Broadcasting with Coded Side Information

Kenneth W. Shum
Institute of Network Coding
The Chinese University of Hong Kong
Shatin, Hong Kong
Email: wkshum@inc.cuhk.edu.hk

Mingjun Dai and Chi Wan Sung
Department of Electronic Engineering
City University of Hong Kong
Kowloon, Hong Kong
Email: mingjudai2@student.cityu.edu.hk,
albert.sung@cityu.edu.hk

***Abstract*—In the original index coding problem, each user has a set of uncoded packets as side information, and wants to decode some other packets from the source node. The source node aims at satisfying the demands of all users as quickly as possible. With linear network coding, this is accomplished by broadcasting linear combinations of the source packets over some finite field. Since the broadcast is performed over a wireless channel, a user may overhear some coded packets that are not intended to him/her. This motivates a generalization of the index coding problem to the case where linearly coded packets are used as side information. We show that this generalized linear index coding problem is equivalent to solving a system of multi-variable polynomial equations. A heuristic solution is constructed and is applied to the broadcast relay channel.**

***Index Terms*—Index coding, broadcast relay channel, network coding.**

I. Background and Motivations

In the index coding problem [1], [2], there is a transmitting node and a group of M users. The transmitting node has N source packets, $P_1, P_2, \dots, P_N$. Each user requests one specific data packet from the transmitting node. Each user has some side information, which is known to the transmitter through a feedback channel. The side information consists of some packets which is not wanted by that particular user. An index coding problem is specified by M "want sets" and M "has sets". The "want set" of user i is a singleton containing the data packet required by user i, and the "has set" of user i is a set containing the packets in user i's cache. The objective of index coding is to satisfy the demands of all users with minimum number of packet transmission. The index coding problem is shown to be NP-hard, and evening finding an approximation solution is hard, under certain complexity assumption [3], [4]. Studies of index coding can be found in [5], [6] and the references therein.

Suppose that the content of a packet is regarded as an element of a finite field, say the finite field with 2^n elements, denoted by $GF(2^n)$. A packet then carries n bits of information. The transmitting node can send linear combination of the source packets, with coefficients taken from $GF(2^n)$. In this case, we say that the index coding is (scalar) *linear*. A linear combination of source packets is called a *coded packet*. (For vector linear index coding, we refer the readers to [7], [8]. In this paper, we focus on the scalar linear case.)

This work was partially supported by a grant from the University Grants Committee (Project No. AoE/E-02/08) of the Hong Kong Special Administrative Region, China.

Time slot	Packet sent	Received by user 1?	Received by user 2?	Received by user 3?
1	P_1	no	yes	no
2	P_2	yes	no	no
3	P_3	yes	yes	no
4	$P_1 + P_2$	no	no	yes
5	$P_1 + P_2 + P_3$	yes	yes	yes

Fig. 1. Illustration of utilizing coded packets as side information.

In some application of index coding in wireless broadcast channel, the "has set" of a user may contain coded packets as well. We give a simple example for motivation. The source node has three packets P_1, P_2 and P_3, which are elements in $GF(2^n)$. There are three users. For $i = 1, 2, 3$, user i wants packet P_i. The transmitted packet is subject to independent erasures. It is assumed that there are feedback channels from the users, informing the transmitting node which packets are successfully received. Consider the following scenario. The source node transmits packets P_1, P_2 and P_3 in time slot 1, 2 and 3 respectively. At the end of time slot 3, user 1 has packets P_2 and P_3, and user 2 has packets P_1 and P_3, while user 3 fails to receive any packet. The source node in time slot 4 transmits the coded packet $P_1 + P_2$, and hope that user 1 and user 2 can decode their packets. For example, user 1 can decode P_1 by adding $P_1 + P_2$ and P_2, and user 2 can decode P_2 by adding $P_1 + P_2$ and P_1. Unfortunately, only user 3 can receive the coded packet $P_1 + P_2$ in time slot 4. There is now a coding opportunity that utilizes the coded packet $P_1 + P_2$ in user 3's cache. The source can send the sum $P_1 + P_2 + P_3$ in time slot 5. If all three users can receive $P_1 + P_2 + P_3$ successfully, then all user can decode the required packets by linearly combining with the packets received earlier (see Fig. 1). For example, user 3 can decode P_3 by adding $P_1 + P_2$ and $P_1 + P_2 + P_3$.

In this paper, the index coding problem is generalized in two ways. Firstly, coded packets in users' cache are also utilized as side information. Secondly, the packets in the transmitting node may be coded or uncoded packets. The second generalization find applications in the broadcast channel with a relay node as helper (Fig. 2). The packets in the relay

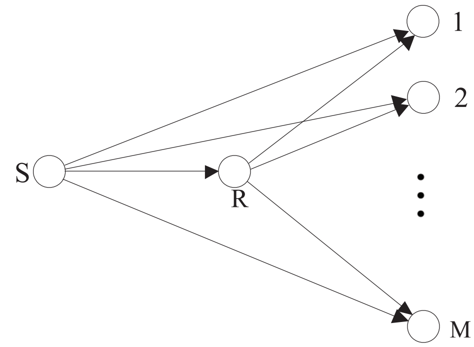

Fig. 2. Broadcast Relay Channel

node are obtained by listening to the previous transmission in the channel, and hence may be coded or uncoded packets. Given the coded side information of the users, the relay node transmits packets obtained by linearly mixing the coded packets in the cache of relay node. We will study in this paper how to apply generalized index coding to the relay node.

The generalized linear index coding problem is formulated in Section II, and is shown to be mathematically equivalent to solving a system of multi-variable quadratic equation in Section III. Because solving multi-variable polynomial equations in general is a hard computational problem, we give a heuristic algorithm that finds suboptimal solution in Section IV. In Section V, we discuss the application to broadcast relay channel with some simulation results.

II. Linear Index Coding with Coded Packets as Side Information

There is a transmitting node, T, and M receiving nodes, called the *users*. Each user wants a particular data packet from the transmitting node. The transmitting node is either the source or the relay node in the broadcast relay channel. The transmitting node can broadcast packets to the M users, and as in the original linear index coding problem, the channel is error-free. The content of a packet is regarded as an element of the finite field of size q, denoted by $GF(q)$, for some prime power q. The content of a packet is linear combination of the N source packets P_1 to P_N, with coefficients drawn from $GF(q)$. The vector formed by the N coefficients is called the *coding vector* of the packet. The side information in each user is obtained by overhearing the packets transmitted earlier in the air, and hence also takes the form of a linear combination of the N source packets. The transmitting node T may not have the message packets P_1 to P_N. Similar to each user, we assume that T has K_T linear combinations of packets P_1 to P_N. The transmitting node sends out linear combinations of the packets in its memory. We ask for the minimum number of packet transmissions such that all users are satisfied. We formulate the problem as follows.

We slightly generalize the users' requirement. For $i = 1, 2, \dots, M$, user i requests a packet with coding vector $\mathbf{r}_i \in GF(q)^N$. When $\mathbf{r}_i$ is a standard basis vector, say the j-th component is 1 and the rests are zero, then user i wants to receive the j-th packet P_j. In what follows, the request vector $\mathbf{r}_i$ can be any N-dimensional vector with components in $GF(q)$. This generalized setting may have application in multi-hop network (see for example [9]).

For $i = 1, 2, \dots, M$, let K_i be the number of side-information packets in user i's cache. These packets are denoted by $Q_1^{(i)}, Q_2^{(i)}, \dots, Q_{K_i}^{(i)}$. For $k = 1, 2, \dots, K_i$, the k-th packet in user i's cache is a linear combination

$$Q_k^{(i)} = c_{1,k}^{(i)} P_1 + c_{2,k}^{(i)} P_2 + \ldots + c_{N,k}^{(i)} P_N.$$

of the source packets, with the coefficients $c_{j,k}^{(i)}$ taken from $GF(q)$. Denote the coding vector corresponding to packet $Q_k^{(i)}$ by the vector

$$\mathbf{c}_k^{(i)} \triangleq (c_{1,k}^{(i)}, c_{2,k}^{(i)}, \dots, c_{N,k}^{(i)}).$$

User i can generate any packet whose coding vector is a linear combination of $\mathbf{c}_1^{(i)}$, $\mathbf{c}_2^{(i)}, \dots, \mathbf{c}_{K_i}^{(i)}$. Let

$$V_i \triangleq \langle \mathbf{c}_1^{(i)}, \mathbf{c}_2^{(i)}, \dots, \mathbf{c}_{K_i}^{(i)} \rangle,$$

where $\langle \mathbf{v}_1, \dots, \mathbf{v}_r \rangle$ is the notation for the subspace in $GF(q)^N$ spanned by vectors $\mathbf{v}_1, \dots, \mathbf{v}_r$.

Let K_T be the number of coded packets in the transmitting node. For $k = 1, 2, \dots, K_T$, the k-th packet is denoted by

$$Q_k^{(T)} = c_{1,k}^{(T)} P_1 + c_{2,k}^{(T)} P_2 + \ldots + c_{N,k}^{(T)} P_N,$$

where

$$(c_{1,k}^{(T)}, c_{2,k}^{(T)}, \dots, c_{N,k}^{(T)}) \triangleq \mathbf{c}_k^{(T)}$$

is the associated coding vector. Let V_T be the vector subspace

$$V_T \triangleq \langle \mathbf{c}_1^{(T)}, \mathbf{c}_2^{(T)}, \dots, \mathbf{c}_{K_T}^{(T)} \rangle.$$

Given two vector subspaces U_1 and U_2 of a vector space U, we define the *sum space* of U_1 and U_2, denoted by $U_1 + U_2$, by

$$U_1 + U_2 \triangleq \{u_1 + u_2 : u_1 \in U_1, u_2 \in U_2\},$$

which is nothing but the smallest subspace in U containing both U_1 and U_2. The requirement of user i can be expressed as

$$\mathbf{r}_i \in V + V_i. \tag{1}$$

A vector subspace V of V_T satisfying (1) for $i = 1, 2, \dots, M$ is called a *feasible solution*. The transmitting node can pick any basis of the subspace V, and send the corresponding linear combinations of packets. The dimension of a feasible solution is thus the number of packet transmissions. If the transmission is error-free, all users can decode the required packets by linearly combining the received packets and the packets already stored in his/her cache.

Without loss of generality, we make the following assumptions.

(i) $\mathbf{r}_i \notin V_i$ for $i = 1, 2, \dots, M$. Otherwise, user i's request has been satisfied already and we do not need to consider user i.

(ii) V_i has dimension K_i for each i, and V_T has dimension K_T. In other words, for each $i = 1, 2, \dots, M$, the K_i coding vectors in user i's cache are linearly independent over $GF(q)$, and the K_T coding vector in the transmitting node's cache are linearly independent over $GF(q)$ as well.

(iii) For $i = 1, 2, \ldots, M$, $\mathbf{r}_i \in V_T + V_i$. This assumption precludes the situation that a user can never be satisfied, no matter what linear combinations are transmitted.

Assumption (iii) guarantees that a feasible solution exists. The objective of the generalized linear index coding problem is to find a feasible solution V with *minimum* dimension.

III. Reduction to a System of Multi-Variable Polynomial Equations

In this section we consider the decision version of the generalized linear index coding problem: given a positive integer d, can we find a feasible solution V of dimension d or less? In other words, we want to determine whether we can find d (not necessarily linearly independent) vectors in V_T, say $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_d$, and coefficients $x_{i,\ell}$ in $GF(q)$ ($i = 1, 2, \ldots, M$, $\ell = 1, 2, \ldots d$) such that

$$\mathbf{r}_i + x_{i,1}\mathbf{v}_1 + x_{i,2}\mathbf{v}_2 + \ldots + x_{i,d}\mathbf{v}_d \in V_i. \tag{2}$$

To this end, we introduce the notion of orthogonal complement. For two vectors $\mathbf{v} = (v_1, v_2, \ldots, v_N)$ and $\mathbf{u} = (u_1, u_2, \ldots, u_N)$ in $GF(q)^N$, let $\mathbf{v}\cdot\mathbf{u}$ denote the inner product

$$\mathbf{v}\cdot\mathbf{u} \triangleq v_1u_1 + v_2u_2 + \ldots v_Nu_N.$$

For a given subspace U in $GF(q)^N$, the set of vectors

$$U^\perp \triangleq \{\mathbf{v} \in GF(q)^N : \mathbf{v}\cdot\mathbf{u} = 0 \text{ for all } \mathbf{u} \in U\}$$

is a subspace and is called the *orthogonal complement* of U. We will use the property of orthogonal complement that a vector $\mathbf{w}$ is in U if and only if $\mathbf{w}\cdot\mathbf{u}' = 0$ for all $\mathbf{u}' \in U^\perp$.

When a basis of vector subspace U is given, we can calculate $U^\perp$ as follows. Let U be a subspace of $GF(q)^N$ and $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_D$ be a basis of U. We extend the basis of U to a basis of $GF(q)^N$ by appending $N - D$ vectors $\mathbf{u}_{D+1}, \mathbf{u}_{D+2}, \ldots \mathbf{u}_N$. We create an $N \times N$ matrix $\mathbf{M}$ by putting the vector $\mathbf{u}_j$ as the j-th column vector in $\mathbf{M}$. This matrix is non-singular because the vector $\mathbf{u}_j$'s are linearly independent. The $N-D$ columns on the right of the transpose of $\mathbf{M}^{-1}$ is a basis of $U^\perp$.

We re-write (2) as:

$$\mathbf{v}'\cdot\Big(\mathbf{r}_i + \sum_{\ell=1}^{d} x_{i,\ell}\mathbf{v}_\ell\Big) = 0 \quad \text{for all } \mathbf{v}' \in V_i^\perp. \tag{3}$$

Using the method described in the previous paragraph, we compute a basis of $V_i^\perp$. Let $\mathbf{v}'_{i,m}$, for $m = 1, 2, \ldots, N - K_i$, be a basis of $V_i^\perp$. It suffices to check (3) for $\mathbf{v}' = \mathbf{v}'_{i,m}$ for $m = 1, 2, \ldots, N - K_i$.

For $k = 1, \ldots, K_T$ and $\ell = 1, \ldots, d$, let $y_{j,k}$ be elements in $GF(q)$ such that

$$\mathbf{v}_\ell = y_{\ell,1}\mathbf{c}_1^{(T)} + y_{\ell,2}\mathbf{c}_2^{(T)} + \ldots + y_{\ell,K_T}\mathbf{c}_{K_T}^{(T)}. \tag{4}$$

Putting (4) into (3), we obtain a system of equations

$$(\mathbf{v}'_{i,m}\cdot\mathbf{r}_i) + \sum_{\ell=1}^{d}\sum_{k=1}^{K_T} x_{i,\ell}y_{\ell,k}(\mathbf{v}'_{i,m}\cdot\mathbf{c}_k^{(T)}) = 0 \tag{5}$$

for $i = 1, 2, \ldots, M$ and $m = 1, 2, \ldots, N - K_i$.

We note that the left-hand side of (5) is a quadratic polynomial with variables $x_{i,\ell}$'s and $y_{\ell,k}$'s. The quantities within the parentheses are constant. We summarize the main result in this section by the following theorem.

Theorem 1: Given V_T, V_i and $\mathbf{r}_i$ for $i = 1, 2, \ldots, M$, we can find a feasible solution V of dimension d or less if and only if we can solve the system of multi-variable polynomials equation in (5) for $i = 1, 2, \ldots, M$ and $m = 1, 2, \ldots, N-K_i$.

We illustrate the reduction by a simple example (see Fig. 3). There are $M = 5$ users and $N = 5$ source packets. The finite field size is $q = 2$. The transmitting node has all the five source packets $P_1, P_2, \ldots, P_5$. For $j = 1, 2, \ldots, N$, denote by $\mathbf{e}_j$ the j-th vector in the standard basis of $GF(q)^N$, i.e., the j-th component of $\mathbf{e}_j$ is 1 while the others are zero. For $i = 1, \ldots, 5$, user i wants the packet P_i, and we set $\mathbf{r}_i = \mathbf{e}_i$. The side-information of the 5 users is listed as follows. User 1 has packets P_2 and P_5. User 2 has packets P_1 and P_5. User 3 has packets P_2 and P_4. User 4 has packets P_2 and P_3. User 5 has a coded packet $P_1 + P_3 + P_4$. We have

$$V_T = \langle \mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3, \mathbf{e}_4, \mathbf{e}_5\rangle,\ V_1 = \langle \mathbf{e}_2, \mathbf{e}_5\rangle,\ V_2 = \langle \mathbf{e}_1, \mathbf{e}_5\rangle,$$
$$V_3 = \langle \mathbf{e}_2, \mathbf{e}_4\rangle,\ V_4 = \langle \mathbf{e}_2, \mathbf{e}_3\rangle,\ V_5 = \langle \mathbf{e}_1 + \mathbf{e}_3 + \mathbf{e}_4\rangle.$$

It is easy to verify that the followings are bases of the orthogonal complements of V_1 to V_5:

$$V_1^\perp = \langle \mathbf{e}_1, \mathbf{e}_3, \mathbf{e}_4\rangle,\ V_2^\perp = \langle \mathbf{e}_2, \mathbf{e}_3, \mathbf{e}_4\rangle,\ V_3^\perp = \langle \mathbf{e}_1, \mathbf{e}_3, \mathbf{e}_5\rangle$$
$$V_4^\perp = \langle \mathbf{e}_1, \mathbf{e}_4, \mathbf{e}_5\rangle,\ V_5^\perp = \langle \mathbf{e}_2, \mathbf{e}_5, \mathbf{e}_1 + \mathbf{e}_3, \mathbf{e}_3 + \mathbf{e}_4\rangle.$$

We want to determine whether the demands of all users can be satisfied by two coded packets. Let the coding vectors of these two packets be

$$\mathbf{v}_1 = \sum_{k=1}^{5} y_{1,k}\mathbf{e}_k, \quad \mathbf{v}_2 = \sum_{k=1}^{5} y_{2,k}\mathbf{e}_k$$

respectively. To satisfy the demand of the first user, we need to find $x_{1,1}$ and $x_{1,2}$ such that

$$\mathbf{e}_1 + x_{1,1}\mathbf{v}_1 + x_{1,2}\mathbf{v}_2 \in V_1.$$

By taking inner product with $\mathbf{e}_1$, $\mathbf{e}_3$ and $\mathbf{e}_4$, we obtain

$$1 + x_{1,1}y_{1,1} + x_{1,2}y_{2,1} = 0 \tag{6}$$
$$x_{1,1}y_{1,3} + x_{1,2}y_{2,3} = 0 \tag{7}$$
$$x_{1,1}y_{1,4} + x_{1,2}y_{2,4} = 0. \tag{8}$$

Similarly, by considering the requirement of users 2 to 5, we

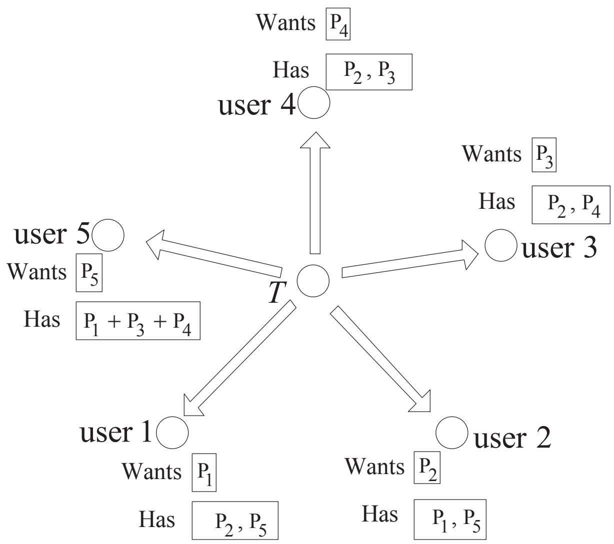

Fig. 3. An example of generalized linear index coding problem.

obtain the following equations,

$$1 + x_{2,1}y_{1,2} + x_{2,2}y_{2,2} = 0 \quad (9)$$
$$x_{2,1}y_{1,3} + x_{2,2}y_{2,3} = 0 \quad (10)$$
$$x_{2,1}y_{1,4} + x_{2,2}y_{2,4} = 0 \quad (11)$$
$$x_{3,1}y_{1,1} + x_{3,2}y_{2,1} = 0 \quad (12)$$
$$1 + x_{3,1}y_{1,3} + x_{3,2}y_{2,3} = 0 \quad (13)$$
$$x_{3,1}y_{1,5} + x_{3,2}y_{2,5} = 0 \quad (14)$$
$$x_{4,1}y_{1,1} + x_{4,2}y_{2,1} = 0 \quad (15)$$
$$1 + x_{4,1}y_{1,4} + x_{4,2}y_{2,4} = 0 \quad (16)$$
$$x_{4,1}y_{1,5} + x_{4,2}y_{2,5} = 0 \quad (17)$$
$$x_{5,1}y_{1,2} + x_{5,2}y_{2,2} = 0 \quad (18)$$
$$1 + x_{5,1}y_{1,5} + x_{5,2}y_{2,5} = 0 \quad (19)$$
$$x_{5,1}(y_{1,1} + y_{1,3}) + x_{5,2}(y_{2,1} + y_{2,3}) = 0 \quad (20)$$
$$x_{5,1}(y_{1,3} + y_{1,4}) + x_{5,2}(y_{2,3} + y_{2,4}) = 0. \quad (21)$$

We can check that

$$(y_{1,1}, y_{1,2}, y_{1,3}, y_{1,4}, y_{1,5}) = (1, 1, 0, 0, 1)$$
$$(y_{2,1}, y_{2,2}, y_{2,3}, y_{2,4}, y_{2,5}) = (0, 1, 1, 1, 0)$$
$$(x_{1,1}, x_{1,2}) = (x_{2,1}, x_{2,2}) = (1, 0)$$
$$(x_{3,1}, x_{3,2}) = (x_{4,1}, x_{4,2}) = (0, 1)$$
$$(x_{5,1}, x_{5,2}) = (1, 1).$$

is a solution to (6) to (21). The transmitting node can send two coded packets $P_1 + P_2 + P_5$ and $P_2 + P_3 + P_4$ in order to satisfy all users. For example, user 5 can decode P_5 by adding the two received packets and the coded packet in cache,

$$(P_1 + P_2 + P_5) + (P_2 + P_3 + P_4) + (P_1 + P_3 + P_4).$$

In general, solving a system of multi-variable quadratic equations is a difficult computational problem. Some algorithms (see e.g. [10]) from the cryptography community are available.

IV. A Suboptimal Solution with Coding Group

We have seen in the previous section that solving the linear index coding problem with minimum number of packet transmissions reduces to solving a system of quadratic polynomial equations, which is hard to solve in general. In this section, we present a suboptimal solution. We say that a set of users, say $\mathcal{A}$, form a *coding group* if we can find a vector $\mathbf{v}$ in V_T such that $\mathbf{r}_i \in \langle \mathbf{v} \rangle + V_i$ for all $i \in \mathcal{A}$. This means that all users in $\mathcal{A}$ can instantly decode the required packets after the packet corresponding to the coding vector $\mathbf{v}$ is received. For example, in the previous example, users 1 and 2 form a coding group, because they can decode packet 1 and packet 2 respectively if both of them receive the coded packet $P_1 + P_2$. The concept of coding group is closely related to the notion of *instantaneously decodable network code* [11] or *immediately decodable coding scheme* [12].

By assumption (iii) in Section II, every single user forms a coding group of size 1. It is obvious from the definition of coding group that if $\mathcal{A}$ is a coding group, then all non-empty subset of $\mathcal{A}$ is also a coding group. A coding group is called *maximal* if it is maximal with respect to set inclusion.

The idea in the suboptimal solution is to partition the users into coding groups. For example, in the previous example, we partition the five users into three groups, $\{1, 2\}, \{3, 4\}, \{5\}$. The transmitting node sends coded packet $P_1 + P_2$ to users 1 and 2, coded packet $P_3 + P_4$ to users 3 and 4, and packet P_5 to user 5. This solves the generalized linear index coding problem with three packet transmissions.

In the following, we show that this heuristic can be implemented efficiently when $q = 2$. Because $d = 1$, the equation in (5) reduces to

$$(\mathbf{v}'_{i,m} \cdot \mathbf{r}_i) + x_{i,1} \sum_{k=1}^{K_T} y_{1,k} (\mathbf{v}'_{i,m} \cdot \mathbf{c}_k^{(T)}) = 0. \quad (22)$$

By assumption (i) in Section II, for each $i \in \{1, 2, \ldots, M\}$, we have $\mathbf{v}'_{i,m} \cdot \mathbf{r}_i \neq 0$ for at least one m. Otherwise $\mathbf{r}_i$ would belong to V_i. Hence the variable $x_{i,1}$ in (22) must be equal to 1. A set of users $\mathcal{A}$ is a coding group if and only if we can solve the system of linear equation

$$(\mathbf{v}'_{i,m} \cdot \mathbf{r}_i) + \sum_{k=1}^{K_T} z_k (\mathbf{v}'_{i,m} \cdot \mathbf{c}_k^{(T)}) = 0. \quad (23)$$

for $i \in \mathcal{A}$ and $m = 1, 2, \ldots, N - K_i$, with variables $z_1, z_2, \ldots, z_{K_T}$ taking values in $GF(2)$. The system of linear equations can be solved efficiently, or shown to be inconsistent, by transforming it into the row-reduced echelon form.

The procedure for checking a coding group for general field size can be found in [13]. In the remaining of this paper, we focus on the case $q = 2$.

To facilitate the implementation of coding group heuristic, we define an undirected graph, G, called the *coding graph* as follows. Let $G = (\mathcal{V}, \mathcal{E})$ be an undirected graph with vertex set $\mathcal{V} = \{1, 2, \ldots, M\}$. Each vertex is identified with a user. Two vertices are adjacent if and only if the two corresponding users form a coding group of size two. The coding graph is constructed by checking each pair of distinct vertices, and see whether they form a size-two coding group. If a group of users is a coding group, then the corresponding vertices in the coding graph form a clique. The converse is however not true.

We can obtain a maximal coding group using the following heuristic. We first compute the coding graph, and pick a vertex v with smallest degree (with tie broken arbitrarily). We try to find a coding group $\mathcal{C}$ containing the vertex v. We initialize the algorithm by setting $\mathcal{C} = \{v\}$ and proceed iteratively. In each iteration, we identify the vertices in the coding graph which are adjacent to all vertices in $\mathcal{C}$. Let this set of vertices be $\mathcal{U}$. If we cannot form a larger coding group by adding a vertex from $\mathcal{U}$ to $\mathcal{C}$, then $\mathcal{C}$ is a maximal coding group. Otherwise, we choose a vertex in $\mathcal{U}$, say x, that has smallest degree in the coding graph, such that $\mathcal{U} \cup \{x\}$ is a coding group.

The procedure of partitioning the set of users into coding groups is summarized in Algorithm 1. We let $\mathcal{B}_T$ be a basis of V_T and for $i = 1, 2, \dots, M$, let $\mathcal{B}_i$ be a basis of V_i.

Algorithm 1 Partition($\mathcal{V}, \mathcal{B}_T, \mathcal{B}_i, \mathbf{r}_i$ for $i \in \mathcal{V}$)

Input: The set of users $\mathcal{V}$, a basis $\mathcal{B}_T$ of V_T, a basis $\mathcal{B}_i$ for user $i \in \mathcal{V}$ and the required coding vector $\mathbf{r}_i$ of user $i \in \mathcal{V}$.
Output: A partition of $\mathcal{V}$ into coding groups

1: **if** $\mathcal{V}$ is the empty set **then**
2:     return $\emptyset$
3: **end if**
4: Compute the coding graph G with vertex set $\mathcal{V}$.
5: Initialize $\mathcal{C} \leftarrow \emptyset$, $\mathcal{U} \leftarrow \mathcal{V}$.
6: **repeat**
7:     Choose $x \in \mathcal{U}$ which has the smallest degree in G
8:     **if** $\{x\} \cup \mathcal{C}$ form a coding group **then**
9:         $\mathcal{C} \leftarrow \mathcal{C} \cup \{x\}$
10:     **end if**
11:     $\mathcal{U} \leftarrow \{v \in \mathcal{U} \setminus \{x\} : v$ is adjacent to all vertices in $\mathcal{C}\}$
12: **until** $\mathcal{U}$ is empty
13: Let $\mathbf{v}$ be a coding vector for the coding group $\mathcal{C}$.
14: For user $j \in \mathcal{V} \setminus \mathcal{C}$, augment the basis $\mathcal{B}_j$ by the coding vector $\mathbf{v}$
15: return $\{\mathcal{C}\} \cup$ Partition($\mathcal{V} \setminus \mathcal{C}, \mathcal{B}_T, \mathcal{B}_j, \mathbf{r}_j$ for $j \in \mathcal{V} \setminus \mathcal{C}$)

V. Application to the Broadcast Relay Channel

We evaluate the heuristic algorithm in a broadcast relay channel with erasure. Let M be the number of users. In this simulation study, we only consider finite field of size 2, i.e., $q = 2$. We assume that the relay is closer to the users then the source, so that the links from the relay node to the users are more reliable. We model the link between the source node to the relay node or a user as a erasure channel. Each transmitted packet is received successfully with probability $1 - \epsilon$, and is erased with probability ϵ, where ϵ is a constant between 0 and 1. The links from the source the relay and users are assumed to be statistically independent. The links between the relay and the users are modeled as perfect data links with no erasure, i.e., if a packet is transmitted by the relay node, all users can receive it correctly without any error. Initially, the source holds M source data packets, while the relay node has no packet in its cache. For $i = 1, 2, \dots, M$, user i wants to download packet i from the source node with the help of the relay.

We remark that in [14] the capacity of the broadcast erasure network without relay is studied. Although the basic setting is similar, there are several features that are different. First of all, the packet erasure probability is assumed known to the source node, i.e., perfect channel-state information is assumed. The transmission schemes considered in this work do not need to know the packet erasure probability. Secondly, the transmission scheme in [14] requires block length approaching infinity in order to achieve the ϵ-capacity of the broadcast erasure channel, while the schemes in this work aim at minimizing the time a user has to wait until he/she can decode the required packet (with probability 1). The work in [14] and the schemes in this paper cannot be compared directly.

In this paper we compare with two uncoded schemes. The first one does not utilize the relay node while the second one does. In the first uncoded scheme, the source node sends packets to the users one by one. For each user, the source node sends the required packet repeatedly until an acknowledgment (ACK) from the user is received. The expected number of packet transmissions for M users is

$$M/(1 - \epsilon). \tag{24}$$

In the second uncoded scheme, the relay is enabled. The source node also sends packets to the users one by one. If the user can receive the packet successfully, then he returns an ACK to the source node. If the user cannot receive the packet but the relay node does, then relay sends the packet to the users and returns an ACK to the source node. The source node sends out the required packet repeatedly until it receives an ACK from either the user or the relay node. A simple exercise shows that the expected number of packet transmissions is

$$M(1 + \epsilon - \epsilon^2)/(1 - \epsilon^2). \tag{25}$$

We compare three transmission schemes with coded packets. In the first coded scheme, called *Scheme A*, the relay node is not utilized. The transmission is divided into two phases. In the first phase, the source node sends each of the M packets once, regardless whether they are correctly received or not. The M users report to the source node whether their packets are received successfully or not. A satisfied user can leave the system if his/her packet is received successfully in the first phase. In the second phase, if there are at least one unsatisfied user, the source node finds a maximal coding group and send a packet for this coding group, and repeats until all remaining users are satisfied. The maximal coding group is obtained by steps 4 to 13 in Algorithm 1. After each packet transmission, the users who get their packets successfully send ACK to the source node, and the source node updates the users' side information. The updated side information is used in generating maximal coding group.

The second coded scheme is called *Scheme B*. The transmission in Scheme B is divided into three phases. The first

	$\epsilon = 0.3$	$\epsilon = 0.5$	$\epsilon = 0.7$
Uncoded scheme without relay	17.1	24	40
Scheme A	15.4	19.9	32.7
Scheme B	15.9	21.5	34.2
Uncoded scheme with relay	16.0	20	28.5
Scheme C	14.8	17.8	25.2

TABLE I
COMPARISON OF TRANSMISSION SCHEMES FOR THE BROADCAST RELAY CHANNEL WITH $M = 12$ USERS.

phase is the same as in Scheme A, i.e., the source node sends each of the M source packets once. In the second phase, the source node linearly mixes the source packets in a random manner, and sends the resultant coded packets. The coefficients of the random linear combinations are generated uniformly and independently. The second phase continues until the relay node can take over the role of transmitter, i.e., until the condition in (1) is satisfied. In the third phase, the relay node partitions the remaining users into coding groups by Algorithm 1, and sends the corresponding coded packets for the coding groups.

The last coded scheme, called *Scheme C*, is similar to Scheme B, except that in the second phase the source node computes maximal coding groups according to steps 4 to 13 in Algorithm 1, and sends the corresponding coded packets for the maximal coding groups instead of randomly coded packets.

In Table I, we compare the expected number of packet transmissions of the above five transmission schemes for 12 users, with link erasure probability equal to 0.3, 0.5 and 0.7. The performance curves for $\epsilon = 0.1, 0.3, 0.5, 0.6, 0.7, 0.8, 0.85$ and 0.9 are plotted in Fig 4. The expected number of of packet transmissions of the two uncoded schemes, shown in dashed lines, are computed from (24) and (25). Schemes A, B and C are in solid lines. Each data point is obtained by averaging over 1000 random channel instances.

Comparing the uncoded scheme with relay and Scheme C, we see that the network coding in the relay can reduce the number of packet transmissions by roughly 10%. We note that the performance of Scheme B is much worse than Scheme C, and is roughly the same as Scheme A in which the relay node is disabled. The only difference between Scheme B and Scheme C is the second phase. The empirical results thus show that coding for coding groups in the second phase is essential.

VI. CONCLUSION

We generalize linear index coding by considering coded packets as side information. It is applied to the broadcast relay channel using the concept of coding group and coding graph. Simulation results show that transmission scheme with generalized linear index coding can reduce the number of packet transmissions by 10%. The simulation in this paper is performed for the binary field only. Further reduction of packet transmissions is possible by working over a larger finite field, at the expense of higher complexity of implementation. The performance for larger field size is an interesting direction for future study.

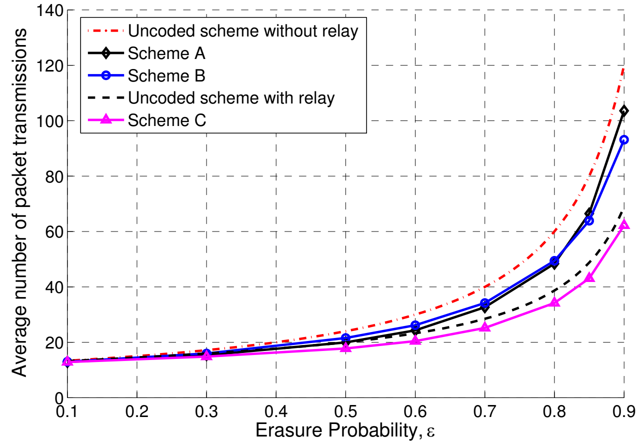

Fig. 4. Average number of packet transmissions of the five transmission schemes with $M = 12$ users.

ACKNOWLEDGEMENTS

We would like to thank the anonymous reviewers for their careful reading and helpful comments.

REFERENCES

[1] Y. Birk and T. Kol, "Informed-source coding-on-demand (ISCOD) over broadcast channels," in *Proc. IEEE INFOCOM*, San Francisco, Mar. 1998, pp. 1257–1264.
[2] Z. Bar-Yossef, Y. Birk, T. S. Jayram, and T. Kol, "Index coding with side information," *IEEE Trans. Inform. Theory*, vol. 57, no. 3, pp. 1479–1494, Mar. 2011.
[3] M. Langberg and A. Sprintson, "On the hardness of approximating the network coding capacity," in *Proc. IEEE Int. Symp. on Inform. Theory*, Toronto, Jul. 2008, pp. 315–319.
[4] R. Peeters, "Orthogonal representations over finite fields and the chromatic number of graphs," *Combinatorica*, vol. 16, no. 3, pp. 417–431, 1996.
[5] S. H. Dau, V. Skachek, and Y. M. Chee, "Optimal index codes with near-extreme rates," http://arxiv.org/pdf/1202.1150v1.pdf, Feb. 2012.
[6] L. Ong and C. K. Ho, "Optimal index codes for a class of multicast networks with receiver side information," http://arxiv.org/pdf/1204.0867v1.pdf, Apr. 2012.
[7] N. Alon, A. Hassidim, E. Lubetzky, U. Stav, and A. Weinstein, "Broadcasting with side information," in *the 49th IEEE Symp. on Foundations of Computer Sci.*, 2008, pp. 823–832.
[8] S. El Rouayheb, A. Sprintson, and C. Georghiades, "On the index coding problem and its relation to network coding and matroid theory," *IEEE Trans. Inform. Theory*, vol. 56, no. 7, pp. 3187–3195, Jul. 2010.
[9] T. A. Courtade and R. D. Wesel, "Coded cooperative data exchange in multihop networks," http://arxiv.org/pdf/1203.3445v1.pdf, Mar. 2012.
[10] N. Courtois, L. Goubin, W. Meier, and J.-D. Tracier, "Solving underdefined systems of multivariate quadratic equations," in *Public Key Cryptography - PKC'02, Proc. of the 5th Int. Workshop on Practice and Theory in Public Key Cryptosystems*, ser. Lecture notes in Computer science, vol. 2274, 2003, pp. 211–227.
[11] D. Traskov, M. Médard, P. Sadeghi, and R. Kötter, "Joint scheduling and instantaneously decodable network coding," in *IEEE Global Telecom. Conf. (GLOBECOM)*, Dec. 2009, pp. 1–6.
[12] X. Li, C.-C. Wang, and X. Lin, "On the capacity of immediately-decodable coding schemes for wireless stored-video broadcast with hard deadline constraints," *IEEE J. on Selected Areas of Comm.*, vol. 29, no. 5, pp. 1094–1105, May 2011.
[13] M. Dai, K. W. Shum, and C. W. Sung, "Linear index coding with coded packets in cache," paper in preparation.
[14] C.-C. Wang, "On the capacity of 1-to-K broadcast packet erasure channels with channel output feedback," *IEEE Trans. Inform. Theory*, vol. 58, no. 2, pp. 931–956, Feb. 2012.