On linear index coding from graph homomorphism perspective

Javad B. Ebrahimi*, Mahdi Jafari Siavoshani†
*Institute of Network Coding, Chinese University of Hong Kong, Hong Kong
†Computer Engineering Department, Sharif University of Technology, Tehran, Iran
Email: javad@inc.cuhk.edu.hk, mjafari@sharif.edu

***Abstract*—In this work, we study the problem of linear index coding from graph homomorphism point of view. We show that the decision version of linear (scalar or vector) index coding problem is equivalent to certain graph homomorphism problem. Using this equivalence expression, we conclude the following results. First we introduce new lower bounds on linear index of graphs. Next, we show that if the linear index of a graph over a finite filed is bounded by a constant, then by changing the ground field, the linear index of the graph may change by at most a constant factor that is independent from the size of the graph. Finally, we show that the decision version of linear index coding problem is NP-Complete unless we want to decide if this quantity is equal to 1 in which case the problem is solvable in polynomial time.**

I. Introduction

The problem of *index coding*, introduced by Birk and Kol in the context of satellite communication [1], has received significant attention during past years (see for example [2]–[12]). This problem has many applications such as satellite communication, multimedia distribution over wireless networks, and distributed caching. Despite its simple description, the index coding problem has a rich structure and it has intriguing connections to some of the information theory problems. It has been recently shown that the feasibility of any network coding problem can be reduce to an equivalent feasibility problem in the index coding problem (and vice versa) [13]. Also an interesting connection between index coding problem and interference alignment technique has been appeared in [10].

In this work, we focus on the index coding problems that can be represented by a side information graph (defined in Section II), i.e., user demands are distinct and there is exactly one receiver for each message. For studying this variation of the index coding problem, we consider the framework that uses ideas from graph homomorphism. More precisely, we show that the minimum broadcast rate of an index coding problem (linear or non-linear) can be upper bounded by the minimum broadcast rate of another index coding problem if there exists a homomorphism from the (directed) complement of the side information graph of the first problem to that of the second problem. Consequently, we show that the chromatic and fractional chromatic number upper bounds are special cases of our results (e.g., see [5], [6]).

For the case of scalar or vector linear index code we also prove the opposite direction, namely, we show that for every pair of positive integers k, l where $k = l = 1$ or $k \geq 2l$ and every prime power q, there exits a digraph $H^q_{k,l}$ such that the q-arry l-length vector linear index (or l-vector index for short) of $H^q_{k,l}$ is at most $\frac{k}{l}$ and the complement of any digraph whose q-arry l-vector index is also at most $\frac{k}{l}$ is homomorph to $\overline{H^q_{k,l}}$. The set of the graphs $H^q_{k,l}$ are analogous to the "graph family G_k" defined in [14] for studying a parameter of the graph called *minrank*. The main difference between the graphs G_k of [14] and the graphs $H^q_{k,l}$ of this work is that the former family of graphs can be used to describe the scalar index of graphs where as the latter family works for the case of vector index as well. Also, while $H^q_{k,l}$ is defined for arbitrary finite field and for directed graphs, G_k is defined only for binary field and undirected graphs.

Using the reduction of the scalar index coding problem to the homomorphism problem and the notion of increasing functions on the set of digraphs, we provide a family of lower bounds on the linear index of digraphs. As a particular example of such lower bounds, we extend the the previously known bound $\log_2(\chi(\overline{G})) \leq \mathrm{lind}_2(G)$ [15] to a similar bound but for arbitrary field size q. As another example, we derive a lower bound for $\overrightarrow{\mathrm{lind}}_q(G)$ (the vector linear index of digraph G) based on the size of G and its maximum clique size $\omega(G)$.

Using the graph homomorphism framework, we study the behaviour of linear index of a digraph when this parameter is evaluated over two different ground fields. In fact, we will show that if the linear index of a graph over a finite filed is bounded by a constant k, then by changing the ground field, the linear index of the graph may change to a quantity that is independent from the size of the graph.

Our next result is about the computational complexity of scalar linear index of a digraph. It is known that deciding whether the scalar linear index of a undirected graph is equal to k or not is NP-complete for $k \geq 3$ and is polynomially decidable for $k = 1, 2$ [16]. For digraphs, it is shown in [17] that for the binary alphabet, the decision problem for $k = 2$

The work described in this paper was partially supported by a grant from University Grants Committee of the Hong Kong Special Administrative Region, China (Project No. AoE/E-02/08). The work of M. Jafari Siavoshani was also partially supported by Institute for Research in Fundamental Sciences (IPM), Tehran, Iran.

is NP-complete. We use graph homomorphism framework to extend this result to arbitrary alphabet.

The remainder of this paper is organised as follows. In Section II we introduce notation, some preliminary concepts about graph homomorphism and give the problem statement. The main results of this paper and their proofs are presented in Section III and Section IV. In Section V, some applications of our main results are stated.

II. Notation and Problem Statement

A. Notation and Preliminaries

For convenience, we use $[m:n]$ to denote for the set of natural numbers $\{m,\ldots,n\}$. Let $x_1,\ldots,x_n$ be a set of variables. Then for any subset $\mathcal{A}\subseteq[1:n]$ we define $x_{\mathcal{A}}\triangleq(x_i:i\in\mathcal{A})$.

All of the vectors are column vectors unless otherwise stated. If $\underline{\mathbf{A}}$ is a matrix, we use $[\underline{\mathbf{A}}]_j$ to denote its jth column. We use $\mathbf{e}_i\in\mathbb{F}_q^k$ to denote for a vector which has one at ith position and zero elsewhere.

A directed graph (digraph) G is represented by $G(V,E)$ where V is the set of vertices and $E\subseteq(V\times V)$ is the set of edges. For $v\in V(G)$ we denote by $N_G^+(v)$ as the set of outgoing neighbours of v, i.e., $N_G^+(v)=\{u\in V:(v,u)\in E(G)\}$. For a digraph G we use $\overline{G}$ to denote for its *directional complement*, i.e., $(u,v)\in E(G)$ iff $(u,v)\notin E(\overline{G})$.

A vertex coloring (coloring for short) of a graph (digraph) G is an assignment of colors to the vertices of G such that there is no edge between the vertices of the same color. A coloring that uses k colors is called a k-coloring. The minimum k such that a k-coloring exists for G is called the *chromatic number*.

The *clique number* of a graph (digraph) is defined as the maximum size of a subset of the vertices such that each element of the subset is connected to every other vertex in the subset by an edge (directed edge). Notice that for the directed case, between any two vertices of the subset there must be two edges in opposite directions.

The *independence number* of a graph G, is the size of the largest independent set[1] and is denoted by $\alpha(G)$. For both directed and undirected graphs, it holds that $\alpha(G)=\omega(\overline{G})$.

Definition 1 (Homomorphism, see [18])**.** *Let G and H be any two digraphs. A* homomorphism *from G to H, written as $\phi:G\mapsto H$ is a mapping $\phi:V(G)\mapsto V(H)$ such that $(\phi(u),\phi(v))\in E(H)$ whenever $(u,v)\in E(G)$. If there exists a homomorphism of G to H we write $G\rightarrow H$, and if there is no such homomorphism we shall write $G\nrightarrow H$. In the former case we say that G is homomorphic to H. We write $\mathrm{Hom}(G,H)$ to denote for the set of all homomorphism from G to H.*

Definition 2. *On the set of all loop-less digraphs $\mathcal{G}$, we define the partial pre order "$\preccurlyeq$" as follows. For every pair of $G,H\in\mathcal{G}$, $G\preccurlyeq H$ if and only if there exists a homomorphism $\phi:\overline{G}\mapsto\overline{H}$. It is straightforward to see that "$\preccurlyeq$" is reflexive and transitive. Moreover, if $G\preccurlyeq H$ and $H\preccurlyeq G$, then the digraphs $\overline{G}$ and $\overline{H}$ are homomorphically equivalent (i.e., $\overline{G}\rightarrow\overline{H}$ and $\overline{H}\rightarrow\overline{G}$). In this case we write $G\sim H$.*

Notice that homomorphically equivalence does not imply isomorphism between graphs (digraphs). For example, all the bipartite graphs are homomorphically equivalent to K_2 and therefore are homomorphically equivalent to each other but they are not necessarily isomorphic.

Definition 3. *Let $\mathcal{D}\subseteq\mathcal{G}$ be an arbitrary set of digraphs. A mapping $h:\mathcal{D}\mapsto\mathbb{R}$ is called* increasing *over $\mathcal{D}$ if for every $G,H\in\mathcal{D}$ such that $G\preccurlyeq H$ then $h(G)\leq h(H)$.*

B. Problem Statement

Consider the communication problem where a transmitter aims to communicate a set of m messages $x_1,\ldots,x_m\in\mathcal{X}$ to m receivers by broadcasting k symbols $y_1,\ldots,y_k\in\mathcal{Y}$, over a public noiseless channel. We assume that for each $j\in[1:m]$, the jth receiver has access to the side information $x_{\mathcal{A}_j}$, i.e., a subset $\mathcal{A}_j\subseteq[1:m]\setminus\{j\}$ of messages. Each receiver j intends to recover x_j from $(y_1,\ldots,y_k,x_{\mathcal{A}_j})$.

This problem, which is the classical setting of the *index coding* problem, can be represented by a *directed side information graph* $G(V,E)$ where V represents the set of receivers/messages and there is an edge from node v_i to v_j, i.e., $(v_i,v_j)\in E$, if the ith receiver has x_j as side information. An index coding problem, as defined above, is completely characterized by the side information sets $\mathcal{A}_j$.

In the following definitions, we formally define validity of an index codes and some other basic concepts in index coding (see also [2], [5], and [11]).

Definition 4 (Valid Index Code)**.** *A* valid index code *for G over an alphabet $\mathcal{X}$ is a set $(\Phi,\{\Psi_i\}_{i=1}^m)$ consisting of:*
(i) an encoding function $\Phi:\mathcal{X}^m\mapsto\mathcal{Y}^k$ which maps m source messages to a transmitted sequence of length k of symbols from $\mathcal{Y}$;
(ii) a set of m decoding functions Ψ_i such that for each $i\in[1:m]$ we have $\Psi_i(\Phi(x_1,\ldots,x_m),x_{\mathcal{A}_i})=x_i$.

Definition 5. *Let G be a digraph, and $\mathcal{X}$ and $\mathcal{Y}$ are the source and the message alphabet, respectively.*
*(i) The "*broadcast rate*" of an index code $(\Phi,\{\Psi_i\})$ is defined as*

$$\mathrm{ind}_{\mathcal{X}}(G,\Phi,\{\Psi_i\})\triangleq\frac{k\log|\mathcal{Y}|}{\log|\mathcal{X}|}.$$

*(ii) The "*index*" of G over $\mathcal{X}$, denoted by $\mathrm{ind}_{\mathcal{X}}(G)$ is defined as*

$$\mathrm{ind}_{\mathcal{X}}(G)=\inf_{\Phi,\{\Psi_i\}}\mathrm{ind}_{\mathcal{X}}(G,\Phi,\{\Psi_i\}).$$

*(iii) If $\mathcal{X}=\mathcal{Y}=\mathbb{F}_q$ (the q-element finite field for some prime power q), the "*scalar linear index*" of G, denoted by $\mathrm{lind}_q(G)$ is defined as*

$$\mathrm{lind}_q(G)\triangleq\inf_{\Phi,\{\Psi_i\}}\mathrm{ind}_{\mathbb{F}_q}(G,\Phi,\{\Psi_i\})$$

in which the infimum is taken over the coding functions of the form $\Phi=(\Phi_1,\ldots,\Phi_k)$ and each Φ_i is a linear combination

[1]An *independent set* of a graph G is a subset of the vertices such that no two vertices in the subset represent an edge of G.

$$
\begin{tikzcd}
\overline{G} \arrow[r, "\phi"] \arrow[d, dash] & \overline{H} \arrow[d, dash] \\
G & H \arrow[l, "\phi^{-1}"']
\end{tikzcd}
$$

Fig. 1. Homomorphism ϕ maps the vertices of G to the vertices of H. The pre-image ϕ^{-1} of the homomorphism can be considered as a mapping from $V(H)$ to $V(G)$, i.e., for every $w \in V(H)$, $\phi^{-1}(w)$ is the set of all the vertices v in $V(G)$ such that $\phi(v) = w$.

of x_j's with coefficients from $\mathbb{F}_q$.
(iv) If $\mathcal{X} = \mathbb{F}_q^l$ and $\mathcal{Y} = \mathbb{F}_q$, the vector linear index *for G, denoted by $\overrightarrow{\mathrm{lind}}_{q,l}(G)$ is defined as*

$$\overrightarrow{\mathrm{lind}}_{q,l}(G) \triangleq \inf_{\Phi,\{\Psi_i\}} \mathrm{ind}_{\mathbb{F}_q^l}(G, \Phi, \{\Psi_i\})$$

where the infimum is taken over all coding functions $\Phi = (\Phi_1, \ldots, \Phi_k)$ such that $\Phi_i : \mathbb{F}_q^{lm} \mapsto \mathbb{F}_q$ are $\mathbb{F}_q$-linear functions.
*(v) The "*minimum broadcast rate*" of the index coding problem of G is defined as*

$$\mathrm{ind}(G) \triangleq \inf_{\mathcal{X}} \inf_{\Phi,\{\Psi_i\}} \mathrm{ind}_{\mathcal{X}}(G, \Phi, \{\Psi_i\}).$$

III. Index Coding via Graph Homomorphism

In this section, we will explain a method for designing index codes from another instance of index coding problem when there exists a homomorphism from the complement of the side information graph of the first problem to that of the second one. As an application to this result, we will show in Section V that some of the previously known results about index code design are special types of our general method.

Theorem 1. *Consider two instances of the index coding problems over digraphs G and H with the source alphabet $\mathcal{X}$. If $G \preccurlyeq H$ then*

$$\mathrm{ind}_{\mathcal{X}}(G) \leq \mathrm{ind}_{\mathcal{X}}(H).$$

In other words, the function $\mathrm{ind}_{\mathcal{X}}(\cdot)$ is a non-decreasing function on the pre order set $(\mathcal{G}, \preccurlyeq)$.

First we explain the proof idea of Theorem 1 which is as follows. If $G \preccurlyeq H$, by definition there exists a homomorphism $\phi : \overline{G} \mapsto \overline{H}$. Notice that the function ϕ maps the vertices of $\overline{G}$ to the vertices of $\overline{H}$. Thus we can also consider, ϕ as a function from $V(G)$ to $V(H)$. For every vertex $w \in V(H)$, we denote by $\phi^{-1}(w)$ to be the set of all the vertices $v \in V(G)$ such that $\phi(v) = w$; (see Figure 1). This way, we partition the vertices of G into the classes of the form $\phi^{-1}(w)$ where $w \in V(H)$.

Next, we take an optimal index code for H over the source alphabet $\mathcal{X}$ that achieves the rate $\mathrm{ind}_{\mathcal{X}}(H)$. Then, we show that we can treat every part $\phi^{-1}(w)$ as a single node and translate the index code of H to one for G. This shows the statement of the theorem, i.e., $\mathrm{ind}_{\mathcal{X}}(G) \leq \mathrm{ind}_{\mathcal{X}}(H)$.

Before we formally define the translation and verify its validity, we will state two technical lemmas that will be required later in the proof of Theorem 1.

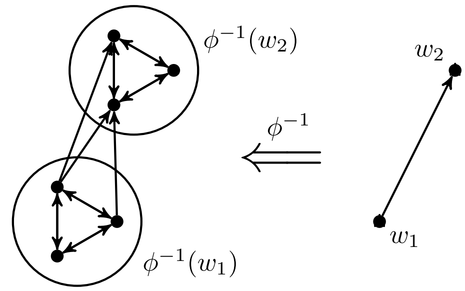

Fig. 2. Demonstration of Lemma 1. Part (i) states that inside each bundle $\phi^{-1}(w_i)$ we have a clique and part (ii) states that if w_2 is an outgoing neighbour of w_1 in H then all of the vertices in $\phi^{-1}(w_1)$ of G are connected to all of the vertices in $\phi^{-1}(w_2)$ of G (note that all of the edges from $\phi^{-1}(w_1)$ to $\phi^{-1}(w_2)$ are not shown in the figure).

Lemma 1. *(i) For every $w \in V(H)$, $\phi^{-1}(w)$ is a clique in G.*
(ii) If $w_2 \in N_H^+(w_1)$, $v_1 \in \phi^{-1}(w_1)$, and $v_2 \in \phi^{-1}(w_2)$ then $v_2 \in N_G^+(v_1)$. (Also see Figure 2).

Proof. (i) If $\phi^{-1}(w)$ is not a clique then $\exists v_1, v_2 \in \phi^{-1}(w)$ such that $(v_1, v_2) \notin E(G)$. Thus $(v_1, v_2) \in E(\overline{G})$ implies that $(\phi(v_1), \phi(v_2)) = (w, w)$ should be an edge of $\overline{H}$, as $\phi : \overline{G} \mapsto \overline{H}$ is a homomorphism. But this is a contradiction since $\overline{H}$ has no loop.
(ii) If $v_2 \notin N_G^+(v_1)$ then $v_2 \in N_{\overline{G}}^+(v_1)$ which implies that $\phi(v_2) \in N_{\overline{H}}^+(\phi(v_1))$ and hence $w_2 \in N_{\overline{H}}^+(w_1)$. Therefore, $w_2 \notin N_H^+(w_1)$ which is a contradiction. $\square$

Definition 6. *For every finite set $\mathcal{X}$ and positive integer m, a function $f : \mathcal{X}^m \mapsto X$ is called* coordinate-wise one-to-one *if by setting the values for every $m-1$ variables of f, it is a one-to-one function of the remaining variable, i.e., for every $j \in [1:m]$ and any choice of $a_1, \ldots, a_{j-1}, a_{j+1}, \ldots, a_m \in \mathcal{X}$, the function $f(a_1, \ldots, a_{j-1}, x, a_{j+1}, \ldots, a_m) : \mathcal{X} \mapsto \mathcal{X}$ is one-to-one.*

Lemma 2. *For every finite set $\mathcal{X}$ and $m \in \mathbb{N}$, there exists a coordinate-wise one-to-one function.*

Proof. Suppose that $|\mathcal{X}| = n$. Let $\gamma : \mathcal{X} \mapsto \mathbb{Z}_n$ be a bijection between $\mathcal{X}$ and integer numbers modulo n. Define $g : \mathcal{X}^m \mapsto \mathcal{X}$ by $g(x_1, \ldots, x_m) \triangleq \gamma^{-1}(\sum_{i=1}^m \gamma(x_i))$. It is straightforward to check that f is coordinate-wise one-to-one. $\square$

Proof of Theorem 1. Suppose that $V(H) = \{w_1, \ldots, w_n\}$ where $n = |V(H)|$. Let $\phi : \overline{G} \mapsto \overline{H}$ be a homomorphism. As stated in Lemma 1, the vertex set of G can be partitioned into n cliques of the form $\phi^{-1}(w_i)$. So, we can list the vertices of G as $V(G) = \{v_{1,1}, \ldots, v_{1,k_1}, \ldots, v_{n,1}, \ldots, v_{n,k_n}\}$ such that $\phi^{-1}(w_i) = \{v_{i,1}, \ldots, v_{i,k_i}\}$ and $k_i = |\phi^{-1}(w_i)|$. Note that $m = |V(G)| = \sum_{i=1}^n k_i$.

Let $k = \mathrm{ind}_{\mathcal{X}}(H)$ and $\Phi^H(x_1, \ldots, x_n) : \mathcal{X}^n \mapsto \mathcal{Y}^k$ (in addition to a set of decoders $\{\Psi_i^H\}$) be an optimal valid index code for H over the source alphabet $\mathcal{X}$ (and the message alphabet $\mathcal{Y}$) where x_i is the variable associated to the node w_i.

Validity of the index code implies that for every node $w_i \in H$, there exists a decoding function $\Psi_i^H : \mathcal{Y}^k \times \mathcal{X}^{|N_H^+(w_i)|} \mapsto \mathcal{X}$ such that

$$\Psi_i^H(\Phi^H(x_1, \dots, x_n), x_{N_H^+(w_i)}) = x_i \tag{1}$$

for every choice of $(x_1, \dots, x_n) \in \mathcal{X}^n$.

Now, we construct a valid index code for G over the same alphabet sets and the same transmission length k; thus it results in an index code for G with the same broadcast rate.

Suppose that the variable associated to the node $v_{i,j} \in V(G)$ is $x_{i,j} \in \mathcal{X}$. First, we construct an instance of index coding problem over H as follows. Then using Lemma 2, we pick n coordinate-wise one-to-one function $g_i : \mathcal{X}^{k_i} \mapsto \mathcal{X}$ and set $x_i = g_i(x_{i,1}, \dots, x_{i,k_i})$. Now, we define the index code encoder function $\Phi^G : \mathcal{X}^{(\sum k_i)} \mapsto \mathcal{Y}^k$ as follows:

$$\begin{aligned}\Phi^G(x_{1,1}, \dots, x_{1,k_1}, \dots, x_{n,1}, \dots, x_{n,k_n}) \triangleq \\ \Phi^H\left(g_1(x_{1,1}, \dots, x_{1,k_1}), \dots, g_n(x_{n,1}, \dots, x_{n,k_n})\right).\end{aligned}$$

To complete the proof, we need to construct the decoding functions for all the receivers $v_{i,j}$. Due to the symmetry, we only construct the decoding function for $v_{1,1}$.

First define the function $h : \mathcal{Y}^k \times \mathcal{X}^{|N_G^+(v_{1,1})|} \mapsto \mathcal{X}$ as follows

$$h(y_1, \dots, y_k, x_{N_G^+(v_{1,1})}) = \Psi_1^H(y_1, \dots, y_k, x_{N_H^+(w_1)}).$$

Note that h is a well defined function since if $x_{N_G^+(v_{1,1})}$ is given as parameter of h, $x_{N_H^+(w_1)}$ is also known. This is due to the fact that for every $w_i \in N_H^+(w_1)$, $\phi^{-1}(w_i) \subseteq N_G^+(v_{1,1})$ by Lemma 1 and $x_i = g_i(x_{i,1}, \dots, x_{i,k_i})$ is known to w_i. Notice that for the defined function h we have

$$\begin{aligned}&h\left(\Phi^G(x_{1,1}, x_{1,2}, \dots, x_{n,k_n}), x_{N_G^+(v_{1,1})}\right)\\ &\quad= \Psi_1^H\Big(\Phi^H\big(g_1(x_{1,1}, \dots, x_{1,k_1}),\\ &\qquad\quad \dots, g_n(x_{n,1}, \dots, x_{n,k_n})\big), x_{N_H^+(w_1)}\Big)\\ &\quad= g_1(x_{1,1}, \dots, x_{1,k_1})\end{aligned}$$

where the first equality is by the definition of h and the second equality is by (1).

Note that by part (i) of Lemma 1, we know that $x_{1,2}, \dots, x_{1,k_1}$ are among the out neighbours of $v_{1,1}$, i.e., $x_{1,i} \in x_{N_G^+(v_{1,1})}$ for $i \in [2 : k_1]$. Define the function $g_{1,1} : \mathcal{X} \mapsto \mathcal{X}$ as $g_{1,1}(x) \triangleq g_1(x, x_{1,2}, x_{1,3}, \dots, x_{1,k_1})$. Therefore

$$\begin{aligned}(g_{1,1})^{-1}\left(h(\Phi^G(x_{1,1}, \dots, x_{n,k_n}), x_{N_G^+(v_{1,1})})\right) = \\ (g_{1,1})^{-1}\left(g_1(x_{1,1}, \dots, x_{1,k_1})\right) = x_{1,1}.\end{aligned}$$

Hence, we can define the decoding function $\Psi_{1,1}^G$ as

$$\begin{aligned}\Psi_{1,1}^G\left(y_1, \dots, y_k, x_{N_G^+(v_{1,1})}\right) \triangleq \\ (g_{1,1})^{-1} \circ h\left(y_1, \dots, y_k, x_{N_G^+(v_{1,1})}\right).\end{aligned}$$

This shows the validity of the proposed index code for the problem defined over G and so completes the proof. □

As a consequence of Theorem 1 we have the following corollary.

Corollary 1. *Consider two instances of the index coding problems over the digraphs G and H. If $G \preccurlyeq H$ then we have*

1) *for general multi-letter index codes:* $\underrightarrow{\mathrm{ind}}(G) \le \underrightarrow{\mathrm{ind}}(H)$,
2) *for linear vector index codes:* $\overrightarrow{\mathrm{lind}}_{q,l}(G) \le \overrightarrow{\mathrm{lind}}_{q,l}(H)$,
3) *for linear scalar index codes:* $\mathrm{lind}_q(G) \le \mathrm{lind}_q(H)$.

Proof. In the inequality of Theorem 1, if we take the infimum of both sides, we derive Part 1. To prove the other parts of the corollary, notice that in both cases of scalar and vector index code, we can define the function g in the proof of Theorem 1 to be the sum function and therefore, it is a linear function. Hence the functions Φ^G and $\Psi_{i,j}^G$ are also linear. This completes the proof. □

IV. An Equivalent Formulation for Linear Index Coding Problem

For $k \ge l \in \mathbb{Z}^+$, let $\mathcal{G}_{k,l}^q$ be the set of all the finite digraphs G for which $\overrightarrow{\mathrm{lind}}_{q,l}(G) \le \frac{k}{l}$. Although $\mathcal{G}_{k,l}^q$ is an infinite family of digraphs, in this section, we will show that $\mathcal{G}_{k,l}^q$ has a maximal member with respect to the pre order "$\preccurlyeq$". We give an explicit construction for a maximal element of $\mathcal{G}_{k,l}^q$ which we call it $H_{k,l}^q$.

First, let us state the following definition.

Definition 7. *A family of graphs $\{G_k\}_{k=1}^\infty$ is called (q,l)-*index code defining ((q,l)-ICD) *if and only if for every (side information) digraph G we have*

$$\overrightarrow{\mathrm{lind}}_{q,l}(G) \le \frac{k}{l} \Longleftrightarrow G \preccurlyeq G_k.$$

It is easy to see that if $\{G_k\}_{k=1}^\infty$ is a (q,l)-ICD, so is the family $\{G'_k\}_{k=1}^\infty$ where G_k and G'_k are homomorphically equivalent. In particular, if $\{G_k\}_{k=1}^\infty$ is a (q,l)-ICD in which no G_k can be replaced with a smaller digraph, then G_k's are cores and conversely, if $\{G_k\}_{k=1}^\infty$ is a (q,l)-ICD, $\{\mathrm{Core}(G_k)\}_{k=1}^\infty$ is the unique smallest (q,l)-ICD, up to isomorphism[2].

Construction 1 (Graph $H_{k,l}^q$)**.** *For every positive integers $k \ge l$ and prime power q, let $\mathcal{V}$ be the set of all full rank matrices in $\mathbb{F}_q^{k\times l}$. We define the set $\mathcal{W}$ to be*

$$\mathcal{W} = \left\{(\underline{\mathbf{v}}, \underline{\mathbf{w}}) \mid \underline{\mathbf{v}}, \underline{\mathbf{w}} \in \mathcal{V},\ \text{and } \underline{\mathbf{v}}^\top \underline{\mathbf{w}} = \underline{\mathbf{I}}_l\right\}$$

where $\underline{\mathbf{I}}_l$ is an $l \times l$ identity matrix.

Now, we construct graph $H_{k,l}^q$ as follows. The vertex set of $H_{k,l}^q$ is $V(H_{k,l}^q) = \mathcal{W}$ and $\left((\underline{\mathbf{v}}, \underline{\mathbf{w}}), (\underline{\mathbf{v}}', \underline{\mathbf{w}}')\right) \in E(H_{k,l}^q)$ if and only if $\underline{\mathbf{v}}^\top \underline{\mathbf{w}}' \ne \underline{\mathbf{0}}_l$. In other

[2]For the definition of core of a graph, see [18, Chapter 1.6].

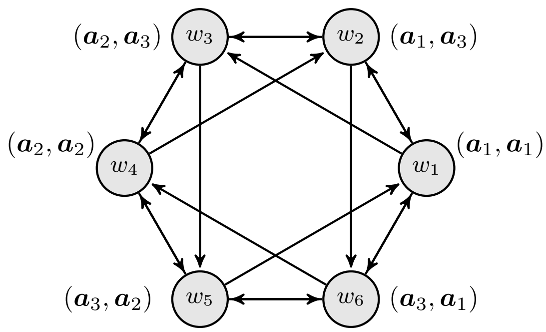

Fig. 3. The digraph H_2^2 consists of 6 vertices. The graph vertices are labelled by pair of vectors (matrices) where each element is one of the following vectors $\boldsymbol{a}_1 = [0 \;\; 1]^\top$, $\boldsymbol{a}_2 = [1 \;\; 0]^\top$, and $\boldsymbol{a}_3 = [1 \;\; 1]^\top$.

words, $\big((\underline{\mathbf{v}}, \underline{\mathbf{w}}), (\underline{\mathbf{v}}', \underline{\mathbf{w}}')\big) \in E(\overline{H_{k,l}^q})$ *if and only if* $(\underline{\mathbf{v}}, \underline{\mathbf{w}}), (\underline{\mathbf{v}}', \underline{\mathbf{w}}') \in \mathcal{W}$ *and* $\underline{\mathbf{v}}^\top \underline{\mathbf{w}}' = \underline{\mathbf{0}}_l$. *This construction leads to a graph of size*

$$|V(H_{k,l}^q)| = q^{l(k-l)} \prod_{i=0}^{l-1} (q^k - q^i).$$

For convenience we drop the index l from $H_{k,l}^q$ when $l = 1$ (i.e., for the case of scalar linear index code).

Example 1. *As an example, let us consider H_2^2. Here we have $\mathcal{V} = \{\boldsymbol{e}_1, \boldsymbol{e}_2, \boldsymbol{e}_1 + \boldsymbol{e}_2\}$. So it can be easily observed that H_2^2 has 6 nodes as follows*

$$\begin{aligned} V(H_2^2) = \big\{&(\boldsymbol{e}_1, \boldsymbol{e}_1), (\boldsymbol{e}_1, \boldsymbol{e}_1 + \boldsymbol{e}_2), (\boldsymbol{e}_2, \boldsymbol{e}_2) \\ &(\boldsymbol{e}_2, \boldsymbol{e}_1 + \boldsymbol{e}_2), (\boldsymbol{e}_1 + \boldsymbol{e}_2, \boldsymbol{e}_1), (\boldsymbol{e}_1 + \boldsymbol{e}_2, \boldsymbol{e}_2)\big\}. \end{aligned}$$

The graph H_2^2 is depicted in Figure 3.

Now, we have the following result.

Theorem 2. *For every prime power q and positive integer l, the family $\{H_{k,l}^q\}_{k=l}^\infty$ introduced above, is (q, l)-ICD.*

Proof. We need to show that $\forall G : \overrightarrow{\mathrm{lind}}_{q,l}(G) \leq k/l \Leftrightarrow G \preccurlyeq H_{k,l}^q$.

First, to prove the direct part, suppose that $\overrightarrow{\mathrm{lind}}_{q,l}(G) \leq k/l$. So we know that there exists an index code of transmitted sequence length k for this problem. We also know that each transmitted message y_j, $j \in [1 : k]$, is a linear combination of the source symbols $\boldsymbol{x} = [x_1^1, \ldots, x_1^l, \ldots, x_m^1, \ldots, x_m^l]^\top \in \mathbb{F}_q^{lm}$ where $\boldsymbol{x}_i = [x_i^1, \ldots, x_i^l]^\top$ is the source symbols assigned to the ith message and $m = |V(G)|$. Let $\boldsymbol{a}_j \in \mathbb{F}_q^{lm}$ be the coefficient of the jth transmitted message. Hence, the set of messages transmitted by the source is equal to

$$\begin{bmatrix} y_1 \\ \vdots \\ y_k \end{bmatrix} = \underline{\mathbf{A}}\boldsymbol{x} = \begin{bmatrix} - \; \boldsymbol{a}_1^\top \; - \\ \vdots \\ - \; \boldsymbol{a}_k^\top \; - \end{bmatrix} \times \begin{bmatrix} x_1^1 \\ \vdots \\ x_m^l \end{bmatrix}$$

where $\underline{\mathbf{A}} \in \mathbb{F}_q^{k \times lm}$.

Let us group the columns of $\underline{\mathbf{A}}$ into submatrices $\underline{\mathbf{E}}_i \in \mathbb{F}_q^{k \times l}$ where each $\underline{\mathbf{E}}_i$ is the encoding coefficients associated to the source symbols $x_i^1, \ldots, x_i^l$, i.e., $\underline{\mathbf{A}} = [\, \underline{\mathbf{E}}_1 \; \cdots \; \underline{\mathbf{E}}_m \,]$. Notice that $\underline{\mathbf{E}}_j$ can be viewed as the contribution of the source symbols $x_j^1, \ldots, x_j^l$ in the set of transmitted messages; therefore, $\mathrm{rank}(\underline{\mathbf{E}}_j) = l$ (consequently, none of the columns of $\underline{\mathbf{E}}_j$ are zero). Otherwise, there does not exist enough linear combinations of $x_j^1, \ldots, x_j^l$ in the transmitted messages and hence the jth receiver cannot recover its demand. Now for the vertex $v_j \in V(G)$ corresponding to the jth message (i.e., source symbols $x_j^1, \ldots, x_j^l$), define the encoding matrix $\underline{\mathbf{E}}(v_j) \triangleq \underline{\mathbf{E}}_j$.

Let v_i be an arbitrary node of G. We know that $\{\boldsymbol{a}_1^\top \boldsymbol{x}, \ldots, \boldsymbol{a}_k^\top \boldsymbol{x}\}$ together with the side information of v_i can be used in order to recover $x_i^1, \ldots, x_i^l$. This means that there exist l linear combinations of the transmitted messages which is sufficient for the ith receiver to recover its demand $x_i^1, \ldots, x_i^l$. Let us assume that these linear combinations are of the following form

$$\underline{\mathbf{D}}_i^\top \underline{\mathbf{A}}\boldsymbol{x} = \sum_{j=1}^m \underline{\mathbf{D}}_i^\top \underline{\mathbf{E}}_j \boldsymbol{x}_j$$

where $\underline{\mathbf{D}}_i \in \mathbb{F}_q^{k \times l}$.

Clearly $\mathrm{rank}(\underline{\mathbf{D}}_i) = l$, since x_i^j's are independent from each other and also because by using its side information alone, v_i cannot recover x_i^j's. Define the decoding matrix $\underline{\mathbf{D}}(v_i)$ assigned to v_i to be $\underline{\mathbf{D}}(v_i) \triangleq \underline{\mathbf{D}}_i$.

Let $r = |N_G^+(v_i)|$ and $\underline{\mathbf{S}}(v_i) \in \mathbb{F}_q^{lr \times lm}$ be the side information matrix of the ith receiver where $\underline{\mathbf{S}}(v_i)\boldsymbol{x}$ determines the side information that v_i has. Without loss of generality we can assume that $\underline{\mathbf{S}}(v_i)$ is a block matrix of the following form

$$\underline{\mathbf{S}}(v_i) = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ \vdots \\ r \end{array} \!\!\! \begin{array}{c} \begin{array}{ccccccc} & v_{j_1} & & v_{j_2} & & v_{j_r} & \end{array} \\ \left[\begin{array}{c|c|c|c|c|c|c} \cdots & \underline{\mathbf{I}}_l & \cdots & \underline{\mathbf{0}}_l & \cdots & \underline{\mathbf{0}}_l & \cdots \\ \hline \cdots & \underline{\mathbf{0}}_l & \cdots & \underline{\mathbf{I}}_l & \cdots & \underline{\mathbf{0}}_l & \cdots \\ \hline \cdots & \underline{\mathbf{0}}_l & \cdots & \underline{\mathbf{0}}_l & \cdots & \underline{\mathbf{0}}_l & \cdots \\ \hline \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \hline \cdots & \underline{\mathbf{0}}_l & \cdots & \underline{\mathbf{0}}_l & \cdots & \underline{\mathbf{I}}_l & \cdots \end{array}\right] \end{array}$$

where $v_{j_1}, \ldots, v_{j_r} \in N_G^+(v_i)$ and each block is an $l \times l$ matrix that is either $\underline{\mathbf{0}}_l$ or $\underline{\mathbf{I}}_l$.

Decodability of $\underline{\mathbf{D}}(v_i)$ means that the node v_i can recover $x_i^1, \ldots, x_i^l$ from $\underline{\mathbf{D}}(v_i)^\top \underline{\mathbf{A}}\boldsymbol{x}$ and its side information $\underline{\mathbf{S}}(v_i)\boldsymbol{x}$. In other words, in the matrix $\underline{\mathbf{D}}(v_i)^\top \underline{\mathbf{A}}$, all the non-zero blocks should be known by v_i (through its side information) except the ith block (i.e., the block $\underline{\mathbf{D}}(v_i)^\top \underline{\mathbf{E}}(v_i)$) where the ith block is also non-zero. Now, by considering the row reduced echelon form of matrix

$$\begin{bmatrix} \underline{\mathbf{D}}(v_i)^\top \underline{\mathbf{A}} \\ \underline{\mathbf{S}}(v_i) \end{bmatrix},$$

it can be observed that we should have

$$\mathrm{rank}\left(\underline{\mathbf{D}}(v_i)^\top \underline{\mathbf{E}}_i(v_i)\right) = l \tag{2}$$

and for $i \neq j$ we should have

$$\underline{\mathbf{D}}(v_i)^\top \underline{\mathbf{E}}(v_j) \neq \underline{\mathbf{0}}_l \Longrightarrow (v_i, v_j) \in E(G) \tag{3}$$

or equivalently,

$$(v_i, v_j) \notin E(G) \Longrightarrow \underline{\mathbf{D}}(v_i)^\top \underline{\mathbf{E}}(v_j) = \underline{\mathbf{0}}_l. \quad (4)$$

Note that if $\underline{\mathbf{D}}(v_i)$ is right multiplied by a full rank matrices the conditions (2)-(4) are not changed. Hence it is possible to further restrict (2) while keeping the decodability of $\underline{\mathbf{D}}(v_i)$. It means that without loss of generality, the condition (2) can be replaced by

$$\underline{\mathbf{D}}(v_i)^\top \underline{\mathbf{E}}_i(v_i) = \underline{\mathbf{I}}_l. \quad (5)$$

Secondly, to complete the proof of the direct part of the theorem, we present a function $\phi : V(\overline{G}) \mapsto V(\overline{H^q_{k,l}})$ and show that ϕ is a homomorphism. For each $v_i \in V(\overline{G})$ define $\phi(v_i) = \big(\underline{\mathbf{D}}(v_i), \underline{\mathbf{E}}(v_i)\big)$. By (5), if $v_i \in V(\overline{G})$ clearly $\underline{\mathbf{D}}(v_i)^\top \underline{\mathbf{E}}(v_i) = \underline{\mathbf{I}}_l$. Hence, $\phi(v_i) \in V(\overline{H^q_{k,l}})$.

Then we need to show that ϕ preserves the edges. Suppose that $(v_i, v_j) \in E(\overline{G})$. So we have $(v_i, v_j) \notin E(G)$ and by (4) $\underline{\mathbf{D}}(v_i)^\top \underline{\mathbf{E}}(v_j) = \underline{\mathbf{0}}$. Now by construction of $H^q_{k,l}$, this implies that

$$\Big(\big(\underline{\mathbf{D}}(v_i), \underline{\mathbf{E}}(v_i)\big), \big(\underline{\mathbf{D}}(v_j), \underline{\mathbf{E}}(v_j)\big)\Big) \in E(\overline{H^q_{k,l}}),$$

namely, $\big(\phi(v_i), \phi(v_j)\big) \in E(\overline{H^q_{k,l}})$. This shows that ϕ is a homomorphism from $\overline{G}$ to $\overline{H^q_{k,l}}$. So the direct part of the theorem is proved.

So far, we have proved that if $\overrightarrow{\mathrm{lind}}_{q,l}(G) \le k/l$ then $G \preccurlyeq H^q_{k,l}$. Now, we show the reverse part; namely, we show that $G \preccurlyeq H^q_{k,l}$ implies $\overrightarrow{\mathrm{lind}}_{q,l}(G) \le k/l$. If $G \preccurlyeq H^q_{k,l}$, by definition, we have $\overline{G} \to \overline{H^q_{k,l}}$. Suppose that $\phi : \overline{G} \to \overline{H^q_{k,l}}$ is a homomorphism. For each $v_i \in V(G)$ let $\phi(v_i) = (\underline{\mathbf{D}}_\phi(v_i), \underline{\mathbf{E}}_\phi(v_i)) \in V(H^q_{k,l})$. Hence, $\underline{\mathbf{D}}_\phi(v_i)$ and $\underline{\mathbf{E}}_\phi(v_i)$ are full rank matrices in $\mathbb{F}_q^{k\times l}$. Since ϕ is a homomorphism, $(v_i, v_j) \in E(\overline{G}) \Rightarrow \underline{\mathbf{D}}_\phi(v_i)^\top \underline{\mathbf{E}}_\phi(v_j) = \underline{\mathbf{0}}$. Equivalently, $\underline{\mathbf{D}}_\phi(v_i)^\top \underline{\mathbf{E}}_\phi(v_j) \neq \underline{\mathbf{0}} \Rightarrow (v_i, v_j) \in E(G)$. Therefore, it is easy to see that the index coding defined by the $k \times lm$ matrix

$$\underline{\mathbf{A}} = \big[\underline{\mathbf{E}}_\phi(v_1) \cdots \underline{\mathbf{E}}_\phi(v_m)\big]$$

is a valid index code of transmitted sequence length k over $\mathbb{F}_q$ for G. Furthermore, the decoding algorithm for each node $v_i \in V(G)$ is to take the linear combination of the transmitted messages (rows of $\underline{\mathbf{A}}$) with coefficients from $\underline{\mathbf{D}}_\phi(v_i)$. Now by Definition 5, we have $\overrightarrow{\mathrm{lind}}_{q,l}(G) \le k/l$. This complete the proof of the theorem. □

A. Properties of graph $H^q_{k,l}$

In this section, we state some properties of the graph family $\{H^q_{k,l}\}_{k=1}^\infty$ where are used in the subsequent sections.

Lemma 3. *For every $k \in \mathbb{Z}^+$ and prime power q, $\mathrm{lind}_q(H^q_k) = k$.*

Proof. Since the identity function from $\overline{H^q_k}$ to itself is a homomorphism, therefore $H^q_k \preccurlyeq H^q_k$ and by Theorem 2, we have $\mathrm{lind}_q(H^q_k) \le k$. Now, if $\mathrm{lind}_q(H^q_k) \neq k$, then $\mathrm{lind}_q(H^q_k) \le k-1$. Let G be the graph with k vertices but no edge. Clearly $\mathrm{lind}_q(G) = k$. By Theorem 2 we have $G \preccurlyeq H^q_k$ and by Theorem 1 we have

$$k = \mathrm{lind}_q(G) \le \mathrm{lind}_q(H^q_k) \le k-1$$

which is a contradiction. □

Lemma 4. *For every $k \ge l \in \mathbb{Z}^+$ and prime power q, graph $H^q_{k,l}$ is vertex-transitive*[3].

Proof. From the definition of vertex transitivity, it is enough to show that for every arbitrary vertex $(\underline{\mathbf{d}}, \underline{\mathbf{e}}) \in V(H^q_{k,l})$, there exists an automorphism $\phi \in \mathrm{Aut}(H^q_{k,l})$ such that $\phi(\underline{\mathbf{d}}, \underline{\mathbf{e}}) = (\underline{\mathbf{B}}, \underline{\mathbf{B}})$ where $\underline{\mathbf{B}} = [\ \underline{\mathbf{I}}_l \quad \underline{\mathbf{0}}_{l\times(k-l)}\ ]^\top \in \mathbb{F}_q^{k\times l}$. Let $\{\boldsymbol{\xi}_1, \ldots, \boldsymbol{\xi}_{k-l}\}$ be a basis for the orthogonal complement of column space of $\underline{\mathbf{e}}$, i.e., $\boldsymbol{\xi}_i^\top \underline{\mathbf{e}} = \mathbf{0}$. Since $(\underline{\mathbf{d}}, \underline{\mathbf{e}}) \in V(H^q_{k,l})$ therefore $\underline{\mathbf{d}}^\top \underline{\mathbf{e}} = \underline{\mathbf{I}}$ and hence $[\underline{\mathbf{d}}]_j \notin \mathrm{Span}(\boldsymbol{\xi}_1, \ldots, \boldsymbol{\xi}_{k-l})$. Thus, $\{\boldsymbol{\xi}_1, \ldots, \boldsymbol{\xi}_{k-l}, [\underline{\mathbf{d}}]_1, \ldots, [\underline{\mathbf{d}}]_l\}$ form a basis for $\mathbb{F}_q^k$. Define the $k \times k$ invertible matrix

$$\underline{\mathbf{X}} = [\underline{\mathbf{d}} \ \ \boldsymbol{\xi}_1 \ \cdots \ \boldsymbol{\xi}_{k-l}]^\top.$$

Notice that $\underline{\mathbf{X}}^{-\top} \underline{\mathbf{d}} = \underline{\mathbf{B}}$ since $\underline{\mathbf{X}}^\top \underline{\mathbf{B}} = \underline{\mathbf{d}}$. Also, notice that $\underline{\mathbf{X}} \cdot \underline{\mathbf{e}} = \underline{\mathbf{B}}$ since $\underline{\mathbf{d}}^\top \underline{\mathbf{e}} = \underline{\mathbf{I}}_l$. Define the function $\phi : V(H^q_{k,l}) \mapsto V(H^q_{k,l})$ as $\phi(\underline{\mathbf{u}}, \underline{\mathbf{v}}) = \big(\underline{\mathbf{X}}^{-\top}\underline{\mathbf{u}}, \underline{\mathbf{X}}\underline{\mathbf{v}}\big)$. Since $(\underline{\mathbf{X}}^{-\top}\underline{\mathbf{u}})^\top \underline{\mathbf{X}}\underline{\mathbf{v}} = \underline{\mathbf{I}}_l$, we conclude that $\phi(\underline{\mathbf{u}}, \underline{\mathbf{v}})$ is indeed an element of $V(H^q_{k,l})$. Last, we need to show that for each edge $\big((\underline{\mathbf{u}}, \underline{\mathbf{v}}), (\underline{\mathbf{u}}', \underline{\mathbf{v}}')\big)$, the image under ϕ is also an edge (more precisely, we need to show that ϕ preserves edges and non-edges). If $\big((\underline{\mathbf{u}}, \underline{\mathbf{v}}), (\underline{\mathbf{u}}', \underline{\mathbf{v}}')\big)$ is an edge in $H^q_{k,l}$ then $\underline{\mathbf{u}}^\top \underline{\mathbf{v}}' \neq \underline{\mathbf{0}}$. Thus, $(\underline{\mathbf{X}}^{-\top}\underline{\mathbf{u}})^\top \underline{\mathbf{X}}\underline{\mathbf{v}}' \neq \underline{\mathbf{0}}$ and therefore $\big(\phi(\underline{\mathbf{u}}, \underline{\mathbf{v}}), \phi(\underline{\mathbf{u}}', \underline{\mathbf{v}}')\big)$ is an edge. By applying the same argument it can be shown that ϕ also preserves non-edges and this completes the proof. □

Obviously, as a result of Lemma 4, we have the following corollary.

Corollary 2. *Graph $\overline{H^q_{k,l}}$ is also vertex transitive.*

In the following, we obtain an upper bound on the chromatic number of $\overline{H^q_{k,l}}$. But before that let us state the following definition.

Definition 8. *A non-zero vector $\boldsymbol{a} \in \mathbb{F}_q^k$ is called* normal *if its first non-zero element is equal to 1, i.e.,*

$$\boldsymbol{a} = (0, \ldots, 0, 1, \star, \ldots, \star)^\top.$$

A matrix $\underline{\mathbf{A}} \in \mathbb{F}_q^{k\times r}$ with non-zero columns is called normal *if all of its columns are normal.*

For a matrix $\underline{\mathbf{A}}$, we define $\Upsilon(\underline{\mathbf{A}})$ to be the normalization of $\underline{\mathbf{A}}$, namely, the operator $\Upsilon(\cdot)$ normalizes every column of $\underline{\mathbf{A}}$ by multiplying it with a (non-zero) constant. In other words, we can write $\Upsilon(\underline{\mathbf{A}}) = \underline{\mathbf{A}} \cdot \underline{\mathbf{\Lambda}}$ where $\underline{\mathbf{\Lambda}} \in \mathbb{F}_q^{r\times r}$ is a diagonal matrix with non-zero elements on its diagonal.

[3]A graph H is said to be vertex-transitive if for any vertices u, v of H some automorphism of H (i.e., a bijective homomorphism of H to H) takes u to v (e.g., see [18, Chapter 1, p.14]).

Lemma 5. *The chromatic number of $\overline{H^q_{k,l}}$ can be upper bounded as*

$$\chi(\overline{H^q_{k,l}}) \leq \frac{\prod_{i=0}^{l-1}(q^k-q^i)}{(q-1)^l}.$$

Proof. To proof the assertion of lemma, we show that there exists a colouring of size $\prod_{i=0}^{l-1}(q^k-q^i)/(q-1)^l$ for $\overline{H^q_{k,l}}$. In fact we show that if $\underline{\mathbf{d}} \in \mathcal{V}$ is the decoding matrix assigned to a vertex of $H^q_{k,l}$ then $\Upsilon(\underline{\mathbf{d}})$ assigned to that vertex is a candidate for such a colouring (see Construction 1). First, notice that there are at most $\prod_{i=0}^{l-1}(q^k-q^i)/(q-1)^l$ of such matrices (colours). Then we need to show that this assignment leads to a proper colouring of $\overline{H^q_{k,l}}$. To this end, consider two vertices $(\underline{\mathbf{d}},\underline{\mathbf{e}}),(\underline{\mathbf{d}}',\underline{\mathbf{e}}') \in V(\overline{H^q_{k,l}})$ which have the same colour, i.e., we have $\Upsilon(\underline{\mathbf{d}}) = \Upsilon(\underline{\mathbf{d}}')$. From Construction 1, we know that $\underline{\mathbf{d}}^\top\underline{\mathbf{e}} = \underline{\mathbf{I}}$ and $\underline{\mathbf{d}}'^\top\underline{\mathbf{e}}' = \underline{\mathbf{I}}$. Because $\Upsilon(\underline{\mathbf{d}}) = \Upsilon(\underline{\mathbf{d}}')$ we can write $\underline{\mathbf{d}} = \underline{\mathbf{N}}\cdot\underline{\mathbf{\Lambda}}_1$ and $\underline{\mathbf{d}}' = \underline{\mathbf{N}}\cdot\underline{\mathbf{\Lambda}}_2$ where $\underline{\mathbf{N}}$ is a normal matrix. Now we can write

$$\begin{aligned}
\underline{\mathbf{d}}^\top\underline{\mathbf{e}}' &= (\underline{\mathbf{N}}\cdot\underline{\mathbf{\Lambda}}_1)^\top\underline{\mathbf{e}}'\\
&= \underline{\mathbf{\Lambda}}_1\underline{\mathbf{N}}^\top\underline{\mathbf{e}}'\\
&= \underline{\mathbf{\Lambda}}_1\underline{\mathbf{\Lambda}}_2^{-1}\\
&\neq \underline{\mathbf{0}}
\end{aligned}$$

which, by using Construction 1, it means that there is no edge in $\overline{H^q_{k,l}}$ from $(\underline{\mathbf{d}},\underline{\mathbf{e}})$ to $(\underline{\mathbf{d}}',\underline{\mathbf{e}}')$. A similar argument shows that there is no edge in the reverse direction as well. So this completes the proof of lemma. □

Lemma 6. *The clique number of $H^q_{k,l}$ is lower bounded as follows*

$$\omega(H^q_{k,l}) = \alpha(\overline{H^q_{k,l}}) \geq q^{l(k-l)}\prod_{i=0}^{l-1}(q^l-q^i).$$

Proof. Consider a set $\mathcal{C}$ of pairs of matrices defined as follows

$$\mathcal{C} = \left\{ (\underline{\mathbf{a}},\underline{\mathbf{b}}) \;\middle|\; \underline{\mathbf{a}} = \left[\frac{\underline{\mathbf{J}}^{-\top}}{\underline{\mathbf{0}}}\right],\ \underline{\mathbf{b}} = \left[\frac{\underline{\mathbf{J}}}{\underline{\mathbf{T}}}\right], \right.$$
$$\left. \underline{\mathbf{J}} \in \mathbb{F}_q^{l\times l},\ \operatorname{rank}(\underline{\mathbf{J}}) = l,\ \underline{\mathbf{T}} \in \mathbb{F}_q^{(k-l)\times l} \right\}.$$

Notice that for each pair of matrices $(\underline{\mathbf{a}},\underline{\mathbf{b}}) \in \mathcal{C}$ we have $\underline{\mathbf{a}}^\top\underline{\mathbf{b}} = \underline{\mathbf{J}}^{-1}\underline{\mathbf{J}} = \underline{\mathbf{I}}_l$ for some full rank matrix $\underline{\mathbf{J}}$. This shows that $\mathcal{C} \subset V(H^q_{k,l})$.

Now, it remains to show that $\mathcal{C}$ forms a clique in $H^q_{k,l}$. Let $(\underline{\mathbf{a}},\underline{\mathbf{b}}),(\underline{\mathbf{a}}',\underline{\mathbf{b}}') \in \mathcal{C}$ be two arbitrary vertices in $\mathcal{C}$. Then we can write

$$\begin{aligned}
\underline{\mathbf{a}}^\top\underline{\mathbf{b}}' &= \underline{\mathbf{J}}^{-1}\underline{\mathbf{J}}'\\
&\neq \underline{\mathbf{0}}
\end{aligned}$$

since $\underline{\mathbf{J}}$ and $\underline{\mathbf{J}}'$ are full rank. By using Construction 1, it means that there is an edge from $(\underline{\mathbf{a}},\underline{\mathbf{b}})$ to $(\underline{\mathbf{a}}',\underline{\mathbf{b}}')$ in $H^q_{k,l}$. Similarly, it can be shown that there is an edge from $(\underline{\mathbf{a}}',\underline{\mathbf{b}}')$ to $(\underline{\mathbf{a}},\underline{\mathbf{b}})$ in $H^q_{k,l}$. This concludes the Lemma. □

V. Applications

In this section, we demonstrate several applications of the results stated in the previous sections.

A. Upper Bounds

Here, we will show that some of the earlier upper bounds are only special cases of Corollary 1.

Example 2. *One of the earliest upper bounds on the* $\operatorname{lind}_2(G)$ *is* $\chi(\overline{G})$ *where* $\chi(\cdot)$ *is the chromatic number of a graph (e.g., see [19]). Notice that in our framework, this result is an immediate consequence of Corollary 1, Part 3. That is, if* $\chi(\overline{G}) = r$ *then* $\overline{G} \to K_r$ *where* K_r *is a complete graph with* r *vertices (e.g., see [18, Chapter 6, p.204]. Thus,* $\operatorname{lind}_q(G) \leq \operatorname{lind}_q(\overline{K_r}) = r = \chi(\overline{G})$. *Notice that using our method, as shown above, the colouring upper bound naturally extends for every prime power* q.

In Example 3, using graph homomorphism framework, we derive the fractional chromatic number upper bound on the length of index code [5]. To this end, let us first state the definition of Kneser graphs.

Definition 9 (Kneser graphs $K(n,l)$)**.** *Given two positive integers* $l \leq n$, *the Kneser graph* $K(n,l)$ *is the graph whose vertices represent the* l*-subsets of* $[1:n]$ *and two vertices are connected if and only if they correspond to disjoint subsets.*

Example 3. *In [5], it is shown that* $\operatorname{ind}(G) \leq \chi_f(\overline{G})$ *where* $\chi_f(\cdot)$ *is the* fractional chromatic number *of a graph. However, using the graph homomorphism framework, this result follows immediately from Corollary 1, Part 2, and the fact that if* $\chi_f(\overline{G}) = \frac{n}{l}$ *then* $\overline{G} \to K(n',l')$ *for some pair of integers* n',l' *with* $\frac{n}{l} = \frac{n'}{l'}$ *(see [18, Theorem 6.23]). Thus,* $\overrightarrow{\operatorname{lind}}_{q,l}(G) \leq \overrightarrow{\operatorname{lind}}_{q,l}(\overline{K(n,l)}) \overset{(a)}{\leq} \frac{n}{l} = \chi_f(\overline{G})$ *where the inequality (a) follows from Lemma 7.*

Lemma 7. *For the vector linear index code of a complement of Kneser graph* $K(n,l)$, *we have*

$$\overrightarrow{\operatorname{lind}}_{q,l}(\overline{K(n,l)}) \leq \frac{n}{l}.$$

Proof. We know that $\chi_f(K(n,l)) = \frac{n}{l}$ (e.g., see [18], Theorem 6.23 and Proposition 6.27). Thus, a natural fractional colouring for $K(n,l)$ is to use the l-subsets of $[1:n]$ assigned to its vertices. Let $S_u \subset [1:n]$ be the set of colours associated to $u \in V(K(n,l))$.

Now, we will show that the sets of colours S_u impose a vector linear index code for the index coding problem defined with the side information graph $\overline{K(n,l)}$. To this end, we assign l independent source variables to each vertex $u \in V(\overline{K(n,l)})$ and label them as $x_i^u \in \mathbb{F}_q$ where $i \in S_u$. Then the transmitter broadcasts the following n messages over the public channel

$$y_i = \sum_{u:\ i\in S_u} x_i^u, \quad \forall i \in [1:n].$$

From the definition of Kneser graphs we know that

$$(u,v) \in E(\overline{K(n,l)}) \iff S_u \cap S_v \neq \varnothing.$$

As a result, for each $i \in S_u$, the receiver u can recover the variable x_i^u because by construction receiver u is connected to all nodes $v \in V(\overline{K(n,l)})$ such that $i \in S_v$ and it has all of the required variables to recover x_i^u.

The above argument presents a scheme which shows that by sending n symbols over $\mathbb{F}_q$, each receiver node can recover a vector of source variables of length l over $\mathbb{F}_q$. This proofs the claim of the lemma. $\square$

The crucial observation in the above examples is that the parameters $\chi(\overline{G})$ and $\chi_f(\overline{G})$ can be defined using existence of homomorphisms from $\overline{G}$ to the family of complete graphs and Kneser graphs, respectively.

Similar to Lemma 3, we can observe that:

Observation 1. *For every $k \in \mathbb{Z}^+$ and prime power q, $\overrightarrow{\mathrm{lind}}_{q,l}(H_{k,l}^q) \leq k/l$.*

Proof. Since $\overline{H_{k,l}^q}$ is homomorphic to itself then the assertion follows directly from Theorem 2. $\square$

Notice that if there exists a graph G such that $\overrightarrow{\mathrm{lind}}_{q,l}(G) = k/l$ then Observation 1 holds with equality. This is because if $\overrightarrow{\mathrm{lind}}_{q,l}(G) = k/l$ then by Theorem 2, $\overline{G}$ is homomorphic to $\overline{H_{k,l}^q}$ and therefore $k/l = \overrightarrow{\mathrm{lind}}_{q,l}(G) \leq \overrightarrow{\mathrm{lind}}_{q,l}(H_{k,l}^q) \leq k/l$. Unfortunately, we do not know if such G exists but we make the following conjecture.

Conjecture 1. *For every prime power q and any pair of (k,l), $k \geq l$ of positive integers, $\overrightarrow{\mathrm{lind}}_{q,l}(\overline{K(k,l)}) = k/l$.*

B. Lower Bounds

As a result of Theorem 2, we can prove the following lemma.

Lemma 8. *Suppose that h is an increasing function on $(\mathcal{G}, \preccurlyeq)$ and r is an upper bound on $h(H_{k,l}^q)$. For every digraph G, if $h(G) > r$ then $\overrightarrow{\mathrm{lind}}_{q,l}(G) > k/l$.*

Proof. If $\overrightarrow{\mathrm{lind}}_{q,l}(G) \leq k/l$ then by Theorem 2, $G \preccurlyeq H_{k,l}^q$ and therefore $h(G) \leq h(H_{k,l}^q) \leq r$ which is a contradiction. $\square$

Lemma 8 is a useful tool to find lower bounds on the scalar linear index of an index coding problem. Actually for every increasing function h on $(\mathcal{G}, \preccurlyeq)$ we have one lower bound on the index coding problem. In the next theorem, using Lemma 8, we provide an alternative proof for the known lower bound on $\mathrm{lind}_q(G)$ (i.e., for the scalar case when $l = 1$) in terms of the chromatic number of $\overline{G}$ [15].

Theorem 3. *For every digraph G we have*

$$\mathrm{lind}_q(G) \geq \log_q\left((q-1)\chi(\overline{G}) + 1\right).$$

Proof. The function $h(G) = \chi(\overline{G})$ is an increasing function on $(\mathcal{G}, \preccurlyeq)$ (e.g., see [18, Corollary 1.8]). Suppose that $\mathrm{lind}_q(G) = k$. Therefore, by Theorem 2, we have $G \preccurlyeq H_k^q$. Thus $\chi(\overline{G}) \leq \chi(\overline{H_k^q}) \leq \frac{q^k-1}{q-1}$ where the last inequality follows from Lemma 5. This completes the proof of theorem. $\square$

In the following we introduce another tool to find lower bounds on $\overrightarrow{\mathrm{lind}}_{q,l}(G)$. Hell and Nesetril in [18, Proposition 1.22] showed that if a graph H is vertex transitive and $\phi : G \to H$ is a homomorphism, then for every graph K we have $\frac{|G|}{N(G,K)} \leq \frac{|H|}{N(H,K)}$ in which $N(L,K)$ is the size of the largest induced subgraph L' of L such that there exists a homomorphism from L' to K. Even though this result is stated for undirected graphs, its proof naturally extends to digraphs. Therefore, using this result and Theorem 2 we can deduce the following theorem.

Theorem 4. *For every digraph G, if there exists a digraph Ksuch that*

$$\frac{|G|}{N(\overline{G},K)} > \frac{|H_{k,l}^q|}{N(\overline{H_{k,l}^q},K)}$$

then $\overrightarrow{\mathrm{lind}}_{q,l}(G) > k/l$.

Proof. We prove the theorem by contradiction. Suppose that $\overrightarrow{\mathrm{lind}}_{q,l}(G) \leq k/l$. Then by Theorem 2, we have $\mathrm{Hom}(\overline{G}, \overline{H_{k,l}^q}) \neq \varnothing$. Also by Corollary 2, $\overline{H_{k,l}^q}$ is a vertex transitive digraph. Now we can apply the result of [18, Proposition 1.22] to conclude that for every digraph K we have $\frac{|G|}{N(\overline{G},K)} \leq \frac{|H_{k,l}^q|}{N(\overline{H_{k,l}^q},K)}$ which is a contradiction. Thus we are done. $\square$

An interesting special case of Theorem 4 is when K is a complete graph with r vertices. In this case $N(G,K)$ is equal to the size of the largest r-colourable induced subgraph of G. In particular the following corollary holds.

Corollary 3. *For every digraph G if*

$$\frac{|G|}{\omega(G)} > \prod_{i=0}^{l-1} \frac{q^k - q^i}{q^l - q^i}$$

then $\overrightarrow{\mathrm{lind}}_{q,l}(G) > k/l$. In other words, we can state the following expression to lower bound $\overrightarrow{\mathrm{lind}}_{q,l}(G)$,

$$\sum_{i=0}^{l-1} \log_q\left(q^{l\,\overrightarrow{\mathrm{lind}}_{q,l}(G)} - q^i\right) \geq \log_q\left[\prod_{i=0}^{l-1}(q^l - q^i)\frac{|G|}{\omega(G)}\right].$$

Proof. In Theorem 4 set K to be K_1. Then $\omega(G) = \alpha(\overline{G}) = N(\overline{G}, K_1)$. Now Lemma 6 completes the proof. $\square$

For the scalar case where $l = 1$, we can derive a slightly stronger lower bound as stated in the following (see [20])

$$\mathrm{lind}_q(G) \geq \log_q\left[1 + \frac{(q^2-1)(q-1)}{4q}\frac{|G|}{\omega(G)}\right].$$

Example 4. *Let G be a directed graph with n vertices so that for every pair (i,j) of the vertices either $(i,j) \in E(G)$ or $(j,i) \in E(G)$ but not both. In this case, $\alpha(G) = \omega(G) = 1$. The lower bound derived above translates to*

$$\mathrm{lind}_q(G) \geq \log_q\left[1 + \frac{(q^2-1)(q-1)}{4q}n\right].$$

This lower bound is slightly better than the lower bound obtained from Theorem 3 and is significantly stronger that the trivial bound $\mathrm{lind}_q(G) \geq \alpha(G)$.

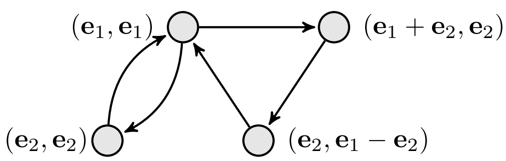

Fig. 4. The induced subgraph D of $\overline{H_k^q}$ which is used in the proof of Theorem 6 to show that the core of $\overline{H_k^q}$ cannot be a directed cycle.

C. Computational Complexity of $\mathrm{lind}_q(\cdot)$

By applying the result of [21] that proves the conjecture [18, Conjecture 5.16] and using Theorem 2, we show that the decision problem of $\mathrm{lind}_q(G) \leq k$ is NP-complete for $k \geq 2$.

First, let us state the following theorem.

Theorem 5 (see [21] and [18, Conjecture 5.16]). *Suppose that H is a digraph with no vertex of in degree or out degree one. If core of H is not a directed cycle then the following decision problem is NP-complete.*

Input:	*A digraph G*
Output:	*If $\hom(G,H) \neq \varnothing$ then return "yes," else return "no."*

We will apply Theorem 5 to digraphs $\overline{H_k^q}$ for every $k \geq 2$.

Theorem 6. *For every finite field $\mathbb{F}_q$ and every $k \geq 2$ the following decision problem is NP-complete.*

Input:	*A digraph G*
Output:	*If $\mathrm{lind}_q(G) \leq k$ return "yes," otherwise return "no."*

Proof. Based on Theorem 2 and Theorem 5, it is sufficient to show that $\overline{H_k^q}$ has no vertex of in/out degree one and also its core is not a directed cycle. From Construction 1 we know that for $k \geq 2$, $\overline{H_k^q}$ has no source or sink. It remains to show that the core of $\overline{H_k^q}$ for any prime power q and any integer k, is not a directed cycle.

To this end, consider the subgraph D of $\overline{H_k^q}$ depicted in Figure 4. Clearly from this induced subgraph D there is no homomorphism to any directed cycle. Thus the core of $\overline{H_k^q}$ cannot be a directed cycle. □

Notice that the NP-completeness of the decision problem $\mathrm{lind}_q(G) \leq k$ was known for $q=2$ and $k \geq 3$, see [14], [16]. In fact this decision problem is NP-complete even when G is an undirected graph [16]. However, for undirected graphs, the decision problem $\mathrm{lind}_q(G) \leq 2$ is polynomially solvable since for undirected graphs we have $\mathrm{lind}_q(G) \leq 2$ if and only if G is complement of a bipartite graph. Theorem 6 shows that for digraphs, even the decision problem $\mathrm{lind}_q(G) \leq 2$ is hard.

D. Index Codes and Change of Field Size

Existence of a certain index code for a given graph over a fixed finite field is equivalent to the existence of linear combinations of the source messages over the ground field with certain Algebraic / Combinatorial constraints. If the ground field is changed, there is no natural way of updating the index code over the new field. In other words, if for a fixed graph G, an index code over a finite field $\mathbb{F}_{q_1}$ is given, there is no natural way to construct some index code for the same graph but over a different field $\mathbb{F}_{q_2}$.

Here we use the results of Theorem 1 and Theorem 2 to show that if the field size is changed, the corresponding linear indices can at most differ by a factor that depends only on the field sizes and is independent from the size of the graph. More precisely the following result holds:

Theorem 7. *Let G be a graph and q_1, q_2 are two different prime powers. Suppose that $\overrightarrow{\mathrm{lind}}_{q_1,l_1}(G) = \frac{k_1}{l_1}$. Then,*

$$\overrightarrow{\mathrm{lind}}_{q_2,l_2}(G) \leq \overrightarrow{\mathrm{lind}}_{q_2,l_2}(\overline{H_{k_1,l_1}^{q_1}}) \leq \frac{\prod_{i=0}^{l_1-1}(q_1^{k_1}-q_1^i)}{(q_1-1)^{l_1}}.$$

Proof. We know that $\overrightarrow{\mathrm{lind}}_{q_1,l_1}(G) = \frac{k_1}{l_1}$. By Theorem 2, $G \preccurlyeq \overline{H_{k_1,l_1}^{q_1}}$ and then by Theorem 1, $\overrightarrow{\mathrm{lind}}_{q_2,l_2}(G) \leq \overrightarrow{\mathrm{lind}}_{q_2,l_2}(\overline{H_{k_1,l_1}^{q_1}})$. The last inequality of the assertion follows from the colouring upper bound, Example 2, Lemma 5, and the fact that $\chi_f(\overline{H_{k_1,l_1}^{q_1}}) \leq \chi(\overline{H_{k_1,l_1}^{q_1}})$. □

Remark 1. *In fact, for the scalar index coding problem, in [3], it has been shown that for every pair of finite fields $\mathbb{F}_p$ and $\mathbb{F}_q$ of different characteristics and for every $0 < \epsilon < 1$, there exists a graph G with arbitrarily large number of vertices n such that $\mathrm{lind}_p(G) < n^\epsilon$ and $\mathrm{lind}_q(G) > n^{1-\epsilon}$. The previous theorem shows that in the result of [3], n^ϵ can not be replaced by a constant.*

Acknowledgement

The authors would like to thank Dr. P. Hell, Dr. S. Jaggi and Dr. A. Rafiey for their invaluable comments.

References

[1] Y. Birk and T. Kol, "Informed-source coding-on-demand (iscod) over broadcast channels," in *in Proc. 17th Ann. IEEE Int. Conf. Comput. Commun. (INFOCOM)*, 1998, pp. 1257–1264.

[2] N. Alon, E. Lubetzky, U. Stav, A. Weinstein, and A. Hassidim, "Broadcasting with side information," in *Proceedings of the 2008 49th Annual IEEE Symposium on Foundations of Computer Science*, ser. FOCS '08, 2008, pp. 823–832.

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

[4] S. El 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, 2010.

[5] A. Blasiak, R. D. Kleinberg, and E. Lubetzky, "Index coding via linear programming," *CoRR*, vol. abs/1004.1379, 2010.

[6] 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, 2011.

[7] Y. Berliner and M. Langberg, “Index coding with outerplanar side information,” in *IEEE Int. Symp. Inf. Theory*, 2011, pp. 806–810.
[8] I. Haviv and M. Langberg, “On linear index coding for random graphs,” in *IEEE Int. Symp. Inf. Theory*, 2012, pp. 2231–2235.
[9] A. Tehrani, A. Dimakis, and M. Neely, “Bipartite index coding,” in *IEEE Int. Symp. Inf. Theory*, 2012, pp. 2246–2250.
[10] H. Maleki, V. R. Cadambe, and S. A. Jafar, “Index coding - an interference alignment perspective,” *CoRR*, vol. abs/1205.1483, 2012.
[11] K. Shanmugam, A. G. Dimakis, and M. Langberg, “Local graph coloring and index coding,” *CoRR*, vol. abs/1301.5359, 2013.
[12] F. Arbabjolfaei, B. Bandemer, Y.-H. Kim, E. Sasoglu, and L. Wang, “On the capacity region for index coding,” in *IEEE Int. Symp. Inf. Theory*, 2013, pp. 962–966.
[13] M. Effros, S. Y. E. Rouayheb, and M. Langberg, “An equivalence between network coding and index coding,” *CoRR*, vol. abs/1211.6660, 2012.
[14] E. Chlamtac and I. Haviv, “Linear index coding via semidefinite programming,” *CoRR*, vol. abs/1107.1958, 2011.
[15] M. Langberg and A. Sprintson, “On the hardness of approximating the network coding capacity,” in *IEEE International Symposium on Information Theory*, 2008, pp. 315–319.
[16] R. Peeters, “Orthogonal representations over finite fields and the chromatic number of graphs,” *Combinatorica*, vol. 16, no. 3, pp. 417–431, 1996.
[17] S. H. Dau, V. Skachek, and Y. M. Chee, “Optimal index codes with near-extreme rates,” *Information Theory, IEEE Transactions on*, vol. 60, no. 3, pp. 1515–1527, 2014.
[18] P. Hell and J. Nesetril, *Graphs and Homomorphisms*, ser. Oxford Lecture Series in Mathematics and Its Applications. OUP Oxford, 2004.
[19] Z. Bar-Yossef, Y. Birk, T. S. Jayram, and T. Kol, “Index coding with side information,” in *Proceedings of the 47th Annual IEEE Symposium on Foundations of Computer Science*, ser. FOCS ’06, 2006, pp. 197–206.
[20] J. Ebrahimi Boroojeni and M. Jafari Siavoshani, “Linear index coding via graph homomorphism,” in *IEEE International Conference on Control, Decision and Information Technologies (CoDIT)*, 2014.
[21] L. Barto, M. Kozik, and T. Niven, “The csp dichotomy holds for digraphs with no sources and no sinks (a positive answer to a conjecture of bang-jensen and hell),” *SIAM Journal on Computing*, vol. 38, no. 5, pp. 1782–1802, 2009.