IEEE Open Journal of the Communications Society

Received 8 September 2022; accepted 8 October 2022. Date of publication 14 October 2022;
date of current version 11 November 2022.

Digital Object Identifier 10.1109/OJCOMS.2022.3213789

On the Optimality of Linear Index Coding Over the Fields With Characteristic Three

ARMAN SHARIFIFAR (Graduate Student Member, IEEE), PARASTOO SADEGHI (Senior Member, IEEE), AND NEDA ABOUTORAB (Senior Member, IEEE)

School of Engineering and Information Technology, University of New South Wales, Canberra, ACT 2600, Australia

CORRESPONDING AUTHOR: A. SHARIFIFAR (e-mail: a.sharififar@unsw.edu.au)

Preliminary results of this paper are presented, in part, in [1]. The arXiv version of this article is available in [2].

ABSTRACT It has been known that the insufficiency of linear coding in achieving the optimal rate of the general index coding problem is rooted in its rate's dependency on the field size. However, this dependency has been described only through the two well-known matroid instances, namely the Fano and non-Fano matroids, which, in turn, limits its scope only to the fields with characteristic two. In this paper, we extend this scope to demonstrate the reliance of linear index coding rate on fields with characteristic three. By constructing two index coding instances of size 29, we prove that for the first instance, linear coding is optimal only over the fields with characteristic three, and for the second instance, linear coding over any field with characteristic three can never be optimal. Then, a variation of the second instance is designed as the third index coding instance of size 58. For this instance, it is proved that while linear coding over any field with characteristic three cannot be optimal, there exists a nonlinear code over the fields with characteristic three, which achieves its optimal rate. Connecting the first and third index coding instances in two specific ways, called no-way and two-way connections, will lead to two new index coding instances of size 87 and 91, for which linear coding is outperformed by nonlinear codes. Another main contribution of this paper is the reduction of the key constraints on the space of the linear coding for the first and second index coding instances, each of size 29, into a matroid instance with the ground set of size 9, whose linear representability is dependent on the fields with characteristic three. The proofs and discussions provided in this paper through using these two relatively small matroid instances will shed light on the underlying reason causing the linear coding to become insufficient for the general index coding problem.

INDEX TERMS Index coding, insufficiency of linear coding, nonlinear code, matroid theory, broadcast with side information.

I. INTRODUCTION

INDEX coding problem was first introduced by Birk and Kol [1] in the context of satellite communication where through a noiseless shared channel, a single server is assigned the task of communicating m messages to multiple users. While each user requests one distinct message from the server, it may have prior knowledge about a subset of the messages requested by other users, which is referred to as its side information. While sending uncoded messages leads to the total m transmissions, by taking advantage of users' side information, the server might be able to satisfy all the users with a smaller number of transmissions. The canonical model of index coding problem can be useful in studying other research areas, including network coding [2], [3], distributed storage [4], coded caching [5], [6], and topological interference management [7], [8].

Different settings have been defined for an index coding instance. An index coding instance is said to be a unicast instance if each of its messages is requested by a single user [9]. However, when at least one of its messages is requested by multiple users, it is referred to as a group-cast index coding instance [10], [11], [12]. An index coding instance is referred to as a symmetric-rate instance if the rates of its messages are all equal. Otherwise, it is said to be an asymmetric-rate index coding instance [8].

Index coding schemes are broadly categorized into linear and nonlinear codes. Although linear index coding has been the center of attention due to its straightforward encoding and decoding processes [1], [8], [13], [14], [15], [16], [17], [18], for the general index coding problem, it can be outperformed by nonlinear codes. The insufficiency of linear coding was proved in the context of network coding [19], where two network coding instances were provided to illustrate the reliance of linear coding rate on the fields with characteristic two. In fact, it was shown that for the first network coding instance, linear coding is optimal only over the fields with characteristic two, while for the second instance, linear coding over any field with characteristic two cannot be optimal. This implies that the insufficiency of linear coding is due to the dependency of its rate on the characteristic of the field on which it is operating. In [20], the authors illustrated how the constraints on the linear space of the aforementioned network coding instances can be equivalently modeled as the well-known matroid instances, namely the Fano and non-Fano matroids. While the Fano matroid is linearly representable only over the fields with characteristic two, the non-Fano matroid has no linear representation over the fields with characteristic two.

The connection of network coding and matroid theory with index coding was established in [2] and [3] by presenting a reduction method to convert any network coding or matroid instance into a groupcast index coding instance. In fact, it was shown that the Fano and non-Fano matroids can be equivalently mapped into two index coding instances. In [8], a systematic technique of turning any groupcast index coding instance into an asymmetric-rate unicast index coding instance was proposed, implying the insufficiency of linear coding for the unicast index coding. This will convert the Fano and non-Fano matroids into two asymmetric-rate unicast index coding instances. In [21], two symmetric-rate unicast index coding instances were directly built for which linear coding can be optimal only over the fields with characteristic two for one and odd characteristic for the other. In [22], it was shown that for specific index coding structures, the gap between the rate of optimal linear code and nonlinear code can grow linearly with the number of messages, underscoring the importance of nonlinear codes. In terms of the scalar linear coding problem, the authors in [23] provided an explicit way of constructing index coding instances to show that the gap between the linear coding rate over different field sizes can be significant, highlighting the strong dependence of scalar linear coding rate on the field's characteristic. However, for the vector index coding problem, the scope of linear coding rate's dependency on the field size has been limited to only the fields with characteristic two.

In this paper, this scope is extended to demonstrate the reliance of linear coding rate on the fields with characteristic three.

First, by directly constructing two symmetric-rate unicast index coding instances of size 29, we prove that for the first instance, linear coding is optimal only over the fields with characteristic three, while for the second instance, linear coding over any field with characteristic three cannot be optimal. It is shown that for each index coding instance, the main constraints on the column space of its encoding matrix can be captured by a matroid instance with the ground set of size 9. Presenting the proofs using these two relatively small matroids is useful to point out the key constraints causing the linear coding rate to become dependent on the field size. In addition, applying the mapping methods in [2] and [8] to these matroids will lead to asymmetric-rate unicast index coding instances, each consisting of more than 1000 users, while the corresponding symmetric-rate unicast index coding instances constructed in this paper are significantly simpler as each instance is of size 29.

Second, we design the third symmetric-rate unicast index coding instance of size 58, which is a variation of the second index coding instance. It is proved that while linear coding over the fields with characteristic three cannot achieve its optimal rate, there exists an optimal nonlinear code over the fields with characteristic three. It is shown that the main constraints on the linear space of its encoding matrix can be captured by a matroid instance with the ground set of size 18, which is not linearly representable over any fields with characteristic three.

Finally, connecting the first and third index coding instances in two specific ways, namely no-way and two-way connections, will result in two new index coding instances of size 87, 91 for which linear coding is outperformed by nonlinear codes.

The contributions and organization of this paper are summarized in Table 1.

II. SYSTEM MODEL AND BACKGROUND

A. NOTATION

Small letters such as n denote an integer where $[n] \triangleq \{1, \dots, n\}$ and $[n : m] \triangleq \{n, n+1, \dots m\}$ for $n < m$. Capital letters such as L denote a set, with $|L|$ denoting its cardinality. Symbols in bold face such as $\boldsymbol{l}$ and $\boldsymbol{L}$, respectively, denote a vector and a matrix, with $\text{rank}(\boldsymbol{L})$ and $\text{col}(\boldsymbol{L})$ denoting the rank and column space of matrix $\boldsymbol{L}$, respectively. A calligraphic symbol such as $\mathcal{L}$ denotes a set whose elements are sets.

We use $\mathbb{F}_q$ to denote a finite field of size q and write $\mathbb{F}_q^{n\times m}$ to denote the vector space of all $n \times m$ matrices over the field $\mathbb{F}_q$. $\boldsymbol{I}_n$ denotes the identity matrix of size $n \times n$, and $\boldsymbol{0}_n$ represents an $n \times n$ matrix whose elements are all zero.

B. SYSTEM MODEL

Consider a broadcast communication system in which a server transmits a set of mt messages $X = \{x_i^j,\ i \in [m],\ j \in [t]\}$, $x_i^j \in \mathcal{X}$, to a number of users $U = \{u_i,\ i \in [m]\}$ through a noiseless broadcast channel. Each user u_i wishes to receive a message of length t, $X_i = \{x_i^j,\ j \in [t]\}$ and

TABLE 1. Contributions and organization of the paper.

Section	Subsection	Content
II	II-B	The system model for index coding problem is established.
	II-C	For any index coding instance, the definitions related to its index code and broadcast rate are provided.
	II-D	For any index coding instance, the definitions related to its linear index code, encoding matrix, linear broadcast rate, vector and scalar linear index code are presented.
	II-E	For any index coding instance, the definitions related to its independent sets, minimal cyclic sets, acyclic sets, are provided based on its interfering message sets.
	II-F	A brief overview of matroid theory and the definitions related to a matroid's basic and circuit sets, vector and scalar linear representation, and also the basic and circuit sets of its linear representation matrix are provided.
III		• First, for any two index coding instances, based on their interfering message sets, we characterize two specific connections, namely no-way and two-way connections. • Then, in Theorem 1, it is proved that the no-way and two-way connections between the first and third index coding instances in this paper will lead to two new index coding instances for which linear coding is outperformed by the nonlinear codes.
IV	IV-A	• Definitions 22 and 23, respectively, characterize the first and second matroid instances $\mathcal{N}_1$ and $\mathcal{N}_2$, each with a ground set of size 9. • In Proposition 6, it is proved that matroid instance $\mathcal{N}_1$ is linearly representable only over fields with characteristic three. • Proposition 7 proves that matroid instance $\mathcal{N}_2$ is linearly representable over the fields with any characteristic other than characteristic three.
	IV-B	Lemmas 1-5 establish reduction techniques to map specific constraints on the encoding matrix of an index coding instance to the constraints on the matrix which linearly represents a matroid instance (their proof are provided in Appendix B).
	IV-C	• Definition 24 characterizes the first index coding instance $\mathcal{I}_1$, comprising 29 users. • Theorem 2 states that the necessary and sufficient condition for a linear index code to be optimal for $\mathcal{I}_1$ is that the chosen field does have characteristic three. The sufficient and necessary conditions are separately proved in Propositions 8 and 9, respectively. – In Proposition 8, it is shown that there exists a linear code over the fields with characteristic three, which is optimal for $\mathcal{I}_1$ (its proof is provided in Appendix C). – In Proposition 9, using Lemmas 1-5, it is proved that the main constraints on the column space of the encoding matrix of index coding instance $\mathcal{I}_1$ are equivalent to the constraints on the column space of the matrix, which is a linear representation of matroid instance $\mathcal{N}_1$. This combined with Proposition 6 implies that linear coding is optimal for $\mathcal{I}_1$ only over the fields with characteristic three. • Definition 25 characterizes the second index coding instance $\mathcal{I}_2$, comprising 29 users. • Theorem 3 states that the necessary and sufficient condition for a linear index code to be optimal for $\mathcal{I}_2$ is that the chosen field does have any characteristic other than characteristic three. The sufficient and necessary conditions are separately proved in Propositions 10 and 11, respectively. – In Proposition 10, it is shown that there exists a linear code over the fields with any characteristic other than characteristic three, which is optimal for $\mathcal{I}_2$ (its proof is provided in Appendix C). – In Proposition 11, using Lemmas 1-5, it is proved that the main constraints on the column space of the encoding matrix of index coding instance $\mathcal{I}_2$ are equivalent to the constraints on the column space of the matrix, which is a linear representation of matroid instance $\mathcal{N}_2$. This combined with Proposition 7 implies that linear coding is optimal for $\mathcal{I}_2$ only over the fields with any characteristic other than characteristic three.
V	V-A	• The concept of quasi-circuit set is defined in Definition 26. • Using the concept of quasi-circuit set, Definition 27 characterizes matroid instance $\mathcal{N}_3$, with the ground set of size 18. • In Proposition 12, it is proved that matroid instance $\mathcal{N}_3$ is not linearly representable over any fields with characteristic three.
	V-B	Lemmas 7-9 establish reduction techniques to map the constraints on the encoding matrix of an index coding instance to the constraints on the representation matrix of a matroid instance (their proof are provided in Appendix D).
	V-C	• Definition 29 characterizes the third index coding instance $\mathcal{I}_3$, comprising 58 users. • Theorem 4 states that the necessary and sufficient condition for a linear index code to be optimal for $\mathcal{I}_3$ is that the chosen field does have any characteristic other than characteristic three. However, there exists a scalar nonlinear code over the fields with characteristic three, which is optimal for $\mathcal{I}_3$. The sufficient and necessary conditions, and the existence of that nonlinear code are separately proved in Propositions 13, 14, and 15, respectively. – In Proposition 13, it is shown that there exists a linear code over the fields with any characteristic other than characteristic three, which is optimal for $\mathcal{I}_3$. – In Proposition 14, using Lemmas 1-3 and Lemmas 7-9, it is proved that the main constraints on the column space of the encoding matrix of index coding instance $\mathcal{I}_3$ are equivalent to the constraints on the column space of the matrix, which is a linear representation of matroid instance $\mathcal{N}_3$ (its proof is provided in Appendix E). This combined with Proposition 12 implies that linear coding is optimal for $\mathcal{I}_3$ only over the fields with any characteristic other than characteristic three. – In Proposition 15, it is shown that there exists a scalar nonlinear code over the fields with characteristic three, which is optimal for index coding instance $\mathcal{I}_3$.

may have a priori knowledge of a subset of the messages $S_i := \{x_l^j,\ l \in A_i,\ j \in [t]\},\ A_i \subseteq [m]\backslash\{i\}$, which is referred to as its side information set. The main objective is to minimize the number of coded messages which is required to be broadcast so as to enable each user to decode its requested message. An instance of index coding problem $\mathcal{I}$ can be either characterized by the side information set of its users as $\mathcal{I} = \{A_i, i \in [m]\}$, or by their interfering message set $B_i = [m] \backslash (A_i \cup \{i\})$ as $\mathcal{I} = \{B_i, i \in [m]\}$.

C. GENERAL INDEX CODE

Definition 1 ($\mathcal{C}_\mathcal{I}$: Index Code for $\mathcal{I}$): Given an instance of index coding problem $\mathcal{I} = \{A_i, i \in [m]\}$, a (t, r) index code is defined as $\mathcal{C}_\mathcal{I} = (\phi_\mathcal{I}, \{\psi^i_\mathcal{I}\})$, where

- $\phi_\mathcal{I} : \mathcal{X}^{mt} \to \mathcal{X}^r$ is the encoding function which maps the mt message symbol $x^j_i \in \mathcal{X}$ to the r coded messages as $Y = \{y_1, \dots, y_r\}$, where $y_k \in \mathcal{X}, \forall k \in [r]$.
- $\psi^i_\mathcal{I}$: represents the decoder function, where for each user $u_i, i \in [m]$, the decoder $\psi^i_\mathcal{I} : \mathcal{X}^r \times \mathcal{X}^{|A_i|t} \to \mathcal{X}^t$ maps the received r coded messages $y_k \in Y, k \in [r]$ and the $|A_i|t$ messages $x^j_l \in S_i$ in the side information to the t messages $\psi^i_\mathcal{I}(Y, S_i) = \{\hat{x}^j_i, j \in [t]\}$, where $\hat{x}^j_i$ is an estimate of x^j_i.

Definition 2 [$\beta(\mathcal{C}_\mathcal{I})$ Broadcast Rate of $\mathcal{C}_\mathcal{I}$]: Given an instance of the index coding problem $\mathcal{I}$, the broadcast rate of a (t, r) index code $\mathcal{C}_\mathcal{I}$ is defined as $\beta(\mathcal{C}_\mathcal{I}) = \frac{r}{t}$.

Definition 3 [$\beta(\mathcal{I})$ Broadcast Rate of $\mathcal{I}$]: Given an instance of the index coding problem $\mathcal{I}$, the broadcast rate $\beta(\mathcal{I})$ is defined as

$$\beta(\mathcal{I}) = \inf_t \inf_{\mathcal{C}_\mathcal{I}} \beta(\mathcal{C}_\mathcal{I}). \tag{1}$$

Thus, the broadcast rate of any index code $\mathcal{C}_\mathcal{I}$ provides an upper bound on the broadcast rate of $\mathcal{I}$, i.e., $\beta(\mathcal{I}) \le \beta(\mathcal{C}_\mathcal{I})$.

D. LINEAR INDEX CODE

Let $\boldsymbol{x} = [\boldsymbol{x}_1, \dots, \boldsymbol{x}_m]^T \in \mathbb{F}_q^{mt\times 1}$ denote the vector message.

Definition 4 (Linear Index Code): Given an instance of the index coding problem $\mathcal{I} = \{B_i, i \in [m]\}$, a (t, r) linear index code is defined as $\mathcal{L}_\mathcal{I} = (\boldsymbol{H}, \{\psi^i_\mathcal{I}\})$, where

- $\boldsymbol{H} : \mathbb{F}_q^{mt\times 1} \to \mathbb{F}_q^{r\times 1}$ is the $r \times mt$ encoding matrix which maps the message vector $\boldsymbol{x} \in \mathbb{F}_q^{mt\times 1}$ to a coded message vector $\bar{\boldsymbol{y}} = [y_1, \dots, y_r]^T \in \mathbb{F}_q^{r\times 1}$ as follows

  $$\boldsymbol{y} = \boldsymbol{H}\boldsymbol{x} = \sum_{i\in[m]} \boldsymbol{H}^{\{i\}}\boldsymbol{x}_i.$$

  Here $\boldsymbol{H}^{\{i\}} \in \mathbb{F}_q^{r\times t}$ is the local encoding matrix of the i-th message $\boldsymbol{x}_i$ such that $\boldsymbol{H} = [\boldsymbol{H}^{\{1\}} | \cdots | \boldsymbol{H}^{\{m\}}] \in \mathbb{F}_q^{r\times mt}$.
- $\psi^i_\mathcal{I}$ represents the linear decoder function for user $u_i, i \in [m]$, where $\psi^i_\mathcal{I}(\boldsymbol{y}, S_i)$ maps the received coded message $\boldsymbol{y}$ and its side information messages S_i to $\hat{\boldsymbol{x}}_i$, which is an estimate of the requested message vector $\boldsymbol{x}_i$.

Proposition 1 [24]: The necessary and sufficient condition for linear decoder $\psi^i_\mathcal{I}, \forall i \in [m]$ to correctly decode the requested message vector $\boldsymbol{x}_i$ is

$$\text{rank}\left(\boldsymbol{H}^{\{i\}\cup B_i}\right) = \text{rank}\left(\boldsymbol{H}^{B_i}\right) + t, \tag{2}$$

where $\boldsymbol{H}^L$ denotes the matrix $[\boldsymbol{H}^{\{l_1\}} | \cdots | \boldsymbol{H}^{\{l_{|L|}\}}]$ for the given set $L = \{l_1, \dots, l_{|L|}\}$.

Definition 5 [$\lambda_q(\mathcal{L}_\mathcal{I})$ Linear Broadcast Rate of $\mathcal{L}_\mathcal{I}$ Over $\mathbb{F}_q$]: Given an instance of index coding problem $\mathcal{I}$, the linear broadcast rate of a (t, r) linear index code $\mathcal{L}_\mathcal{I}$ over field $\mathbb{F}_q$ is defined as $\lambda_q(\mathcal{L}_\mathcal{I}) = \frac{r}{t}$.

Definition 6 [$\lambda_q(\mathcal{I})$ Linear Broadcast Rate of $\mathcal{I}$ Over $\mathbb{F}_q$]: Given an instance of index coding problem $\mathcal{I}$, the linear broadcast rate $\lambda_q(\mathcal{I})$ over field $\mathbb{F}_q$ is defined as

$$\lambda_q(\mathcal{I}) = \inf_t \inf_{\mathcal{L}_\mathcal{I}} \lambda_q(\mathcal{L}_\mathcal{I}).$$

Definition 7 [$\lambda(\mathcal{I})$ Linear Broadcast Rate for $\mathcal{I}$]: Given an instance of index coding problem $\mathcal{I}$, the linear broadcast rate is defined as

$$\lambda(\mathcal{I}) = \min_q \lambda_q(\mathcal{I}). \tag{3}$$

Definition 8 (Scalar and Vector Linear Index Code): The linear index code $\mathcal{C}_\mathcal{I}$ is said to be scalar if $t = 1$. Otherwise, it is called a vector (or fractional) code. For scalar codes, we use $x_i = x^1_i, i \in [m]$, for simplicity.

E. GRAPH DEFINITIONS

Given an index coding instance $\mathcal{I}$, the following concepts are defined based on its interfering message sets, which are, in fact, related to its graph representation [21].

Definition 9 (Independent Set of $\mathcal{I}$): We say that set $M \subseteq [m]$ is an independent set of $\mathcal{I}$ if $B_i \cap M = M \backslash \{i\}$ for all $i \in M$.

Definition 10 (Minimal Cyclic Set of $\mathcal{I}$): Let $M = \{i_j, j \in [|M|]\} \subseteq [m]$. Now, M is referred to as a minimal cyclic set of $\mathcal{I}$ if

$$B_{i_j} \cap M = \begin{cases} M\backslash\{i_j, i_{j+1}\}, & j \in [|M| - 1], \\ M\backslash\{i_{|M|}, i_1\}, & j = i_{|M|}. \end{cases} \tag{4}$$

Definition 11 (Acyclic Set of $\mathcal{I}$): We say that $M \subseteq [m]$ is an acyclic set of $\mathcal{I}$, if none of its subsets $M' \subseteq M$ forms a minimal cyclic set of $\mathcal{I}$. We note that each independent set is an acyclic set as well.

Proposition 2 [25]: Let $\mathcal{I} = \{B_i, i \in [m]\}$. It can be shown that

- if set $[m]$ is an acyclic set of $\mathcal{I}$, then $\lambda_q(\mathcal{I}) = \beta(\mathcal{I}) = m$.
- if set $[m]$ is a minimal cyclic set of $\mathcal{I}$, then $\lambda_q(\mathcal{I}) = \beta(\mathcal{I}) = m - 1$.

Definition 12 (Maximum Acyclic Induced Subgraph (MAIS) of $\mathcal{I}$): Let $\mathcal{M}$ be the set of all sets $M \subseteq [m]$ which are acyclic sets of $\mathcal{I}$. Then, set $M \in \mathcal{M}$ with the maximum size $|M|$ is referred to as the MAIS set of $\mathcal{I}$, and $\beta_{\text{MAIS}}(\mathcal{I}) = |M|$ is called the MAIS bound for $\lambda_q(\mathcal{I})$, as we always have [26]

$$\lambda_q(\mathcal{I}) \ge \beta_{\text{MAIS}}(\mathcal{I}). \tag{5}$$

Remark 1: Equation (5) establishes a sufficient condition for optimality of linear coding rate as follows. Given an index coding instance $\mathcal{I}$, if $\lambda_q(\mathcal{I}) = \beta_{\text{MAIS}}(\mathcal{I})$, then linear coding rate is optimal for $\mathcal{I}$. In this paper, the encoding matrix which achieves this optimal rate is denoted by $\boldsymbol{H}_*$.

Example 1: Consider the index coding instance $\mathcal{I} = \{B_i, i \in [4]\}$ where

$$B_1 = \{3\}, B_2 = \{1\}, B_3 = \{2\}, B_4 = \{1, 2, 3\}. \quad (6)$$

Now, it can be seen that set {1,2,3} is a minimal cyclic set of $\mathcal{I}$, and each set $\{1, 2, 4\}, \{1, 3, 4\}$ and $\{2, 3, 4\}$ is an acyclic and also a MAIS set of $\mathcal{I}$. Thus, $\beta_{\text{MAIS}}(\mathcal{I}) = 3$. Now, it can be easily verified that the following encoding matrix $\boldsymbol{H}_*$ achieves the MAIS bound, and so, it is optimal for $\mathcal{I}$

$$\boldsymbol{H}_* = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

F. OVERVIEW OF MATROID THEORY

Definition 13 ($\mathcal{N}$: Matroid Instance [2], [27]): A matroid instance $\mathcal{N} = \{f(N), N \subseteq [n]\}$ is a set of functions $f : 2^{[n]} \to \{0, 1, 2, \ldots\}$ that satisfy the following three conditions:

$$f(N) \leq |N|, \quad \forall N \subseteq [n],$$
$$f(N_1) \leq f(N_2), \quad \forall N_1 \subseteq N_2 \subseteq [n],$$
$$f(N_1 \cup N_2) + f(N_1 \cap N_2) \leq f(N_1) + f(N_2), \quad \forall N_1, N_2 \subseteq [n]. \quad (7)$$

Here, set $[n]$ and function $f(\cdot)$, respectively, are called the ground set and the rank function of $\mathcal{N}$. The rank of matroid $\mathcal{N}$ is defined as $f(\mathcal{N}) = f([n])$.

Definition 14 (Basis and Circuit Sets of $\mathcal{N}$): Consider a matroid $\mathcal{N}$ of rank $f(\mathcal{N})$. We say that $N \subseteq [n]$ is an independent set of $\mathcal{N}$ if $f(N) = |N|$. Otherwise, N is said to be a dependent set. A maximal independent set N is referred to as a basis set. A minimal dependent set N is referred to as a circuit set. Let sets $\mathcal{B}$ and $\mathcal{C}$, respectively, denote the set of all basis and circuit sets of $\mathcal{N}$. It can be shown that

$$f(\mathcal{N}) = f(N) = |N|, \quad \forall N \in \mathcal{B},$$
$$f(N\backslash\{i\}) = |N| - 1, \quad \forall i \in N, \ \forall N \in \mathcal{C}. \quad (8)$$

Definition 15 [(t)-linear Representation of $\mathcal{N}$ Over $\mathbb{F}_q$]: We say that matroid $\mathcal{N} = \{f(N), N \subseteq [n]\}$ of rank $f(\mathcal{N})$ has a (t)-linear representation over $\mathbb{F}_q$ if there exists a matrix $\boldsymbol{H} = [\boldsymbol{H}^{\{1\}} | \cdots | \boldsymbol{H}^{\{n\}}] \in \mathbb{F}_q^{f(\mathcal{N})t \times nt}$ such that

$$\text{rank}\big(\boldsymbol{H}^N\big) = f(N)t, \quad \forall N \subseteq [n]. \quad (9)$$

Now, based on Definitions 14 and 15, the concepts of basis and circuit sets can also be defined for matrix $\boldsymbol{H}$.

Definition 16 (Basis and Circuit Sets of $\boldsymbol{H}$): Let $N \subseteq [n]$. We say that N is an independent set of $\boldsymbol{H}$, if $\text{rank}(\boldsymbol{H}^N) = |N|t$, otherwise N is a dependent set of $\boldsymbol{H}$. The independent set N is a basis set of $\boldsymbol{H}$ if $\text{rank}(\boldsymbol{H}) = \text{rank}(\boldsymbol{H}^N) = |N|t$. The dependent set N is a circuit set of $\boldsymbol{H}$ if

$$\text{rank}\big(\boldsymbol{H}^{N\backslash\{j\}}\big) = \text{rank}\big(\boldsymbol{H}^N\big) = (|N| - 1)t, \quad \forall j \in N, \quad (10)$$

which requires that

$$\boldsymbol{H}^{\{j\}} = \sum_{i \in N\backslash\{j\}} \boldsymbol{H}^{\{i\}} \boldsymbol{M}_{j,i} \quad (11)$$

where each $\boldsymbol{M}_{j,i}$ is invertible.

Definition 17 (Scalar and Vector Linear Representation): If matroid $\mathcal{N}$ has linear representation with $t = 1$, it is said that $\mathcal{N}$ has a scalar linear representation. Otherwise, the linear representation is called a vector representation.

Example 2: Consider matroid instance $\mathcal{N}$ with the ground set of size $n = 3$ and rank $f(\mathcal{N}) = 2$ such that sets $\{1, 2\}, \{1, 3\}, \{2, 3\}$ are basis sets, and set $\{1, 2, 3\}$ is a circuit set. Then, the following matrix $\boldsymbol{H}$ is a scalar linear representation of $\mathcal{N}$

$$\boldsymbol{H} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}.$$

Remark 2: Note that the condition (2) requires that

$$\text{rank}\big(\boldsymbol{H}^{\{i\}}\big) = t, \ \forall i \in [m].$$

Thus, for matrix $\boldsymbol{H}$, which is a linear representation of matroid $\mathcal{N}$ with the ground set $[n]$, we also assume that

$$\text{rank}\big(\boldsymbol{H}^{\{i\}}\big) = t, \ \forall i \in [n]. \quad (12)$$

Remark 3: According to Definition 13, to define a matroid instance $\mathcal{N} = \{f(N), N \subseteq [n]\}$, a nonnegative integer value must be assigned to $f(N)$ for each set $N \subseteq [n]$, such that the three conditions in (7) are met. However, a matroid instance can also be characterized by determining some of its basis and circuit sets. This is because basis and circuit sets along with equations (7) and (8) can determine the value of $f(N)$ for each set $N \subseteq [n]$. In fact, this representation is more commonly used to characterize matroid instances, including the Fano and non-Fano matroids [20]. The matroid instances in this paper will also be characterized using their basis and circuit sets. Example 8 is provided in Appendix A to elaborate more on this.

1) THE FANO AND NON-FANO MATROID INSTANCES $\mathcal{N}_{\text{F}}$ AND $\mathcal{N}_{\text{NF}}$

Definition 18 (Fano Matroid Instance $\mathcal{N}_F$ [20]): Consider matroid instance $\mathcal{N}_{\text{F}} = \{(N, f(N)), N \subseteq [n]\}$ with $n = 7$ and $f(\mathcal{N}_{\text{F}}) = 3$. Now, matroid $\mathcal{N}_{\text{F}}$ is referred to as the Fano matroid instance if set $N_0 = [3]$ is a basis set, and the following sets $N_i, i \in [7]$ are circuit sets.

$$N_1 = \{1, 2, 4\},$$
$$N_2 = \{1, 3, 5\},$$
$$N_3 = \{2, 3, 6\},$$
$$N_4 = \{1, 6, 7\},$$
$$N_5 = \{2, 5, 7\},$$
$$N_6 = \{3, 4, 7\},$$
$$N_7 = \{4, 5, 6\}.$$

Proposition 3 [20]: The Fano matroid instance $\mathcal{N}_{\text{nF}}$ is linearly representable over field $\mathbb{F}_q$ if and only if field $\mathbb{F}_q$ does have characteristic two.

Definition 19 (Non-Fano Matroid Instance $\mathcal{N}_{nF}$ [20]): Consider matroid instance $\mathcal{N}_{\text{nF}} = \{(N, f(N)), N \subseteq [n]\}$ with $n = 7$ and $f(\mathcal{N}_{\text{nF}}) = 3$. Now, matroid $\mathcal{N}_{\text{nF}}$ is referred to as the non-Fano matroid instance if each set $N_0 = [3]$ and $N_7 = \{4, 5, 6\}$ is a basis set, and the following sets $N_i, i \in [6]$ are circuit sets.

$$N_1 = \{1, 2, 4\},$$
$$N_2 = \{1, 3, 5\},$$
$$N_3 = \{2, 3, 6\},$$
$$N_4 = \{1, 6, 7\},$$
$$N_5 = \{2, 5, 7\},$$
$$N_6 = \{3, 4, 7\}.$$

Proposition 4 [20]: The non-Fano matroid instance $\mathcal{N}_{\text{nF}}$ is linearly representable over field $\mathbb{F}_q$ if and only if field $\mathbb{F}_q$ does have odd characteristic (i.e., any characteristic other than characteristic two).

It is worth noting that the Fano and non-Fano matroid instances are exactly the same, with only differing in set $N_7 = \{4, 5, 6\}$. While set N_7 is a circuit set for the Fano matroid, it is a basis set for the non-Fano matroid.

III. MAIN RESULTS

This section presents two new index coding instances of size 87 and 91 for which linear coding is outperformed by nonlinear codes. Each instance is composed of two index coding subinstances, which are connected using two specific ways, referred to as no-way and two-way connections. In the following sections of this paper, it will be proved that for one of these subinstances, linear coding is optimal only over the fields with characteristic three, and for the other instance, while linear coding cannot be optimal over the fields with characteristic three, there exists a nonlinear code over the fields with characteristic three, which achieves its optimal rate. This implies that although linear coding over any field cannot simultaneously be optimal for these two subinstances, there exists a nonlinear code over the fields with characteristic three, which can achieve their optimal rate at the same time.

Definition 20 ($\mathcal{I}_1 \nleftrightarrow \mathcal{I}_2$: No-way Connection of $\mathcal{I}_1$ and $\mathcal{I}_2$): Given two index coding instances $\mathcal{I}_1 = \{B^1_i, i \in [m_1]\}$ and $\mathcal{I}_2 = \{B^2_i, i \in [m_2]\}$, no-way connection of $\mathcal{I}_1$ and $\mathcal{I}_2$, denoted by $\mathcal{I}_1 \nleftrightarrow \mathcal{I}_2$, is defined as a new index coding instance $\mathcal{I} = \{B_i, i \in [m]\}$, where $m = m_1 + m_2$ and

$$\begin{cases} B_i = B^1_i \cup \big([m]\backslash[m_1]\big), \ \forall i \in [m_1], \\ B_{i+m_1} = B^2_i \cup [m_1], \qquad \forall i \in [m_2], \end{cases}$$

which means that the new instance $\mathcal{I}$ is a concatenation of the two subinstances $\mathcal{I}_1$ and $\mathcal{I}_2$ such that each user in $\mathcal{I}_1$ has all the messages requested by the users in $\mathcal{I}_2$ in its interfering message set and vice versa.

Definition 21 ($\mathcal{I}_1 \leftrightarrow \mathcal{I}_2$: Two-way Connection of $\mathcal{I}_1$ and $\mathcal{I}_2$): Given two index coding instances $\mathcal{I}_1 = \{B^1_i, i \in [m_1]\}$ and $\mathcal{I}_2 = \{B^2_i, i \in [m_2]\}$, two-way connection of $\mathcal{I}_1$ and $\mathcal{I}_2$, denoted by $\mathcal{I}_1 \leftrightarrow \mathcal{I}_2$, is defined as a new index coding instance $\mathcal{I}' = \{B'_i, i \in [m']\}$, where $m' = m_1 + m_2$ and

$$\begin{cases} B'_i = B^1_i, \qquad \forall i \in [m_1], \\ B'_{i+m_1} = B^2_i, \ \forall i \in [m_2], \end{cases}$$

which means that the new instance $\mathcal{I}'$ is a concatenation of the two subinstances $\mathcal{I}_1$ and $\mathcal{I}_2$ such that each user in $\mathcal{I}_1$ has all the messages requested by the users in $\mathcal{I}_2$ in its side information set and vice versa.

Proposition 5 (Blasiak et al. [22]): Let $\lambda_q(\mathcal{I}_1)$ and $\lambda_q(\mathcal{I}_2)$, respectively, denote the linear broadcast rate of $\mathcal{I}_1$ and $\mathcal{I}_2$ over $\mathbb{F}_q$. Then, for the linear broadcast rate of $\mathcal{I} = \mathcal{I}_1 \nleftrightarrow \mathcal{I}_2$ and $\mathcal{I}' = \mathcal{I}_1 \leftrightarrow \mathcal{I}_2$ over $\mathbb{F}_q$, we have

$$\begin{cases} \lambda_q(\mathcal{I}) = \lambda_q(\mathcal{I}_1) + \lambda_q(\mathcal{I}_2), \\ \lambda_q\big(\mathcal{I}'\big) = \max\big\{\lambda_q(\mathcal{I}_1), \lambda_q(\mathcal{I}_2)\big\}. \end{cases}$$

Theorem 1: Other than the index coding instances in [2] and [21], two new index coding instances of size 87 and 91 are designed in this paper, for which linear coding is insufficient for achieving their broadcast rate.

Proof: We prove that for the following two index coding instances $\mathcal{I} = \{B_i, i \in [m = 87]\}$, $\mathcal{I}' = \{B'_i, i \in [m' = 91]\}$, linear coding is outperformed by the nonlinear codes:

$$\begin{cases} \mathcal{I} = \mathcal{I}_1 \nleftrightarrow \mathcal{I}_3, \\ \mathcal{I}' = (\mathcal{I}_1 \nleftrightarrow \mathcal{I}_a) \leftrightarrow \mathcal{I}_3, \end{cases}$$

where subinstance $\mathcal{I}_a$ is an acyclic index coding instance of size 4, subinstances $\mathcal{I}_1$ and $\mathcal{I}_3$ are of size 29 and 58, respectively, and will be characterized, respectively, in Sections IV-C and V, with the following properties:

- In Theorem 2, it is proved that $\lambda_q(\mathcal{I}_1) = \beta(\mathcal{I}_1) = 4$ if and only if field $\mathbb{F}_q$ does have characteristic three.
- In Theorem 4, it is proved that $\lambda_q(\mathcal{I}_3) = \beta(\mathcal{I}_3) = 8$ if and only if field $\mathbb{F}_q$ does have any characteristic other than characteristic three.

From Theorems 2 and 4, it is concluded that linear coding over any field cannot simultaneously be optimal for both subinstances $\mathcal{I}_1$ and $\mathcal{I}_3$. This is because if the characteristic of $\mathbb{F}_q$ is three, then $\lambda_q(\mathcal{I}_3) > 8$, and if it is not three, then $\lambda_q(\mathcal{I}_1) > 4$.

From Proposition 2, $\lambda_q(\mathcal{I}_a) = 4$ over $\mathbb{F}_q$ with any characteristic.

Thus, according to Proposition 5, the linear broadcast rate of $\mathcal{I}$ and $\mathcal{I}'$ will be

$$\begin{cases} \lambda(\mathcal{I}) = \min_q\big(\lambda_q(\mathcal{I}_1) + \lambda_q(\mathcal{I}_3)\big) > 12, \\ \lambda\big(\mathcal{I}'\big) = \min_q \max\big\{\lambda_q(\mathcal{I}_1) + 3, \lambda_q(\mathcal{I}_3)\big\} > 8. \end{cases} \tag{13}$$

Then,

- In Proposition 8, we show that for subinstance $\mathcal{I}_1$, there is an optimal scalar linear code with the encoding matrix $\boldsymbol{H}_* \in \mathbb{F}_q^{4\times 29}$ and four output coded messages $\{y_1, y_2, y_3, y_4\}$.
- In Proposition 15, for subinstance $\mathcal{I}_3$, we design an optimal nonlinear code with the encoder $\phi_{\mathcal{I}_3}$ and eight output coded messages $\{z_1, \ldots, z_8\}$.

- According to Proposition 2, $\lambda_q(\mathcal{I}_a) = 4$. Assume that the coded messages $\{y_5, y_6, y_7, y_8\}$ are the optimal linear code for $\mathcal{I}_a$.

Now, it can be easily checked that the following coded messages are the optimal code for $\mathcal{I}$ and $\mathcal{I}'$:

$$\begin{cases} \mathcal{I} : \{y_1, \ldots, y_4\} \cup \{z_1, \ldots, z_8\}, \\ \mathcal{I}' : \{y_1 + z_1, \ldots, y_8 + z_8\}, \end{cases} \tag{14}$$

which completes the proof. ■

IV. THE DEPENDENCY OF LINEAR CODING RATE ON THE FIELDS WITH CHARACTERISTIC THREE

This section presents two index coding instances $\mathcal{I}_1$ and $\mathcal{I}_2$. We prove that while linear coding is optimal for $\mathcal{I}_1$ only over the fields with characteristic three, it can never be optimal for $\mathcal{I}_2$ over any field with characteristic three. To prove this, we first define two matroid instances $\mathcal{N}_1$ and $\mathcal{N}_2$ and show that their linear representation is dependent on the fields with characteristic three. Then, we show that the main constraints on the column space of the encoding matrices of $\mathcal{I}_1$ and $\mathcal{I}_2$ can be reduced to the constraints on the column space of the matrices, which are the linear representation of $\mathcal{N}_1$ and $\mathcal{N}_2$, respectively.

A. MATROID INSTANCES $\mathcal{N}_1$ AND $\mathcal{N}_2$

1) MATROID INSTANCE $\mathcal{N}_1$

Definition 22 (Matroid Instance $\mathcal{N}_1$): Consider matroid instance $\mathcal{N}_1 = \{f(N), N \subseteq [n]\}$, where $n = 9$, $f(\mathcal{N}_1) = 4$, set $N_0 = [4]$ is a basis, and the following N_i's, $i \in [9]$, are circuit sets:

$$\begin{aligned} N_1 &= \{1, 2, 3, 5\}, \\ N_2 &= \{1, 2, 4, 6\}, \\ N_3 &= \{1, 3, 4, 7\}, \\ N_4 &= \{2, 3, 4, 8\}, \\ N_5 &= \{1, 8, 9\}, \\ N_6 &= \{2, 7, 9\}, \\ N_7 &= \{3, 6, 9\}, \\ N_8 &= \{4, 5, 9\}, \\ N_9 &= \{5, 6, 7, 8\}. \end{aligned} \tag{15}$$

Proposition 6: Matroid instance $\mathcal{N}_1$ is linearly representable over field $\mathbb{F}_q$, if and only if field $\mathbb{F}_q$ does have characteristic three.

Proof: For the *if* condition, it can be checked that matrix $\boldsymbol{H}_{\mathcal{N}} \in \mathbb{F}_q^{4\times 9}$, shown in Figure 1, is a scalar linear representation of matroid instance $\mathcal{N}_1$, where $\mathbb{F}_q$ has characteristic three. The key part of $\boldsymbol{H}_{\mathcal{N}}$ is its submatrix $\boldsymbol{H}_{\mathcal{N}}^{N_9=\{5,6,7,8\}}$, which is as follows

$$\boldsymbol{H}_{\mathcal{N}}^{N_9} = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix} \in \mathbb{F}_q^{4\times 4}. \tag{16}$$

	1	2	3	4	5	6	7	8	9
1	1	0	0	0	1	1	1	0	1
2	0	1	0	0	1	1	0	1	1
3	0	0	1	0	1	0	1	1	1
4	0	0	0	1	0	1	1	1	1

FIGURE 1. $\boldsymbol{H}_{\mathcal{N}} \in \mathbb{F}_q^{4\times 9}$: If $\mathbb{F}_q$ has characteristic three (such as $GF(3)$), then $\boldsymbol{H}_{\mathcal{N}}$ is a scalar linear representation of matroid $\mathcal{N}_1$, and if $\mathbb{F}_q$ does have any characteristic other than characteristic three (such as $GF(2)$), then $\boldsymbol{H}_{\mathcal{N}}$ is a scalar linear representation of matroid $\mathcal{N}_2$.

First, it can be seen that

$$\text{rank}\left(\boldsymbol{H}_{\mathcal{N}}^{N_9\backslash\{i\}}\right) = 3, \ \ \forall i \in N_9. \tag{17}$$

Second, applying the Gaussian elimination method to $\boldsymbol{H}_{\mathcal{N}}^{N_9}$ will result in

$$\begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & -1 & 0 & 1 \\ 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & 1+1+1 \end{bmatrix} \in \mathbb{F}_q^{4\times 4}. \tag{18}$$

Now, if field $\mathbb{F}_q$ has characteristic three (such as $GF(3)$), then 1+1+1 will be equal to zero, which leads to

$$\text{rank}\left(\boldsymbol{H}_{\mathcal{N}}^{N_9}\right) = 3. \tag{19}$$

From (17) and (19), it is observed that set N_9 is a circuit set of $\boldsymbol{H}_{\mathcal{N}} \in \mathbb{F}_q^{4\times 9}$ if field $\mathbb{F}_q$ has characteristic three.

The *converse* is proved as follows.

First, since set [4] is a basis set, we get

$$\text{rank}\left(\boldsymbol{H}^{[4]}\right) = 4t. \tag{20}$$

Since each $N_i, i \in [9]$ forms a circuit set, we have

$$\begin{aligned} N_1 &\to \boldsymbol{H}^{\{5\}} = \boldsymbol{H}^{\{1\}}\boldsymbol{M}_{5,1} + \boldsymbol{H}^{\{2\}}\boldsymbol{M}_{5,2} + \boldsymbol{H}^{\{3\}}\boldsymbol{M}_{5,3}, & (21)\\ N_2 &\to \boldsymbol{H}^{\{6\}} = \boldsymbol{H}^{\{1\}}\boldsymbol{M}_{6,1} + \boldsymbol{H}^{\{2\}}\boldsymbol{M}_{6,2} + \boldsymbol{H}^{\{4\}}\boldsymbol{M}_{6,4}, & (22)\\ N_3 &\to \boldsymbol{H}^{\{7\}} = \boldsymbol{H}^{\{1\}}\boldsymbol{M}_{7,1} + \boldsymbol{H}^{\{3\}}\boldsymbol{M}_{7,3} + \boldsymbol{H}^{\{4\}}\boldsymbol{M}_{7,4}, & (23)\\ N_4 &\to \boldsymbol{H}^{\{8\}} = \boldsymbol{H}^{\{2\}}\boldsymbol{M}_{8,2} + \boldsymbol{H}^{\{3\}}\boldsymbol{M}_{8,3} + \boldsymbol{H}^{\{4\}}\boldsymbol{M}_{8,4}, & (24)\\ N_5 &\to \boldsymbol{H}^{\{9\}} = \boldsymbol{H}^{\{1\}}\boldsymbol{M}_{9,1} + \boldsymbol{H}^{\{8\}}\boldsymbol{M}_{9,8}, & (25)\\ N_6 &\to \boldsymbol{H}^{\{9\}} = \boldsymbol{H}^{\{2\}}\boldsymbol{M}_{9,2} + \boldsymbol{H}^{\{7\}}\boldsymbol{M}_{9,7}, & (26)\\ N_7 &\to \boldsymbol{H}^{\{9\}} = \boldsymbol{H}^{\{3\}}\boldsymbol{M}_{9,3} + \boldsymbol{H}^{\{6\}}\boldsymbol{M}_{9,6}, & (27)\\ N_8 &\to \boldsymbol{H}^{\{9\}} = \boldsymbol{H}^{\{4\}}\boldsymbol{M}_{9,4} + \boldsymbol{H}^{\{5\}}\boldsymbol{M}_{9,5}, & (28)\\ N_9 &\to \boldsymbol{H}^{\{8\}} = \boldsymbol{H}^{\{5\}}\boldsymbol{M}_{8,5} + \boldsymbol{H}^{\{6\}}\boldsymbol{M}_{8,6} + \boldsymbol{H}^{\{7\}}\boldsymbol{M}_{8,7}, & (29) \end{aligned}$$

where all matrices $\boldsymbol{M}_{j,i}$ are invertible. Now, in (25)-(28), we replace $\boldsymbol{H}^{\{5\}}, \boldsymbol{H}^{\{6\}}, \boldsymbol{H}^{\{7\}}$ and $\boldsymbol{H}^{\{8\}}$, respectively, with their equal terms in (21)-(24). Thus, $\boldsymbol{H}^{\{9\}}$ will be equal to

$$\begin{aligned} \boldsymbol{H}^{\{9\}} &= \boldsymbol{H}^{\{1\}}\boldsymbol{M}_{9,1} + \left(\boldsymbol{H}^{\{2\}}\boldsymbol{M}_{8,2} + \boldsymbol{H}^{\{3\}}\boldsymbol{M}_{8,3} + \boldsymbol{H}^{\{4\}}\boldsymbol{M}_{8,4}\right)\boldsymbol{M}_{9,8}, \\ \boldsymbol{H}^{\{9\}} &= \boldsymbol{H}^{\{2\}}\boldsymbol{M}_{9,2} + \left(\boldsymbol{H}^{\{1\}}\boldsymbol{M}_{7,1} + \boldsymbol{H}^{\{3\}}\boldsymbol{M}_{7,3} + \boldsymbol{H}^{\{4\}}\boldsymbol{M}_{7,4}\right)\boldsymbol{M}_{9,7}, \\ \boldsymbol{H}^{\{9\}} &= \boldsymbol{H}^{\{3\}}\boldsymbol{M}_{9,3} + \left(\boldsymbol{H}^{\{1\}}\boldsymbol{M}_{6,1} + \boldsymbol{H}^{\{2\}}\boldsymbol{M}_{6,2} + \boldsymbol{H}^{\{4\}}\boldsymbol{M}_{6,4}\right)\boldsymbol{M}_{9,6}, \\ \boldsymbol{H}^{\{9\}} &= \boldsymbol{H}^{\{4\}}\boldsymbol{M}_{9,4} + \left(\boldsymbol{H}^{\{1\}}\boldsymbol{M}_{5,1} + \boldsymbol{H}^{\{2\}}\boldsymbol{M}_{5,2} + \boldsymbol{H}^{\{3\}}\boldsymbol{M}_{5,3}\right)\boldsymbol{M}_{9,5}. \end{aligned}$$

Now, due to (20), the above four equations, representing $\boldsymbol{H}^{\{9\}}$, are all equal only if their coefficients of $\boldsymbol{H}^{\{1\}}, \boldsymbol{H}^{\{2\}}, \boldsymbol{H}^{\{3\}}$

and $\boldsymbol{H}^{\{4\}}$, are equal. Thus, by equating the coefficients of $\boldsymbol{H}^{\{1\}}, \boldsymbol{H}^{\{2\}}, \boldsymbol{H}^{\{3\}}$ and $\boldsymbol{H}^{\{4\}}$, respectively, we have

$$\boldsymbol{M}_{9,1} = \boldsymbol{M}_{5,1}\boldsymbol{M}_{9,5} = \boldsymbol{M}_{6,1}\boldsymbol{M}_{9,6} = \boldsymbol{M}_{7,1}\boldsymbol{M}_{9,7}, \quad (30)$$
$$\boldsymbol{M}_{9,2} = \boldsymbol{M}_{5,2}\boldsymbol{M}_{9,5} = \boldsymbol{M}_{6,2}\boldsymbol{M}_{9,6} = \boldsymbol{M}_{8,2}\boldsymbol{M}_{9,8}, \quad (31)$$
$$\boldsymbol{M}_{9,3} = \boldsymbol{M}_{5,3}\boldsymbol{M}_{9,5} = \boldsymbol{M}_{7,3}\boldsymbol{M}_{9,7} = \boldsymbol{M}_{8,3}\boldsymbol{M}_{9,8}, \quad (32)$$
$$\boldsymbol{M}_{9,4} = \boldsymbol{M}_{6,4}\boldsymbol{M}_{9,6} = \boldsymbol{M}_{7,4}\boldsymbol{M}_{9,7} = \boldsymbol{M}_{8,4}\boldsymbol{M}_{9,8}. \quad (33)$$

Now, we have

$$(30) \rightarrow \boldsymbol{M}_{9,5} = \boldsymbol{M}_{5,1}^{-1}\boldsymbol{M}_{6,1}\boldsymbol{M}_{9,6} = \boldsymbol{M}_{5,1}^{-1}\boldsymbol{M}_{7,1}\boldsymbol{M}_{9,7}, \quad (34)$$
$$(31) \rightarrow \boldsymbol{M}_{9,5} = \boldsymbol{M}_{5,2}^{-1}\boldsymbol{M}_{6,2}\boldsymbol{M}_{9,6} = \boldsymbol{M}_{5,2}^{-1}\boldsymbol{M}_{8,2}\boldsymbol{M}_{9,8}, \quad (35)$$
$$(32) \rightarrow \boldsymbol{M}_{9,5} = \boldsymbol{M}_{5,3}^{-1}\boldsymbol{M}_{7,3}\boldsymbol{M}_{9,7} = \boldsymbol{M}_{5,3}^{-1}\boldsymbol{M}_{8,3}\boldsymbol{M}_{9,8}. \quad (36)$$

Thus,

$$(34), (35) \rightarrow \boldsymbol{M}_{5,1}^{-1}\boldsymbol{M}_{6,1} = \boldsymbol{M}_{5,2}^{-1}\boldsymbol{M}_{6,2}, \quad (37)$$
$$(35), (36) \rightarrow \boldsymbol{M}_{5,2}^{-1}\boldsymbol{M}_{8,2} = \boldsymbol{M}_{5,3}^{-1}\boldsymbol{M}_{8,3}, \quad (38)$$
$$(34), (36) \rightarrow \boldsymbol{M}_{5,1}^{-1}\boldsymbol{M}_{7,1} = \boldsymbol{M}_{5,3}^{-1}\boldsymbol{M}_{7,3}. \quad (39)$$

On the other hand, in (29), we replace $\boldsymbol{H}^{\{5\}}, \boldsymbol{H}^{\{6\}}, \boldsymbol{H}^{\{7\}}$ and $\boldsymbol{H}^{\{8\}}$, with their equal terms in (21)-(24). By equating the coefficients of $\boldsymbol{H}^{\{1\}}, \boldsymbol{H}^{\{2\}}, \boldsymbol{H}^{\{3\}}$ and $\boldsymbol{H}^{\{4\}}$, we get

$$\boldsymbol{0}_t = \boldsymbol{M}_{5,1}\boldsymbol{M}_{8,5} + \boldsymbol{M}_{6,1}\boldsymbol{M}_{8,6} + \boldsymbol{M}_{7,1}\boldsymbol{M}_{8,7}, \quad (40)$$
$$\boldsymbol{M}_{8,2} = \boldsymbol{M}_{5,2}\boldsymbol{M}_{8,5} + \boldsymbol{M}_{6,2}\boldsymbol{M}_{8,6}, \quad (41)$$
$$\boldsymbol{M}_{8,3} = \boldsymbol{M}_{5,3}\boldsymbol{M}_{8,5} + \boldsymbol{M}_{7,3}\boldsymbol{M}_{8,7}, \quad (42)$$
$$\boldsymbol{M}_{8,4} = \boldsymbol{M}_{6,4}\boldsymbol{M}_{8,6} + \boldsymbol{M}_{7,4}\boldsymbol{M}_{8,7}. \quad (43)$$

Now, if (41) and (42) are multiplied by $\boldsymbol{M}_{5,2}^{-1}$ and $\boldsymbol{M}_{5,3}^{-1}$, respectively, we have

$$\boldsymbol{M}_{5,2}^{-1}\boldsymbol{M}_{8,2} = \boldsymbol{M}_{8,5} + \boldsymbol{M}_{5,2}^{-1}\boldsymbol{M}_{6,2}\boldsymbol{M}_{8,6}, \quad (44)$$
$$\boldsymbol{M}_{5,3}^{-1}\boldsymbol{M}_{8,3} = \boldsymbol{M}_{8,5} + \boldsymbol{M}_{5,3}^{-1}\boldsymbol{M}_{7,3}\boldsymbol{M}_{8,7}. \quad (45)$$

Now, combining (38), (44) and (45) results in

$$\boldsymbol{M}_{5,2}^{-1}\boldsymbol{M}_{6,2}\boldsymbol{M}_{8,6} = \boldsymbol{M}_{5,3}^{-1}\boldsymbol{M}_{7,3}\boldsymbol{M}_{8,7} \quad (46)$$
$$\rightarrow \boldsymbol{M}_{5,1}^{-1}\boldsymbol{M}_{6,1}\boldsymbol{M}_{8,6} = \boldsymbol{M}_{5,1}^{-1}\boldsymbol{M}_{7,1}\boldsymbol{M}_{8,7} \quad (47)$$
$$\rightarrow \boldsymbol{M}_{6,1}\boldsymbol{M}_{8,6} = \boldsymbol{M}_{7,1}\boldsymbol{M}_{8,7}, \quad (48)$$

where (47) is due to (37) and (39).

Now, we prove $\boldsymbol{M}_{5,1}\boldsymbol{M}_{8,5} = \boldsymbol{M}_{7,1}\boldsymbol{M}_{8,7}$. From (31)-(33), we have

$$(30) \rightarrow \boldsymbol{M}_{9,6} = \boldsymbol{M}_{6,1}^{-1}\boldsymbol{M}_{5,1}\boldsymbol{M}_{9,5} = \boldsymbol{M}_{6,1}^{-1}\boldsymbol{M}_{7,1}\boldsymbol{M}_{9,7}, \quad (49)$$
$$(31) \rightarrow \boldsymbol{M}_{9,6} = \boldsymbol{M}_{6,2}^{-1}\boldsymbol{M}_{5,2}\boldsymbol{M}_{9,5} = \boldsymbol{M}_{6,2}^{-1}\boldsymbol{M}_{8,2}\boldsymbol{M}_{9,8}, \quad (50)$$
$$(33) \rightarrow \boldsymbol{M}_{9,6} = \boldsymbol{M}_{6,4}^{-1}\boldsymbol{M}_{7,4}\boldsymbol{M}_{9,7} = \boldsymbol{M}_{6,4}^{-1}\boldsymbol{M}_{8,4}\boldsymbol{M}_{9,8}. \quad (51)$$

Thus,

$$(49), (50) \rightarrow \boldsymbol{M}_{6,1}^{-1}\boldsymbol{M}_{5,1} = \boldsymbol{M}_{6,2}^{-1}\boldsymbol{M}_{5,2}, \quad (52)$$
$$(50), (51) \rightarrow \boldsymbol{M}_{6,2}^{-1}\boldsymbol{M}_{8,2} = \boldsymbol{M}_{6,4}^{-1}\boldsymbol{M}_{8,4}, \quad (53)$$
$$(49), (51) \rightarrow \boldsymbol{M}_{6,1}^{-1}\boldsymbol{M}_{7,1} = \boldsymbol{M}_{6,4}^{-1}\boldsymbol{M}_{7,4}. \quad (54)$$

If (41) and (43) are multiplied by $\boldsymbol{M}_{6,2}^{-1}$ and $\boldsymbol{M}_{6,4}^{-1}$, respectively, we have

$$\boldsymbol{M}_{6,2}^{-1}\boldsymbol{M}_{8,2} = \boldsymbol{M}_{6,2}^{-1}\boldsymbol{M}_{5,2}\boldsymbol{M}_{8,5} + \boldsymbol{M}_{8,6}, \quad (55)$$
$$\boldsymbol{M}_{6,4}^{-1}\boldsymbol{M}_{8,4} = \boldsymbol{M}_{6,4}^{-1}\boldsymbol{M}_{7,4}\boldsymbol{M}_{8,7} + \boldsymbol{M}_{8,6}. \quad (56)$$

Since, based on (53), $\boldsymbol{M}_{6,2}^{-1}\boldsymbol{M}_{8,2} = \boldsymbol{M}_{6,4}^{-1}\boldsymbol{M}_{8,4}$, (55) and (56) will lead to

$$\boldsymbol{M}_{6,2}^{-1}\boldsymbol{M}_{5,2}\boldsymbol{M}_{8,5} = \boldsymbol{M}_{6,4}^{-1}\boldsymbol{M}_{7,4}\boldsymbol{M}_{8,7} \quad (57)$$
$$\rightarrow \boldsymbol{M}_{6,1}^{-1}\boldsymbol{M}_{5,1}\boldsymbol{M}_{8,5} = \boldsymbol{M}_{6,1}^{-1}\boldsymbol{M}_{7,1}\boldsymbol{M}_{8,7}, \quad (58)$$
$$\rightarrow \boldsymbol{M}_{5,1}\boldsymbol{M}_{8,5} = \boldsymbol{M}_{7,1}\boldsymbol{M}_{8,7}, \quad (59)$$

where (58) is due to (52) and (54).

Now, (40), (48) and (59) will lead to

$$\begin{aligned}\boldsymbol{0}_t &= \boldsymbol{M}_{7,1}\boldsymbol{M}_{8,7} + \boldsymbol{M}_{7,1}\boldsymbol{M}_{8,7} + \boldsymbol{M}_{7,1}\boldsymbol{M}_{8,7}\\ &= (\boldsymbol{I}_t + \boldsymbol{I}_t + \boldsymbol{I}_t)\boldsymbol{M}_{7,1}\boldsymbol{M}_{8,7}, \end{aligned} \quad (60)$$

which is possible only over the fields with characteristic three as both $\boldsymbol{M}_{7,1}$ and $\boldsymbol{M}_{8,7}$ are invertible. This completes the proof. ■

2) MATROID INSTANCE $\mathcal{N}_2$

Definition 23 (Matroid Instance $\mathcal{N}_2$): Consider matroid instance $\mathcal{N}_2 = \{f(N), N \subseteq [n]\}$, where $n = 9$, $f(\mathcal{N}_2) = 4$, each set $N_0 = [4]$ and $N_9 = \{5, 6, 7, 8\}$ forms a basis, and the following N_i's, $i \in [8]$, are circuit sets:

$$\begin{aligned} N_1 &= \{1, 2, 3, 5\},\\ N_2 &= \{1, 2, 4, 6\},\\ N_3 &= \{1, 3, 4, 7\},\\ N_4 &= \{2, 3, 4, 8\},\\ N_5 &= \{1, 8, 9\},\\ N_6 &= \{2, 7, 9\},\\ N_7 &= \{3, 6, 9\},\\ N_8 &= \{4, 5, 9\}. \end{aligned} \quad (61)$$

It is worth noting that matroid instances $\mathcal{N}_1$ and $\mathcal{N}_2$ are exactly the same, with only differing in set $N_9 = \{5, 6, 7, 8\}$. While set N_9 is a circuit set for matroid instance $\mathcal{N}_1$, it is a basis set for matroid instance $\mathcal{N}_2$.

Proposition 7: Matroid instance $\mathcal{N}_2$ is linearly representable over field $\mathbb{F}_q$ if and only if field $\mathbb{F}_q$ does have any characteristic other than characteristic three.

Proof: For the *if* condition, it can be verified that matrix $\boldsymbol{H}_{\mathcal{N}} \in \mathbb{F}_q^{4\times 9}$, shown in Figure 1, is a scalar linear representation of $\mathcal{N}_2$, where $\mathbb{F}_q$ does have any characteristic other than characteristic three. The key part of $\boldsymbol{H}_{\mathcal{N}}$ is its submatrix $\boldsymbol{H}_{\mathcal{N}}^{N_9=\{5,6,7,8\}}$ in (16). From (18), it can be seen that if field $\mathbb{F}_q$ has any characteristic other than three (such as $GF(2)$), then $1 + 1 + 1$ will be a nonzero element, leading to

$$\operatorname{rank}\left(\boldsymbol{H}_{\mathcal{N}}^{N_9}\right) = 4.$$

This means that set N_9 is a basis set of $\boldsymbol{H}_{\mathcal{N}} \in \mathbb{F}_q^{4\times 9}$ if field $\mathbb{F}_q$ has any characteristic other than characteristic three.

The *converse* is proved as follows.

Since sets $N_0, \dots, N_8$ in matroid $\mathcal{N}_2$ are exactly the same as the sets in matroid $\mathcal{N}_1$, equations (30)-(36) can also be derived for matroid $\mathcal{N}_2$. Now, since matrices $\boldsymbol{M}_{5,j}, \boldsymbol{M}_{6,j}, \boldsymbol{M}_{7,j}, \boldsymbol{M}_{8,j}$ are invertible for all $j \in [3]$, then according to equations (34), (35) and (36), we have

$$\mathrm{col}(\boldsymbol{M}_{9,5}) = \mathrm{col}(\boldsymbol{M}_{9,6}) = \mathrm{col}(\boldsymbol{M}_{9,7}) = \mathrm{col}(\boldsymbol{M}_{9,8}). \quad (62)$$

Now, equations (62) and (30)-(33) will lead to

$$\mathrm{col}(\boldsymbol{M}_{9,1}) = \mathrm{col}(\boldsymbol{M}_{9,2}) = \mathrm{col}(\boldsymbol{M}_{9,3}) = \mathrm{col}(\boldsymbol{M}_{9,4}). \quad (63)$$

Thus, each $\boldsymbol{M}_{9,j}, j \in [4]$ must be invertible, since otherwise, it leads to $\mathrm{rank}(\boldsymbol{H}^{\{9\}}) < t$, which contradicts (12) for $i = 9$.

Now, assuming that the field has characteristic three, (30)-(33), respectively, will result in

$$\boldsymbol{0}_t = \boldsymbol{M}_{5,1}\boldsymbol{M}_{9,5} + \boldsymbol{M}_{6,1}\boldsymbol{M}_{9,6} + \boldsymbol{M}_{7,1}\boldsymbol{M}_{9,7}, \quad (64)$$
$$2\boldsymbol{M}_{8,2}\boldsymbol{M}_{9,8} = \boldsymbol{M}_{5,2}\boldsymbol{M}_{9,5} + \boldsymbol{M}_{6,2}\boldsymbol{M}_{9,6}, \quad (65)$$
$$2\boldsymbol{M}_{8,3}\boldsymbol{M}_{9,8} = \boldsymbol{M}_{5,3}\boldsymbol{M}_{9,5} + \boldsymbol{M}_{7,3}\boldsymbol{M}_{9,7}, \quad (66)$$
$$2\boldsymbol{M}_{8,4}\boldsymbol{M}_{9,8} = \boldsymbol{M}_{6,4}\boldsymbol{M}_{9,6} + \boldsymbol{M}_{7,4}\boldsymbol{M}_{9,7}, \quad (67)$$

which can be rewritten as

$$2\begin{bmatrix}\boldsymbol{0}_t\\ \boldsymbol{M}_{8,2}\\ \boldsymbol{M}_{8,3}\\ \boldsymbol{M}_{8,4}\end{bmatrix}\boldsymbol{M}_{9,8} = \begin{bmatrix}\boldsymbol{M}_{5,1}\\ \boldsymbol{M}_{5,2}\\ \boldsymbol{M}_{5,3}\\ \boldsymbol{0}_t\end{bmatrix}\boldsymbol{M}_{9,5} + \begin{bmatrix}\boldsymbol{M}_{6,1}\\ \boldsymbol{M}_{6,2}\\ \boldsymbol{0}_t\\ \boldsymbol{M}_{6,4}\end{bmatrix}\boldsymbol{M}_{9,6} + \begin{bmatrix}\boldsymbol{M}_{7,1}\\ \boldsymbol{0}_t\\ \boldsymbol{M}_{7,3}\\ \boldsymbol{M}_{7,4}\end{bmatrix}\boldsymbol{M}_{9,7},$$

which means that

$$2\boldsymbol{H}^{\{8\}}\boldsymbol{M}_{9,8} = \boldsymbol{H}^{\{5\}}\boldsymbol{M}_{9,5} + \boldsymbol{H}^{\{6\}}\boldsymbol{M}_{9,6} + \boldsymbol{H}^{\{7\}}\boldsymbol{M}_{9,7}. \quad (68)$$

Now, since each $\boldsymbol{M}_{9,5}, \boldsymbol{M}_{9,6}, \boldsymbol{M}_{9,7}$ and $\boldsymbol{M}_{9,8}$ is invertible, from (68), it is concluded that set $\{5, 6, 7, 8\}$ forms a circuit set, which contradicts the assumption that set $N_9 = \{5, 6, 7, 8\}$ is a basis set of matroid $\mathcal{N}_2$. This completes the proof. ∎

B. ON THE REDUCTION PROCESS FROM INDEX CODING TO MATROID

In this subsection, through Lemmas 1-5, we establish some reduction techniques to map specific constraints on the column space of the encoder matrix of an index coding instance to the constraints on the column space of the matrix, which is a linear representation of a matroid instance. Proofs of Lemmas 1-5 are provided in Appendix B.

Remark 4: Note that the reduction technique from matroid to index coding, proposed in [2], requires all the basis sets $\mathcal{B}$ and circuit sets $\mathcal{C}$ of a matroid to map the constraints on its linear representation matrix to the constraints on the encoding matrix of an index coding instance. This results in a groupcast index coding instance, with significantly high number of users. For example, applying this method to matroid instances $\mathcal{N}_1$ and $\mathcal{N}_2$ results in two groupcast index coding instances, each with more than 300 users. Moreover, applying the reduction method in [8] (from groupcast to unicast index coding instance) will lead to two asymmetric-rate unicast index coding instances, each comprising more than 1000 users. However, in the reduction techniques in this paper (Lemmas 1-5), we efficiently use some specific constraints to build the two symmetric-rate unicast index coding instances $\mathcal{I}_1$ and $\mathcal{I}_2$, containing only 29 users.

In this subsection, we assume that $M \subseteq [m]$, $i, l \in M$, and $j \in [m]\backslash M$.

Lemma 1: Assume M is an acyclic set of $\mathcal{I}$. Then, the condition in (2) for all $i \in M$ requires $\mathrm{rank}(\boldsymbol{H}^M) = |M|t$, implying that M must be an independent set of $\boldsymbol{H}$.

Lemma 2: Let M be a minimal cyclic set of $\mathcal{I}$. To have $\mathrm{rank}(\boldsymbol{H}^M) = (|M| - 1)t$, M must be a circuit set of $\boldsymbol{H}$.

Example 3: Consider the index coding instance $\mathcal{I} = \{B_i, i \in [4]\}$, where

$$B_1 = \{2, 3\}, \quad B_2 = \{3, 4\},$$
$$B_3 = \{1, 4\}, \quad B_4 = \{1, 2\}. \quad (69)$$

First, since set [3] is an acyclic set of $\mathcal{I}$, according to Lemma 1, we must have $\mathrm{rank}(\boldsymbol{H}^{[3]}) = 3t$. Besides, set [4] is a minimal cyclic set of $\mathcal{I}$. To have $\mathrm{rank}(\boldsymbol{H}^{[4]}) = 3t$, according to Lemma 2, set [4] must be a circuit set of $\boldsymbol{H}$. It can be easily seen that the users can be all satisfied by the following encoder matrix

$$\boldsymbol{H} = \begin{bmatrix}1 & 0 & 0 & 1\\ 0 & 1 & 0 & 1\\ 0 & 0 & 1 & 1\end{bmatrix}. \quad (70)$$

Lemma 3: Assume M is an independent set of $\mathcal{I}$, and $j \in B_i, \forall i \in M\backslash\{l\}$ for some $l \in M$. Then, if $\mathrm{col}(\boldsymbol{H}^{\{j\}}) \subseteq \mathrm{col}(\boldsymbol{H}^M)$, we must have $\mathrm{col}(\boldsymbol{H}^{\{j\}}) = \mathrm{col}(\boldsymbol{H}^{\{l\}})$.

Example 4: Consider the index coding instance $\mathcal{I} = \{B_i, i \in [4]\}$, where

$$B_1 = \{2, 3\},\ B_2 = \{1, 3, 4\},\ B_3 = \{1, 2, 4\},\ B_4 = \emptyset.$$

Since set [3] is an independent set of $\mathcal{I}$, Lemma 1 requires that $\mathrm{rank}(\boldsymbol{H}^{[3]}) = 3t$. Now, if we desire $\mathrm{rank}(\boldsymbol{H}^{[4]}) = 3t$, then we must have $\mathrm{col}(\boldsymbol{H}^{\{4\}}) \subseteq \mathrm{col}(\boldsymbol{H}^{[3]})$. Since $4 \in B_i, i \in [3]\backslash\{1\}$, according to Lemma 3, we must have $\mathrm{col}(\boldsymbol{H}^{\{4\}}) = \mathrm{col}(\boldsymbol{H}^{\{1\}})$. It can be easily checked that the following encoder matrix can satisfy all the four users

$$\begin{bmatrix}1 & 0 & 0 & 1\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\end{bmatrix}. \quad (71)$$

Lemma 4: Let $M \subseteq [m]$ and $j \in [m]\backslash M$. Assume that

(i) M is an independent set of $\boldsymbol{H}$,
(ii) $\mathrm{col}(\boldsymbol{H}^{\{j\}}) \subseteq \mathrm{col}(\boldsymbol{H}^M)$,
(iii) M forms a minimal cyclic set of $\mathcal{I}$,
(iv) $j \in B_i, \forall i \in M$.

Now, the condition in (2) for all $i \in [m]$ requires set $\{j\} \cup M$ to be a circuit set of $\boldsymbol{H}$.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
1	1	0	0	0	1	1	1	0	1	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	0	1	0	0
2	0	1	0	0	1	1	0	1	1	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	1	0	0	0
3	0	0	1	0	1	0	1	1	1	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	0	1
4	0	0	0	1	0	1	1	1	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	1	0

FIGURE 2. $\boldsymbol{H}_* \in \mathbb{F}_q^{4\times 29}$: If $\mathbb{F}_q$ does have characteristic three (such as $GF(3)$), then $\boldsymbol{H}_*$ is an encoding matrix for the index coding instance $\mathcal{I}_1$, and if $\mathbb{F}_q$ does have any characteristic other than characteristic three (such as $GF(2)$), then $\boldsymbol{H}_*$ is an encoding matrix for the index coding instance $\mathcal{I}_2$.

Example 5: Consider the index coding instance $\mathcal{I} = \{B_i, i \in [4]\}$, where

$$B_1 = \{2, 4\}, B_2 = \{3, 4\}, B_3 = \{1, 4\}, B_4 = \emptyset. \tag{72}$$

Assume that for the encoder matrix $\boldsymbol{H}$, we have $\text{rank}(\boldsymbol{H}^{[3]}) = 3t$, as follows

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

It can be seen that set [3] is a minimal cyclic set of $\mathcal{I}$. Now, if we desire $\text{col}(\boldsymbol{H}^{\{4\}}) \subseteq \text{col}(\boldsymbol{H}^{[3]})$, due to $4 \in B_i, i \in [3]$, set [4] must be a circuit set of $\boldsymbol{H}$, as follows

$$\begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}.$$

Lemma 5: Assume for matrix $\boldsymbol{H} \in \mathbb{F}_q^{4t\times 9t}$,

(i) set [4] is a basis set,

(ii) each set $\{1, 2, 3, 5\}, \{1, 2, 4, 6\}, \{1, 3, 4, 7\}, \{2, 3, 4, 8\}$ is a circuit set,

(iii)

$$\text{col}\left(\boldsymbol{H}^{\{9\}}\right) \subseteq \text{col}\left(\boldsymbol{H}^{\{4,5\}}\right),$$
$$\text{col}\left(\boldsymbol{H}^{\{9\}}\right) \subseteq \text{col}\left(\boldsymbol{H}^{\{3,6\}}\right),$$
$$\text{col}\left(\boldsymbol{H}^{\{9\}}\right) \subseteq \text{col}\left(\boldsymbol{H}^{\{2,7\}}\right),$$
$$\text{col}\left(\boldsymbol{H}^{\{9\}}\right) \subseteq \text{col}\left(\boldsymbol{H}^{\{1,8\}}\right).$$

Then, each set $\{1, 8, 9\}, \{2, 7, 9\}, \{3, 6, 9\}, \{4, 5, 9\}$ is also a circuit set.

C. INDEX CODING INSTANCES $\mathcal{I}_1$ AND $\mathcal{I}_2$

This subsection characterizes the index coding instances $\mathcal{I}_1$ and $\mathcal{I}_2$, each of size 29, and each with the broadcast rate $\beta(\mathcal{I}_1) = \beta(\mathcal{I}_2) = 4$. The interfering message set of all the users in $\mathcal{I}_1$ and $\mathcal{I}_2$ are exactly the same, except for users $u_i, i \in [5:9]$. Theorems 2 and 3 establish the sufficient and necessary conditions for linear coding to be optimal for $\mathcal{I}_1$ and $\mathcal{I}_2$, respectively.

- Sufficient condition: It is shown that scalar linear coding with the encoding matrix $\boldsymbol{H}_* \in \mathbb{F}_q^{4\times 29}$, shown in Figure 2, achieves the optimal broadcast rate of $\mathcal{I}_1$ if its field $\mathbb{F}_q$ does have characteristic three (such as $GF(3)$), and it is optimal for $\mathcal{I}_2$ if its field $\mathbb{F}_q$ does have any characteristic other than characteristic three (such as $GF(2)$).
- Necessary condition: Using Lemmas 1-5, it is proved that the constraints on the column space of the local encoding matrix of the first 9 users $\boldsymbol{H}^{[9]}$ in $\mathcal{I}_1$ and $\mathcal{I}_2$, respectively, are equivalent to the constraints on the column space of the matrices, which linearly represent matroid instances $\mathcal{N}_1$ and $\mathcal{N}_2$. This implies that an encoding matrix $\boldsymbol{H}$ is optimal for $\mathcal{I}_1$ only if field does have characteristic three, and it is optimal for $\mathcal{I}_2$ only if field does have any characteristic other than characteristic three.

1) INDEX CODING INSTANCE $\mathcal{I}_1$

Definition 24 (Index Coding Instance $\mathcal{I}_1$): The index coding instance $\mathcal{I}_1 = \{B_i, i \in [29]\}$ is characterized as follows

$$\begin{aligned}
B_1 &= ([4]\backslash\{1\}) \cup \{8\} \cup ([10:25]\backslash\{10, 14, 18, 22\}),\\
B_2 &= ([4]\backslash\{2\}) \cup \{7\} \cup ([10:25]\backslash\{11, 15, 19, 23\}),\\
B_3 &= ([4]\backslash\{3\}) \cup \{6\} \cup ([10:25]\backslash\{12, 16, 20, 24\}),\\
B_4 &= ([4]\backslash\{4\}) \cup \{5\} \cup ([10:25]\backslash\{13, 17, 21, 25\}),\\
B_5 &= \{7, 8\},\\
B_6 &= \{5, 8\},\\
B_7 &= \{5, 6\},\\
B_8 &= \{6, 7\},\\
B_9 &= \{5, 6, 7, 8\},\\
B_{10} &= \{5, 11\},\\
B_{11} &= \{5, 12\},\\
B_{12} &= \{5, 10\},\\
B_{13} &= \{1, 8, 9\},\\
B_{14} &= \{6, 15\},\\
B_{15} &= \{6, 17\},\\
B_{16} &= \{4, 5, 9\},\\
B_{17} &= \{6, 14\},\\
B_{18} &= \{7, 20\},\\
B_{19} &= \{3, 6, 9\},\\
B_{20} &= \{7, 21\},\\
B_{21} &= \{7, 18\},\\
B_{22} &= \{2, 7, 9\},\\
B_{23} &= \{8, 24\},\\
B_{24} &= \{8, 25\},\\
B_{25} &= \{8, 23\},\\
B_{26} &= \{4, 5, 9, 16\},
\end{aligned}$$

$$B_{27} = \{3, 6, 9, 19\},$$
$$B_{28} = \{2, 7, 9, 22\},$$
$$B_{29} = \{1, 8, 9, 13\}. \quad (73)$$

Theorem 2: $\lambda_q(\mathcal{I}_1) = \beta_{\text{MAIS}}(\mathcal{I}_1) = 4$ if and only if $\mathbb{F}_q$ does have characteristic three. In other words, linear coding is optimal for $\mathcal{I}_1$ only over the fields with characteristic three.

The proof can be concluded from Propositions 8 and 9.

Proposition 8: There exists a scalar linear code ($t = 1$) over a field with characteristic three, which is optimal for $\mathcal{I}_1$.

Proof: In Appendix C, it is shown that the encoding matrix $\boldsymbol{H}_* \in \mathbb{F}_q^{4\times 29}$, shown in Figure 2, will satisfy all users in $\mathcal{I}_1$, where the field $\mathbb{F}_q$ has characteristic three. The key part of $\boldsymbol{H}_*$ is its submatrix $\boldsymbol{H}_*^{\{5,6,7,8\}}$, where $\text{rank}(\boldsymbol{H}_*^{\{5,6,7,8\}}) = 3$ is achievable over the fields with characteristic three. This satisfies condition (2) for user u_9 with $B_9 = \{5, 6, 7, 8\}$. ■

Proposition 9: Matrix $\boldsymbol{H} \in \mathbb{F}_q^{4t\times 29t}$ is an encoding matrix for index coding instance $\mathcal{I}_1$ only if its submatrix $\boldsymbol{H}^{[9]}$ is a linear representation of matroid instance $\mathcal{N}_1$.

Proof: We prove that set $N_0 = [4]$ is a basis set of $\boldsymbol{H}$, and each set $N_i, i \in [9]$ in (15) is a circuit set of $\boldsymbol{H}$. The proof is described as follows.

- First, since $\beta_{\text{MAIS}}(\mathcal{I}_1) = 4$, we must have $\text{rank}(\boldsymbol{H}) = 4t$. Now, from $B_i, i \in [4]$ in (73), it can be seen that set [4] is an independent set of $\mathcal{I}_1$, so based on Lemma 1, set [4] is an independent set of $\boldsymbol{H}$. Since $\text{rank}(\boldsymbol{H}) = 4t$, set $N_0 = [4]$ will be a basis set of $\boldsymbol{H}$. Now, in order to have $\text{rank}(\boldsymbol{H}) = 4t$, for all $j \in [29]\backslash[4]$, we must have $\text{col}(\boldsymbol{H}^{\{j\}}) \subseteq \text{col}(\boldsymbol{H}^{[4]})$.
- According to Lemma 3, from $B_i, i \in [4]$, it can be seen that:
  - for each $j \in \{10, 14, 18, 22\}$,
  $$j \in B_i, i \in [4]\backslash\{1\} \rightarrow \text{col}\left(\boldsymbol{H}^{\{j\}}\right) = \text{col}\left(\boldsymbol{H}^{\{1\}}\right), \quad (74)$$
  - for each $j \in \{11, 15, 19, 23\}$,
  $$j \in B_i, i \in [4]\backslash\{2\} \rightarrow \text{col}\left(\boldsymbol{H}^{\{j\}}\right) = \text{col}\left(\boldsymbol{H}^{\{2\}}\right), \quad (75)$$
  - for each $j \in \{12, 16, 20, 24\}$,
  $$j \in B_i, i \in [4]\backslash\{3\} \rightarrow \text{col}\left(\boldsymbol{H}^{\{j\}}\right) = \text{col}\left(\boldsymbol{H}^{\{3\}}\right), \quad (76)$$
  - for each $j \in \{13, 17, 21, 25\}$,
  $$j \in B_i, i \in [4]\backslash\{4\} \rightarrow \text{col}\left(\boldsymbol{H}^{\{j\}}\right) = \text{col}\left(\boldsymbol{H}^{\{4\}}\right). \quad (77)$$

  Let $M_1 = \{10, 11, 12\}, M_2 = \{14, 15, 17\}, M_3 = \{18, 20, 21\}$ and $M_4 = \{23, 24, 25\}$. Now, (74)-(77) lead to
  $$\text{col}\left(\boldsymbol{H}^{M_1}\right) = \text{col}\left(\boldsymbol{H}^{[4]\backslash\{4\}}\right), \quad (78)$$
  $$\text{col}\left(\boldsymbol{H}^{M_2}\right) = \text{col}\left(\boldsymbol{H}^{[4]\backslash\{3\}}\right), \quad (79)$$
  $$\text{col}\left(\boldsymbol{H}^{M_3}\right) = \text{col}\left(\boldsymbol{H}^{[4]\backslash\{2\}}\right), \quad (80)$$
  $$\text{col}\left(\boldsymbol{H}^{M_4}\right) = \text{col}\left(\boldsymbol{H}^{[4]\backslash\{1\}}\right). \quad (81)$$
  Thus, each M_1, M_2, M_3 and M_4 is an independent set of $\boldsymbol{H}$.
- To have $\text{rank}(\boldsymbol{H}) = 4t$, one must have $\text{rank}(\boldsymbol{H}^{B_i}) = 3t, i \in [29]$. Since [4] is a basis set, from $B_i, i \in [4]$, we must have
  $$B_4 \rightarrow \text{col}\left(\boldsymbol{H}^{\{5\}}\right) \subseteq \text{col}\left(\boldsymbol{H}^{[4]\backslash\{4\}}\right) \overset{(78)}{=} \text{col}\left(\boldsymbol{H}^{M_1}\right), \quad (82)$$
  $$B_3 \rightarrow \text{col}\left(\boldsymbol{H}^{\{6\}}\right) \subseteq \text{col}\left(\boldsymbol{H}^{[4]\backslash\{3\}}\right) \overset{(79)}{=} \text{col}\left(\boldsymbol{H}^{M_2}\right), \quad (83)$$
  $$B_2 \rightarrow \text{col}\left(\boldsymbol{H}^{\{7\}}\right) \subseteq \text{col}\left(\boldsymbol{H}^{[4]\backslash\{2\}}\right) \overset{(80)}{=} \text{col}\left(\boldsymbol{H}^{M_3}\right), \quad (84)$$
  $$B_1 \rightarrow \text{col}\left(\boldsymbol{H}^{\{8\}}\right) \subseteq \text{col}\left(\boldsymbol{H}^{[4]\backslash\{1\}}\right) \overset{(81)}{=} \text{col}\left(\boldsymbol{H}^{M_4}\right). \quad (85)$$
- From $B_i, i \in M_1, M_2, M_3$ and M_4, it can be verified that
  $$M_1 \text{ is a minimal cyclic set of } \mathcal{I}_1 \;\&\; 5 \in B_i, i \in M_1, \quad (86)$$
  $$M_2 \text{ is a minimal cyclic set of } \mathcal{I}_1 \;\&\; 6 \in B_i, i \in M_2, \quad (87)$$
  $$M_3 \text{ is a minimal cyclic set of } \mathcal{I}_1 \;\&\; 7 \in B_i, i \in M_3, \quad (88)$$
  $$M_4 \text{ is a minimal cyclic set of } \mathcal{I}_1 \;\&\; 8 \in B_i, i \in M_4. \quad (89)$$
- Now, all the four conditions in Lemma 4 are satisfied for set M_1 with $j = 5$, set M_2 with $j = 6$, set M_3 with $j = 7$, and set M_4 with $j = 8$. So, based on Lemma 4, each set $\{5\} \cup M_1, \{6\} \cup M_2, \{7\} \cup M_3$ and $\{8\} \cup M_4$ is a circuit set of $\boldsymbol{H}$. Now, based on (78)-(81), each set $N_1 = \{1, 2, 3, 5\}, N_2 = \{1, 2, 4, 6\}, N_3 = \{1, 3, 4, 7\}$ and $N_4 = \{2, 3, 4, 8\}$ is also a circuit set.
- Due to $\text{rank}(\boldsymbol{H}^{B_i}) = 3t, i \in \{26, 27, 28, 29\}$, we must have
  $$\text{rank}\left(\boldsymbol{H}^{\{4,5,9,16\}}\right) = 3t, \quad (90)$$
  $$\text{rank}\left(\boldsymbol{H}^{\{3,6,9,19\}}\right) = 3t, \quad (91)$$
  $$\text{rank}\left(\boldsymbol{H}^{\{2,7,9,22\}}\right) = 3t, \quad (92)$$
  $$\text{rank}\left(\boldsymbol{H}^{\{1,8,9,13\}}\right) = 3t. \quad (93)$$
  Now, since $B_{16} = \{4, 5, 9\}, B_{19} = \{3, 6, 9\}, B_{22} = \{2, 7, 9\}$ and $B_{13} = \{1, 8, 9\}$, we must have
  $$(90) \rightarrow \text{rank}\left(\boldsymbol{H}^{\{4,5,9\}}\right) = 2t, \quad (94)$$
  $$(91) \rightarrow \text{rank}\left(\boldsymbol{H}^{\{3,6,9\}}\right) = 2t, \quad (95)$$
  $$(92) \rightarrow \text{rank}\left(\boldsymbol{H}^{\{2,7,9\}}\right) = 2t, \quad (96)$$
  $$(93) \rightarrow \text{rank}\left(\boldsymbol{H}^{\{1,8,9\}}\right) = 2t. \quad (97)$$

  Thus,
  $$(94) \rightarrow \text{col}\left(\boldsymbol{H}^{\{9\}}\right) \subseteq \text{col}\left(\boldsymbol{H}^{\{4,5\}}\right),$$
  $$(95) \rightarrow \text{col}\left(\boldsymbol{H}^{\{9\}}\right) \subseteq \text{col}\left(\boldsymbol{H}^{\{3,6\}}\right),$$
  $$(96) \rightarrow \text{col}\left(\boldsymbol{H}^{\{9\}}\right) \subseteq \text{col}\left(\boldsymbol{H}^{\{2,7\}}\right),$$
  $$(97) \rightarrow \text{col}\left(\boldsymbol{H}^{\{9\}}\right) \subseteq \text{col}\left(\boldsymbol{H}^{\{1,8\}}\right).$$

Hence, based on Lemma 5, each set $N_5 = \{1, 8, 9\}, N_6 = \{2, 7, 9\}, N_7 = \{3, 6, 9\}, N_8 = \{4, 5, 9\}$ is a circuit set.

- Finally, from B_5, B_6, B_7 and B_8, it can be seen that set $\{5, 6, 7, 8\}$ is a minimal cyclic set of $\mathcal{I}_1$. Moreover, from B_9, we must have $\text{rank}(\boldsymbol{H}^{B_9}) = \text{rank}(\boldsymbol{H}^{\{5,6,7,8\}}) = 3t$. Thus, based on Lemma 2, set $N_9 = \{5, 6, 7, 8\}$ must be a circuit set of $\boldsymbol{H}$. This completes the proof. ■

2) INDEX CODING INSTANCE $\mathcal{I}_2$

Definition 25 (Index Coding Instance $\mathcal{I}_2$): For the index coding instance $\mathcal{I}_2 = \{B_i, i \in [29]\}$, the interfering message sets are all the same as the ones in (73), except sets $B_i, i \in \{5, 6, 7, 8, 9\}$, which are as follows

$$B_i = \{5, 6, 7, 8\}\backslash\{i\}, \quad i \in \{5, 6, 7, 8\},$$
$$B_9 = \emptyset. \tag{98}$$

Theorem 3: $\lambda_q(\mathcal{I}_2) = \beta_{\text{MAIS}}(\mathcal{I}_2) = 4$ if and only if $\mathbb{F}_q$ does have any characteristic other than characteristic three. In other words, linear coding is optimal for $\mathcal{I}_1$ only over the fields with any characteristic other than characteristic three.

The proof can be concluded from Propositions 10 and 11.

Proposition 10: There exists a scalar linear code ($t = 1$) over a field of any characteristic other than characteristic three, which is optimal for $\mathcal{I}_2$.

Proof: In Appendix C, it is shown that the encoding matrix $\boldsymbol{H}_* \in \mathbb{F}_q^{4\times 29}$, shown in Figure 2, will satisfy all users in $\mathcal{I}_2$, where the field $\mathbb{F}_q$ has any characteristic other than characteristic three. The key part of $\boldsymbol{H}_*$ is its submatrix $\boldsymbol{H}_*^{\{5,6,7,8\}}$, where $\text{rank}(\boldsymbol{H}_*^{\{5,6,7,8\}}) = 4$ is achievable over fields with any characteristic other than three. This satisfies the condition in (2) for users $u_i, i \in \{5, 6, 7, 8\}$. ■

Proposition 11: Matrix $\boldsymbol{H} \in \mathbb{F}_q^{4t\times 29t}$ is an encoding matrix for index coding instance $\mathcal{I}_2$ only if its submatrix $\boldsymbol{H}^{[9]}$ is a linear representation of matroid instance $\mathcal{N}_2$.

Proof: Since the interfering message sets $B_i, \in [29]\backslash\{5, 6, 7, 8, 9\}$ of $\mathcal{I}_2$ are the same as the sets in (73), we can borrow the results from Proposition 9, where set [4] is a basis set, and sets $\{1, 2, 3, 5\}, \{1, 2, 4, 6\}, \{1, 3, 4, 7\}, \{2, 3, 4, 8\}, \{1, 8, 9\}, \{2, 7, 9\}, \{3, 6, 9\}$ and $\{4, 5, 9\}$ are circuit sets. Now, due to (98), the set $\{5, 6, 7, 8\}$ must also be a basis set, which completes the proof. ■

V. INDEX CODING INSTANCE $\mathcal{I}_3$

This subsection provides index coding instance $\mathcal{I}_3$ with the MAIS bound $\beta_{\text{MAIS}}(\mathcal{I}_3) = 8$. First, we prove that linear coding cannot achieve the optimal rate over any field with characteristic three. To prove this, we first define a matroid instances $\mathcal{N}_3$ and show that it is not linearly representable over the fields with characteristic three. Then, we show that the main constraints on the column space of the encoding matrix of $\mathcal{I}_3$ can be reduced to the constraints on the column space of the matrix, which is the linear representation of $\mathcal{N}_3$.

Finally, we provide a scalar nonlinear code over the fields with characteristic three, which is optimal for $\mathcal{I}_3$.

In this subsection, we assume that $M \subseteq [m], N \subseteq [n]$, and the value of each $m, n, |M|$ and $|N|$ is an even integer.

A. MATROID INSTANCE $\mathcal{N}_3$

In this subsection, we first define the concept of quasi-circuit set of a matrix which is similar to the concept of circuit set (where this similarity can be seen by comparing Equations (99) and (101), respectively, with Equations (10) and (11)).

Definition 26 (Qausi-circuit Set of Matrix $\boldsymbol{H}$): Let $L \subseteq [\frac{n}{2}]$. We say that set $N = \{2j-1, 2j, j \in L\} \subseteq [n]$ is a quasi-circuit set of $\boldsymbol{H}$, if for all $j \in L$, we have

$$\text{rank}\Big(\boldsymbol{H}^{\{2j-1,2j\}}\Big) = 2t,$$
$$\text{rank}\Big(\boldsymbol{H}^{N\backslash\{2j-1,2j\}}\Big) = \text{rank}\Big(\boldsymbol{H}^{N}\Big) = (|N| - 2)t. \tag{99}$$

Lemma 6: Let $L \subseteq [\frac{n}{2}]$. Assume $N = \{2j - 1, 2j, j \in L\}$ is a quasi-circuit set of $\boldsymbol{H}$ and

$$\boldsymbol{N}_{j,i} \triangleq \begin{bmatrix} \boldsymbol{M}_{2j-1,2i-1} & \boldsymbol{M}_{2j,2i-1} \\ \boldsymbol{M}_{2j-1,2i} & \boldsymbol{M}_{2j,2i} \end{bmatrix}. \tag{100}$$

Now, for any $j \in L$, we have

$$\boldsymbol{H}^{\{2j-1,2j\}} = \sum_{i\in L\backslash\{j\}} \boldsymbol{H}^{\{2i-1,2i\}}\boldsymbol{N}_{j,i}, \tag{101}$$

such that each $\boldsymbol{N}_{j,i}$ is invertible.

Proof: Equation (99) requires that

$$\text{col}\Big(\boldsymbol{H}^{\{2j-1,2j\}}\Big) \subseteq \text{col}\Big(\boldsymbol{H}^{N\backslash\{2j-1,2j\}}\Big)\Big).$$

Thus, we must have $\boldsymbol{H}^{\{2j-1,2j\}} = \sum_{i\in L\backslash\{j\}} \boldsymbol{H}^{\{2i-1,2i\}}\boldsymbol{N}_{j,i}$. Now, if one of the $\boldsymbol{N}_{j,i}, i = l \in L\backslash\{j\}$ is not invertible, then $\text{rank}(\boldsymbol{H}^{N\backslash\{2l-1,2l\}}) < (|N| - 2)t$, which contradicts (99). Thus, all $\boldsymbol{N}_{j,i}, i \in L\backslash\{j\}$ must be invertible. ■

Example 6: It can be seen that for the following matrix

$$\boldsymbol{H} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}, \tag{102}$$

set [6] is a quasi-circuit set as we have

$$\text{rank}\Big(\boldsymbol{H}^{\{1,2\}}\Big) = \text{rank}\Big(\boldsymbol{H}^{\{3,4\}}\Big) = \text{rank}\Big(\boldsymbol{H}^{\{5,6\}}\Big) = 2,$$
$$\text{rank}\Big(\boldsymbol{H}^{\{1,2,3,4\}}\Big) = \text{rank}\Big(\boldsymbol{H}^{\{1,2,5,6\}}\Big) = \text{rank}\Big(\boldsymbol{H}^{\{3,4,5,6\}}\Big) = 4$$
$$\text{rank}\Big(\boldsymbol{H}^{[6]}\Big) = 4. \tag{103}$$

Definition 27 (Matroid Instance $\mathcal{N}_3$): Consider the matroid instance $\mathcal{N}_3 = \{f(N), N \subseteq [n]\}$, where $n = 18$, $f(\mathcal{N}_3) = 8$, set $N_0 = [8]$ is a basis set, the sets N_i's, $i \in [8]$ are quasi-circuit sets, which are as follows

$$N_1 = \{1, 2, 3, 4, 5, 6, 9, 10\},$$

$$
\begin{array}{c|cccc|cccc|c}
 & 1,2 & 3,4 & 5,6 & 7,8 & 9,10 & 11,12 & 13,14 & 15,16 & 17,18 \\
1,2 & \boldsymbol{I}_2 & 0_2 & 0_2 & 0_2 & \boldsymbol{I}_2 & \boldsymbol{I}_2 & \boldsymbol{I}_2 & 0_2 & \boldsymbol{I}_2 \\
3,4 & 0_2 & \boldsymbol{I}_2 & 0_2 & 0_2 & \boldsymbol{I}_2 & \boldsymbol{I}_2 & 0_2 & \boldsymbol{I}_2 & \boldsymbol{I}_2 \\
5,6 & 0_2 & 0_2 & \boldsymbol{I}_2 & 0_2 & \boldsymbol{I}_2 & 0_2 & \boldsymbol{I}_2 & \boldsymbol{I}_2 & \boldsymbol{I}_2 \\
7,8 & 0_2 & 0_2 & 0_2 & \boldsymbol{I}_2 & 0_2 & \boldsymbol{I}_2 & \boldsymbol{I}_2 & \boldsymbol{I}_2 & \boldsymbol{I}_2
\end{array}
$$

FIGURE 3. $H_{\mathcal{N}_3} \in \mathbb{F}_q^{8\times 18}$: If $\mathbb{F}_q$ does have any characteristic other than characteristic three (such as $GF(2)$), then $H_{\mathcal{N}_3}$ is a scalar linear representation of matroid $\mathcal{N}_3$.

$$
\begin{aligned}
N_2 &= \{1,2,3,4,7,8,11,12\},\\
N_3 &= \{1,2,5,6,7,8,13,14\},\\
N_4 &= \{3,4,5,6,7,8,15,16\},\\
N_5 &= \{1,2,15,16,17,18\},\\
N_6 &= \{3,4,13,14,17,18\},\\
N_7 &= \{5,6,11,12,17,18\},\\
N_8 &= \{7,8,9,10,17,18\}, \qquad (104)
\end{aligned}
$$

and

$$f(N_9 = [9{:}16]) \geq 7. \qquad (105)$$

Proposition 12: Matroid instance $\mathcal{N}_3$ is not linearly representable over any field with characteristic three.

Proof: First, it can be verified that matrix $\boldsymbol{H}_{\mathcal{N}_3} \in \mathbb{F}_q^{8*58}$, shown in Figure 3, is a scalar linear representation of $\mathcal{N}_3$ if field $\mathbb{F}_q$ has any characteristic other than characteristic three. The key part of $\boldsymbol{H}_{\mathcal{N}}$ is its submatrix $\boldsymbol{H}_{\mathcal{N}}^{[9:16]}$, which is as follows

$$
\boldsymbol{H}_{\mathcal{N}_3}^{[9:16]} = \begin{bmatrix} \boldsymbol{I}_2 & \boldsymbol{I}_2 & \boldsymbol{I}_2 & 0_2 \\ \boldsymbol{I}_2 & \boldsymbol{I}_2 & 0_2 & \boldsymbol{I}_2 \\ \boldsymbol{I}_2 & 0_2 & \boldsymbol{I}_2 & \boldsymbol{I}_2 \\ 0_2 & \boldsymbol{I}_2 & \boldsymbol{I}_2 & \boldsymbol{I}_2 \end{bmatrix}.
$$

It can be seen that $\operatorname{rank}(\boldsymbol{H}_{\mathcal{N}_3}^{[9:16]}) = 8$ is achievable over fields with any characteristic other than three. This satisfies the condition for set $N_9 = [9:16]$ in (105).

Since set [8] is a basis set, and each $N_i, i \in [8]$ in (104) is a quasi-circuit set, (101) results in

$$
\begin{aligned}
\boldsymbol{H}^{\{9,10\}} &= \boldsymbol{H}^{\{1,2\}}\boldsymbol{N}_{5,1} + \boldsymbol{H}^{\{3,4\}}\boldsymbol{N}_{5,2} + \boldsymbol{H}^{\{5,6\}}\boldsymbol{N}_{5,3}, && (106)\\
\boldsymbol{H}^{\{11,12\}} &= \boldsymbol{H}^{\{1,2\}}\boldsymbol{N}_{6,1} + \boldsymbol{H}^{\{3,4\}}\boldsymbol{N}_{6,2} + \boldsymbol{H}^{\{7,8\}}\boldsymbol{N}_{6,4}, && (107)\\
\boldsymbol{H}^{\{13,14\}} &= \boldsymbol{H}^{\{1,2\}}\boldsymbol{N}_{7,1} + \boldsymbol{H}^{\{5,6\}}\boldsymbol{N}_{7,3} + \boldsymbol{H}^{\{7,8\}}\boldsymbol{N}_{7,4}, && (108)\\
\boldsymbol{H}^{\{15,16\}} &= \boldsymbol{H}^{\{3,4\}}\boldsymbol{N}_{8,2} + \boldsymbol{H}^{\{5,6\}}\boldsymbol{N}_{8,3} + \boldsymbol{H}^{\{7,8\}}\boldsymbol{N}_{8,4}, && (109)\\
\boldsymbol{H}^{\{17,18\}} &= \boldsymbol{H}^{\{1,2\}}\boldsymbol{N}_{9,1} + \boldsymbol{H}^{\{15,16\}}\boldsymbol{N}_{9,8}, && (110)\\
\boldsymbol{H}^{\{17,18\}} &= \boldsymbol{H}^{\{3,4\}}\boldsymbol{N}_{9,2} + \boldsymbol{H}^{\{13,14\}}\boldsymbol{N}_{9,7}, && (111)\\
\boldsymbol{H}^{\{17,18\}} &= \boldsymbol{H}^{\{5,6\}}\boldsymbol{N}_{9,3} + \boldsymbol{H}^{\{11,12\}}\boldsymbol{N}_{9,6}, && (112)\\
\boldsymbol{H}^{\{17,18\}} &= \boldsymbol{H}^{\{7,8\}}\boldsymbol{N}_{9,4} + \boldsymbol{H}^{\{9,10\}}\boldsymbol{N}_{9,5}. && (113)
\end{aligned}
$$

Now, since each $\boldsymbol{N}_{j,i}$ is invertible (according to Lemma 6), equations (106)-(113) are similar to equations (21)-(28). Therefore, over the fields with characteristic three, we can achieve the similar result in (68), as follows

$$
\begin{aligned}
&2\boldsymbol{H}^{\{15,16\}}\boldsymbol{N}_{9,8}\\
&\quad = \boldsymbol{H}^{\{9,10\}}\boldsymbol{N}_{9,5} + \boldsymbol{H}^{\{11,12\}}\boldsymbol{N}_{9,6} + \boldsymbol{H}^{\{13,14\}}\boldsymbol{N}_{9,7}, \qquad (114)
\end{aligned}
$$

where each $\boldsymbol{N}_{9,5}, \boldsymbol{N}_{9,6}, \boldsymbol{N}_{9,7}$, end $\boldsymbol{N}_{9,8}$ is invertible. Thus,

$$\operatorname{rank}\left(\boldsymbol{H}^{\{9:16\}}\right) = \operatorname{rank}\left(\boldsymbol{H}^{\{9:14\}}\right) \leq 6, \qquad (115)$$

which contradicts (105). This completes the proof. ■

B. ON THE REDUCTION PROCESS FROM INDEX CODING TO MATROID

In this subsection, first we define the concept of quasi-minimal cyclic set of an index coding instance, which is similar to the concept of minimal cyclic set (where this similarity can be seen by comparing Equation (4) with Equations (116) and (116)). Then, through Lemmas 7-9, we establish some reduction techniques to map specific constraints on the column space of the encoder matrix of an index coding instance to the constraints on the column space of the matrix, linearly representing a matroid instance. Lemmas 7 and 8, respectively, are variations of Lemmas 4 and 5, where the concept of quasi-minimal cyclic set is used instead of the concept of minimal cyclic set. Proof of Lemmas 7-9 are provided in Appendix D.

Here, we assume that m is an even integer, $L' \subseteq L = [\frac{m}{2}]$, $M' = \{2i-1, 2i, i \in L'\} \subseteq M = \{2i-1, 2i, i \in L\} \subseteq [m]$.

Definition 28 (Qausi-Minimal Cyclic Set of $\mathcal{I}$): Let $M = \{i_{2j-1}, i_{2j}, j \in [\frac{|M|}{2}]\}$. Now, M is referred to as a quasi-minimal cyclic set of $\mathcal{I}$ if

$$
\begin{aligned}
B_{i_{2j-1}} \cap M &= \begin{cases} M \backslash \{i_{2j-1}, i_{2j+1}, i_{2j+2}\}, & j \in \left[\frac{|M|}{2} - 1\right], \\ M \backslash \{i_{2j-1}, i_1, i_2\}, & j = \frac{|M|}{2}. \end{cases}\\
B_{i_{2j}} \cap M &= \begin{cases} M \backslash \{i_{2j}, i_{2j+1}, i_{2j+2}\}, & j \in \left[\frac{|M|}{2} - 1\right], \\ M \backslash \{i_{2j}, i_1, i_2\}, & j = \frac{|M|}{2}. \end{cases} \qquad (116)
\end{aligned}
$$

Example 7: Consider the index coding instance $\mathcal{I} = \{B_i, i \in [6]\}$, where

$$
\begin{aligned}
B_1 &= \{2,3,4\}, \ B_2 = \{1,3,4\},\\
B_3 &= \{4,5,6\}, \ B_4 = \{3,5,6\},\\
B_5 &= \{1,2,6\}, \ B_6 = \{1,2,5\}.
\end{aligned}
$$

It can be seen that set [6] is a quasi-minimal cyclic set of $\mathcal{I}$. It can be also checked that the matrix in (102) is an encoding matrix for $\mathcal{I}$ and can satisfy all the users $u_i, \in [6]$.

Lemma 7: Assume

(i) M is an independent set of $\boldsymbol{H}$,
(ii) $\operatorname{col}(\boldsymbol{H}^{\{2j-1,2j\}}) \subseteq \operatorname{col}(\boldsymbol{H}^M)$,
(iii) M forms a quasi-minimal cyclic set of $\mathcal{I}$,

(iv) $\{2j-1, 2j\} \subseteq B_i, \forall i \in M$.

Now, the condition in (2) for all $i \in [m]$ requires set $\{2j-1, 2j\} \cup M$ to be a quasi-circuit set of $\boldsymbol{H}$.

Lemma 8: Suppose for matrix $\boldsymbol{H} \in \mathbb{F}_q^{8t \times 18}$,

(i) set [8] is a basis set,

(ii) each set $\{1,2,3,4,5,6,9,10\}$, $\{1,2,3,4,7,8,11,12\}$, $\{1,2,5,6,7,8,13,14\}$ and $\{3,4,5,6,7,8,15,16\}$ is a quasi-circuit set,

(iii)

$$\mathrm{col}\left(\boldsymbol{H}^{\{17,18\}}\right) \subseteq \mathrm{col}\left(\boldsymbol{H}^{\{7,8,9,10\}}\right).$$
$$\mathrm{col}\left(\boldsymbol{H}^{\{17,18\}}\right) \subseteq \mathrm{col}\left(\boldsymbol{H}^{\{5,6,11,12\}}\right),$$
$$\mathrm{col}\left(\boldsymbol{H}^{\{17,18\}}\right) \subseteq \mathrm{col}\left(\boldsymbol{H}^{\{3,4,13,14\}}\right),$$
$$\mathrm{col}\left(\boldsymbol{H}^{\{17,18\}}\right) \subseteq \mathrm{col}\left(\boldsymbol{H}^{\{1,2,15,16\}}\right),$$

Then, each set $\{1,2,15,16,17,18\}$, $\{3,4,13,14,17,18\}$, $\{5,6,11,12,17,18\}$ and $\{7,8,9,10,17,18\}$ will also be a quasi-circuit set.

Lemma 9: Let matrix $\boldsymbol{H}$ be an encoding matrix for index coding instance $\mathcal{I} = \{B_i, i \in [m]\}$. Assume $M' \subseteq M \subseteq [m]$. Now, if $M \backslash \{i\} \subseteq B_i$ for all $i \in M'$, then we must have

$$\mathrm{rank}\left(\boldsymbol{H}^{M}\right) = \mathrm{rank}\left(\boldsymbol{H}^{M \backslash M'}\right) + |M'|t.$$

C. INDEX CODING INSTANCE $\mathcal{I}_3$

Definition 29 (Index Coding Instance $\mathcal{I}_3$): The index coding instance $\mathcal{I}_3 = \{B_i, i \in [58]\}$ is characterized as follows

$$\begin{aligned}
B_1 &= ([8]\backslash\{1\}) \cup \{15,16\} \cup ([19:50]\backslash\{19,27,35,43\}),\\
B_2 &= ([8]\backslash\{2\}) \cup \{15,16\} \cup ([19:50]\backslash\{20,28,36,44\}),\\
B_3 &= ([8]\backslash\{3\}) \cup \{13,14\} \cup ([19:50]\backslash\{21,29,37,45\}),\\
B_4 &= ([8]\backslash\{4\}) \cup \{13,14\} \cup ([19:50]\backslash\{22,30,38,46\}),\\
B_5 &= ([8]\backslash\{5\}) \cup \{11,12\} \cup ([19:50]\backslash\{23,31,39,47\}),\\
B_6 &= ([8]\backslash\{6\}) \cup \{11,12\} \cup ([19:50]\backslash\{24,32,40,48\}),\\
B_7 &= ([8]\backslash\{7\}) \cup \{9,10\} \cup ([19:50]\backslash\{25,33,41,49\}),\\
B_8 &= ([8]\backslash\{8\}) \cup \{9,10\} \cup ([19:50]\backslash\{26,34,42,50\}),\\
B_9 &= [9:16]\backslash\{9\},\\
B_{10} &= \{9,12,14\},\\
B_{11} &= [9:16]\backslash\{11\},\\
B_{12} &= \{11,14,16\},\\
B_{13} &= [9:16]\backslash\{13\},\\
B_{14} &= \{13,10,16\},\\
B_{15} &= [9:16]\backslash\{15\},\\
B_{16} &= \{15,10,12\},\\
B_{17} &= \{18\},\\
B_{18} &= \{17\},\\
B_{19} &= \{9,10,20,21,22\},\\
B_{20} &= \{9,10,19,21,22\},\\
B_{21} &= \{9,10,22,23,24\},\\
B_{22} &= \{9,10,21,23,24\},\\
B_{23} &= \{9,10,19,20,24\},\\
B_{24} &= \{9,10,19,20,23\},\\
B_{25} &= \{1,2,15,16,17,18,26\},\\
B_{26} &= \{1,2,15,16,17,18,25\},\\
B_{27} &= \{11,12,28,29,30\},\\
B_{28} &= \{11,12,27,29,30\},\\
B_{29} &= \{11,12,30,33,34\},\\
B_{30} &= \{11,12,29,33,34\},\\
B_{31} &= \{7,8,9,10,17,18,32\},\\
B_{32} &= \{7,8,9,10,17,18,31\},\\
B_{33} &= \{11,12,27,28,34\},\\
B_{34} &= \{11,12,27,28,33\},\\
B_{35} &= \{13,14,36,39,40\},\\
B_{36} &= \{13,14,35,39,40\},\\
B_{37} &= \{5,6,11,12,17,18,38\},\\
B_{38} &= \{5,6,11,12,17,18,37\},\\
B_{39} &= \{13,14,40,41,42\},\\
B_{40} &= \{13,14,39,41,42\},\\
B_{41} &= \{13,14,35,36,42\},\\
B_{42} &= \{13,14,35,36,41\},\\
B_{43} &= \{3,4,13,14,17,18,44\},\\
B_{44} &= \{3,4,13,14,17,18,43\},\\
B_{45} &= \{15,16,46,47,48\},\\
B_{46} &= \{15,16,45,47,48\},\\
B_{47} &= \{15,16,48,49,50\},\\
B_{48} &= \{15,16,47,49,50\},\\
B_{49} &= \{15,16,45,46,50\},\\
B_{50} &= \{15,16,45,46,49\},\\
B_{51} &= \{7,8,9,10,17,18,31,32,52\},\\
B_{52} &= \{7,8,9,10,17,18,31,32,51\},\\
B_{53} &= \{5,6,11,12,17,18,37,38,54\},\\
B_{54} &= \{5,6,11,12,17,18,37,38,53\},\\
B_{55} &= \{3,4,13,14,17,18,43,44,56\},\\
B_{56} &= \{3,4,13,14,17,18,43,44,55\},\\
B_{57} &= \{1,2,15,16,17,18,25,26,58\},\\
B_{58} &= \{1,2,15,16,17,18,25,26,57\}.
\end{aligned} \tag{117}$$

Theorem 4: $\lambda_q(\mathcal{I}_3) = \beta_{\mathrm{MAIS}}(\mathcal{I}_3) = 8$ if and only if $\mathbb{F}_q$ does have any characteristic other than characteristic three. In other words, linear coding is optimal for $\mathcal{I}_3$ only over the fields with any characteristic other than characteristic three. However, there exists a scalar nonlinear code over the fields with characteristic three, which is optimal for $\mathcal{I}_3$.

Proof: The proof can be concluded from Propositions 13, 14, and 15. ■

$$
\begin{array}{c} \\ 1,2 \\ 3,4 \\ 5,6 \\ 7,8 \end{array}
\begin{array}{c}
\begin{array}{cccc|cccc|c|cccc|cccc|cccc|cccc|cccc}
1,2 & 3,4 & 5,6 & 7,8 & 9,10 & 11,12 & 13,14 & 15,16 & 17,18 & 19,20 & 21,22 & 23,24 & 25,26 & 27,28 & 29,30 & 31,32 & 33,34 & 35,36 & 37,38 & 39,40 & 41,42 & 43,44 & 45,46 & 47,48 & 49,50 & 51,52 & 53,54 & 55,56 & 57,58
\end{array} \\
\left[\begin{array}{cccc|cccc|c|cccc|cccc|cccc|cccc|cccc}
\boldsymbol{I}_2 & \mathbf{0}_2 & \mathbf{0}_2 & \mathbf{0}_2 & \boldsymbol{I}_2 & \boldsymbol{I}_2 & \boldsymbol{I}_2 & \mathbf{0}_2 & \boldsymbol{I}_2 & \boldsymbol{I}_2 & \mathbf{0}_2 & \mathbf{0}_2 & \mathbf{0}_2 & \boldsymbol{I}_2 & \mathbf{0}_2 & \mathbf{0}_2 & \mathbf{0}_2 & \boldsymbol{I}_2 & \mathbf{0}_2 & \mathbf{0}_2 & \mathbf{0}_2 & \boldsymbol{I}_2 & \mathbf{0}_2 & \mathbf{0}_2 & \mathbf{0}_2 & \mathbf{0}_2 & \boldsymbol{I}_2 & \mathbf{0}_2 & \mathbf{0}_2 \\
\mathbf{0}_2 & \boldsymbol{I}_2 & \mathbf{0}_2 & \mathbf{0}_2 & \boldsymbol{I}_2 & \boldsymbol{I}_2 & \mathbf{0}_2 & \boldsymbol{I}_2 & \boldsymbol{I}_2 & \mathbf{0}_2 & \boldsymbol{I}_2 & \mathbf{0}_2 & \mathbf{0}_2 & \mathbf{0}_2 & \boldsymbol{I}_2 & \mathbf{0}_2 & \mathbf{0}_2 & \mathbf{0}_2 & \boldsymbol{I}_2 & \mathbf{0}_2 & \mathbf{0}_2 & \mathbf{0}_2 & \boldsymbol{I}_2 & \mathbf{0}_2 & \mathbf{0}_2 & \boldsymbol{I}_2 & \mathbf{0}_2 & \mathbf{0}_2 & \mathbf{0}_2 \\
\mathbf{0}_2 & \mathbf{0}_2 & \boldsymbol{I}_2 & \mathbf{0}_2 & \boldsymbol{I}_2 & \mathbf{0}_2 & \boldsymbol{I}_2 & \boldsymbol{I}_2 & \boldsymbol{I}_2 & \mathbf{0}_2 & \mathbf{0}_2 & \boldsymbol{I}_2 & \mathbf{0}_2 & \mathbf{0}_2 & \mathbf{0}_2 & \boldsymbol{I}_2 & \mathbf{0}_2 & \mathbf{0}_2 & \mathbf{0}_2 & \boldsymbol{I}_2 & \mathbf{0}_2 & \mathbf{0}_2 & \mathbf{0}_2 & \boldsymbol{I}_2 & \mathbf{0}_2 & \mathbf{0}_2 & \mathbf{0}_2 & \mathbf{0}_2 & \boldsymbol{I}_2 \\
\mathbf{0}_2 & \mathbf{0}_2 & \mathbf{0}_2 & \boldsymbol{I}_2 & \mathbf{0}_2 & \boldsymbol{I}_2 & \boldsymbol{I}_2 & \boldsymbol{I}_2 & \boldsymbol{I}_2 & \mathbf{0}_2 & \mathbf{0}_2 & \mathbf{0}_2 & \boldsymbol{I}_2 & \mathbf{0}_2 & \mathbf{0}_2 & \mathbf{0}_2 & \boldsymbol{I}_2 & \mathbf{0}_2 & \mathbf{0}_2 & \mathbf{0}_2 & \boldsymbol{I}_2 & \mathbf{0}_2 & \mathbf{0}_2 & \mathbf{0}_2 & \boldsymbol{I}_2 & \mathbf{0}_2 & \mathbf{0}_2 & \boldsymbol{I}_2 & \mathbf{0}_2
\end{array}\right]
\end{array}
$$

FIGURE 4. $H_* \in \mathbb{F}_q^{8\times 58}$: If $\mathbb{F}_q$ does have any characteristic other than characteristic three (such as $GF(2)$), then H_* is an encoding matrix for index coding instance $\mathcal{I}_3$.

Proposition 13: There exists a scalar linear coding over a field of any characteristic other than characteristic three, which is optimal for $\mathcal{I}_3$.

Proof: It can be verified that the encoding matrix $\boldsymbol{H}_* \in \mathbb{F}_q^{8\times 58}$, shown in Figure 4, will satisfy all users in $\mathcal{I}_3$, where the field $\mathbb{F}_q$ has any characteristic other than characteristic three. The key part of $\boldsymbol{H}_*$ is its submatrix $\boldsymbol{H}_*^{[9:16]}$, where $\text{rank}(\boldsymbol{H}_*^{[9:16]}) = 8$ is achievable over fields with any characteristic other than three. This satisfies the condition in (2) for users $u_i, i \in \{9, 11, 13, 15\}$. ■

Proposition 14: Matrix $\boldsymbol{H} \in \mathbb{F}_q^{8t\times 58t}$ is an encoding matrix for index coding instance $\mathcal{I}_3$ only if submatrix $\boldsymbol{H}^{[18]}$ is a linear representation of matroid instance $\mathcal{N}_3$.

Proof: Refer to Appendix E. ■

D. AN OPTIMAL NONLINEAR CODE FOR $\mathcal{I}_3$ OVER FIELDS WITH CHARACTERISTIC THREE

Definition 30 [Nonlinear Function $g(\cdot)$]: Let $x_i, x_j, x_l, x_v \in \mathbb{F}_q = GF(3)$. Now, the nonlinear function $g(\cdot) : \mathbb{F}_q^4 \to \mathbb{F}_q$ is defined as follows:

$$
\begin{aligned}
g\big(x_i, x_j, x_l, x_v\big) = 2x_ix_i\big(x_j + x_l + x_v\big) \\
&+ 2x_jx_j(x_i + x_l + x_v) \\
&+ 2x_lx_l\big(x_i + x_j + x_v\big) \\
&+ 2x_vx_v\big(x_i + x_j + x_l\big) \\
&+ 2\big(x_ix_j + x_ix_l + x_ix_v \\
&+ x_jx_l + x_jx_v + x_lx_v\big) \\
&+ x_ix_jx_l + x_ix_jx_v + x_ix_lx_v + x_jx_lx_v. \quad (118)
\end{aligned}
$$

Lemma 10: Let $x_i, x_j, x_l, x_v, x_w \in GF(3)$. Then, using the value of x_w and the following five combinations:

$$
\begin{aligned}
&g\big(x_i, x_j, x_l, x_w\big) + g\big(x_i, x_j, x_v, x_w\big) \\
&g(x_i, x_l, x_v, x_w) + g\big(x_j, x_l, x_v, x_w\big), \\
&x_i + x_j + x_l, \\
&x_i + x_j + x_v, \\
&x_i + x_l + x_v, \\
&x_j + x_l + x_v,
\end{aligned}
$$

we can find the value of each x_i, x_j, x_l, and x_v.

Proof: Refer to Appendix F. ■

Lemma 11: Using the value of x_i, x_j, x_l and $x_v + x_w$, we can find the value of $g(x_i, x_j, x_v, x_w) + 2g(x_i, x_l, x_v, x_w)$.

Proof: Refer to Appendix F. ■

Proposition 15: There exists a scalar nonlinear code over the fields with characteristic three, which can achieve the broadcast rate of $\mathcal{I}_3$.

Proof: First, it can be seen that set [8] is a MAIS set of $\mathcal{I}_3$. So, $\beta_{\text{MAIS}}(\mathcal{I}_3) = 8$. Now, we prove that $\beta(\mathcal{C}_{\mathcal{I}_3}) = 8$ for a scalar nonlinear index code $\mathcal{C}_{\mathcal{I}_3} = (\phi_{\mathcal{I}_3}, \{\psi^i_{\mathcal{I}_3}\})$, where the encoder and decoder do as below.

First, function $\phi_{\mathcal{I}_3}$ encodes messages $x_i, i \in [58]$ into eight coded messages $z_k, k \in [8]$, as follows

$$
\big\{z_j, j \in [8]\big\} = \phi_{\mathcal{I}_3}(\{x_i, i \in [58]\}), \quad (119)
$$

where

$$
\begin{aligned}
z_1 &= x_1 + x_9 + x_{11} + x_{13} + x_{17} + x_{19} + x_{27} + x_{35} + x_{43} + x_{53}, \\
z_2 &= x_2 + x_{10} + x_{12} + x_{14} + x_{18} + x_{20} + x_{28} + x_{36} + x_{44} + x_{54} \\
&\quad + g(x_9, x_{11}, x_{13}, x_{17}), \\
z_3 &= x_3 + x_9 + x_{11} + x_{15} + x_{17} + x_{21} + x_{29} + x_{37} + x_{45} + x_{51}, \\
z_4 &= x_4 + x_{10} + x_{12} + x_{16} + x_{18} + x_{22} + x_{30} + x_{38} + x_{46} + x_{52} \\
&\quad + g(x_9, x_{11}, x_{15}, x_{17}), \\
z_5 &= x_5 + x_9 + x_{13} + x_{15} + x_{17} + x_{23} + x_{31} + x_{39} + x_{47} + x_{57}, \\
z_6 &= x_6 + x_{10} + x_{14} + x_{16} + x_{18} + x_{24} + x_{32} + x_{40} + x_{48} + x_{58} \\
&\quad + g(x_9, x_{13}, x_{15}, x_{17}), \\
z_7 &= x_7 + x_{11} + x_{13} + x_{15} + x_{17} + x_{25} + x_{33} + x_{41} + x_{49} + x_{55}, \\
z_8 &= x_8 + x_{12} + x_{14} + x_{16} + x_{18} + x_{26} + x_{34} + x_{42} + x_{50} + x_{56} \\
&\quad + g(x_{11}, x_{13}, x_{15}, x_{17}).
\end{aligned}
$$

Now, we show how the i-th decoder $\psi^i_{\mathcal{I}_3}$ recovers the requested message x_i using the coded messages $z_k, k \in [8]$ along with the messages in its side information.

- Each user $u_i, i \in [8]$ can directly decode its requested message x_i, from the coded message z_i.
- User u_9 decodes $(x_9 + x_{11} + x_{13})$, $(x_9 + x_{11} + x_{15})$, $(x_9 + x_{13} + x_{15})$, and $(x_{11} + x_{13} + x_{15})$, respectively, from z_1, z_3, z_5 and z_7. It also adds $z_2 + z_4 + z_6 + z_8$ to achieve $g(x_9, x_{11}, x_{13}, x_{17})+ g(x_9, x_{11}, x_{15}, x_{17})+ g(x_9, x_{13}, x_{15}, x_{17})+ g(x_{11}, x_{13}, x_{15}, x_{17})$. Now, according to Lemma 10, by having x_{17}, it is able to recover its requested message x_9.
- User u_{10} first decodes x_9 and $x_{12} + x_{14}$, respectively, from z_1 and z_8. Then, it can decode its requested message x_{10} from z_2.
- User u_{11} decodes $(x_9 + x_{11} + x_{13})$, $(x_9 + x_{11} + x_{15})$, $(x_9 + x_{13} + x_{15})$, and $(x_{11} + x_{13} + x_{15})$, respectively, from z_1, z_3, z_5 and z_7. It also adds $z_2 + z_4 + z_6 + z_8$ to achieve $g(x_9, x_{11}, x_{13}, x_{17})+ g(x_9, x_{11}, x_{15}, x_{17})+ g(x_9, x_{13}, x_{15}, x_{17})+ g(x_{11}, x_{13}, x_{15}, x_{17})$. Now, according to Lemma 10, by having x_{17}, it is able to recover its requested message x_{11}.

- User u_{12} first decodes x_{11} and $x_{14}+x_{16}$, respectively, from z_3 and z_6. Then, it can decode its requested message x_{12} from z_4.
- User u_{13} decodes $(x_9+x_{11}+x_{13})$, $(x_9+x_{11}+x_{15})$, $(x_9+x_{13}+x_{15})$, and $(x_{11}+x_{13}+x_{15})$, respectively, from z_1, z_3, z_5 and z_7. It also adds $z_2+z_4+z_6+z_8$ to achieve $g(x_9, x_{11}, x_{13}, x_{17})+$ $g(x_9, x_{11}, x_{15}, x_{17})+$ $g(x_9, x_{13}, x_{15}, x_{17})+$ $g(x_{11}, x_{13}, x_{15}, x_{17})$. Now, according to Lemma 10, by having x_{17}, it is able to recover its requested message x_{13}.
- User u_{14} first decodes x_{13} and $x_{10}+x_{16}$, respectively, from z_5 and z_4. Then, it can decode its requested message x_{14} from z_6.
- User u_{15} decodes $(x_9+x_{11}+x_{13})$, $(x_9+x_{11}+x_{15})$, $(x_9+x_{13}+x_{15})$, and $(x_{11}+x_{13}+x_{15})$, respectively, from z_1, z_3, z_5 and z_7. It also adds $z_2+z_4+z_6+z_8$ to achieve $g(x_9, x_{11}, x_{13}, x_{17})+$ $g(x_9, x_{11}, x_{15}, x_{17})+$ $g(x_9, x_{13}, x_{15}, x_{17})+$ $g(x_{11}, x_{13}, x_{15}, x_{17})$. Now, according to Lemma 10, by having x_{17}, it is able to recover its requested message x_{15}.
- User u_{16} first decodes x_{15} and $x_{10}+x_{12}$, respectively, from z_7 and z_2. Then, it can decode its requested message x_{16} from z_8.
- User u_{17} can decode its desired message x_{17} from z_1.
- User u_{18} can decode its desired message x_{18} from z_2.
- User u_{19} first decodes x_9 from z_5. Then, it can decode x_{19} from z_1.
- User u_{20} first decodes x_9 from z_5. Then, it decodes x_{10} from z_6. Finally, it can decode x_{20} from z_2.
- User u_{21} first decodes x_9 from z_1. Then, it can decode x_{21} from z_3.
- User u_{22} first decodes x_9 from z_1. Then, it decodes x_{10} from z_2. Finally, it can decode x_{22} from z_4.
- User u_{23} first decodes x_9 from z_3. Then, it can decode x_{23} from z_5.
- User u_{24} first decodes x_9 from z_3. Then, it decodes x_{10} from z_4. Finally, it can decode x_{24} from z_6.
- User u_{25} first decodes $x_{15}+x_{17}$ from z_3. Then, it can decode x_{25} from z_7.
- User u_{26} first decodes $x_{15}+x_{17}$ from z_3. Then, it adds z_6 and $2z_8$ to achieve $g(x_9+x_{13}+x_{15}+x_{17})+2g(x_{11}+x_{13}+x_{15}+x_{17})+2x_{26}$ (note, term $x_{16}+x_{18}$ is canceled out). Now, since u_{26} knows x_9, x_{11}, x_{13} and $x_{15}+x_{17}$, according to Lemma 11, it can achieve $g(x_9+x_{13}+x_{15}+x_{17})+2g(x_{11}+x_{13}+x_{15}+x_{17})$. Thus, it can decode its desired message x_{26}.
- User u_{27} first decodes x_{11} from z_7. Then, it can decode x_{27} from z_1.
- User u_{28} first decodes x_{11} from z_7. Then, it decodes x_{12} from z_8. Finally, it can decode x_{28} from z_2.
- User u_{29} first decodes x_{11} from z_1. Then, it can decode x_{29} from z_3.
- User u_{30} first decodes x_{11} from z_1. Then, it decodes x_{12} from z_2. Finally, it can decode x_{30} from z_4.
- User u_{31} first decodes x_9+x_{17} from z_1. Then, it can decode x_{31} from z_5.
- User u_{32} first decodes x_9+x_{17} from z_1. Then, it adds z_4 and $2z_6$ to achieve $g(x_9+x_{11}+x_{15}+x_{17})+2g(x_9+x_{13}+x_{15}+x_{17})+2x_{32}$ (note, term $x_{10}+x_{18}$ is canceled out). Now, since u_{32} knows x_{11}, x_{13}, x_{15} and x_9+x_{17}, according to Lemma 11, it can achieve $g(x_9+x_{11}+x_{15}+x_{17})+2g(x_9+x_{13}+x_{15}+x_{17})$. Thus, it can decode its desired message x_{32}.
- User u_{33} first decodes x_{11} from z_3. Then, it can decode x_{33} from z_7.
- User u_{34} first decodes x_{11} from z_3. Then, it decodes x_{12} from z_4. Finally, it can decode x_{34} from z_8.
- User u_{35} first decodes x_{13} from z_7. Then, it can decode x_{35} from z_1.
- User u_{36} first decodes x_{13} from z_7. Then, it decodes x_{14} from z_8. Finally, it can decode x_{36} from z_2.
- User u_{37} first decodes $x_{11}+x_{17}$ from z_7. Then, it can decode x_{37} from z_3.
- User u_{38} first decodes $x_{11}+x_{17}$ from z_7. Then, it adds z_2 and $2z_4$ to achieve $g(x_9+x_{11}+x_{13}+x_{17})+2g(x_9+x_{11}+x_{15}+x_{17})+2x_{38}$ (note, term $x_{12}+x_{18}$ is canceled out). Now, since u_{38} knows x_9, x_{13}, x_{15} and $x_{11}+x_{17}$, according to Lemma 11, it can achieve $g(x_9+x_{11}+x_{13}+x_{17})+2g(x_9+x_{11}+x_{15}+x_{17})$. Thus, it can decode its desired message x_{38}.
- User u_{39} first decodes x_{13} from z_1. Then, it can decode x_{39} from z_5.
- User u_{40} first decodes x_{13} from z_1. Then, it decodes x_{14} from z_2. Finally, it can decode x_{40} from z_6.
- User u_{41} first decodes x_{13} from z_5. Then, it can decode x_{41} from z_7.
- User u_{42} first decodes x_{13} from z_5. Then, it decodes x_{14} from z_6. Finally, it can decode x_{42} from z_8.
- User u_{43} first decodes $x_{13}+x_{17}$ from z_5. Then, it can decode x_{43} from z_1.
- User u_{44} first decodes $x_{13}+x_{17}$ from z_5. Then, it adds z_6 and $2z_2$ to achieve $g(x_9+x_{13}+x_{15}+x_{17})+2g(x_9+x_{11}+x_{13}+x_{17})+2x_{44}$ (note, term $x_{14}+x_{18}$ is canceled out). Now, since u_{44} knows x_9, x_{11}, x_{15} and $x_{13}+x_{17}$, according to Lemma 11, it can achieve $g(x_9+x_{13}+x_{15}+x_{17})+2g(x_9+x_{11}+x_{13}+x_{17})$. Thus, it can decode its desired message x_{44}.
- User u_{45} first decodes x_{15} from z_7. Then, it can decode x_{45} from z_3.
- User u_{46} first decodes x_{15} from z_7. Then, it decodes x_{16} from z_8. Finally, it can decode x_{46} from z_4.
- User u_{47} first decodes x_{15} from z_3. Then, it can decode x_{47} from z_5.
- User u_{48} first decodes x_{15} from z_3. Then, it decodes x_{16} from z_4. Finally, it can decode x_{48} from z_6.
- User u_{49} first decodes x_{15} from z_5. Then, it can decode x_{49} from z_7.
- User u_{50} first decodes x_{15} from z_5. Then, it decodes x_{16} from z_6. Finally, it can decode x_{50} from z_8.
- User u_{51} first decodes x_9+x_{17} from z_1. Then, it can decode x_{51} from z_3.

- User u_{52} first decodes $x_9 + x_{17}$ from z_1. Then, it adds z_2 and $2z_4$ to achieve $g(x_9+x_{11}+x_{13}+x_{17})+2g(x_9+x_{11}+x_{15}+x_{17})+2x_{52}$ (note, term $x_{10}+x_{18}$ is canceled out). Now, since u_{52} knows x_{11}, x_{13}, x_{15} and $x_9 + x_{17}$, according to Lemma 11, it can find $g(x_9+x_{11}+x_{13}+x_{17})+2g(x_9+x_{11}+x_{15}+x_{17})$. Thus, it can decode its desired message x_{52}.
- User u_{53} first decodes $x_{11} + x_{17}$ from z_7. Then, it can decode x_{53} from z_1.
- User u_{54} first decodes $x_{11} + x_{17}$ from z_7. Then, it adds z_8 and $2z_2$ to achieve $g(x_{11}+x_{13}+x_{15}+x_{17})+2g(x_9+x_{11}+x_{13}+x_{17})+2x_{54}$ (note, term $x_{12}+x_{18}$ is canceled out). Now, since u_{54} knows x_9, x_{13}, x_{15} and $x_{11} + x_{17}$, according to Lemma 11, it can find $g(x_{11}+x_{13}+x_{15}+x_{17})+2g(x_9+x_{11}+x_{13}+x_{17})$. Thus, it can decode its desired message x_{54}.
- User u_{55} first decodes $x_{13} + x_{17}$ from z_5. Then, it can decode x_{55} from z_7.
- User u_{56} first decodes $x_{13} + x_{17}$ from z_5. Then, it adds z_6 and $2z_8$ to achieve $g(x_9+x_{13}+x_{15}+x_{17})+2g(x_{11}+x_{13}+x_{15}+x_{17})+2x_{56}$ (note, term $x_{14}+x_{18}$ is canceled out). Now, since u_{56} knows x_9, x_{11}, x_{15} and $x_{13} + x_{17}$, according to Lemma 11, it can find $g(x_9+x_{13}+x_{15}+x_{17})+2g(x_{11}+x_{13}+x_{15}+x_{17})$. Thus, it can decode its desired message x_{56}.
- User u_{57} first decodes $x_{15} + x_{17}$ from z_3. Then, it can decode x_{57} from z_5.
- User u_{58} first decodes $x_{15} + x_{17}$ from z_3. Then, it adds z_4 and $2z_6$ to achieve $g(x_9+x_{11}+x_{15}+x_{17})+2g(x_9+x_{13}+x_{15}+x_{17})+2x_{58}$ (note, term $x_{16}+x_{18}$ is canceled out). Now, since u_{58} knows x_9, x_{11}, x_{13} and $x_{15} + x_{17}$, according to Lemma 11, it can find $g(x_9+x_{11}+x_{15}+x_{17})+2g(x_9+x_{13}+x_{15}+x_{17})$. Thus, it can decode its desired message x_{58}. ■

VI. CONCLUSION

The suboptimality of linear coding rate for the general index coding problem is due to its dependency on the field size. This dependency has been illustrated through the two well-known matroid instances, namely the Fano and non-Fano matroids, which, in turn, limits its scope only to fields with characteristic two. In this paper, this scope of dependency was extended to the fields with characteristic three by designing two index coding instances of size 29 such that for the first instance, linear coding is optimal only over the fields with characteristic three, while for the second instance, linear coding is optimal over fields with any characteristic other than characteristic three. For each instance, it was shown that the key constraints on the column space of its encoding matrix can be captured by a matroid with the ground set of size 9, for which the existence of its linear representation is dependent on the fields with characteristic three. Presenting the proofs and discussions using these two relatively small matroids is helpful in pointing out the key constraints causing the linear coding rate to become dependent on the field size. Finally, we designed the third index coding instance of size 58 such that while linear coding cannot achieve its optimal rate over fields with characteristic three, there exists an optimal nonlinear code over fields with characteristic three. It was shown that connecting the first and third index coding instances in two specific ways, called no-way and two-way connections, will lead to two new index coding instances of size 87 and 91, for which linear coding is outperformed by nonlinear codes.

Extending the results of this paper to find the matroid instances and their corresponding index coding instances whose linear representation and linear coding rate is dependent on fields with higher characteristics would be an interesting direction for future studies. Another intriguing direction is to design a general optimal nonlinear coding scheme as an extension of the minrank coding scheme [25], which is the optimal linear code for the general index coding problem.

APPENDIX A
EXPANDED DEFINITION OF MATROID INSTANCES $\mathcal{N}_1$ AND $\mathcal{N}_2$

To characterize matroid instances $\mathcal{N}_1$ and $\mathcal{N}_2$, we need to assign nonnegative integer values to $f(N), N \subseteq [n = 9]$ which satisfy the three conditions in (7). In this section, first by providing a simple example, we show that how a matroid instance can be characterized by some of its basis and circuit sets. This will then be followed by the expanded definition of matroid instances $\mathcal{N}_1$ and $\mathcal{N}_2$.

Lemma 12: Given a matroid instance $\mathcal{N} = \{f(N), N \subseteq [n]\}$, if set N is a basis or circuit set, then the value of each $f(N_1 \subseteq N)$ is determined as follows:

- If set N is a basis set, then $f(N_1 \subseteq N) = |N_1|$.
- If set N is a circuit set, then $f(N_1 \subset N) = |N_1|$, and $f(N) = |N| - 1$.

Proof: We only need to prove that if $f(N) = |N|$, then $f(N_1 \subseteq N) = |N_1|$. The proof can be easily described using the first and third conditions in (7), as follows:

- According to the first condition in (7), we have

$$\begin{aligned} f(N_1) &\leq |N_1|, \\ f(N \backslash N_1) &\leq |N \backslash N_1| = |N| - |N_1|. \end{aligned} \tag{120}$$

- According to the third condition in (7), we have

$$f(\emptyset) + f(N) \leq f(N \backslash N_1) + f(N_1). \tag{121}$$

Now, since $f(\emptyset) = 0$ (as $f(\emptyset) \leq |\emptyset| = 0$) and $f(N) = |N|$, from (120) and (121), we must have $f(N_1) = |N_1|$. ■

Example 8: Consider matroid instance $\mathcal{N} = \{(N, f(N)), N \subseteq [n]\}$ with $n = 4$ and $f(\mathcal{N}) = 3$ such that set $\{1, 2, 3\}$ is a basis set, and set $\{1, 2, 4\}$ is a circuit set. Now, we show that using (7) and (8), all the values of $f(N), N \subseteq [n]$ are determined. First, note that based on Lemma 12, we have

$$\begin{aligned} &f(N \subseteq \{1, 2, 3\}) = |N|, \\ &f(N \subset \{1, 2, 4\}) = |N|, \quad f(\{1, 2, 4\}) = 2. \end{aligned}$$

Now, only the values of $f(N)$ for sets $\{3,4\}$, $\{1,3,4\}$, $\{2,3,4\}$ and $\{1,2,3,4\}$ need to be determined. Using (7), we show that each set $\{1,3,4\}$ and $\{2,3,4\}$ is a basis set, as follows:

$$\begin{aligned} f(\{1,3,4\})+f(\{1,2,4\}) &\geq f(\{1,4\})+f(\{1,2,3,4\}) \quad (122)\\ &\geq f(\{1,4\})+f(\{1,2,3\})\\ &=5, \quad (123)\end{aligned}$$

where (122) and (123), respectively, are due to the third and second conditions in (7). Since $f(\{1,2,4\})=2$, we have $f(\{1,3,4\})\geq 3$, and due to the first condition, $f(\{1,3,4\})\leq 3$, which leads to $f(\{1,3,4\})=3$. This means that set $\{1,3,4\}$ is a basis set, and thus, $f(\{3,4\})=2$.

Similarly for set $\{2,3,4\}$, we have

$$\begin{aligned} f(\{2,3,4\})+f(\{1,2,4\}) &\geq f(\{2,4\})+f(\{1,2,3,4\})\\ &\geq f(\{2,4\})+f(\{1,2,3\})\\ &=5,\end{aligned}$$

leading to $f(\{1,3,4\})=3$.

Finally, we get $f(\{1,2,3,4\})=3$, as follows:

$$3=f(\{1,2,3\})\leq f(\{1,2,3,4\})\leq f(\mathcal{N})=3. \quad (124)$$

A. MATROID INSTANCES $\mathcal{N}_1$ AND $\mathcal{N}_2$

Here, for both matroid instances $\mathcal{N}_1$ and $\mathcal{N}_2$, we consider the following sets, where $N_i, i\in[9]$ are equal to (15):

$$\begin{aligned} \mathcal{T}_1 &= \{N_i, i\in[9]\},\\ \mathcal{T}_2 &= \{\{1,2\}\cup N, N\subseteq\{7,8,9\}, N\neq\emptyset\},\\ \mathcal{T}_3 &= \{\{1,3\}\cup N, N\subseteq\{6,8,9\}, N\neq\emptyset\},\\ \mathcal{T}_4 &= \{\{1,4\}\cup N, N\subseteq\{5,8,9\}, N\neq\emptyset\},\\ \mathcal{T}_5 &= \{\{2,3\}\cup N, N\subseteq\{6,7,9\}, N\neq\emptyset\},\\ \mathcal{T}_6 &= \{\{2,4\}\cup N, N\subseteq\{5,7,9\}, N\neq\emptyset\},\\ \mathcal{T}_7 &= \{\{3,4\}\cup N, N\subseteq\{5,6,9\}, N\neq\emptyset\}, \quad (125)\end{aligned}$$

Definition 31 (Expanded Definition of Matroid Instance $\mathcal{N}_1$): Matroid instance $\mathcal{N}_1=\{f(N), N\subseteq[n]\}$ of size $n=9$ and rank $f(\mathcal{N}_1)=4$, is characterized as follows:

$$\begin{aligned} f(N) &= 3, \qquad \forall N\in\mathcal{T}_i, i\in[7],\\ f(N) &= \min\{4,|N|\}, \qquad \forall N\subseteq[n], N\notin\mathcal{T}_i, i\in[7] \quad (126)\end{aligned}$$

Using the three conditions in (7), it can be shown that Definition 22 will lead to (126). Here for the sake of brevity, we only show that (126) holds for sets $N\in\mathcal{T}_i, i\in[7]$, but this can also be shown in the same way for the remaining sets.

- $\mathcal{T}_1$: Since each set $N_i\in\mathcal{T}_1, i\in[9]$ is a circuit set, based on Lemma 12, for all $i\in[9]$, we have

$$f(N_i)=|N_i|-1, \quad f(N\subset N_i)=|N|. \quad (127)$$

- $\mathcal{T}_2$: First, we show that $f(\{1,2,7\})=3$, as follows:

$$\begin{aligned} f(\{1,2,7\})+f(\{1,3,4,7\}) &\geq f(\{1,7\})+f(\{1,2,3,4,7\})\\ &\geq f(\{1,7\})+f(\{1,2,3,4\})\\ &=6.\end{aligned}$$

Since $f(N_3=\{1,3,4,7\})=3$, we get $f(\{1,2,7\})=3$. Similarly, we get $f(\{1,2,8\})=3$, as follows:

$$\begin{aligned} f(\{1,2,8\})+f(\{2,3,4,8\}) &\geq f(\{2,8\})+f(\{1,2,3,4,8\})\\ &\geq f(\{2,8\})+f(\{1,2,3,4\})\\ &=6.\end{aligned}$$

Since $f(N_4=\{2,3,4,8\})=3$, we get $f(\{1,2,8\})=3$. Now, we show $f(\{1,2,7,8\})=f(\{1,2,7,9\})=f(\{1,2,8,9\})=f(\{1,2,7,8,9\})=3$, as follows:

$$\begin{aligned} f(\{9\})+f(\{1,2,7,8,9\}) &\leq f(\{1,8,9\})+f(\{2,7,9\})\\ &=4.\end{aligned}$$

Due to $f(\{9\})=1$, we get $f(\{1,2,7,8,9\})\leq 3$. Now, since $f(\{1,2,7\})=f(\{1,2,8\})=3$, we get $f(\{1,2,7,8\})=f(\{1,2,7,9\})=f(\{1,2,8,9\})=f(\{1,2,7,8,9\})=3$.

- $\mathcal{T}_3$: First, we show that $f(\{1,3,6\})=3$, as follows:

$$\begin{aligned} f(\{1,3,6\})+f(\{1,2,4,6\}) &\geq f(\{1,6\})+f(\{1,2,3,4,6\})\\ &\geq f(\{1,6\})+f(\{1,2,3,4\})\\ &=6.\end{aligned}$$

Since $f(N_2=\{1,2,4,6\})=3$, we get $f(\{1,3,6\})=3$. Similarly, we get $f(\{1,3,8\})=3$, as follows:

$$\begin{aligned} f(\{1,3,8\})+f(\{2,3,4,8\}) &\geq f(\{3,8\})+f(\{1,2,3,4,8\})\\ &\geq f(\{3,8\})+f(\{1,2,3,4\})\\ &=6.\end{aligned}$$

Since $f(N_4=\{2,3,4,8\})=3$, we get $f(\{1,3,8\})=3$. Now, we show $f(\{1,3,6,8\})=f(\{1,3,6,9\})=f(\{1,3,8,9\})=f(\{1,3,6,8,9\})=3$, as follows:

$$\begin{aligned} f(\{9\})+f(\{1,3,6,8,9\}) &\leq f(\{1,8,9\})+f(\{3,6,9\})\\ &=4.\end{aligned}$$

Due to $f(\{9\})=1$, we get $f(\{1,3,6,8,9\})\leq 3$. Now, since $f(\{1,3,6\})=f(\{1,3,8\})=3$, we get $f(\{1,3,6,8\})=f(\{1,3,6,9\})=f(\{1,3,8,9\})=f(\{1,3,6,8,9\})=3$.

- $\mathcal{T}_4$: First, we show that $f(\{1,4,5\})=3$, as follows:

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

Since $f(N_1=\{1,2,3,5\})=3$, we get $f(\{1,4,5\})=3$. Similarly, we get $f(\{1,4,8\})=3$, as follows:

$$\begin{aligned} f(\{1,4,8\})+f(\{2,3,4,8\}) &\geq f(\{4,8\})+f(\{1,2,3,4,8\})\\ &\geq f(\{4,8\})+f(\{1,2,3,4\})\\ &=6.\end{aligned}$$

Since $f(N_4=\{2,3,4,8\})=3$, we get $f(\{1,4,8\})=3$. Now, we show $f(\{1,4,5,8\})=f(\{1,4,5,9\})=f(\{1,4,8,9\})=f(\{1,4,5,8,9\})=3$, as follows:

$$f(\{9\})+f(\{1,4,5,8,9\}) \leq f(\{1,8,9\})+f(\{4,5,9\}) = 4.$$

Due to $f(\{9\}) = 1$, we get $f(\{1,4,5,8,9\}) \leq 3$. Now, since $f(\{1,4,5\}) = f(\{1,4,8\}) = 3$, we get $f(\{1,4,5,8\}) = f(\{1,4,5,9\}) = f(\{1,4,8,9\}) = f(\{1,4,5,8,9\}) = 3$.

- $\mathcal{T}_5$: First, we show that $f(\{2,3,6\}) = 3$, as follows:

$$\begin{aligned} f(\{2,3,6\})+f(\{1,2,4,6\}) &\geq f(\{2,6\})+f(\{1,2,3,4,6\}) \\ &\geq f(\{2,6\})+f(\{1,2,3,4\}) \\ &= 6. \end{aligned}$$

Since $f(N_2 = \{1,2,4,6\}) = 3$, we get $f(\{2,3,6\}) = 3$. Similarly, we get $f(\{2,3,7\}) = 3$, as follows:

$$\begin{aligned} f(\{2,3,7\})+f(\{1,3,4,7\}) &\geq f(\{3,7\})+f(\{1,2,3,4,7\}) \\ &\geq f(\{3,7\})+f(\{1,2,3,4\}) \\ &= 6. \end{aligned}$$

Since $f(N_3 = \{1,3,4,7\}) = 3$, we get $f(\{2,3,7\}) = 3$. Now, we show $f(\{2,3,6,7\}) = f(\{2,3,6,9\}) = f(\{2,3,7,9\}) = f(\{2,3,6,7,9\}) = 3$, as follows:

$$f(\{9\})+f(\{2,3,6,7,9\}) \leq f(\{2,7,9\})+f(\{3,6,9\}) = 4.$$

Due to $f(\{9\}) = 1$, we get $f(\{2,3,6,7,9\}) \leq 3$. Now, since $f(\{2,3,6\}) = f(\{2,3,7\}) = 3$, we get $f(\{2,3,6,7\}) = f(\{2,3,6,9\}) = f(\{2,3,7,9\}) = f(\{2,3,6,7,9\}) = 3$.

- $\mathcal{T}_6$: First, we show that $f(\{2,4,5\}) = 3$, as follows:

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

Since $f(N_1 = \{1,2,3,5\}) = 3$, we get $f(\{2,4,5\}) = 3$. Similarly, we get $f(\{2,4,7\}) = 3$, as follows:

$$\begin{aligned} f(\{2,4,7\})+f(\{1,3,4,7\}) &\geq f(\{4,7\})+f(\{1,2,3,4,7\}) \\ &\geq f(\{4,7\})+f(\{1,2,3,4\}) \\ &= 6. \end{aligned}$$

Since $f(N_3 = \{1,3,4,7\}) = 3$, we get $f(\{2,4,7\}) = 3$. Now, we show $f(\{2,4,5,7\}) = f(\{2,4,5,9\}) = f(\{2,4,7,9\}) = f(\{2,4,5,7,9\}) = 3$, as follows:

$$f(\{9\})+f(\{2,4,5,7,9\}) \leq f(\{2,7,9\})+f(\{4,5,9\}) = 4.$$

Due to $f(\{9\}) = 1$, we get $f(\{2,4,5,7,9\}) \leq 3$. Now, since $f(\{2,4,5\}) = f(\{2,4,7\}) = 3$, we get $f(\{2,4,5,7\}) = f(\{2,4,5,9\}) = f(\{2,4,7,9\}) = f(\{2,4,5,7,9\}) = 3$.

- $\mathcal{T}_7$: First, we show that $f(\{3,4,5\}) = 3$, as follows:

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

Since $f(N_1 = \{1,2,3,5\}) = 3$, we get $f(\{3,4,5\}) = 3$. Similarly, we get $f(\{3,4,6\}) = 3$, as follows:

$$\begin{aligned} f(\{3,4,6\})+f(\{1,2,4,6\}) &\geq f(\{4,6\})+f(\{1,2,3,4,6\}) \\ &\geq f(\{4,6\})+f(\{1,2,3,4\}) \\ &= 6. \end{aligned}$$

Since $f(N_2 = \{1,2,4,6\}) = 3$, we get $f(\{3,4,6\}) = 3$. Now, we show $f(\{3,4,5,6\}) = f(\{3,4,5,9\}) = f(\{3,4,6,9\}) = f(\{3,4,5,6,9\}) = 3$, as follows:

$$f(\{9\})+f(\{3,4,5,6,9\}) \leq f(\{3,6,9\})+f(\{4,5,9\}) = 4.$$

Due to $f(\{9\}) = 1$, we get $f(\{3,4,5,6,9\}) \leq 3$. Now, since $f(\{3,4,5\}) = f(\{3,4,6\}) = 3$, we get $f(\{3,4,5,6\}) = f(\{3,4,5,9\}) = f(\{3,4,6,9\}) = f(\{3,4,5,6,9\}) = 3$.

Similarly, it can be shown that (61) is equivalent to the following definition.

Definition 32 (Expanded Definition of Matroid Instance $\mathcal{N}_2$): For matroid instance $\mathcal{N}_2 = \{f(N), N \subseteq [n]\}$ of size $n = 9$ and rank $f(\mathcal{N}_2) = 4$, the values assigned to $f(N), N \subseteq [n]$ are the same as (126), except for set $N_9 = \{5,6,7,8\}$, which is $f(N_9) = |N_9| = 4$. This is because set N_9 is a basis set for $\mathcal{N}_2$.

APPENDIX B
PROOF OF LEMMAS 1-5

Remark 5: It can be verified that the decoding condition in (2) along with the properties of the rank function gives the following results.

$$\text{rank}\left(\boldsymbol{H}^{\{i\}\cup M}\right) = \text{rank}\left(\boldsymbol{H}^{M}\right) + t, \forall M \subseteq B_i, \quad \forall i \in [m], \tag{128}$$

$$\text{rank}\left(\boldsymbol{H}^{\{i\}}\right) = t, \quad \forall i \in [m], \tag{129}$$

$$\text{rank}\left(\boldsymbol{H}^{M_1}\right) \leq \text{rank}\left(\boldsymbol{H}^{M_2}\right), \quad \forall M_1 \subseteq M_2 \subseteq [m]. \tag{130}$$

A. PROOF OF LEMMA 1

If M is an acyclic set, then we can find a sequence of its elements $i_1, \dots, i_{|M|} \in M$ such that $M_j \subseteq B_{i_j}, \forall j \in [|M|]$, where $M_j = \{i_{j+1}, \dots, i_{|M|}\}, \forall j \in [|M|-1]$ and $M_{|M|} = \emptyset$. Note $M = \{i_1\} \cup M_1$ and $M_j = \{i_{j+1}\} \cup M_{j+1}, \forall j \in [|M|-1]$. By applying the condition in (128) for each $i = i_1, \dots, i_{|M|}$, we have

$$\begin{aligned} \text{rank}\left(\boldsymbol{H}^{M=\{i_1\}\cup M_1}\right) &= \text{rank}\left(\boldsymbol{H}^{M_1=\{i_2\}\cup M_2}\right) + t \\ &= \text{rank}\left(\boldsymbol{H}^{M_2=\{i_3\}\cup M_3}\right) + 2t \\ &= \cdots \\ &= |M|t, \end{aligned}$$

which means that M is a basis set of $\boldsymbol{H}$.

B. PROOF OF LEMMA 2

First, note that for any $l \in M$, set $M\backslash\{l\}$ is an acyclic set. Then, according to Lemma 1,

$$\text{rank}\left(\boldsymbol{H}^{M\backslash\{l\}}\right) = (|M|-1)t, \quad \forall l \in M. \tag{131}$$

So, having $\text{rank}(\boldsymbol{H}^M) = (|M|-1)t$ requires $\boldsymbol{H}^{\{l\}} = \sum_{i\in M\backslash\{l\}} \boldsymbol{H}^{\{i\}}\boldsymbol{M}_{l,i}$. Now, if one of the $\boldsymbol{M}_{l,i}, i \in M\backslash\{l\}$ is not invertible, then $\text{rank}(\boldsymbol{H}^{M\backslash\{i\}}) < (|M|-1)t$, which contradicts (131). Thus, each $\boldsymbol{M}_{l,i}$ must be invertible, which means that M is a circuit set of $\boldsymbol{H}$.

C. PROOF OF LEMMA 3

First, because M is an independent set, then $M\backslash\{i\} \subseteq B_i, \forall i \in M$. Moreover, since M is an acyclic set of $\mathcal{I}$, then according to Lemma 1, $\text{rank}(\boldsymbol{H}^M) = |M|t$. Now, in order to have $\text{col}(\boldsymbol{H}^{\{j\}}) \subseteq \text{col}(\boldsymbol{H}^M)$, one must have $\boldsymbol{H}^{\{j\}} = \sum_{i\in M}\boldsymbol{H}^{\{i\}}\boldsymbol{M}_{j,i}$. Since $j \in [m]\backslash M$ and $j \in B_l$ for some $i \in M\backslash\{l\}$, then $\{j\} \cup M\backslash\{l\} \subseteq B_l$. Now, assume $\boldsymbol{M}_{j,i}$ is a nonzero matrix (i.e., $\text{rank}(\boldsymbol{M}_{j,i}) \geq 1$). Then,

$$\begin{aligned}
\text{rank}\left(\boldsymbol{H}^{\{j\}\cup M}\right) &= \text{rank}\left(\boldsymbol{H}^{\{l\}\cup(\{j\}\cup M\backslash\{l\})}\right) \\
&= \text{rank}\left(\boldsymbol{H}^{\{j\}\cup M\backslash\{l\}}\right) + t \qquad (132)\\
&= \text{rank}\left(\left[\boldsymbol{H}^{\{j\}}\middle|\boldsymbol{H}^{M\backslash\{l\}}\right]\right) + t \\
&= \text{rank}\left(\left[\textstyle\sum_{i\in M}\boldsymbol{H}^{\{i\}}\boldsymbol{M}_{j,i}\middle|\boldsymbol{H}^{M\backslash\{l\}}\right]\right) + t \\
&\geq \text{rank}\left(\left[\boldsymbol{H}^{\{l\}}\boldsymbol{M}_{j,l}\middle|\boldsymbol{H}^{M\backslash\{l\}}\right]\right) + t \qquad (133)\\
&= \text{rank}\left(\boldsymbol{H}^{\{l\}}\boldsymbol{M}_{j,l}\right) + (|M|-1)t + t \qquad (134)\\
&> |M|t, \qquad (135)
\end{aligned}$$

where (132) is due to (128), (133) is because of the property of the rank function by removing the term $\sum_{i\in M\backslash\{l\}}\boldsymbol{H}^{\{i\}}\boldsymbol{M}_{j,i}$ from $\sum_{i\in M}\boldsymbol{H}^{\{i\}}\boldsymbol{M}_{j,l}$ as it is a linear combination of the columns of $\boldsymbol{H}^{M\backslash\{l\}}$. (134) is based on Lemma 1 and the fact that M is an acyclic set of $\mathcal{I}$. Thus, the column space of $\boldsymbol{H}^{\{l\}}$ is linearly independent of column space of $\boldsymbol{H}^{M\backslash\{l\}}$. Finally, (135) is due to the fact that $\boldsymbol{H}^{\{l\}}$ is invertible and $\text{rank}(\boldsymbol{M}_{j,i}) \geq 1$. The result in (135) contradicts the assumption that $\text{rank}(\boldsymbol{H}^{\{j\}\cup M}) = |M|t$, and hence, we must have $\boldsymbol{M}_{j,i} = \boldsymbol{0}_t$. The same argument for $i \in M\backslash\{l\}$ gives $\boldsymbol{M}_{j,i} = \boldsymbol{0}_t, \forall i \in M\backslash\{l\}$. Therefore, $\boldsymbol{H}^{\{j\}} = \boldsymbol{H}^{\{l\}}\boldsymbol{M}_{j,l}$ and $\boldsymbol{M}_{j,l}$ must be invertible to have rank $\boldsymbol{H}^{\{j\}} = t$.

D. PROOF OF LEMMA 4

Corollaries 1-4 can be derived from earlier results and will be used in the proof of Lemma 4.

Corollary 1: Let M be an independent set of $\boldsymbol{H}$. Now, if $\text{col}(\boldsymbol{H}^{\{j\}}) \subseteq \text{col}(\boldsymbol{H}^M)$, then there exists one subset $M' \subseteq M$, such that $\{j\} \cup M'$ is a circuit set of $\boldsymbol{H}$.

Proof: Since $\text{col}(\boldsymbol{H}^{\{j\}}) \subseteq \text{col}(\boldsymbol{H}^M)$, we must have $\boldsymbol{H}^{\{j\}} = \sum_{i\in M}\boldsymbol{H}^{\{i\}}\boldsymbol{M}_{j,i}$ such that only matrices $\boldsymbol{M}_{j,i}, i \in M' \subseteq M$ are invertible. Thus, according to Definition 16, set $\{j\} \cup M'$ forms a circuit set of $\boldsymbol{H}$. ■

Corollary 2: If M is a minimal cyclic set of $\mathcal{I}$, then according to Definitions 10 and 11, any of its proper subsets $M' \subset M$ will be an acyclic set of $\mathcal{I}$.

Corollary 3 [25]: If M is an acyclic set of $\mathcal{I}$, then there exists at least one $l \in M$ such that $M\backslash\{l\} \subseteq B_l$.

Corollary 4: Suppose $\{j\} \cup M$ is a circuit set of $\boldsymbol{H}$. Then for any $l \in M$, we have $\text{col}(\boldsymbol{H}^{\{j\}\cup M\backslash\{l\}}) = \text{col}(\boldsymbol{H}^M)$.

Proof: Since $\{j\} \cup M$ is a circuit set of $\boldsymbol{H}$, we have $\boldsymbol{H}^{\{j\}} = \sum_{i\in M}\boldsymbol{H}^{\{j\}}\boldsymbol{M}_{j,i}$ such that each $\boldsymbol{M}_{j,i}$ is invertible. Now, assume $l \in M$. Then, we have

$$\begin{aligned}
\text{col}\left(\boldsymbol{H}^{\{j\}\cup M\backslash\{l\}}\right) &= \text{col}\left(\left[\boldsymbol{H}^{\{j\}}|\boldsymbol{H}^{M\backslash\{l\}}\right]\right) \\
&= \text{col}\left(\left[\sum_{i\in M}\boldsymbol{H}^{\{i\}}\boldsymbol{M}_{j,i}|\boldsymbol{H}^{M\backslash\{l\}}\right]\right) \\
&= \text{col}\left(\left[\boldsymbol{H}^{\{l\}}\boldsymbol{M}_{j,l}|\boldsymbol{H}^{M\backslash\{l\}}\right]\right) \\
&= \text{col}\left(\boldsymbol{H}^M\right), \qquad (136)
\end{aligned}$$

where (136) is due to the invertibility of $\boldsymbol{M}_{j,l}$. ■

1) PROOF OF LEMMA 4

Since M is an independent set of $\boldsymbol{H}$, and $\text{col}(\boldsymbol{H}^{\{j\}}) \subseteq \text{col}(\boldsymbol{H}^M)$, then according to Corollary 1, there exists a subset $M' \subseteq M$ such that $\{j\} \cup M'$ is a circuit set. Now, we show that $M' = M$, otherwise it leads to a contradiction. Assume $M' \subset M$. First, since M is a minimal cyclic set of $\mathcal{I}$, based on Corollary 2, $M' \subset M$ is an acyclic set of $\mathcal{I}$. Second, according to Corollary 3, there exists $l \in M'$ such that $M'\backslash\{l\} \subseteq B_l$. Also, due to $j \in B_l$, we get $\{j\} \cup (M'\backslash\{l\}) \subseteq B_l$. Thus,

$$\begin{aligned}
l \in M' &\rightarrow \text{col}\left(\boldsymbol{H}^{\{l\}}\right) \subseteq \text{col}\left(\boldsymbol{H}^{M'}\right), \\
\{j\} \cup \left(M'\backslash\{l\}\right) \subseteq B_l &\rightarrow \text{col}\left(\boldsymbol{H}^{\{j\}\cup(M'\backslash\{l\})}\right) \subseteq \text{col}\left(\boldsymbol{H}^{B_l}\right). \qquad (137)
\end{aligned}$$

Third, since $\{j\} \cup M'$ is a circuit set, Corollary 4 leads to

$$\text{col}\left(\boldsymbol{H}^{\{j\}\cup M'\backslash\{l\}}\right) = \text{col}\left(\boldsymbol{H}^{M'}\right). \tag{138}$$

Now, from (137) and (138), we have

$$\text{col}\left(\boldsymbol{H}^{\{l\}}\right) \subseteq \text{col}\left(\boldsymbol{H}^{M'}\right) = \text{col}\left(\boldsymbol{H}^{\{j\}\cup M'\backslash\{l\}}\right) \subseteq \text{col}\left(\boldsymbol{H}^{B_l}\right),$$

which contradicts the decoding condition in (2) for user u_l as $\text{col}(\boldsymbol{H}^{\{l\}}) \subseteq \text{col}(\boldsymbol{H}^{B_l})$. Therefore, we must have $M' = M$.

E. PROOF OF LEMMA 5

Since $\text{col}(\boldsymbol{H}^{\{9\}}) \subseteq \text{col}(\boldsymbol{H}^{\{1,8\}})$, we have

$$\boldsymbol{H}^{\{9\}} = \boldsymbol{H}^{\{1\}}\boldsymbol{M}_{9,1} + \boldsymbol{H}^{\{8\}}\boldsymbol{M}_{9,8}. \tag{139}$$

Moreover, since set $\{2, 3, 4, 8\}$ is a circuit set, we must have

$$\boldsymbol{H}^{\{8\}} = \boldsymbol{H}^{\{2\}}\boldsymbol{M}_{8,2} + \boldsymbol{H}^{\{3\}}\boldsymbol{M}_{8,3} + \boldsymbol{H}^{\{4\}}\boldsymbol{M}_{8,4}, \tag{140}$$

where each $\boldsymbol{M}_{8,2}, \boldsymbol{M}_{8,3}, \boldsymbol{M}_{8,4}$ is invertible. Thus, based on (139) and (140), $\boldsymbol{H}^{\{9\}}$ is equal to

$$\begin{aligned}
&\boldsymbol{H}^{\{1\}}\boldsymbol{M}_{9,1} + \left(\boldsymbol{H}^{\{2\}}\boldsymbol{M}_{8,2} + \boldsymbol{H}^{\{3\}}\boldsymbol{M}_{8,3} + \boldsymbol{H}^{\{4\}}\boldsymbol{M}_{8,4}\right)\boldsymbol{M}_{9,8} \\
&\quad = \boldsymbol{H}^{\{1\}}\boldsymbol{M}_{9,1} + \boldsymbol{H}^{\{2\}}\boldsymbol{M}'_{8,2} + \boldsymbol{H}^{\{3\}}\boldsymbol{M}'_{8,3} + \boldsymbol{H}^{\{4\}}\boldsymbol{M}'_{8,4}, \qquad (141)
\end{aligned}$$

where $M'_{8,i} = M_{8,i}M_{9,8}$, $i = 2, 3, 4$. On the other hand, since $\{1, 3, 4, 7\}$ is a circuit set, we get

$$H^{\{7\}} = H^{\{1\}}M_{7,1} + H^{\{3\}}M_{7,3} + H^{\{4\}}M_{7,4}, \tag{142}$$

where each $M_{7,1}, M_{7,3}, M_{7,4}$ is invertible. Now, for set $\{2, 7, 9\}$, we have

$$\begin{aligned}\text{rank}\left(H^{\{2,7,9\}}\right) &= \text{rank}\left(\left[H^{\{2\}}|H^{\{7\}}|H^{\{9\}}\right]\right)\\ &= \text{rank}\left(\left[H^{\{2\}}|H^{\{7\}}|H^{\{9\}} - H^{\{2\}}M'_{8,2}\right]\right)\\ &= t + \text{rank}\left(\left[H^{\{7\}}|H^{\{9\}} - H^{\{2\}}M'_{8,2}\right]\right). \end{aligned} \tag{143}$$

Now, since $\text{col}(H^{\{9\}})$ must be a subspace of $\text{col}(H^{\{2,7,9\}})$, we must have $\text{rank}(H^{\{2,7,9\}}) = 2t$. Thus, in (143), $H^{\{9\}} - H^{\{2\}}M'_{8,2}$ must be linearly dependent on $H^{\{7\}}$, which based on (141) and (142) requires each $M_{9,1}, M'_{8,3}, M'_{8,4}$ to be invertible. Besides, each $M'_{8,3}, M'_{8,4}$ is invertible only if $M_{9,8}$ is invertible. Thus, since both $M_{9,1}$ and $M_{9,8}$ are invertible, set $\{1, 8, 9\}$ forms a circuit set of H. Similarly, it can be shown that all sets $\{2, 7, 9\}$, $\{3, 6, 9\}$ and $\{4, 5, 9\}$ are circuit sets.

APPENDIX C
PROOF OF PROPOSITIONS 8 AND 10

A. PROOF OF PROPOSITIONS 8

We show that matrix $H_* \in \mathbb{F}_q^{4\times 29}$, presented in Figure 2, will satisfy all users u_i, *in* $\in [29]$ of the index coding instance $\mathcal{I}_1$ if the field $\mathbb{F}_q$ has characteristic three. Let $y = H_*x$ and $\mathbb{F}_q = GF(3)$. Now, we show that encoding matrix H_* satisfies the decoding condition in (2) for all $i \in [29]$. Figures 5 and 6 present $H_*^{\{i\}\cup B_i}$ for all $i \in [29]$.

- It can be seen that user u_i, $i \in [4]$ can decode its desired message x_i from the coded message y_i (or the i-th row of H_*).
- User u_5 first decodes $x_7 + x_8$ from y_4. Then, it can decode x_5 from y_3.
- User u_6 first decodes $x_5 + x_8$ from y_3. Then, it can decode x_6 from y_2.
- User u_7 first decodes $x_5 + x_6$ from y_2. Then, it can decode x_7 from y_1.
- User u_8 first decodes $x_6 + x_7$ from y_1. Then, it can decode x_8 from y_4.
- User u_9 adds y_1, y_2, y_3, y_4 to achieve x_9 as follows

$$\begin{aligned} y_1 + y_2 + y_3 + y_4 &= 3(x_5 + x_6 + x_7 + x_8) + 4x_9\\ &= x_9, \end{aligned} \tag{144}$$

  where (144) follows from the fact that $3 = 0$ and $4 = 1$ over the Galois field $GF(3)$.
- User u_{10} first decodes x_5 from y_3. Then, it can decode x_{10} from y_1.
- User u_{11} decodes x_5 from y_1. Then, it can decode x_{11} from y_2.
- User u_{12} decodes x_5 from y_2. Then, it can decode x_{12} from y_3.
- User u_{13} first decodes $x_8 + x_9$ from y_2 or y_3. Then, it can decode x_{13} from y_4.
- User u_{14} first decodes x_6 from y_4. Then, it can decode x_{14} from y_1.
- User u_{15} first decodes x_6 from y_1. Then, it can decode x_{15} from y_2.
- User u_{16} first decodes $x_5 + x_9$ from y_1 or y_2. Then, it can decode x_{16} from y_3.
- User u_{17} first decodes x_6 from y_2. Then, it can decode x_{17} from y_4.
- User u_{18} first decodes x_7 from y_4. Then, it can decode x_{18} from y_1.
- User u_{19} first decodes $x_6 + x_9$ from y_1 or y_4. Then, it can decode x_{19} from y_2.
- User u_{20} first decodes x_7 from y_1. Then, it can decode x_{20} from y_3.
- User u_{21} first decodes x_7 from y_3. Then, it can decode x_{21} from y_4.
- User u_{22} first decodes $x_7 + x_9$ from y_3 or y_4. Then, it can decode x_{22} from y_1.
- User u_{23} first decodes x_8 from y_4. Then, it can decode x_{23} from y_2.
- User u_{24} first decodes x_8 from y_2. Then, it can decode x_{24} from y_3.
- User u_{25} first decodes x_8 from y_3. Then, it can decode x_{25} from y_4.
- User u_{26} first decodes $x_5 + x_9$ from y_1. Then, it can decode x_{26} from y_2.
- User u_{27} first decodes $x_6 + x_9$ from y_4. Then, it can decode x_{27} from y_1.
- User u_{28} first decodes $x_7 + x_9$ from y_3. Then, it can decode x_{28} from y_4.
- User u_{29} first decodes $x_8 + x_9$ from y_2. Then, it can decode x_{29} from y_3.

B. PROOF OF PROPOSITIONS 10

We show that matrix $H_* \in \mathbb{F}_q^{4\times 29}$, shown in Figure 2, will satisfy all users $u_i, \in [29]$ of the index coding instance $\mathcal{I}_2$ if the field $\mathbb{F}_q$ does have any characteristic other than characteristic three. Let $y = H_*x$. Since all the users except $u_i, i \in [29]\backslash\{5, 6, 7, 8, 9\}$ have the same interfering message set as the users in the index coding instance $\mathcal{I}_1$, we can use the same argument in the previous subsection to show that these users will be satisfied by H_*, shown in Figure 2. We note that the characteristic of the field does not affect the results for users $u_i, i \in [29]\backslash\{5, 6, 7, 8, 9\}$. Thus, we just need to prove that users $u_i, i \in \{5, 6, 7, 8, 9\}$ will be satisfied.

Due to $B_9 = \emptyset$, user u_9 can easily decode its desired message x_9 from any of the coded messages $y_i, i \in [4]$.

For the users $u_i, i \in \{5, 6, 7, 8\}$, we have

$$H_*^{\{i\}\cup B_i} = H_*^{\{5,6,7,8\}} = \begin{bmatrix} 1 & 1 & 1 & 0\\ 1 & 1 & 0 & 1\\ 1 & 0 & 1 & 1\\ 0 & 1 & 1 & 1 \end{bmatrix}, \quad i \in \{5, 6, 7, 8\}$$

$$u_5: \ y_1 + y_2 + y_3 - y_4 - y_4 = 3x_5,$$

	1	2	3	4	8	11	12	13	15	16	17	19	20	21	23	24	25
1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	1	0	0	1	1	0	0	1	0	0	1	0	0	1	0	0
3	0	0	1	0	1	0	1	0	0	1	0	0	1	0	0	1	0
4	0	0	0	1	1	0	0	1	0	0	1	0	0	1	0	0	1

(a) $\boldsymbol{H}_*^{\{1\}\cup B_1}$

	1	2	3	4	7	10	12	13	14	16	17	18	20	21	22	24	25
1	1	0	0	0	1	1	0	0	1	0	0	1	0	0	1	0	0
2	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	1	0	1	0	1	0	0	1	0	0	1	0	0	1	0
4	0	0	0	1	1	0	0	1	0	0	1	0	0	1	0	0	1

(b) $\boldsymbol{H}_*^{\{2\}\cup B_2}$

	1	2	3	4	6	10	11	13	14	15	17	18	19	21	22	23	25
1	1	0	0	0	1	1	0	0	1	0	0	1	0	0	1	0	0
2	0	1	0	0	1	0	1	0	0	1	0	0	1	0	0	1	0
3	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	1	1	0	0	1	0	0	1	0	0	1	0	0	1

(c) $\boldsymbol{H}_*^{\{3\}\cup B_3}$

	1	2	3	4	5	10	11	12	14	15	16	18	19	20	22	23	24
1	1	0	0	0	1	1	0	0	1	0	0	1	0	0	1	0	0
2	0	1	0	0	1	0	1	0	0	1	0	0	1	0	0	1	0
3	0	0	1	0	1	0	0	1	0	0	1	0	0	1	0	0	1
4	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0

(d) $\boldsymbol{H}_*^{\{4\}\cup B_4}$

	5	7	8
1	1	1	0
2	1	0	1
3	1	1	1
4	0	1	1

(e) $\boldsymbol{H}_*^{\{5\}\cup B_5}$

	5	6	8
1	1	1	0
2	1	1	1
3	1	0	1
4	0	1	1

(f) $\boldsymbol{H}_*^{\{6\}\cup B_6}$

	5	6	7
1	1	1	1
2	1	1	0
3	1	0	1
4	0	1	1

(g) $\boldsymbol{H}_*^{\{7\}\cup B_8}$

	6	7	8
1	1	1	0
2	1	0	1
3	0	1	1
4	1	1	1

(h) $\boldsymbol{H}_*^{\{8\}\cup B_8}$

	5	6	7	8	9
1	1	1	1	0	1
2	1	1	0	1	1
3	1	0	1	1	1
4	0	1	1	1	1

(i) $\boldsymbol{H}_*^{\{9\}\cup B_9}$

	5	10	11
1	1	1	0
2	1	0	1
3	1	0	0
4	0	0	0

(j) $\boldsymbol{H}_*^{\{10\}\cup B_{10}}$

	5	11	12
1	1	0	0
2	1	1	0
3	1	0	1
4	0	0	0

(k) $\boldsymbol{H}_*^{\{11\}\cup B_{11}}$

	5	10	12
1	1	1	0
2	1	0	0
3	1	0	1
4	0	0	0

(l) $\boldsymbol{H}_*^{\{12\}\cup B_{12}}$

	1	8	9	13
1	1	0	1	0
2	0	1	1	0
3	0	1	1	0
4	0	1	1	1

(m) $\boldsymbol{H}_*^{\{13\}\cup B_{13}}$

	6	14	15
1	1	1	0
2	1	0	1
3	0	0	0
4	1	0	0

(n) $\boldsymbol{H}_*^{\{14\}\cup B_{14}}$

	6	15	17
1	1	0	0
2	1	1	0
3	0	0	0
4	1	0	1

(o) $\boldsymbol{H}_*^{\{15\}\cup B_{15}}$

	4	5	9	16
1	0	1	1	0
2	0	1	1	0
3	0	1	1	1
4	1	0	1	0

(p) $\boldsymbol{H}_*^{\{16\}\cup B_{16}}$

	6	14	17
1	1	1	0
2	1	0	0
3	0	0	0
4	1	0	1

(q) $\boldsymbol{H}_*^{\{17\}\cup B_{17}}$

FIGURE 5. $\boldsymbol{H}_*^{\{i\}\cup B_i}$, $i \in [17]$.

$$
\begin{aligned}
u_6 &: y_1 + y_2 + y_4 - y_3 - y_3 = 3x_6,\\
u_7 &: y_1 + y_3 + y_4 - y_2 - y_2 = 3x_7,\\
u_8 &: y_2 + y_3 + y_4 - y_1 - y_1 = 3x_8.
\end{aligned} \tag{145}
$$

Since number 3 is invertible in the fields with any characteristic other than characteristic three, all users $u_i, i \in \{5, 6, 7, 8\}$ can decode their requested message. This completes the proof.

	7	18	20
1	1	1	0
2	0	0	0
3	1	0	1
4	1	0	0

(a) $\boldsymbol{H}_*^{\{18\}\cup B_{18}}$

	3	6	9	19
1	0	1	1	0
2	0	1	1	1
3	1	0	1	0
4	0	1	1	0

(b) $\boldsymbol{H}_*^{\{19\}\cup B_{19}}$

	7	20	21
1	1	0	0
2	0	0	0
3	1	1	0
4	1	0	1

(c) $\boldsymbol{H}_*^{\{20\}\cup B_{20}}$

	7	18	21
1	1	1	0
2	0	0	0
3	1	0	0
4	1	0	1

(d) $\boldsymbol{H}_*^{\{21\}\cup B_{21}}$

	2	7	9	22
1	0	1	1	1
2	1	0	1	0
3	0	1	1	0
4	0	1	1	0

(e) $\boldsymbol{H}_*^{\{22\}\cup B_{22}}$

	8	23	24
1	0	0	0
2	1	1	0
3	1	0	1
4	1	0	0

(f) $\boldsymbol{H}_*^{\{23\}\cup B_{23}}$

	8	24	25
1	0	0	0
2	1	0	0
3	1	1	0
4	1	0	1

(g) $\boldsymbol{H}_*^{\{24\}\cup B_{24}}$

	8	23	25
1	0	0	0
2	1	1	0
3	1	0	0
4	1	0	1

(h) $\boldsymbol{H}_*^{\{25\}\cup B_{25}}$

	4	5	9	16	26
1	0	1	1	0	0
2	0	1	1	0	1
3	0	1	1	1	0
4	1	0	1	0	0

(i) $\boldsymbol{H}_*^{\{26\}\cup B_{26}}$

	3	6	9	19	27
1	0	1	1	0	1
2	0	1	1	1	0
3	1	0	1	0	0
4	0	1	1	0	0

(j) $\boldsymbol{H}_*^{\{27\}\cup B_{27}}$

	2	7	9	22	28
1	0	1	1	1	0
2	1	0	1	0	0
3	0	1	1	0	0
4	0	1	1	0	1

(k) $\boldsymbol{H}_*^{\{28\}\cup B_{28}}$

	1	8	9	13	29
1	1	0	1	0	0
2	0	1	1	0	0
3	0	1	1	0	1
4	0	1	1	1	0

(l) $\boldsymbol{H}_*^{\{29\}\cup B_{29}}$

FIGURE 6. $\boldsymbol{H}_*^{\{i\}\cup B_i}$, $i \in [29]\backslash[17]$.

APPENDIX D
PROOF OF LEMMAS 7-9
A. PROOF OF LEMMA 7

Corollaries 5-8 can be derived from earlier results and will be used in the proof of Lemma 7.

Corollary 5: Let M be an independent set of $\boldsymbol{H}$. Now, if $\mathrm{col}(\boldsymbol{H}^{\{2j-1,2j\}}) \subseteq \mathrm{col}(\boldsymbol{H}^{M})$, then there exists one subset $M' \subseteq M$, such that $\{2j-1, 2j\} \cup M'$ is a quasi-circuit set of $\boldsymbol{H}$.

Proof: Since $\mathrm{col}(\boldsymbol{H}^{\{2j-1,2j\}}) \subseteq \mathrm{col}(\boldsymbol{H}^{M})$, we must have $\boldsymbol{H}^{\{2j-1,2j\}} = \sum_{i\in L} \boldsymbol{H}^{\{i\}}\boldsymbol{N}_{j,i}$ such that only matrices $\boldsymbol{N}_{j,i}$, $i \in L' \subseteq L$ are invertible. Thus, according to Lemma 6, set $\{2j-1, 2j\} \cup M'$ forms a circuit set of $\boldsymbol{H}$ where $M' = \{2i-1, 2i, i \in L'\} \subseteq M$. ■

Corollary 6: If M is a quasi-minimal cyclic set of $\mathcal{I}$, then according to Definitions 28 and 11, its proper subsets $M' \subset M$ will be an acyclic set of $\mathcal{I}$.

Corollary 7 [25]: If M is an acyclic set of $\mathcal{I}$, then there exists at least one $2i-1 \in M$ such that $M\backslash\{2i-1, 2i\} \subseteq B_{2i-1}$.

Corollary 8: Suppose $\{2j-1, 2j\} \cup M$ is a quasi-circuit set of $\boldsymbol{H}$. Then for any $\{2l-1, 2l\} \subseteq M$, we have $\mathrm{col}(\boldsymbol{H}^{\{2j-1,2j\}\cup M\backslash\{2i-1,2i\}}) = \mathrm{col}(\boldsymbol{H}^{M})$.

Proof: Since $\{2j-1, 2j\} \cup M$ is a quasi-circuit set of $\boldsymbol{H}$, we have $\boldsymbol{H}^{\{2j-1,2j\}} = \sum_{i\in L} \boldsymbol{H}^{\{2i-1,2i\}}\boldsymbol{N}_{j,i}$ such that each $\boldsymbol{N}_{j,i}$ is invertible. Now, assume $\{2l-1, 2l\} \subseteq M$. Then, we have

$$\begin{aligned}
&\mathrm{col}\Big(\boldsymbol{H}^{\{2j-1,2j\}\cup M\backslash\{2l-1,2l\}}\Big)\\
&= \mathrm{col}\Big(\Big[\boldsymbol{H}^{\{2j-1,2j\}}|\boldsymbol{H}^{M\backslash\{2l-1,2l\}}\Big]\Big)\\
&= \mathrm{col}\Big(\Big[\sum_{i\in L} \boldsymbol{H}^{\{2i-1,2i\}}\boldsymbol{N}_{j,i}|\boldsymbol{H}^{M\backslash\{2l-1,2l\}}\Big]\Big)\\
&= \mathrm{col}\Big(\Big[\boldsymbol{H}^{\{2l-1,2l\}}\boldsymbol{N}_{j,l}|\boldsymbol{H}^{M\backslash\{2l-1,2l\}}\Big]\Big)\\
&= \mathrm{col}\Big(\boldsymbol{H}^{M}\Big), \qquad (146)
\end{aligned}$$

where (146) is due to the invertibility of $\boldsymbol{N}_{j,l}$. ■

1) PROOF OF LEMMA 7

Since M is an independent set of $\boldsymbol{H}$, and $\mathrm{col}(\boldsymbol{H}^{\{2j-1,2j\}}) \subseteq \mathrm{col}(\boldsymbol{H}^{M})$, then according to Corollary 5, there exists a subset $M' \subseteq M$ such that $\{2j-1, 2j\} \cup M'$ is a quasi-circuit set. Now, we show that $M' = M$, otherwise it leads to a contradiction. Assume $M' \subset M$. First, since M is a quasi-minimal cyclic set of $\mathcal{I}$, based on Corollary 6, $M' \subset M$ is an acyclic set of $\mathcal{I}$. Second, according to Corollary 3, there exists $\{2l-1, 2l\} \subseteq M'$ such that $M'\backslash\{2l-1, 2l\} \subseteq B_{2l-1}, B_{2l}$. Moreover, due to $\{2j-1, 2j\} \subseteq B_{2l-1}, B_{2l}$, we get $\{2j-1, 2j\} \cup (M'\backslash\{2l-1, 2l\}) \subseteq B_{2l-1}, B_{2l}$. Thus,

$$\begin{aligned}
&\{2l-1, 2l\} \subseteq M' \to \mathrm{col}\Big(\boldsymbol{H}^{\{2l-1,2l\}}\Big) \subseteq \mathrm{col}\Big(\boldsymbol{H}^{M'}\Big),\\
&\{2j-1, 2j\} \cup \big(M'\backslash\{2l-1, 2l\}\big) \subseteq B_{2l-1} \to \qquad (147)\\
&\mathrm{col}\Big(\boldsymbol{H}^{\{2j-1,2j\}\cup(M'\backslash\{2l-1,2l\})}\Big) \subseteq \mathrm{col}\Big(\boldsymbol{H}^{B_{2l-1}}\Big). \qquad (148)
\end{aligned}$$

Third, since $\{2j-1, 2j\} \cup M'$ is a quasi-circuit set, Corollary 8 leads to

$$\mathrm{col}\Big(\boldsymbol{H}^{\{2j-1,2j\}\cup M'\backslash\{2l-1,2l\}}\Big) = \mathrm{col}\Big(\boldsymbol{H}^{M'}\Big). \qquad (149)$$

Now, from (147), (148) and (138), we have

$$\mathrm{col}\left(\boldsymbol{H}^{\{2l-1,2l\}}\right) \subseteq \mathrm{col}\left(\boldsymbol{H}^{M'}\right) = \mathrm{col}\left(\boldsymbol{H}^{\{2j-1,2j\}\cup M'\backslash\{2l-1,2l\}}\right) \subseteq \mathrm{col}\left(\boldsymbol{H}^{B_{2l-1}}\right),$$

which contradicts the decoding condition in (2) for user u_{2l-1} as $\mathrm{col}(\boldsymbol{H}^{\{2l-1\}}) \subseteq \mathrm{col}(\boldsymbol{H}^{B_{2l-1}})$. Therefore, we must have $M' = M$.

B. PROOF OF LEMMA 8

Since $\mathrm{col}(\boldsymbol{H}^{\{17,18\}}) \subseteq \mathrm{col}(\boldsymbol{H}^{\{1,2,15,16\}})$, we have

$$\boldsymbol{H}^{\{17,18\}} = \boldsymbol{H}^{\{1,2\}}\boldsymbol{N}_{9,1} + \boldsymbol{H}^{\{15,16\}}\boldsymbol{N}_{9,8}. \tag{150}$$

Moreover, since set $\{3, 4, 5, 6, 7, 8, 15, 16\}$ is a quasi-circuit set, we must have

$$\boldsymbol{H}^{\{15,16\}} = \boldsymbol{H}^{\{3,4\}}\boldsymbol{N}_{8,2} + \boldsymbol{H}^{\{5,6\}}\boldsymbol{N}_{8,3} + \boldsymbol{H}^{\{7,8\}}\boldsymbol{N}_{8,4}, \tag{151}$$

where each $\boldsymbol{N}_{8,2}, \boldsymbol{N}_{8,3}, \boldsymbol{N}_{8,4}$ is invertible. Thus, based on (150) and (151), $\boldsymbol{H}^{\{17,18\}}$ is equal to

$$\begin{aligned}&\boldsymbol{H}^{\{1,2\}}\boldsymbol{N}_{9,1} + \left(\boldsymbol{H}^{\{3,4\}}\boldsymbol{N}_{8,2} + \boldsymbol{H}^{\{5,6\}}\boldsymbol{N}_{8,3} + \boldsymbol{H}^{\{7,8\}}\boldsymbol{N}_{8,4}\right)\boldsymbol{N}_{9,8}\\ &= \boldsymbol{H}^{\{1,2\}}\boldsymbol{N}_{9,1} + \boldsymbol{H}^{\{3,4\}}\boldsymbol{N}'_{8,2} + \boldsymbol{H}^{\{5,6\}}\boldsymbol{N}'_{8,3} + \boldsymbol{H}^{\{7,8\}}\boldsymbol{N}'_{8,4},\end{aligned} \tag{152}$$

where $\boldsymbol{N}'_{8,i} = \boldsymbol{N}_{8,i}\boldsymbol{N}_{9,8}, i = 2, 3, 4$. On the other hand, since $\{1, 2, 5, 6, 7, 8, 13, 14\}$ is a quasi-circuit set, we get

$$\boldsymbol{H}^{\{13,14\}} = \boldsymbol{H}^{\{1,2\}}\boldsymbol{N}_{7,1} + \boldsymbol{H}^{\{5,6\}}\boldsymbol{N}_{7,3} + \boldsymbol{H}^{\{7,8\}}\boldsymbol{N}_{7,4}, \tag{153}$$

where each $\boldsymbol{N}_{7,1}, \boldsymbol{N}_{7,3}, \boldsymbol{N}_{7,4}$ is invertible. Now, for set $\{3, 4, 13, 14, 17, 18\}$, we have

$$\begin{aligned}\mathrm{rank}\left(\boldsymbol{H}^{\{3,4,13,14,17,18\}}\right) &= \mathrm{rank}\left(\left[\boldsymbol{H}^{\{3,4\}}|\boldsymbol{H}^{\{13,14\}}|\boldsymbol{H}^{\{17,18\}}\right]\right)\\ &= \mathrm{rank}\left(\left[\boldsymbol{H}^{\{3,4\}}|\boldsymbol{H}^{\{13,14\}}|\boldsymbol{H}^{\{17,18\}} - \boldsymbol{H}^{\{3,4\}}\boldsymbol{N}'_{8,2}\right]\right)\\ &= 2t + \mathrm{rank}\left(\left[\boldsymbol{H}^{\{13,14\}}|\boldsymbol{H}^{\{17,18\}} - \boldsymbol{H}^{\{3,4\}}\boldsymbol{N}'_{8,2}\right]\right).\end{aligned} \tag{154}$$

Now, since $\mathrm{col}(\boldsymbol{H}^{\{17,18\}})$ must be a subspace of $\mathrm{col}(\boldsymbol{H}^{\{3,4,13,14,17,18\}})$, we must have $\mathrm{rank}(\boldsymbol{H}^{\{3,4,13,14,17,18\}}) = 4t$. Thus, in (154), $\boldsymbol{H}^{\{17,18\}} - \boldsymbol{H}^{\{3,4\}}\boldsymbol{N}'_{8,2}$ must be linearly dependent on $\boldsymbol{H}^{\{13,14\}}$, which based on (152) and (153) requires each $\boldsymbol{N}_{9,1}, \boldsymbol{N}'_{8,3}, \boldsymbol{N}'_{8,4}$ to be invertible. Besides, each $\boldsymbol{N}'_{8,3}, \boldsymbol{N}'_{8,4}$ is invertible only if $\boldsymbol{N}_{9,8}$ is invertible. Thus, since both $\boldsymbol{N}_{9,1}$ and $\boldsymbol{N}_{9,8}$ are invertible, set $\{1, 2, 15, 16, 17, 18\}$ forms a quasi-circuit set of $\boldsymbol{H}$. Similarly, it can be shown that all sets $\{3, 4, 13, 14, 15, 16\}$, $\{5, 6, 11, 12, 17, 18\}$ and $\{7, 8, 9, 10, 17, 18\}$ are quasi-circuit sets.

C. PROOF OF LEMMA 9

Assume $M' = \{i_1, \ldots, i_{|M'|}\}$. Then, applying the decoding condition in Remark 5 for $i_1, \ldots, i_{|M'|}$, will result in

$$\begin{aligned}\mathrm{rank}\left(\boldsymbol{H}^{M}\right) &= t + \mathrm{rank}\left(\boldsymbol{H}^{M\backslash\{i_1\}}\right),\\ &= \cdots,\\ &= |M'|t + \mathrm{rank}\left(\boldsymbol{H}^{M\backslash\left\{i_1,\ldots,i_{|M'|}\right\}}\right),\\ &= |M'|t + \mathrm{rank}\left(\boldsymbol{H}^{M\backslash M'}\right),\end{aligned}$$

which completes the proof.

APPENDIX E
PROOF OF PROPOSITION 14

We prove that $N_0 = [8]$ is a basis set of $\boldsymbol{H}$, each set $N_i, i \in [8]$ in (104) will be a quasi-circuit set of $\boldsymbol{H}$, and $\mathrm{rank}(\boldsymbol{H}^{[9:18]}) \geq 7$. The proof is described as follows.

- First, since $\beta_{\text{MAIS}}(\mathcal{I}_3) = 8$, we must have $\mathrm{rank}(\boldsymbol{H}) = 8t$. Now, from $B_i, i \in [8]$ in (117), it can be seen that set $[8]$ is an independent set of $\mathcal{I}_3$, so according to Lemma 1, set $[8]$ is an independent set of $\boldsymbol{H}$. Moreover, since $\mathrm{rank}(\boldsymbol{H}) = 8t$, set $N_0 = [8]$ will be a basis set of $\boldsymbol{H}$. Now, in order to have $\mathrm{rank}(\boldsymbol{H}) = 8t$, for all $j \in [29]\backslash[8]$, we must have $\mathrm{col}(\boldsymbol{H}^{\{2j-1,2j\}}) \subseteq \mathrm{col}(\boldsymbol{H}^{[8]})$.
- According to Lemma 3, from $B_i, i \in [8]$, it can be seen that:
  - for each $j \in \{19, 27, 35, 43\}$,
  $$j \in B_i, i \in [8]\backslash\{1\} \to \mathrm{col}\left(\boldsymbol{H}^{\{j\}}\right) = \mathrm{col}\left(\boldsymbol{H}^{\{1\}}\right), \tag{155}$$
  - for each $j \in \{20, 28, 36, 44\}$,
  $$j \in B_i, i \in [8]\backslash\{2\} \to \mathrm{col}\left(\boldsymbol{H}^{\{j\}}\right) = \mathrm{col}\left(\boldsymbol{H}^{\{2\}}\right), \tag{156}$$
  - for each $j \in \{21, 29, 37, 45\}$,
  $$j \in B_i, i \in [8]\backslash\{3\} \to \mathrm{col}\left(\boldsymbol{H}^{\{j\}}\right) = \mathrm{col}\left(\boldsymbol{H}^{\{3\}}\right), \tag{157}$$
  - for each $j \in \{22, 30, 38, 46\}$,
  $$j \in B_i, i \in [8]\backslash\{4\} \to \mathrm{col}\left(\boldsymbol{H}^{\{j\}}\right) = \mathrm{col}\left(\boldsymbol{H}^{\{4\}}\right). \tag{158}$$
  - for each $j \in \{23, 31, 39, 47\}$,
  $$j \in B_i, i \in [8]\backslash\{5\} \to \mathrm{col}\left(\boldsymbol{H}^{\{j\}}\right) = \mathrm{col}\left(\boldsymbol{H}^{\{5\}}\right), \tag{159}$$
  - for each $j \in \{24, 32, 40, 48\}$,
  $$j \in B_i, i \in [8]\backslash\{6\} \to \mathrm{col}\left(\boldsymbol{H}^{\{j\}}\right) = \mathrm{col}\left(\boldsymbol{H}^{\{6\}}\right), \tag{160}$$

– for each $j \in \{25, 33, 41, 49\}$,

$$j \in B_i, i \in [8]\backslash\{7\} \rightarrow \mathrm{col}\left(\boldsymbol{H}^{\{j\}}\right) = \mathrm{col}\left(\boldsymbol{H}^{\{7\}}\right), \tag{161}$$

– for each $j \in \{26, 34, 42, 50\}$,

$$j \in B_i, i \in [8]\backslash\{8\} \rightarrow \mathrm{col}\left(\boldsymbol{H}^{\{j\}}\right) = \mathrm{col}\left(\boldsymbol{H}^{\{8\}}\right). \tag{162}$$

Let

$$M_1 = \{19, 20, 21, 22, 23, 24\},$$
$$M_2 = \{27, 28, 29, 30, 33, 34\},$$
$$M_3 = \{35, 36, 39, 40, 41, 42\},$$
$$M_4 = \{45, 46, 47, 48, 49, 50\}.$$

From (155)-(158), it can be seen that

$$\mathrm{col}\left(\boldsymbol{H}^{M_1}\right) = \mathrm{col}\left(\boldsymbol{H}^{[8]\backslash\{7,8\}}\right), \tag{163}$$
$$\mathrm{col}\left(\boldsymbol{H}^{M_2}\right) = \mathrm{col}\left(\boldsymbol{H}^{[8]\backslash\{5,6\}}\right), \tag{164}$$
$$\mathrm{col}\left(\boldsymbol{H}^{M_3}\right) = \mathrm{col}\left(\boldsymbol{H}^{[8]\backslash\{3,4\}}\right), \tag{165}$$
$$\mathrm{col}\left(\boldsymbol{H}^{M_4}\right) = \mathrm{col}\left(\boldsymbol{H}^{[8]\backslash\{1,2\}}\right). \tag{166}$$

Thus, each set M_1, M_2, M_3 and M_4 is an independent set of $\boldsymbol{H}$.

- To have $\mathrm{rank}(\boldsymbol{H}) = 8t$, one must have $\mathrm{rank}(\boldsymbol{H}^{B_i}) = 7t, i \in [58]$. Now, since set $[8]$ is a basis set, then from $B_i, i \in [8]$ we must have

$$B_7, B_8 \rightarrow \mathrm{col}\left(\boldsymbol{H}^{\{9,10\}}\right) \subseteq \mathrm{col}\left(\boldsymbol{H}^{[8]\backslash\{7,8\}}\right) \overset{(163)}{=} \mathrm{col}\left(\boldsymbol{H}^{M_1}\right), \tag{167}$$
$$B_5, B_6 \rightarrow \mathrm{col}\left(\boldsymbol{H}^{\{11,12\}}\right) \subseteq \mathrm{col}\left(\boldsymbol{H}^{[8]\backslash\{5,6\}}\right) \overset{(164)}{=} \mathrm{col}\left(\boldsymbol{H}^{M_2}\right), \tag{168}$$
$$B_3, B_4 \rightarrow \mathrm{col}\left(\boldsymbol{H}^{\{13,14\}}\right) \subseteq \mathrm{col}\left(\boldsymbol{H}^{[8]\backslash\{3,4\}}\right) \overset{(165)}{=} \mathrm{col}\left(\boldsymbol{H}^{M_3}\right), \tag{169}$$
$$B_1, B_2 \rightarrow \mathrm{col}\left(\boldsymbol{H}^{\{15,16\}}\right) \subseteq \mathrm{col}\left(\boldsymbol{H}^{[8]\backslash\{1,2\}}\right) \overset{(166)}{=} \mathrm{col}\left(\boldsymbol{H}^{M_4}\right). \tag{170}$$

- From $B_i, i \in M_1, M_2, M_3$ and M_4, it can be verified that

$$M_1 \text{ is a quasi-minimal cyclic set } \& \ \{9, 10\} \in B_i, i \in M_1, \tag{171}$$
$$M_2 \text{ is a quasi-minimal cyclic set } \& \ \{11, 12\} \in B_i, i \in M_2, \tag{172}$$
$$M_3 \text{ is a quasi-minimal cyclic set } \& \ \{13, 14\} \in B_i, i \in M_3, \tag{173}$$
$$M_4 \text{ is a quasi-minimal cyclic set } \& \ \{15, 16\} \in B_i, i \in M_4. \tag{174}$$

- Now, all the four conditions in Lemma 7 are satisfied for set M_1 with $j = 5$, set M_2 with $j = 6$, set M_3 with $j = 7$, and set M_4 with $j = 8$. Thus, according to Lemma 4, each set $\{9, 10\} \cup M_1$, $\{11, 12\} \cup M_2$, $\{13, 14\} \cup M_3$ and $\{15, 16\} \cup M_4$ will be a quasi-circuit set of $\boldsymbol{H}$. Now, according to (163)-(166), each set

$$N_1 = \{1, 2, 3, 4, 5, 6, 9, 10\},$$
$$N_2 = \{1, 2, 3, 4, 7, 8, 11, 12\},$$
$$N_3 = \{1, 2, 5, 6, 7, 8, 13, 14\},$$
$$N_4 = \{3, 4, 5, 6, 7, 8, 15, 16\},$$

will also form a quasi-circuit set.

- Since

$$\{7, 8, 9, 10, 17, 18, 31, 32, 51, 52\} \backslash\{i\} \subseteq B_i, i \in \{51, 52\}, \tag{175}$$
$$\{5, 6, 11, 12, 17, 18, 37, 38, 53, 54\}\backslash\{i\} \subseteq B_i, i \in \{53, 54\}, \tag{176}$$
$$\{3, 4, 13, 14, 17, 18, 43, 44, 55, 56\}\backslash\{i\} \subseteq B_i, i \in \{55, 56\}, \tag{177}$$
$$\{1, 2, 15, 16, 17, 18, 25, 26, 57, 58\}\backslash\{i\} \subseteq B_i, i \in \{57, 58\}, \tag{178}$$

based on Lemma 9, we must have

$$(175) \rightarrow \mathrm{rank}\left(\boldsymbol{H}^{\{7,8,9,10,17,18,31,32\}}\right) \leq 6t, \tag{179}$$
$$(176) \rightarrow \mathrm{rank}\left(\boldsymbol{H}^{\{5,6,11,12,17,18,37,38\}}\right) \leq 6t, \tag{180}$$
$$(177) \rightarrow \mathrm{rank}\left(\boldsymbol{H}^{\{3,4,13,14,17,18,43,44\}}\right) \leq 6t, \tag{181}$$
$$(178) \rightarrow \mathrm{rank}\left(\boldsymbol{H}^{\{1,2,15,16,17,18,25,26\}}\right) \leq 6t. \tag{182}$$

Now, since

$$\{7, 8, 9, 10, 17, 18, 31, 32\} \backslash\{i\} \subseteq B_i, i \in \{31, 32\}, \tag{183}$$
$$\{5, 6, 11, 12, 17, 18, 37, 38\}\backslash\{i\} \subseteq B_i, i \in \{37, 38\}, \tag{184}$$
$$\{3, 4, 13, 14, 17, 18, 43, 44\}\backslash\{i\} \subseteq B_i, i \in \{43, 44\}, \tag{185}$$
$$\{1, 2, 15, 16, 17, 18, 25, 26\}\backslash\{i\} \subseteq B_i, i \in \{25, 26\}, \tag{186}$$

based on Lemma 9, we must have

$$(179), (183) \rightarrow \mathrm{rank}\left(\boldsymbol{H}^{\{7,8,9,10,17,18\}}\right) \leq 4t, \tag{187}$$
$$(180), (184) \rightarrow \mathrm{rank}\left(\boldsymbol{H}^{\{5,6,11,12,17,18\}}\right) \leq 4t, \tag{188}$$
$$(181), (185) \rightarrow \mathrm{rank}\left(\boldsymbol{H}^{\{3,4,13,14,17,18\}}\right) \leq 4t, \tag{189}$$
$$(182), (186) \rightarrow \mathrm{rank}\left(\boldsymbol{H}^{\{1,2,15,16,17,18\}}\right) \leq 4t. \tag{190}$$

Thus,

$$(187) \rightarrow \mathrm{col}\left(\boldsymbol{H}^{\{17,18\}}\right) \subseteq \mathrm{col}\left(\boldsymbol{H}^{\{7,8,9,10\}}\right).$$
$$(188) \rightarrow \mathrm{col}\left(\boldsymbol{H}^{\{17,18\}}\right) \subseteq \mathrm{col}\left(\boldsymbol{H}^{\{5,6,11,12\}}\right),$$
$$(189) \rightarrow \mathrm{col}\left(\boldsymbol{H}^{\{17,18\}}\right) \subseteq \mathrm{col}\left(\boldsymbol{H}^{\{3,4,13,14\}}\right),$$
$$(190) \rightarrow \mathrm{col}\left(\boldsymbol{H}^{\{17,18\}}\right) \subseteq \mathrm{col}\left(\boldsymbol{H}^{\{1,2,15,16\}}\right),$$

Hence, based on Lemma 8, each set

$$N_5 = \{1, 2, 15, 16, 17, 18\},$$
$$N_6 = \{3, 4, 13, 14, 17, 18\},$$
$$N_7 = \{5, 6, 11, 12, 17, 18\},$$
$$N_8 = \{7, 8, 9, 10, 17, 18\},$$

is a quasi-circuit set.

- Finally, from $B_i, i \in [9 : 16]$, it can be seen that

$$[9 : 16]\backslash\{i\} \subseteq B_i, i \in \{9, 11, 13, 15\}. \tag{191}$$

Thus, according to Lemma 9, we get

$$\mathrm{rank}\left(\boldsymbol{H}^{\{10,12,14,16\}}\right) = \mathrm{rank}\left(\boldsymbol{H}^{[9:16]}\right) - 4t, \tag{192}$$

On the other hand, it can be observed that set $\{10, 12, 14, 16\}$ is a minimal cyclic set of $\mathcal{I}_3$. Thus, according to Proposition 2, we have

$$\text{rank}\left(\boldsymbol{H}^{\{10,12,14,16\}}\right) \geq 3t, \tag{193}$$

Now, (192) and (193) will result in

$$\text{rank}\left(\boldsymbol{H}^{N_9=[9:16]}\right) \geq 7t, \tag{194}$$

which completes the proof.

APPENDIX F
PROOF OF LEMMAS 10 AND 11

A. PROOF OF LEMMA 10

Let

$$\begin{aligned} a_1 &= g(x_i, x_j, x_l, x_w) + g(x_i, x_j, x_v, x_w) \\ &\quad + g(x_i, x_l, x_v, x_w) + g(x_j, x_l, x_v, x_w), \\ a_2 &= (x_i + x_j + x_l)(x_i + x_j + x_v)(x_i + x_l + x_v), \\ a_3 &= 2(x_i + x_j + x_l)(x_i + x_j + x_l)(2x_i + x_j + x_l + 2x_v) \\ &\quad + 2(x_i + x_j + x_v)(x_i + x_j + x_v)(2x_i + x_j + x_v + 2x_l) \\ &\quad + 2(x_i + x_l + x_v)(x_i + x_l + x_v)(2x_i + x_l + x_v + 2x_j), \\ a_4 &= 2(x_i + x_j + x_l)(x_i + x_j + x_l) \\ &\quad + 2(x_i + x_j + x_v)(x_i + x_j + x_v) \\ &\quad + 2(x_i + x_l + x_v)(x_i + x_l + x_v) \\ &\quad + 2(x_j + x_l + x_v)(x_j + x_l + x_v). \end{aligned} \tag{195}$$

It can be verified that

$$\begin{aligned} a_1 = &\ x_ix_i(x_j + x_l + x_v) + x_jx_j(x_i + x_l + x_v) \\ &+ x_lx_l(x_i + x_j + x_v) + x_vx_v(x_i + x_j + x_l) \\ &+ (x_ix_j + x_ix_l + x_ix_v + x_jx_l + x_jx_v + x_lx_v)(1 + 2x_w) \\ &+ x_ix_jx_l + x_ix_jx_v + x_ix_lx_v + x_jx_lx_v, \end{aligned} \tag{196}$$

$$\begin{aligned} a_2 = &\ x_ix_ix_i + 2x_ix_i(x_j + x_l + x_v)x_jx_j(x_i + x_l + x_v) + \\ &+ x_lx_l(x_i + x_j + x_v) + x_vx_v(x_i + x_j + x_l)2x_jx_lx_v, \end{aligned} \tag{197}$$

$$\begin{aligned} a_3 = &\ x_jx_jx_j + x_lx_lx_l + x_vx_vx_v + x_jx_j(x_i + x_l + x_v) \\ &+ x_lx_l(x_i + x_j + x_v) + x_vx_v(x_i + x_j + x_l) \\ &+ 2(x_ix_jx_l + x_ix_jx_v + x_ix_lx_v), \end{aligned} \tag{198}$$

$$a_4 = 2(x_ix_j + x_ix_l + x_ix_v + x_jx_l + x_jx_v + x_lx_v). \tag{199}$$

Now, it can be seen that

$$\begin{aligned} &a_1 + a_2 + a_3 + a_4(1 + 2x_w) \\ &\quad = x_ix_ix_i + x_jx_jx_j + x_lx_lx_l + x_vx_vx_v \\ &\quad = x_i + x_j + x_l + x_v, \end{aligned} \tag{200}$$

where (200) follows from the fact that for any $x_i \in GF(3)$, we have $x_ix_ix_i = x_i$. Thus, by having $x_i+x_j+x_l$, $x_i+x_j+x_v$, $x_i+x_l+x_v$, and $x_j+x_l+x_v$, each x_i, x_j, x_l and x_v is decodable from (200). This completes the proof.

B. PROOF OF LEMMA 11

It can be verified that function $g(x_i, x_j, x_v, x_w)$ can be rewritten as follows

$$\begin{aligned} g(x_i, x_j, x_v, x_w) = &\ 2x_ix_i(x_j + x_v + x_w) \\ &+ 2x_jx_j(x_i + x_v + x_w) \\ &+ 2(x_vx_v + x_wx_w)(x_i + x_j) \\ &+ 2(x_vx_vx_w + x_wx_wx_v) \\ &+ 2x_ix_j + 2(x_i + x_j)(x_v + x_w) + 2x_vx_w \\ &+ x_ix_j(x_v + x_w) + x_vx_w(x_i + x_j). \end{aligned} \tag{201}$$

It can be seen that

$$\begin{aligned} &2(x_vx_v + x_wx_w)(x_i + x_j) + x_vx_w(x_i + x_j) \\ &\quad = 2(x_vx_v + x_wx_w + 2x_vx_w)(x_i + x_j) \\ &\quad = 2(x_v + x_w)(x_v + x_w)(x_i + x_j). \end{aligned} \tag{202}$$

Since terms x_i, x_j and $x_v + x_w$ are known, from (201) and (202), it can be observed that only term $2(x_vx_vx_w + x_wx_wx_v + x_vx_w)$ is unknown.

Similarly, in $g(x_i, x_l, x_v, x_w)$, since the terms x_i, x_l and $x_v + x_w$ are known, only term $2(x_vx_vx_w + x_wx_wx_v + x_vx_w)$ is unknown.

Thus, in $g(x_i, x_j, x_v, x_w) + 2g(x_i, x_l, x_v, x_w)$, the unknown terms $2(x_vx_vx_w + x_wx_wx_v + x_vx_w)$ is canceled out. Hence, using the value of x_i, x_j, x_l and $x_v + x_w$, the value of $g(x_i, x_j, x_v, x_w) + 2g(x_i, x_l, x_v, x_w)$ will be found.

REFERENCES

[1] Y. Birk and T. Kol, "Informed-source coding-on-demand (ISCOD) over broadcast channels," in *Proc. IEEE Int. Conf. Comput. Commun. (INFOCOM)*, 1998, pp. 1257–1264.

[2] S. E. Rouayheb, A. Sprintson, and C. Georghiades, "On the index coding problem and its relation to network coding and Matroid theory," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3187–3195, Jul. 2010.

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

[4] S. Li, M. A. Maddah-ali, Q. Yu, and S. Avestimehr, "A fundamental tradeoff between computation and communication in distributed computing," *IEEE Trans. Inf. Theory*, vol. 64, no. 1, pp. 109–128, Jan. 2018.

[5] M. A. Maddah-ali and U. Niesen, "Fundamental limits of caching," *IEEE Trans. Inf. Theory*, vol. 60, no. 5, pp. 2856–2867, May 2014.

[6] K. Wan, D. Tuninetti, and P. Piantanida, "An index coding approach to caching with uncoded cache placement," *IEEE Trans. Inf. Theory*, vol. 66, no. 3, pp. 1318–1332, Mar. 2020.

[7] S. A. Jafar, "Topological interference management through index coding," *IEEE Trans. Inf. Theory*, vol. 60, no. 1, pp. 529–568, Jan. 2014.

[8] H. Maleki, V. R. Cadambe, and S. A. Jafar, "Index coding—An interference alignment perspective," *IEEE Trans. Inf. Theory*, vol. 60, no. 9, pp. 5402–5432, Sep. 2014.

[9] N. S. Karat, S. Samuel, and B. S. Rajan, "Optimal error correcting index codes for some generalized index coding problems," *IEEE Trans. Commun.*, vol. 67, no. 2, pp. 929–942, Feb. 2019.

[10] A. S. Tehrani, A. G. Dimakis, and M. J. Neely, "Bipartite index coding," in *Proc. IEEE Int. Symp. Inf. Theory*, 2012, pp. 2246–2250.

[11] K. Shanmugam, A. G. Dimakis, and M. Langberg, "Graph theory versus minimum rank for index coding," in *Proc. IEEE Int. Symp. Inf. Theory*, 2014, pp. 291–295.

[12] A. Sharififar, N. Aboutorab, Y. Liu, and P. Sadeghi, "Independent user partition multicast scheme for the groupcast index coding problem," in *Proc. Int. Symp. Inf. Theory Appl. (ISITA)*, 2020, pp. 314–318.

[13] A. Sharififar, N. Aboutorab, and P. Sadeghi, "Update-based maximum column distance coding scheme for index coding problem," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, 2021, pp. 575–580.

[14] F. Arbabjolfaei, B. Bandemer, Y. Kim, E. Şaşoğlu, and L. Wang, "On the capacity region for index coding," in *Proc. IEEE Int. Symp. Inf. Theory*, 2013, pp. 962–966.

[15] Y. Liu, P. Sadeghi, and Y.-H. Kim, "Three-layer composite coding for index coding," in *Proc. IEEE Inf. Theory Workshop (ITW)*, 2018, pp. 1–5.

[16] C. Thapa, L. Ong, and S. J. Johnson, "Interlinked cycles for index coding: Generalizing cycles and cliques," *IEEE Trans. Inf. Theory*, vol. 63, no. 6, pp. 3692–3711, Jun. 2017.

[17] A. Thomas and B. S. Rajan, "Binary informed source codes and index codes using certain near-MDS codes," *IEEE Trans. Commun.*, vol. 66, no. 5, pp. 2181–2190, May 2018.

[18] B. Asadi, L. Ong, and S. J. Johnson, "On index coding in noisy broadcast channels with receiver message side information," *IEEE Commun. Lett.*, vol. 18, no. 4, pp. 640–643, Apr. 2014.

[19] 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.

[20] 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.

[21] A. Sharififar, P. Sadeghi, and N. Aboutorab, "Broadcast rate requires nonlinear coding in a Unicast index coding instance of size 36," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, 2021, pp. 208–213.

[22] A. Blasiak, R. Kleinberg, and E. Lubetzky, "Lexicographic products and the power of non-linear network coding," in *Proc. IEEE Annu. Symp. Found. Comput. Sci.*, 2011, pp. 609–618.

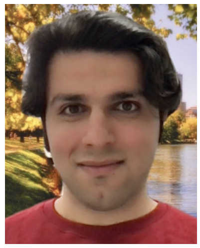
[23] E. Lubetzky and U. Stav, "Nonlinear index coding outperforming the linear optimum," *IEEE Trans. Inf. Theory*, vol. 55, no. 8, pp. 3544–3551, Aug. 2009.

[24] A. Sharififar, N. Aboutorab, and P. Sadeghi, "An update-based maximum column distance coding scheme for index coding," *IEEE J. Sel. Areas Inf. Theory*, vol. 2, no. 4, pp. 1282–1299, Dec. 2021.

[25] F. Arbabjolfaei and Y.-H. Kim, "Fundamentals of index coding," *Found. Trends® Commun. Inf. Theory*, vol. 14, nos. 3–4, pp. 163–346, 2018. [Online]. Available: http://dx.doi.org/10.1561/0100000094

[26] Z. Bar-Yossef, Y. Birk, T. S. Jayram, and T. Kol, "Index coding with side information," *IEEE Trans. Inf. Theory*, vol. 57, no. 3, pp. 1479–1494, Mar. 2011.

[27] A. Thomas and B. S. Rajan, "A discrete Polymatroidal framework for differential error-correcting index codes," *IEEE Trans. Commun.*, vol. 67, no. 7, pp. 4593–4604, Jul. 2019.



ARMAN SHARIFIFAR (Graduate Student Member, IEEE) received the B.Sc. degree in electrical engineering from Bahonar University, Iran, and the M.Sc. degree in the field of coding and communication systems from Shiraz University, Iran. He is currently pursuing the Ph.D. degree with the School of Engineering and Information Technology, The University of New South Wales, Canberra, Australia. His research interests include index and network coding, private and secured index coding, coded caching, and space-time coding in the MIMO systems.

PARASTOO SADEGHI (Senior Member, IEEE) received the bachelor's and master's degrees in electrical engineering from the Sharif University of Technology, Tehran, Iran, in 1995 and 1997, respectively, and the Ph.D. degree in electrical engineering from the University of New South Wales (UNSW) Sydney, in 2006. She is currently a Professor with the School of Engineering and Information Technology, UNSW Canberra. She has coauthored the book Hilbert Space Methods in Signal Processing (Cambridge University Press, 2013) and more than 200 refereed journal articles and conference papers. Her research interests include information theory, data privacy, index coding, and network coding. She was awarded a Future Fellowship from the Australian Research Council in 2019. From 2016 to 2019, she served as an Associate Editor for the IEEE TRANSACTIONS ON INFORMATION THEORY. She is currently serving as the Secretary for the Board of Governors of the IEEE Information Theory Society.

NEDA ABOUTORAB (Senior Member, IEEE) received the Ph.D. degree in electrical engineering from the University of Sydney, Sydney, Australia, in 2012. She is currently an Associate Professor with the School of Engineering and Information Technology, The University of New South Wales, Canberra, Australia. From 2012 to 2015, she was a Postdoctoral Research Fellow with the Research School of Engineering, The Australian National University. Her research interests include index coding, network coding, wireless communications, data caching and storage systems, Internet of Things, and signal processing.