ϕ_{g_e} is group characterizable [15]. Note that, since we do not assume groups $\{G_f : f \in \mathcal{S} \cup \{e\}\}$ are Abelian, G' is not necessarily Abelian. \square

IV. PROOF OF THEOREM 3

Proof. By assumption, $\phi_{g_e^*}$ is K -piece-wise CWL with K subfunctions $\{\phi_{g_e^*}^{(k)} : G_{\mathcal{S}} \mapsto G_{e^*}\}_{k \in [K]}$. By an averaging argument, there exists some $k' \in [K]$ corresponding to the subfunction $\phi_{g_e^*}^{(k')}$ for which $|S^{(k')}| \geq |G_{\mathcal{S}}|/K$. For every $i \in \mathcal{S}$

$$|S_i^{(k')}| \geq \frac{|G_i|}{K}, \quad (18)$$

as otherwise $\prod_{i \in \mathcal{S}} |S_i^{(k')}| < \prod_{i \in \mathcal{S}} |G_i|/K = |G_{\mathcal{S}}|/K$.

For any $i \in \mathcal{S}$, let $G_{e^*}(i) = \{\phi_{g_e^*}^{(k')}(x_i, \mathbf{i}_{\mathcal{S} \setminus i}) : x_i \in G_i\}$. For any $x_{e^*} \in G_{e^*}(i)$, we define $A_i(x_{e^*}) = \{x_i \in G_i : \phi_{g_e^*}^{(k')}(x_i, \mathbf{i}_{\mathcal{S} \setminus i}) = x_{e^*}\}$. The set $A_i(x_{e^*})$ is defined similarly to $A_i(y)$ in the proof of Theorem 2. By Lemma 1 for any $x_{e^*}, \bar{x}_{e^*} \in G_{e^*}(i)$, we have $|A_i(x_{e^*})| = |A_i(\bar{x}_{e^*})|$. For any $i \in \mathcal{S}$, we call the elements in $S_i^{(k')}$ “good” and elements in $G_i \setminus S_i^{(k')}$ “bad”. By an averaging argument there exists $x_{e^*}(i) \in G_{e^*}(i)$, such that $A_i(x_{e^*}(i))$ contains at least a fraction of $\frac{|S_i^{(k')}|}{|G_i|}$ “good” elements. We define $G'_i = \{x_i \in A_i(x_{e^*}(i)) : x_i \text{ is good}\}$, accordingly

$$|G'_i| \geq \frac{|S_i^{(k')}|}{|G_i|} |A_i(x_{e^*}(i))|. \quad (19)$$

We use $\prod_{i \in \mathcal{S}} G'_i$ to construct a new code $\{X'_f : f \in \mathcal{S} \cup \mathcal{E}\}$. Here, X'_i is uniformly distributed over G'_i , such that $H(X'_i) = nR'_i = \log |G'_i|$. For the new code, sources are independent since there is no cooperation during transmission. As the supports of new source random variables are subsets of the original ones ($G'_i \subset G_i$ for any $i \in \mathcal{S}$), we apply the original encoding and decoding functions to the new code. As $\phi_{ge^*}^{(k')}$ is CWL, the message $x_{e^*} = \phi_{ge^*}^{(k')}(g)$ for any $g \in \prod_{i \in \mathcal{S}} G'_i$ transmitted through e^* equals $\underset{i \in \mathcal{S}}{\circ} x_{e^*}(i)$ which is constant. Thus no information needs to be transmitted through edge e^* and we may consider it removed. As $|G_{e^*}(i)| \leq |G_{e^*}|$, we know $|A_i(x_{e^*}(i))| = |G_i|/|G_{e^*}(i)| \geq |G_i|/|G_{e^*}|$, with (18) and (19), we have

$$|G'_i| \geq \frac{|S_i^{(k')}|}{|G_i|} |A_i(x_{e^*}(i))| \geq \frac{|A_i(x_{e^*}(i))|}{K} = \frac{|G_i|}{|G_{e^*}| \cdot K}. \quad (20)$$

Since $H(X'_i) = nR'_i = \log |G'_i|$, $H(X_i) = nR_i = \log |G_i|$ and $H(X_{e^*}) \leq nR_{e^*} = \log |G_{e^*}|$, by (20) we have

$$R'_i \geq R_i - R_{e^*} - \frac{\log K}{n}.$$

□

Remarks: As we can see, the proof of Theorem 3 is limited to the 0-error case. Roughly speaking, our proof does not naturally extend to the ϵ -error case due to our use of an averaging argument on $\{1 \dots k\}$. To prove Theorem 3 for ϵ -error one could need the averaging argument to preserve error, which is not necessarily the case.

V. CASE STUDIES OF STATEMENT 2

A. The network instance of [14]

The network instance of [14], referred to as N_3 , includes three subnetworks, referred here as networks A , B and C (from left to right). In [14] it is shown that N_3 is solvable but not linearly solvable. In Fig. A the original zero-error blocklength $n = 1$ non-linear solution for N_3 of [14] is presented. For all edges e^* in networks A and B , the original code is linear. We thus focus on the validity of the CWL statement when e^* is taken from network C . Toward this end, we suggest a modified code for which all edges in network C are linear (at the “price” of modifying the encoding on edges of network B to be non-linear). Our modified code preserves the original encoding presented in Fig. A on all edges of network A . Using the notation of [14] for network B we set the encoding functions to be:

$$\begin{aligned} e_{15,19} &= a + b + t(c) \\ e_{8,23} &= a + b \\ e_{24,32} &= a + t(c) \\ e_{25,33} &= b + t(c) \end{aligned}$$

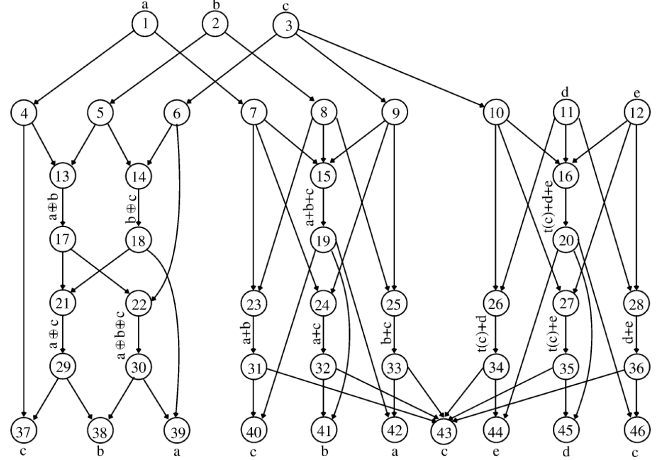


Fig. 2. The network N_3 and coding scheme from [14]. Figure taken from [14].

For network C we set the linear encoding functions to be:

$$\begin{aligned} e_{16,20} &= c + d + e \\ e_{26,34} &= c + d \\ e_{27,35} &= c + e \\ e_{28,36} &= d + e \end{aligned}$$

It now follows that the demands are met:

$$\begin{aligned} n_{40} : c &= t(e_{19,40} - e_{31,40}) = t(a + b + t(c) - (a + b)) \\ n_{41} : b &= e_{19,41} - e_{32,41} = a + b + t(c) - (a + t(c)) \\ n_{42} : a &= e_{19,42} - e_{33,42} = a + b + t(c) - (b + t(c)) \\ n_{43} : c &= (e_{33,43} + e_{32,43} - e_{31,43}) \\ &\quad + t(e_{34,43} + e_{35,43} - e_{36,43}) \\ &= t(a + t(c) + b + t(c) - (a + b)) \\ &\quad + t(c + d + c + e - (d + e)) \\ &= t(2c) + 2t(c) \\ n_{44} : e &= e_{20,44} - e_{34,44} = (c + d + e) - (c + d) \\ n_{45} : d &= e_{20,45} - e_{35,45} = (c + d + e) - (c + e) \\ n_{46} : c &= e_{20,46} - e_{36,46} = (c + d + e) - (d + e) \end{aligned}$$

B. The network instance of [15]

In [15], a duality between entropy functions and network codes is introduced. For the network instance N given in Figure B and for a given rate vector \mathbf{R} (induced by an entropy vector which violates the Ingleton inequality) that is not linearly feasible, [15] present a $(0, \mathbf{R}, n)$ -feasible non-linear code.

Using the notation from [15], let $\mathcal{N} = \{1, 2, 3, 4\}$ and consider an entropy function h of four quasi-uniform random

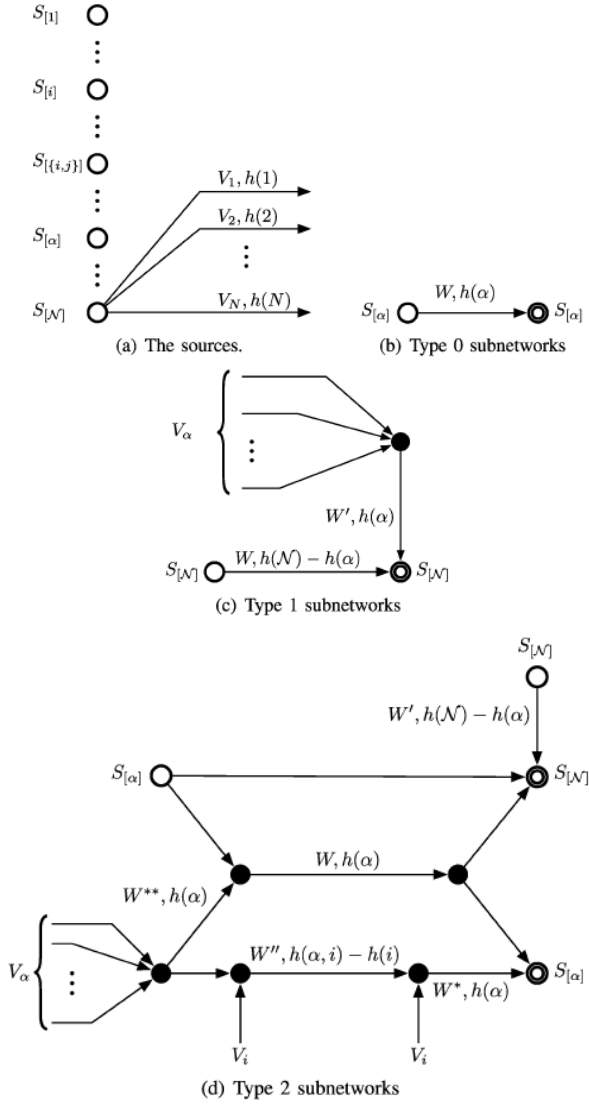


Fig. 3. The network N from [15] with corresponding notation used in our analysis. The Figure is taken from [15].

variables U_1, U_2, U_3, U_4 , such that

$$\begin{aligned}
h(1) &= h(2) = h(3) = h(4) = \log 13 \\
h(1, 2) &= \log 6 + \log 13 \\
h(3, 4) &= \log 13 + \log 12 \\
h(1, 3) &= h(1, 4) = h(2, 3) = h(2, 4) = \log 13 + \log 4 \\
h(i, j, k) &= \log 13 + \log 12 \\
&= h(1, 2, 3, 4), \quad \forall \text{distinct } i, j, k.
\end{aligned}$$

It is easy to show that h violates the Ingleton inequality. [15] show that the rate vector $\mathbf{R} = (R_{\alpha})_{\alpha \subseteq \mathcal{S}}$ induced from h is achievable on N (with a non-linear code), where $R_{\alpha} = h(\alpha)$ is the rate of source $S_{[\alpha]}$ for $\alpha \subseteq \mathcal{N}$. For every e^* in N , we modify the code of [15], such that (a) it remains feasible, and (b) the encoding function on e^* is CWL. We address edges of

each subnetwork specified in Figure B separately. Before we start, we prove the following lemma used in our analysis.

Lemma 5. *Let A, B be two sets of size p, q , respectively for which q divides p . Let g be a balanced function that maps A to B , i.e., the pre-image of every b under g is of size p/q . Then there exists a CWL function f that maps A onto B that equals g .*

Proof. Since q divides p , we have $p = kq$, here k is a positive integer. First, we relabel elements in A, B as elements in $G_k \times G_q, G_q$, respectively. Here $G_k = \{0, 1, \dots, k-1\}$ and $G_q = \{0, 1, \dots, q-1\}$ are the additive groups with addition modulo k and q respectively. The relabeling is done according to function g . Namely, for each $j \in B$, let A_j be the pre-image of j under g . By our assumptions, A_j is of size k . We label element i of A_j by $(i, j) \in G_k \times G_q$. Now, define $f : A \mapsto B$ by $f(i, j) = j$. Note that f is equal to g . For any two elements $a = (i, j), a' = (i', j')$ of A we have $f(a + a') = j + j' = f(a) + f(a')$ which implies that f is CWL. \square

Subnetwork (a): The sources. We study the outgoing edge carrying message V_i for each $i \in \mathcal{N}$. Using the definitions in [15] we have $H(S_{[N]}) = h(\mathcal{N}), H(V_i) = h(i)$ and $S_{[N]}, V_i$ are quasi-uniform. This implies that the supports of $S_{[N]}$ and V_i are of sizes 13×12 and 13 respectively. We relabel the supports $S_{[N]}, V_i$ as groups of size $13 \times 12, 13$, respectively. By Lemma 5, once we relabel the elements in $S_{[N]}, V_i$ the global encoding function corresponding to message V_i is CWL.

Subnetwork (b): Type 0 subnetworks. For the edge carrying message W , the encoding function is CWL since W is uncoded and equals $S_{[\alpha]}$.

Subnetwork (c): Type 1 subnetworks. The edge carrying W' is of capacity $h(\alpha)$. As $2^{h(\alpha)}$ divides $2^{h(\mathcal{N})}$ for any $\alpha \subseteq \mathcal{N}$, by Lemma 5 the quasi-uniform V_{α} can be represented as a CWL function of $S_{[N]}$.

For the edge carrying W , we note that $2^{h(\mathcal{N})-h(\alpha)}$ divides $2^{h(\mathcal{N})}$ for any $\alpha \subset \mathcal{N}$ and that the function corresponding to W is balanced in the solution of [15]. Thus, by Lemma 5, there exists a coding scheme such that W is a CWL function of source message $S_{[N]}$.

Subnetwork (d): Type 2 subnetworks. Using the same argument as in Type 1 subnetworks, one can represent W', W^* and W^{**} as CWL functions. For the edge carrying W , following the analysis on Type 1 networks, V_{α} can be represented as a CWL function of $S_{[N]}$. Let G_{α} be the group corresponding to V_{α} . Since $H(S_{[\alpha]}) = H(V_{\alpha}) = h(\alpha)$, we may relabel the support of $S_{[\alpha]}$ as the group G_{α} of size $2^{h(\alpha)}$. Then the function that takes the pair $S_{[N]}$ and $S_{[\alpha]}$ and returns the corresponding combination $V_{\alpha} \circ S_{[\alpha]}$, where \circ is the group operation of G_{α} , is CWL.

For W'' , similar to the analysis for W in Type 1 networks, we have that W'' of [15] is balanced and thus can be represented as a CWL function.

C. The network instance of [16]

In [16], a class of networks which is solvable but not linearly solvable is introduced. Using the notation of [16], a

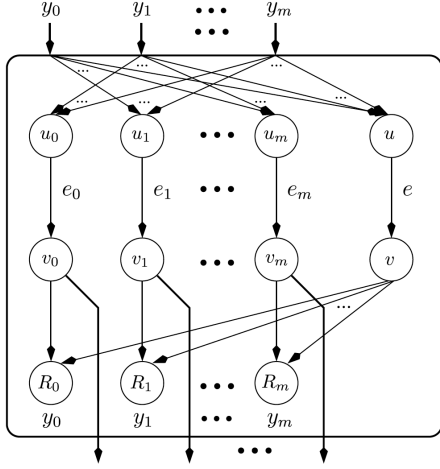


Fig. 4. The building block $B(m)$ from [16] with the corresponding notation used in our analysis. The figure is taken from [16].

non-linearly solvable network $N_4(m)$ is constructed by taking a disjoint union of component networks $N_1(m)$, $N_2(m, w)$, $N_3(m_1, m_2)$ with carefully chosen parameters. The later networks, in turn, are constructed from a certain building block $B(m)$, see Fig. 4.

In $B(m)$ the only encoding edges are the edges carrying message e_0, e_1, \dots, e_m, e , all the other edges forward messages without encoding. Also, the edges carrying e_0, e_1, \dots, e_m, e are directly connected to sources such that the local and global encoding function on these edges are identical (as the incoming edge messages are the source messages). Now we show, for any edge in the network N_4 defined in [16] that we can modify the code of [16] and make the global encoding function ϕ_{ge} CWL.

1) *Subnetwork: $N_1(m)$:* In the coding scheme of [16] all edges in $N_1(m)$ have a linear global encoding function.

2) *Subnetwork: $N_2(m, w)$:* By Lemma IV.4 of [16], a solution for $N_2(m, w)$ is given as a single blocklength code over the ring \mathbf{Z}_{mw} for each $l = 1, 2, \dots, w$ by

$$e_0^{(l)} = \sum_{j=1}^{m+1} x_j^{(l)},$$

$$e_i^{(l)} = \pi_l(z) + \sum_{j=1, j \neq i}^{m+1} x_j^{(l)} \quad (i = 1, 2, \dots, m+1),$$

$$e^{(l)} = \pi_l(z) + \sum_{j=1}^{m+1} x_j^{(l)}.$$

From the expressions we notice that the edge message $e_0^{(l)}$ is a linear function of source messages. By the proof of Lemma IV.2 of [16], for each integer y , there exist unique integers q_y, r_y such that $y = q_y m + r_y$ and $0 \leq r_y < m$. For each $a = q_a m + r_a \in \mathbf{Z}_{mw}$ s.t. $0 \leq r_a < m$, let \hat{r}_a be the unique integer in $\{0, 1, \dots, m-1\}$ such that $\hat{r}_a = r_a + 1 \pmod{m}$

and for each $l = 1, 2, \dots, w-1$, define a permutation of \mathbf{Z}_{mw} as follows:

$$\pi_l(a) = \begin{cases} q_a m + \hat{r}_a, & \text{if } q_a = l \\ q_a m + r_a, & \text{otherwise} \end{cases}$$

$$\pi_w(a) = a = q_a m + r_a.$$

Note that if $\pi_l(z)$ is the identity permutation, the corresponding edge messages $e_i^{(l)}$ and $e^{(l)}$ are linear functions of the source messages $((x_i)_{i \in [m+1]}, z)$. By the decoding scheme given in the proof of Lemma IV.2 of [16], reassigning the permutation for each $l \in \{1, \dots, w\}$ from the set of permutations $\{\pi_l(a) : l = 1, \dots, w\}$ would not affect the validity of decoding. Now, for edges carrying messages indexed by l , we can set π_l to be the identity permutation (originally $\pi_w(a)$), such that the encoding function on the edges carrying $e_i^{(l)}$ and $e^{(l)}$ turn to be linear and in particular CWL.

3) *Subnetwork: $N_3(m_1, m_2)$:* By Lemma V.4 of [16], a solution for $N_3(m_1, m_2)$ ($m_1 = m$ and $m_2 = sm^\alpha$) is given as a single blocklength code over the ring $\mathbf{Z}_{m^{\alpha+1}}$ for each $l = 1, 2$ by

$$e_0^{(l)} = \sum_{j=1}^{m_l} x_j^{(l)},$$

$$e_i^{(l)} = \pi_l(z) + \sum_{j=1, j \neq i}^{m_l} x_j^{(l)} \quad (i = 1, 2, \dots, m+1),$$

$$e^{(l)} = \pi_l(z) + \sum_{j=1}^{m_l} x_j^{(l)}.$$

By the encoding functions given above, we know for $l = 1, 2$ that $e_0^{(l)}$ is a linear function of source messages. By the proof of Lemma V.2 of [16], permutations π_1, π_2 of $\mathbf{Z}_{m^{\alpha+1}}$ are defined as follows. For each $\mathbf{Z}_{m^{\alpha+1}}$, let

$$a = \sum_{i=0}^{\alpha} m^i a_i$$

denote the base m representation of a . [16] define

$$\pi_1(a) = m^\alpha a_0 + \sum_{i=1}^{\alpha} m^{i-1} a_i$$

$$\pi_2(a) = a = \sum_{i=0}^{\alpha} m^i a_i.$$

As π_2 is the identity permutation, the encoding functions on edges carrying $\{e_0^{(2)}, e_i^{(2)}, e^{(2)} : i = 1, 2, \dots, m+1\}$ are linear.

Now we show an alternative solution that have linear encoding functions on $\{e_0^{(1)}, e_i^{(1)}, e^{(1)} : i = 1, 2, \dots, m+1\}$. We define the permutations as follows

$$\pi_1(a) = a = \sum_{i=0}^{\alpha} m^i a_i \quad (21)$$

$$\pi_2(a) = a_\alpha + \sum_{i=0}^{\alpha-1} m^{i+1} a_i \quad (22)$$

By the new definition, $\pi_1(a)$ is the identity permutation, and thus the encoding functions on edges carrying $\{e_0^{(1)}, e_i^{(1)}, e^{(1)} : i = 1, 2, \dots, m+1\}$ are linear. Now we show the validity of the decoding scheme regarding to the new encoding functions. That is, by [16] for each $a \in \mathbf{Z}_{m^{\alpha+1}}$, it suffices to show that the mapping given by

$$a \mapsto (m\pi_1(a), sm^\alpha\pi_2(a))$$

is injective. For each $a, b \in \mathbf{Z}_{m^{\alpha+1}}$, suppose

$$m\pi_1(a) = m\pi_1(b), \quad (\text{mod } m^{\alpha+1}) \quad (23)$$

$$sm^\alpha\pi_2(a) = sm^\alpha\pi_2(b), \quad (\text{mod } m^{\alpha+1}) \quad (24)$$

where $a = \sum_{i=0}^{\alpha} m^i a_i$ and $b = \sum_{i=0}^{\alpha} m^i b_i$. Then from (21),(23) we have

$$\sum_{i=0}^{\alpha-1} m^{i+1} a_i = \sum_{i=0}^{\alpha-1} m^{i+1} b_i \quad (\text{mod } m^{\alpha+1})$$

Therefore as $0 \leq a_i, b_i < m$

$$a_i = b_i \quad (i = 0, 1, \dots, \alpha - 1)$$

and from (22) and (24)

$$sm^\alpha a_\alpha = sm^\alpha b_\alpha \quad (\text{mod } m^{\alpha+1}).$$

Thus, from $\gcd(m, s)=1$

$$m^\alpha a_\alpha = m^\alpha b_\alpha \quad (\text{mod } m^{\alpha+1}).$$

We conclude as $0 \leq a_\alpha, b_\alpha < m$ that

$$a_\alpha = b_\alpha.$$

Thus $a = b$ and we have a valid code with linear encoding functions on $\{e_0^{(1)}, e_i^{(1)}, e^{(1)} : i = 1, 2, \dots, m+1\}$.

VI. THE ϵ -ERROR PROBLEM ON ABELIAN GROUP NETWORK CODES

In this section we follow the definitions and models in [8].

Theorem 4. *Let \mathcal{I} be a network coding instance. Let $\epsilon < 1/2$. If \mathcal{I} is $(\epsilon, \mathbf{R}, n)$ -feasible by a group network code then \mathcal{I} is $(0, \mathbf{R}, n)$ -feasible by a group network code.*

Fix any $0 < \epsilon < 1/2$. We start with an $(\epsilon, \mathbf{R}, n)$ -feasible group network code for network instance \mathcal{I} . This group code can be characterized by a finite group G and its subgroups. We define $G_S = \cap_{i \in S} G_i$. Without loss of generality, we assume $|G_S| = 1$ ($G_S = \{\mathbf{i}\}$) [8], here we denote the identity element of G as \mathbf{i} .

We define the binary operation “ \cdot ” on the group G . For simplicity of notations we neglect the symbol in the following sections. We may represent singletons $\{\mathbf{i}\}$ as \mathbf{i} .

Let t be a terminal who demands $i' \in \mathcal{S}$, let $\phi_{I_n(t)}$ be the global encoding function that encodes the source message vector $X_S = (X_i)_{i \in S}$ to the incoming message $X_{I_n(t)}$. We denote the original decoding function as ϕ_t . We assume the encoding functions are group characterizable and there is no restriction on the decoding functions.

By the definition of group characterization, the source message vector X_S and the incoming message (of terminal t) $X_{I_n(t)}$ can be characterized by subgroups $G_S = \mathbf{i}$ and $G_{I_n(t)}$, respectively. Namely, the source message x_S and the incoming message $x_{I_n(t)}$ corresponds to the coset $gG_S (= g)$ and $gG_{I_n(t)}$ respectively.

By our assumption, all sources random variables are uniform. Thus, for an element g uniformly distributed over G , for each $i \in \mathcal{S}$, the source random variable is distributed uniformly over the coset of G_i which contains g .

The encoding function takes $gG_S = g$ as the input and outputs $gG_{I_n(t)} \supset gG_S$.

All in all, the communication process to terminal t can be described as follows:

$$g \xrightarrow{\phi_{I_n(t)}} gG_{I_n(t)} \xrightarrow{\phi_t} \bar{g}G_i$$

Claim 2. *In the context of group network codes, if $G_{I_n(t)} \not\subseteq G_i$, then for any decoding scheme the error probability is at least $1/2$.*

Proof. Let $q = |G_{I_n(t)}|/|G_{I_n(t)} \cap G_i|$. By Lagrange's theorem, q must be an integer larger or equal than 2.

Thus, each coset of $G_{I_n(t)}$ contains q different cosets of $G_{I_n(t)} \cap G_i$ which in turn implies that each coset of $G_{I_n(t)}$ intersects with q different cosets of G_i .

Now we show that conditioned on an incoming message to terminal t , the q messages corresponding to X_i are sent with equal probabilities. Let g be the message vector sent from the sources, $g_t G_{I_n(t)}$ be an incoming message received by the terminal t and $g_i G_i$ be a message sent by source i .

If $(g_i G_i) \cap (g_t G_{I_n(t)}) = \phi$, we have

$$\Pr(g_i G_i \text{ is sent} | g_t G_{I_n(t)} \text{ is received}) = 0.$$

Since g is uniform in G , we have

$$\begin{aligned} & \Pr(g_i G_i \text{ is sent} | g_t G_{I_n(t)} \text{ is received}) \\ &= \Pr(g \in g_i G_i | g \in g_t G_{I_n(t)}) \\ &= \frac{\Pr(g \in g_i G_i, g \in g_t G_{I_n(t)})}{\Pr(g \in g_t G_{I_n(t)})} \\ &= \frac{\Pr(g \in g_i G_i \cap g_t G_{I_n(t)})}{\Pr(g \in g_t G_{I_n(t)})} \\ &= \frac{|G_{I_n(t)} \cap G_i|/|G|}{|G_{I_n(t)}|/|G|} = 1/q \end{aligned}$$

At terminal t , the decoding function needs to determine the output among the q different messages X_i , which are conditionally uniform given the incoming message. Thus the optimal correct decoding probability is $1/q$. As $q \geq 2$, for any decoding scheme, the error probability is at least $1/2$. \square

Claim 3. *In the context of group network codes, if $G_{I_n(t)} \subseteq G_i$, then there exists a decoding scheme ϕ'_t with zero decoding error probability.*

Proof. Since $G_{I_n(t)} \subseteq G_i$, we can design a decoding scheme that takes the coset of $G_{I_n(t)}$ as input and outputs the coset

of G_i which includes $G_{I_n(t)}$. For such scheme, the decoding error probability is zero.

□

With the results above, we prove Theorem 4.

Proof. Consider a group network code for \mathcal{I} that is $(\epsilon, \mathbf{R}, n)$ -feasible for which $\epsilon \in (0, 1/2)$. We discuss two scenarios for the given network code.

We first show that it cannot be the case that there exists a terminal decoding X_i for which $G_{I_n(t)} \not\subseteq G_i$. As in that case, by Claim 2, for any decoder, we know that an error occurs with decoding error probability at least $1/2$ which contradicts our assumption that $\epsilon < \frac{1}{2}$.

Otherwise, for all terminals by Claim 3 there exists a decoding scheme with zero error probability.

□