Towards the Capacity Region of Multiplicative Linear Operator Broadcast Channels

Yimin Pang
Department of Information Science
and Electronic Engineering
Zhejiang University
Hangzhou, China, 310027
Email: yimin.pang@zju.edu.cn

Thomas Honold*
Department of Information Science
and Electronic Engineering
Zhejiang University
Hangzhou, China, 310027
Email: honold@zju.edu.cn

Abstract—Recent research indicates that packet transmission employing random linear network coding can be regarded as transmitting subspaces over a linear operator channel (LOC). In this paper we propose the framework of linear operator broadcast channels (LOBCs) to model packet broadcasting over LOCs, and we do initial work on the capacity region of constant-dimension multiplicative LOBCs (CMLOBCs), a generalization of broadcast erasure channels. Two fundamental problems regarding CMLOBCs are addressed—finding necessary and sufficient conditions for degradation and deciding whether time sharing suffices to achieve the boundary of the capacity region in the degraded case.

Index Terms—linear operator channel, network coding, broadcast channel, capacity region, superposition coding, subspace codes

I. INTRODUCTION

Random linear network coding [1] is an efficient alternative to achieve the network capacity proposed in [2]. In a random linear network coding channel packets are transmitted in generations and are regarded as n-dimensional row vectors over some finite field \( \mathbb{F}_q \). Due to the subspace preserving property, packet transmission over an acyclic noisy network may be thought of as conveying subspaces over a linear operator channel (LOC) [3], whose input and output symbols are taken from the set of all subspaces of \( \mathbb{F}_q^m \) (referred to as “ambient space”). In [4] Silva et al. investigated the capacity of a random linear network coding channel with matrices as input/output symbols. Later, by regarding a LOC as a particular DMC, Úchôa-Filho and Nóbrega [5] studied the capacity of constant-dimension multiplicative LOCs (CMLOCs), a generalization of broadcast erasure channels. Two fundamental problems regarding CMLOCs are addressed—finding necessary and sufficient conditions for degradation and deciding whether time sharing suffices to achieve the boundary of the capacity region in the degraded case.

In this paper we propose the framework of linear operator broadcast channels (LOBCs) to model packet broadcasting over LOCs, and we do initial work on the capacity region of multiple source access LOCs was investigated. In [8] the general non-constant multiplicative LOC capacity. In [8] the Uchôa-Filho and Nóbrega [5] studied the capacity of constant symbols. Later, by regarding a LOC as a particular DMC, linear network coding channel with matrices as input/output space”). In [4] Silva et al. investigated the capacity of a random linear network coding channel with matrices as input/output symbols. In [4] the rate region of multiple source access LOCs was investigated.

We will denote the set of all i-dimensional subspaces of \( \mathbb{F}_q^m \) by \( \mathcal{P}(\mathbb{F}_q^m, i) \). The following notation will be used in the sequel. Symbols X, Y and U denote random variables with values from subspace alphabets \( \mathbb{F}_q \), \( \mathcal{Y} \), respectively \( U \). The symbols X, Y and U denote subspaces in \( \mathbb{F}_q \), \( \mathcal{Y} \) and \( U \), respectively.

Constant-dimension multiplicative LOCs (CMLOCs) deserve our interest, since they capture most packet transmission scenarios. A precise definition of CMLOCs from the information theory point-of-view is the following.

Definition 1. A constant-dimension multiplicative LOC (CMLOC) of constant dimension \( l \) is a discrete memoryless channel (DMC) with input alphabet \( \mathcal{X} = \mathcal{P}(\mathbb{F}_q^m, l) \), output alphabet \( \mathcal{Y} = \bigcup_{i=0}^{l} \mathcal{P}(\mathbb{F}_q^m, i) \) and transfer probabilities

\[
 p(Y|X) = p_{Y|X}(Y|X) = p(Y = Y|X = X) \quad (X \in \mathcal{X}, Y \in \mathcal{Y})
\]

satisfying

\[
 p(Y|X) = \left\{ \begin{array}{ll}
 \frac{\dim(Y)}{\dim(X)} & \text{if } Y \subseteq X, \\
 0 & \text{otherwise.}
\end{array} \right.
\]

Here \( \epsilon_i, 0 \leq i \leq l, \) denotes the probability of receiving an i-dimensional subspace, and \( \binom{m}{l} \) is the familiar Gaussian binomial coefficient.

Our definition of a CMLOC is slightly different from that in [5], where instead of \( \epsilon \) the rank deficiency distribution \( p_{Y}(i) \) (related to our distribution by \( p_{Y}(i) = \epsilon_{l-i} \)) occurs. In our case the total erasure probability is \( \epsilon_0 + \epsilon_1 + \cdots + \epsilon_{l-1} = 1 - \epsilon_l \), and \( \epsilon_l \) is the probability of error-free transmission. The capacity of a CMLOC is given in [5] Th. 4.

As we know, only packet multicasting benefits from network coding and on the other hand multicasting at a constant rate would either starve receivers with high band-width or overwhelm those with a poor connection. This provides our motivation to investigate broadcasting over LOCs.

Basic knowledge on broadcast channels can be found in [9–11]. Recent work showed that the computation of the capacity region of a discrete memoryless degraded broadcast channel is a non-convex DC problem [12]. Later Yasui et al. [13] applied the Arimoto-Blahut algorithm [14, 15] for numerically computing the channel capacity.

The framework of general Linear Operator Broadcast Channels (LOBCs) is presented in Section II with emphasis on constant-dimension multiplicative LOBCs (CMLOBCs), a generalization of the well-known binary erasure broadcast channel (BEBC). Two fundamental questions about CMLOBCs are addressed: First, when will a CMLOBC be stochastically degraded? While for BEBCs the solution is quite obvious, for CMLOBCs the rich structure of possible erasures...
makes the problem quite intriguing. Our discussion is detailed in Section III. Second, in the case of a degraded CMLOBC this is not always true and further discuss the shape of the capacity region of CMLOBCs with subspaces taken from the projective plain PG(2, 2). Plenty of numerical analysis are shown on different cases of CMLOBCs over PG(2, 2), via Arimoto-Blahut type algorithm in [13]. Section V concludes the paper. Proofs can be found in the appendix (Section VII).

II. LINEAR OPERATOR BROADCAST CHANNELS (LOBCs)

A. LOBC Module

We consider the case of a multiple user LOC where a sender communicates with $K$ receivers $u_1, u_2, ..., u_K$ simultaneously. The subchannels from the sender to $u_k$, $k = 1, 2, ..., K$, are linear operator channels with input and output alphabets $X, Y_i \subseteq \mathbb{F}_q^n$, where $m$ and $q$ are fixed. Let $X, Y_1, ..., Y_K$ be the corresponding random variables. The output at every receiver is taken subject to some joint transfer probability distribution $p(Y_1, Y_2, ..., Y_K|X) = p(Y_1 = Y_1, Y_2 = Y_2, ..., Y_K = Y_K|X = X)$. Such a channel is called Linear Operator Broadcast Channel (LOBC). For simplicity we restrict ourselves to a LOBC with two receivers and let $\mathcal{M}_1, \mathcal{M}_2$ be the alphabets of private messages for user $u_1$ and $u_2$, respectively.

Definition 2. A broadcast (multishot) subspace code of length $n$ for the LOBC consists of a set $\mathcal{C} \subseteq \mathbb{F}_q^n$ of codewords and a corresponding encoder/decoder pair. The LOBC encoder $\gamma : \mathcal{M}_1 \times \mathcal{M}_2 \rightarrow \mathcal{C}$ maps a message pair $(M_1, M_2)$ to a codeword $X = (X_1, ..., X_n) \in \mathcal{C}$ (for every transmission generation). The LOBC decoder $\delta = (\delta_1, \delta_2)$ consists of two decoding functions $\delta_i : \mathcal{Y}^n \rightarrow \mathcal{M}_i$ ($i = 1, 2$) and maps the corresponding pair $(Y_1, Y_2) \in \mathcal{Y}^n \times \mathcal{Y}^n$ of received words to the message pair $(M_1, M_2) = (\delta_1(Y_1), \delta_2(Y_2))$.

The rate pair $(R_1, R_2)$, in unit of $q$-ary symbols per subspace transmission, of the broadcast subspace code is defined as

$$R_1 = \frac{\log_q |\mathcal{M}_1|}{n}, \quad R_2 = \frac{\log_q |\mathcal{M}_2|}{n}. \quad (2)$$

As in [9 Ch. 14.6] we can rewrite the encoding map as

$$\gamma : (1, 2, ..., q^{nR_1}) \times (1, 2, ..., q^{nR_2}) \rightarrow \mathcal{C}$$

and associate with the broadcast subspace code the parameters $((q^{nR_1}, q^{nR_2}), n)$.

Definition 3. A rate pair $(R_1, R_2)$ is said to be achievable if there exists a sequence of $((q^{nR_1}, q^{nR_2}), n)$ broadcast subspace codes, for which the corresponding probabilities $p_n = p_n(M_1 \neq M_1 \lor M_2 \neq M_2)$ of decoding error satisfy $p_n \rightarrow 0$ when $n \rightarrow \infty$. The capacity region (or rate region) of a LOBC is defined as the closure of the set of all achievable rate pairs.

B. CMLOBCs

If every subchannel in a LOBC is a CMLOC (necessarily with the same $l$, cf. Def. [1]), we call it a constant-dimension multiplicative LOBC (CMLOBC). For CMLOBCs with ambient space $\mathbb{F}_q^m$ and constant dimension $l$ the normalized rate pair $(R_1, R_2)$ can be defined in accordance with [2] as

$$R_1 = \frac{\log_q |\mathcal{M}_1|}{lmn}, \quad R_2 = \frac{\log_q |\mathcal{M}_2|}{lmn}. \quad (3)$$

By the principle of time division, it is clear that the capacity region of a CMLOBC should be at least the triangle area with three corner points $-(0,0), (C_2,0)$ and $(0, C_1)$ on the $(R_1, R_2)$ plane, where $C_i$ refers to the channel capacity of $X \rightarrow Y_i$, and all points $(R_1, R_2)$ satisfy $R_1/C_1 + R_2/C_2 = 1$ and $R_1 \geq 0$ constitute the so called time sharing line.

III. DEGRADATION THEOREM FOR CMLOBCs

The following definition of degraded broadcast channels is taken from [11].

Definition 4. A CMLOBC with transfer probabilities $p(Y_1, Y_2|X)$ is said to be (stochastically) degraded if the conditional marginals $p(Y_1|X)$, $p(Y_2|X)$ are related by $p(Y_2|X) = \sum_{Y_1} p(Y_1|X)p(Y_2|Y_1)$ for some conditional distribution $p(Y_2|Y_1)$.

From Def. [1] it is obvious that CMLOBCs with $(m, q, l) = (2, 2, 1)$ (the smallest nontrivial examples) are equivalent to ternary erasure broadcast channels with erasure probabilities $\epsilon_0$, $\epsilon_1$ for the two subchannels. Like a BEBC such broadcast channels are always degraded. In general, however, CMLOBCs are not degraded. Theorem [1] in this section gives a necessary and sufficient condition for a CMLOBC to be degraded. For its proof we need several lemmas.

Lemma 1. Let $\epsilon^{(1)} = (\epsilon_0^{(1)}, \epsilon_1^{(1)}, ..., \epsilon_l^{(1)})$ and $\epsilon^{(2)} = (\epsilon_0^{(2)}, \epsilon_1^{(2)}, ..., \epsilon_l^{(2)})$ be probability vectors. Then the following two statements are equivalent:

(i) $\sum_{j=0}^l \epsilon_j^{(1)} \leq \sum_{j=0}^l \epsilon_j^{(2)}$ for $0 \leq i \leq l$

(ii) There exists a lower triangular stochastic matrix $\Lambda$ (such that $\epsilon^{(1)} = \epsilon^{(2)}$)

Proof: See Appendix [VII-A].

For $0 \leq l, s \leq m$ let $D_{ls}$ be the incidence structure “$l$-dimensional vs. $s$-dimensional subspaces of $\mathbb{F}_q^m$ with respect to set inclusion”. Relative to suitable orderings of the input and output alphabet, the channel matrix of the CMLOC of constant dimension $l$ with probability vector $\epsilon = (\epsilon_0, \epsilon_1, ..., \epsilon_l)$ can be partitioned as

$$S = (\epsilon_0 S_{00} | \epsilon_1 S_{11} | \cdots | \epsilon_l S_{ll}) \quad (4)$$

where $S_{ls}$ ("stochastic incidence matrix" of $D_{ls}$) denotes an appropriate scalar multiple of the incidence matrix of $D_{ls}$,
determined by the requirement that \( S_{ls} \) be a (row) stochastic matrix.

**Lemma 2.** For integers \( l, s, t \in \{0, 1, \ldots, m\} \) with \( l \geq s \geq t \) we have \( S_{ls}S_{st} = S_{lt} \).

**Proof:** See Appendix VII-B

A CMLOBC with subchannels having channel matrices \( S^{(1)}, S^{(2)} \) is degraded if and only if there exists a stochastic matrix \( T \in \mathbb{R}^{M \times M} \) (where \( M = \sum_{s=0}^{m} \binom{m}{s} \)) such that \( S^{(2)} = S^{(1)}T \) (see [9, Ch. 14.6]). Partitioning \( S^{(1)}, S^{(2)} \) as in (4) and \( T \) accordingly, we can write this as

\[
\begin{pmatrix}
\epsilon^{(1)}_0 S_{l0} & \epsilon^{(1)}_1 S_{l1} & \cdots & \epsilon^{(1)}_l S_{ll} \\
\epsilon^{(2)}_0 S_{l0} & \epsilon^{(2)}_1 S_{l1} & \cdots & \epsilon^{(2)}_l S_{ll}
\end{pmatrix}
\]

\[
= \begin{pmatrix}
\begin{pmatrix}
T_{00} & T_{01} & \cdots & T_{0l} \\
T_{10} & T_{11} & \cdots & T_{1l} \\
\vdots & \vdots & \ddots & \vdots \\
T_{l0} & T_{l1} & \cdots & T_{ll}
\end{pmatrix}
\end{pmatrix}
\]

With these preparations it is possible to prove

**Theorem 1.** Let \( \epsilon^{(1)} \) and \( \epsilon^{(2)} \) be probability vectors associated with the two subchannels \( X \rightarrow Y_1 \) and \( X \rightarrow Y_2 \), respectively, of a CMLOBC with ambient space \( \mathbb{F}^m_q \) and constant dimension \( l < m \). The CMLOBC is degraded (in the sense that \( Y_2 \) is a degraded version of \( Y_1 \)) if and only if \( \epsilon^{(1)} \) and \( \epsilon^{(2)} \) satisfy

\[
\sum_{j=0}^{i} \epsilon^{(1)}_j \leq \sum_{j=0}^{i} \epsilon^{(2)}_j \quad \text{for } 0 \leq i \leq l \]  

**Proof:** See Appendix VII-C

The excluded case \( l = m \) is indeed exceptional: In this case there is only one input subspace, so that the channel matrices reduce to probability vectors \( s^{(1)}, s^{(2)} \) of length \( M \), where \( M = \sum_{s=0}^{m} \binom{m}{s} \) is the total number of subspaces of \( \mathbb{F}^m_q \). However any two probability vectors \( s^{(1)}, s^{(2)} \) are related by \( s^{(1)}T = s^{(2)} \) for some stochastic matrix \( T \) of the appropriate size. (The matrix \( T = js^{(2)} \), where \( j \) is the all-one column vector of the same dimension as \( s \), does the job.) This shows that in the case \( l = m \) the broadcast channel is degraded for all choices of \( \epsilon^{(1)}, \epsilon^{(2)} \).

**Corollary 1.** Under the assumptions of Th. 1 suppose that \( \epsilon^{(1)} \) and \( \epsilon^{(2)} \) satisfy

\[
\epsilon^{(1)}_i \leq \epsilon^{(2)}_i \quad \text{for every } i \in \{0, 1, 2, \ldots, l-1\}.
\]

(and consequently \( \epsilon^{(1)}_l \geq \epsilon^{(2)}_l \)) Then the CMLOBC is degraded (in the sense that \( Y_2 \) is a degraded version of \( Y_1 \)).

**Remark 1.** If Case (i) holds for a degraded CMLOBC, then there exist superposition coding schemes which are superior to time sharing with respect to channel throughput. On the other hand, the family of joint distributions (1) does not necessarily determine the boundary of the capacity region. In particular we cannot conclude that in Case (ii) or (iii) of Lemma 3 the boundary is the time-sharing line.

### IV. The Capacity Region of Degraded CMLOBCs over the Projective Plane PG(2, 2)

#### A. Degraded CMLOBCs over the Projective Plane PG(2, 2)

Let \( q = 2, m = 3, l = 2 \) and \( p(Y_i | X_i), i = 1, 2 \), be defined through the channel matrices

\[
S^{(i)} = (\epsilon^{(i)}_0 J_{7 \times 1} | \epsilon^{(i)}_1 S_{21} | \epsilon^{(i)}_2 I_{7 \times 7}),
\]

where \( J_{7 \times 1}, I_{7 \times 7} \) denote the all-one, respectively, the identity matrix of the indicated sizes and \( S_{21} \) is a stochastic incidence matrix of 2-dimensional vs. 1-dimensional subspaces of \( \mathbb{F}_2^3 \) (in other words, an incidence matrix of the smallest projective plane \( PG(2, 2) \)). For example, we can take

\[
S_{21} = \frac{1}{3} \begin{pmatrix}
1 & 1 & 0 & 1 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 1 & 0 & 0 \\
0 & 1 & 1 & 0 & 0 & 1 & 0 \\
0 & 0 & 1 & 1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 0
\end{pmatrix}
\]

By Th. 1 the CMLOBC is degraded if and only if \( \epsilon^{(1)}_0 \leq \epsilon^{(2)}_0 \cap (\epsilon^{(1)}_1 + \epsilon^{(1)}_2 \leq \epsilon^{(2)}_1 + \epsilon^{(2)}_2 ) \) or, equivalently, \( \epsilon^{(1)}_0 \leq \epsilon^{(2)}_0 \cap (\epsilon^{(1)}_1 \geq \epsilon^{(2)}_1 ) \).

Taking into account symmetry properties and keeping in mind the example of binary symmetric broadcast channels discussed in [9, Ch. 14.6], one might conjecture that the boundary of the rate region is obtained by taking the joint distribution \( p(U, X) \) which arises from a 7-ary symmetric channel \( U \rightarrow X \) and the uniform input distribution on \( U \). This one-parameter family of distributions can be written in matrix form as

\[
(p(U_i, X_j)) = \frac{1}{7} \left( \frac{2}{6} J_{7 \times 7} + \left(1 - \frac{2}{6} \right) I_{7 \times 7} \right), \quad 0 \leq \sigma \leq \frac{6}{7}.
\]

**Lemma 3.** For the degraded CMLOBCs described by (8), let \( p_{0, X}(U, X) \) be chosen as in (10), and with \( R_1(\sigma) = I(X, Y_1 | U), R_2(\sigma) = I(U, Y_2) \) let \( \Gamma = \{(R_1(\sigma), R_2(\sigma)) | \sigma \in [0, 6/7]\} \). Then the curve \( \Gamma \) is considered as a function \( R_2 = f(R_1) \) is defined on \( [0, C_1] \), strictly decreasing, and satisfies \( f(0) = C_2, f(C_1) = 0 \). Further we have:

(i) \( f \) is strictly concave \((\gamma)\) when \( \epsilon^{(1)}_1 \epsilon^{(2)}_2 > \epsilon^{(1)}_2 \epsilon^{(2)}_1 \);

(ii) \( f \) is strictly convex \((\cup)\) when \( \epsilon^{(1)}_1 \epsilon^{(2)}_2 < \epsilon^{(1)}_2 \epsilon^{(2)}_1 \);

(iii) \( f \) is linear (i.e. \( \Gamma \) coincides with the time-sharing line) when \( \epsilon^{(1)}_1 \epsilon^{(2)}_2 = \epsilon^{(1)}_2 \epsilon^{(2)}_1 \).

**Proof:** See Appendix VII-D
B. Numerical Analysis

In each figure about the capacity region of some CMLOBC, we use a “filter” to delete points located below the time sharing line on the rate region plane and we always display two subfigures “before filter” and “after filter” at the same time. All the figures have enough pixel information to allow enlarging details. Relevant M-files can be found at [17]. Our analysis was done using MATLAB on a Linux system.

**Example 1.** Let \( \epsilon^{(1)} = (0.05, 0.24, 0.71) \), \( \epsilon^{(2)} = (0.30, 0.15, 0.55) \). Then the condition of Case (i) is satisfied. Numerical results obtained by using the Arimoto-Blahut type algorithm from [13] are shown in Fig. 1.

Figure 1: Capacity region of Example 1, \( \epsilon^{(1)} = (0.05, 0.24, 0.71) \), \( \epsilon^{(2)} = (0.30, 0.15, 0.55) \).

**Example 2.** Let \( \epsilon^{(1)} = (0.05, 0.20, 0.75) \), \( \epsilon^{(2)} = (0.30, 0.15, 0.55) \), the condition of case (ii) is satisfied. Numerical results are shown in Fig. 2 indicating that time sharing might be sufficient to exhaust the capacity region.

Figure 2: Capacity region of Example 2, \( \epsilon^{(1)} = (0.05, 0.20, 0.75) \), \( \epsilon^{(2)} = (0.30, 0.15, 0.55) \).

**Example 3.** Let \( \epsilon^{(1)} = (\rho_1^2, \rho_1, 1-\rho_1-\rho_1^2) \), \( \epsilon^{(2)} = (\rho_2^2, \rho_2, 1-\rho_2-\rho_2^2) \), where \( 0 \leq \rho_1 \leq \rho_2 \leq (-1+\sqrt{5})/2 \). This corresponds to Case (ii). Numerical results are shown in Fig. 3 for the particular case \( \rho_1 = 0.1, \rho_2 = 0.3 \) indicating that time sharing is sufficent to exhaust the capacity region.

Figure 3: Capacity Region of Example 3, \( \epsilon^{(1)} = (0.01, 0.1, 0.89) \), \( \epsilon^{(2)} = (0.09, 0.3, 0.61) \).

**Example 4.** Let \( q = 2, m = 3, l = 2 \), and define \( \epsilon^{(1)} = (0, \rho_1, 1-\rho_1) \), \( \epsilon^{(2)} = (0, \rho_2, 1-\rho_2) \), with \( 0 \leq \rho_1 \leq \rho_2 \leq 1 \), the condition of case (ii) is satisfied. Numerical results are shown in Fig. 4 for the particular case \( \rho_1 = 0.1, \rho_2 = 0.3 \) indicating that time sharing is suffice to exhaust the capacity region.

Figure 4: Capacity Region of Example 4, \( \epsilon^{(1)} = (0, 0.1, 0.9) \), \( \epsilon^{(2)} = (0, 0.3, 0.7) \).

C. A Conjecture on the Convexity of Capacity Region

Overall the analysis supports the conclusion that super-position coding on CMLOBCs has no benefit over simple time-sharing unless we are in Case (i). However, proving the conjecture in full generality seems to be difficult.

**Conjecture.** For the degraded CMLOBCs described by [8], the capacity region is strictly concave (\( \cap \)) if and only if \( \epsilon^{(1)}, \epsilon^{(2)} > \epsilon^{(1)} > \epsilon^{(2)} \).

D. A special example–The 7-ary erasure broadcast channel

**Example 5.** Let \( \epsilon^{(1)} = (\rho_1, 0, 1-\rho_1) \), \( \epsilon^{(2)} = (\rho_2, 0, 1-\rho_2) \), where \( 0 \leq \rho_1 \leq \rho_2 \leq 1 \). Then the condition of Case (iii) is satisfied. Since (apart from unused output subspaces) there is now only one erasure symbol (the output subspace \{0\}), the subchannels of the CMLOBC become 7-ary erasure channels.

The capacity region of this broadcast channel, more generally of any CMLOBC with \( \epsilon^{(i)} = (\rho_i, 0, 1-\rho_i) \) for \( i = 1, 2 \), where \( 0 \leq \rho_1 \leq \rho_2 \leq 1 \), is determined by the next theorem. For the proof we need the following lemma.

**Lemma 4.** Let \( U, X \) and \( Y \) be random variables with alphabets \( U, X \) and \( Y \), respectively, forming a Markov chain \( U \rightarrow X \rightarrow Y \). Suppose that \( X \rightarrow Y \) is described by
Then we have the relationships
\[
I(U; Y) = (1 - \rho)I(U; X),
\]
\[
I(X; Y|U) = (1 - \rho)I(X; X|U).
\]

This follows from linearity of mutual information with respect to the decomposition (11) and \(I(X; Y|U) = I(X; Y) - I(U; Y)\).

Theorem 2. Suppose that the two subchannels of a CMLOBC are described by
\[
S^{(i)} = (\rho_iJ_{|X| \times 1} + (1 - \rho_i)I_{|X| \times |X|}),
\]
where \(X = P(\mathbb{F}_q^m, l)\) and \(0 \leq \rho_1 \leq \rho_2 \leq 1\). Then its capacity region is the set of all pairs of \((R_1, R_2)\) satisfying \(R_1, R_2 \geq 0\) and
\[
\frac{R_1}{(1 - \rho_1)\log |X|} + \frac{R_2}{(1 - \rho_2)\log |X|} \leq 1.
\]

Proof: See Appendix VII-E.

VII. APPENDIX

A. Proof of Lemma 7

Proof: Suppose first that (ii) holds. Postmultiplying the equation \(e^{(1)}\Lambda = e^{(2)}\) by the matrix
\[
L = \begin{pmatrix}
1 & 0 & \cdots & 0 \\
1 & 1 & \cdots & 0 \\
& \vdots & \ddots & 0 \\
1 & 1 & \cdots & 1
\end{pmatrix}
\]
we obtain \(e^{(1)}\Lambda L = e^{(2)}L\). The matrix \(\Delta = \Lambda L = (\delta_{ij})\) is lower triangular with entries \(\delta_{ij} \leq 1\). (This follows from \(\delta_{ij} = \sum_{k=0}^l \lambda_{ik}l_{kj} = \sum_{k=j}^l \lambda_{ik} \leq \sum_{k=0}^l \lambda_{ik} = 1\).) Hence we have
\[
\sum_{i=j}^l \epsilon_i^{(2)} = (e^{(2)}L)_j = (e^{(1)}\Delta)_j
\]
\[
= \sum_{i=j}^l \epsilon_i^{(1)} \delta_{ij} \leq \sum_{i=j}^l \epsilon_i^{(1)} (0 \leq j \leq l).
\]
Then
\[
\sum_{i=0}^j \epsilon_i^{(1)} = 1 - \sum_{i=j}^l \epsilon_i^{(1)} \leq 1 - \sum_{i=j}^l \epsilon_i^{(2)} = \sum_{i=0}^j \epsilon_i^{(2)}
\]
which implies (i).

Now suppose that (i) holds. First we consider the special case where \(e^{(1)}\) and \(e^{(2)}\) are related in the following way: There exist \(0 \leq i < j \leq l\) and a real number \(0 \leq \lambda \leq 1\) such that \(\epsilon_i^{(2)} = \epsilon_i^{(1)} + \lambda \epsilon_j^{(1)}\), \(\epsilon_j^{(2)} = (1 - \lambda)\epsilon_j^{(1)}\) and \(\epsilon_k^{(1)} = \epsilon_k^{(2)}\) for \(k \in \{0, 1, \ldots, l\} \setminus \{i, j\}\). In this case we have \(e^{(1)}\Lambda = e^{(2)}\), where \(\Lambda\) differs from the identity matrix only in the submatrix corresponding to rows and columns No. \(i, i + 1, \ldots, j\). The corresponding submatrix of \(\Lambda\) is
\[
\begin{pmatrix}
1 & \cdots & 0 \\
& \ddots & \vdots \\
& & 1 - \lambda
\end{pmatrix},
\]
so that \(\Lambda\) is clearly lower triangular and stochastic. In general, as is easily proved by induction, a new \(e^{(2)}\) can be updated from \(e^{(1)}\) and last \(e^{(2)}\) by a sequence of transformations of the above form (i.e., add \(\lambda\) times the \(j\)-th component to the \(i\)-th component and subtract it from the \(j\)-th component for some \(0 \leq i < j \leq l\) and \(0 \leq \lambda \leq 1\)). Since the set of lower triangular stochastic matrices is closed under matrix multiplication, the result follows.

B. Proof of Lemma 2

Proof: Working with the ordinary incidence matrices \(D_{ls}, D_{lt}\), the (\(i,j\))-entry of \(D_{ls}D_{lt}\) is equal to the number of subspaces \(V \in P(\mathbb{F}_q^m, s)\) satisfying \(U_i \supseteq V \supseteq W_j\), where \(U_i \in P(\mathbb{F}_q^m, l)\) and \(W_j \in P(\mathbb{F}_q^m, t)\) denote the \(i\)-th resp. \(j\)-th...
subspace in the given ordering on \( P(\mathbb{P}_q^m, l) \) resp. \( P(\mathbb{P}_q^m, l) \). Thus
\[
(D_{s\ell} D_{st})_{ij} = \begin{cases} \binom{l-i}{s-t} & \text{if } U_i \supseteq W_j, \\ 0 & \text{if } U_i \nsubseteq W_j. \end{cases}
\] (18)

This shows that \( D_{s\ell} D_{st} = \binom{l-i}{s-t} D_{\ell t} \) is a scalar multiple of \( D_{\ell t} \). Obviously we then also have \( S_{ij} S_{st} = \lambda S_{\ell t} \) for some scalar \( \lambda \). Since \( S_{ij} S_{st} \) as well as \( S_{\ell t} \) are stochastic, we must have \( \lambda = 1 \), proving the lemma.

**C. Proof of Theorem 1**

**Proof:** Suppose first that Condition 5 is satisfied. In 5 we choose \( T_{ij} = \lambda_{ij} S_{ij} \) with \( \lambda_{ij} \in \mathbb{R} \) (where it is understood that \( S_{ij} = 0 \) whenever \( i < j \)). Using Lemma 2 we obtain
\[
S^{(1)} T = \left( \begin{array}{cc} \log S_{00} & 0 \\ \lambda_{01} S_{01} & \lambda_{11} S_{11} \\ \vdots & \vdots \\ \lambda_{l0} S_{l0} & \lambda_{11} S_{11} \\ & \vdots \\ \lambda_{ll} S_{ll} & \lambda_{ll} S_{ll} \end{array} \right) \left( \begin{array}{c} \epsilon_0^{(1)} S_{00} \\ \epsilon_1^{(1)} S_{11} \\ \vdots \\ \epsilon_l^{(1)} S_{ll} \end{array} \right) = \left( \begin{array}{c} \epsilon_1^{(1)} (\lambda_{00} S_{00} + \epsilon_0^{(1)} \lambda_{10} S_{10} + \cdots + \epsilon_l^{(1)} \lambda_{l0} S_{l0}) \\ \epsilon_1^{(1)} (\lambda_{11} S_{11} + \epsilon_0^{(1)} \lambda_{21} S_{21} + \cdots + \epsilon_l^{(1)} \lambda_{l1} S_{l1}) \end{array} \right)
\] (19)

By Lemma 1 we can further choose \( \Lambda = (\lambda_{ij}) \) as a lower triangular stochastic matrix satisfying \( \epsilon^{(1)} \Lambda = \epsilon^{(2)} \). Then the resulting matrix \( T = (\lambda_{ij} S_{ij}) \) is stochastic and satisfies 5. Hence in this case the broadcast channel is degraded.

Conversely suppose the broadcast channel is degraded, so that 5 holds for some stochastic (block) matrix \( T = (T_{ij}) \). First we will show that we can assume (without loss of generality) that \( T_{ij} = 0 \) for \( i < j \). 5 says
\[
\sum_{i=0}^{l} \epsilon_{i}^{(1)} (S_{ij} T_{ij}) = \epsilon_{j}^{(2)} S_{ij} \quad \text{for } 0 \leq j \leq l
\]

If \( \epsilon_{i}^{(1)} = 0 \) then we can replace each block \( T_{ij} \), \( 0 \leq j \leq l \), by the corresponding all-zero matrix. Hence the assumption is true in this case. On the other hand, if \( \epsilon_{i}^{(1)} > 0 \) then every positive entry in \( S_{ij} T_{ij} \) forces a positive entry of \( S_{ij} \) in the same position. Now suppose \( T_{ij} \) has a nonzero (i.e. positive) entry in a position indexed by some subspaces \( V \in P(\mathbb{P}_q^m, i) \), \( W \in P(\mathbb{P}_q^m, j) \). Then \( S_{ij} T_{ij} \) has a positive entry in each position indexed by the same subspace \( W \) (as a column index) and any subspace \( U \in P(\mathbb{P}_q^m, l) \) which contains \( V \) (as a row index).

If \( i < j \) then we can find a subspace \( U \in P(\mathbb{P}_q^m, l) \) which contains \( V \) but not \( W \). This can be seen as follows: The space \( \mathbb{P}_q = (W + V)/V \) is a nonzero subspace of \( \mathbb{P}_q^m/V \). Hence there exists a subspace \( U \) of \( \mathbb{P}_q^m/V \) of dimension \( l-i < m-i \) which does not contain \( \mathbb{P}_q \). Then the preimage \( U \) of \( \mathbb{P}_q \) in \( \mathbb{P}_q^m \) has the required property. (The assumption \( l < m \) is essential here!)

Since \( U \) contains \( V \) but not \( W \), the matrix \( S_{ij} T_{ij} \) has an entry > 0 in the position corresponding to \( (U, W) \) and \( S_{ij} \) has a zero in this position. This contradiction shows that \( \epsilon_{i}^{(1)} > 0 \) implies \( T_{ij} = 0 \) for \( i < j \), and so that from now on we can indeed assume \( T_{ij} = 0 \) for all \( i < j \).

Now we postmultiply (5) by
\[
L = \begin{pmatrix} S_{00} & 0 & \cdots & 0 \\ S_{10} & S_{11} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ S_{l0} & S_{l1} & \cdots & S_{ll} \end{pmatrix}
\] (21)

Using Lemma 2 on the left-hand side and setting \( \Delta = TL = (\Delta_{ij}) \) on the right-hand side we obtain
\[
\sum_{i=j}^{l} \epsilon_{i}^{(1)} S_{ii} \Delta_{ij} = \left( \sum_{i=j}^{l} \epsilon_{i}^{(2)} \right) S_{ij} \quad (0 \leq j \leq l).
\] (22)

Applying these matrix equations to the all-one column vectors \( j \) of the appropriate dimensions gives, in view of \( S_{ij} j = j \) and \( S_{ii} \Delta_{ij} j = S_{ii} \Delta_{ij} i \leq S_{ij} j \), the required inequalities \( \sum_{i=j}^{l} \epsilon_{i}^{(2)} \leq \sum_{i=j}^{l} \epsilon_{i}^{(1)} \leq \sum_{i=j}^{l} \sum_{i=0}^{l} \epsilon_{i}^{(1)} \), which completes the proof of the theorem.

**D. Proof of Lemma 3**

**Proof:** During the proof we write \( Y^{(i)} \), \( i = 1, 2 \), for the subchannel outputs (here \( Y^{(i)} \) corresponds to the probability vector \( e^{(i)} \)) and \( Y_s \), \( s = 0, 1, 2 \), for the dimension \( s \) component of \( Y^{(i)} \) (corresponding to the \( s \)-th block in the decomposition (8)), which is independent of \( i \). We will use the (easily established) fact that mutual information is linear in the following sense:
\[
I(X; Y^{(1)} | U) = \sum_{s=0}^{2} \epsilon_{s}^{(1)} I(X; Y_s | U),
\]
\[
I(U; Y^{(2)}) = \sum_{s=0}^{2} \epsilon_{s}^{(2)} I(U; Y_s),
\]
which generalizes to arbitrary decompositions of the form (4).

Clearly \( I(X; Y_0) = I(U; Y_0) = 0 \). The (symmetric) channels \( X \rightarrow Y_1 \), \( X \rightarrow Y_2 \), \( U \rightarrow Y_2 \) have channel matrices \( S_{21}, I_{7 \times 7}, S_{21}(J_{7 \times 7} + (1 - \frac{2}{3}) I_{7 \times 7}) \), respectively. The channel \( U \rightarrow Y_1 \) has channel matrix
\[
\left( \frac{2}{3} I_{7 \times 7} + (1 - \frac{2}{3}) I_{7 \times 7} \right) S_{21} = \frac{2}{3} I_{7 \times 7} + (1 - \frac{2}{3}) S_{21}
\]
The input distribution on \( \mathcal{U} \) (and hence the distribution on \( \mathcal{X} \) as well) is uniform, this gives
\[
R_2(\sigma) = I(U; Y^{(2)})
\]
\[
= \epsilon_{2}^{(2)} \left( -H \left( \frac{2}{3} \right) + \log \frac{2}{3} \right) \\
+ \epsilon_{2}^{(1)} \left( H \left( \frac{2}{3} \right) + \log \frac{2}{3} \right)
\]
\[
R_1(\sigma) = I(X; Y^{(1)} | U)
\]
\[
= \epsilon_{1}^{(1)} \left( H \left( \frac{2}{3} \right) + \log \frac{2}{3} \right) \\
+ \epsilon_{1}^{(2)} \left( H \left( \frac{2}{3} \right) + \log \frac{2}{3} \right),
\]
where \( H(x) = -x \log x - (1-x) \log (1-x) \) denotes the binary entropy function. To simplify the expressions below, we will
take log as the natural logarithm, for which $H'(x) = \log \frac{1 - x}{x}$, $H''(x) = -\frac{1}{x(1-x)}$. We have further

$$R'_2(\sigma) = \epsilon_1^{(2)} \left(-\sigma \log \frac{1-2\sigma/3}{\sigma/3} - \frac{2}{\sigma} \log \sigma\right)$$

$$+ \epsilon_2^{(2)} \left(-\sigma \log \frac{1-\sigma}{\sigma} - \log 6\right),$$

$$R'_1(\sigma) = \epsilon_1^{(1)} \frac{2}{\sigma} \log \frac{1-2\sigma/3}{\sigma} + \epsilon_2^{(2)} \log \frac{6(1-\sigma)}{\sigma}.$$  

From this one verifies at once that $R'_2(\sigma) > 0$, $R'_2(\sigma) < 0$ for $0 < \sigma < \frac{\delta}{7}$ (and $R'_1(\delta/7) = R'_1(\delta) = 0$). Hence, by results from standard calculus, $f$ is well-defined and $f'(R_1(\sigma)) = R'_2(\sigma)/R'_1(\sigma) < 0$, so that $f$ is strictly decreasing. Moreover, since $R_1(0) = 0$, $R_2(0) = \epsilon_1^{(2)} \log \frac{7}{3} + \epsilon_2^{(2)} \log 7 = C_2$, $R_1(\frac{\delta}{7}) = \epsilon_1^{(1)} \log \frac{7}{3} + \epsilon_2^{(1)} \log 7 = C_1$, $R_2(\frac{\delta}{7}) = 0$, we have $f : [0, C_1] \rightarrow [0, C_2]$, $f(0) = C_2$, and $f(C_2) = 0$.

In order to decide whether $f$ is convex/concave/linear, we use the second derivative test from standard calculus. We have to determine the sign of

$$f''(R_1(\sigma)) = \frac{R''_2(\sigma)R'_1(\sigma) - R'_2(\sigma)R'_2(\sigma)}{R'_1(\sigma)^3}$$

for $\sigma \in (0, \frac{\delta}{7})$, which is the same as the sign of

$$R''_2(\sigma)R'_1(\sigma) - R'_2(\sigma)R'_2(\sigma) =$$

$$2\left(\epsilon_1^{(2)} \epsilon_2^{(1)} - \epsilon_1^{(1)} \epsilon_2^{(2)}\right) \left(1 - \sigma\right) \log \frac{6(1-\sigma)}{\sigma}$$

$$- \left(1 - \frac{2\sigma}{3}\right) \log \frac{2(1-2\sigma/3)}{\sigma}\right).$$

It may be verified that the right-hand factor

$$g(\sigma) = (1 - \sigma) \log(1 - \sigma) - \left(1 - \frac{2\sigma}{3}\right) \log \left(1 - \frac{2\sigma}{3}\right)$$

$$+ \frac{1}{\sigma} \log \sigma + (1 - \sigma) \log 6 - \left(1 - \frac{2\sigma}{3}\right) \log 2$$

satisfies $g(0) = g(\frac{\delta}{7}) = 0$ and

$$g''(\sigma) = \frac{1}{(1 - \sigma)(3 - 2\sigma)} < 0$$

for $0 < \sigma < \frac{\delta}{7}$, from which it follows that $g(\sigma)$ is positive in $(0, \frac{\delta}{7})$. Hence the sign of $f''$ in $(0, \frac{\delta}{7})$ is constant and equal to that of $\epsilon_1^{(2)} \epsilon_2^{(1)} - \epsilon_1^{(1)} \epsilon_2^{(2)}$. This concludes the proof.  

E. Proof of Theorem 2

Proof: It is clear from Lemma A that the capacities of the subchannels are $C_i = (1 - \rho_i) \log |X|$ $(i = 1, 2)$. Further, for an arbitrary joint distribution $p(U, X)$ Lemma A gives

$$C_2 I(X; Y_1 | U) + C_1 I(U; Y_2)$$

$$= (1 - \rho_2) \log |X| (1 - \rho_1) I(X; X|U)$$

$$+ (1 - \rho_1) \log |X| (1 - \rho_2) I(U; X)$$

$$= \frac{C_1 C_2}{\log |X|} I(X; X)$$

$$= \frac{C_1 C_2}{\log |X|} H(X) \leq C_1 C_2,$$

which implies [15].

References

[1] T. Ho, M. Medard, R. Koetter, D. Karger, M. Effros, J. Shi, and B. Leong, “A random linear network coding approach to multicast,” Information Theory, IEEE Transactions on, vol. 52, no. 10, pp. 4413 –4430, Oct. 2006.

[2] R. Ahlswede, N. Cai, S.-Y. Li, and R. Yeung, “Network information flow,” Information Theory, IEEE Transactions on, vol. 46, no. 4, pp. 1204 –1216, Jul 2000.

[3] R. Koetter and F. Kschischang, “Coding for errors and erasures in random network coding,” Information Theory, IEEE Transactions on, vol. 54, no. 8, pp. 3579 –3591, Aug. 2008.

[4] D. Silva, F. Kschischang, and R. Koetter, “Communication over finite-field matrix channels,” Information Theory, IEEE Transactions on, vol. 56, no. 3, pp. 1296 –1305, Mar. 2010.

[5] B. Uchôa-Filho and R. Nóbrega, “The capacity of random linear coding networks as subspace channels,” Arxiv preprint arXiv:1001.1021, 2010.

[6] S. Yang, S. Ho, J. Meng, and E. Hui Yang, “Optimality of subspace coding for linear operator channels over finite fields,” in Proc. IEEE Information Theory Workshop, 2010.

[7] S. Yang, S. Ho, J. Meng, and E. Yang, “Linear operator channels over finite fields,” Arxiv preprint arXiv:1002.2293, 2010.

[8] M. Jafari, S. Mohajer, C. Fragouli, and S. Diggavi, “On the capacity of non-coherent network coding,” in Proceedings of the 2009 IEEE international conference on Symposium on Information Theory—Volume 1. Institute of Electrical and Electronics Engineers Inc., The, 2009, pp. 273–277.

[9] T. Cover and J. Thomas, “Elements of information theory,” Wiley Series In Telecommunications, p. 542, 1991.

[10] E. van der Meulen, “A survey of multi-way channels in information theory: 1961-1976,” Information Theory, IEEE Transactions on, vol. 23, no. 1, pp. 1 – 37, Jan. 1977.

[11] T. Cover, “Comments on broadcast channels,” Information Theory, IEEE Transactions on, vol. 44, no. 6, pp. 2524 –2530, Oct 1998.

[12] E. Calvo, D. Palomar, J. Fonollosa, and J. Vidal, “The computation of the capacity region of the discrete degraded bc is a nonconvex dc problem,” in Information Theory, 2008. ISIT 2008. IEEE International Symposium on, 2008, pp. 1721 –1725.

[13] K. Yasui and T. Matsushima, “Toward computing the capacity region of degraded broadcast channel,” in Information Theory Proceedings (ISIT), 2010 IEEE International Symposium on, 2010, pp. 570 –574.

[14] S. Arimoto, “An algorithm for computing the capacity of arbitrary discrete memoryless channels,” vol. 18, no. 1, pp. 14–20, Jan. 1972.

[15] R. E. Blahut, “Computation of channel capacity and rate-distortion functions,” vol. 18, no. 4, pp. 460–473, Jul. 1972.

[16] A. Dana and B. Hassibi, “The capacity region of multiple-input erasure broadcast channels,” in Information Theory, 2005. ISIT 2005. Proceedings. International Symposium on, 4-9 2005, pp. 2315 –2319.

[17] Y. Pang and T. Honold, “M-files to compute the capacity region of degraded CMLOBCs,” 2010. [Online]. Available: http://rapidshare.com/files/439653424/DegradedCMLOBCs.zip