Fundamentals of Index Coding
Other titles in Foundations and Trends® in Communications and Information Theory

Multi-way Communications: An Information Theoretic Perspective
Anas Chaaban and Aydin Sezgin
ISBN: 978-1-60198-788-4

An Approximation Approach to Network Information Theory
A. Salman Avestimehr, Suhas N. Diggavi, Chao Tian and David N. C. Tse

Energy Efficiency in Wireless Networks via Fractional Programming Theory
Alessio Zappone and Eduard Jorswieck

Asymptotic Estimates in Information Theory with Non-Vanishing Error Probabilities
Vincent Y. F. Tan
978-1-60198-852-2
Fundamentals of Index Coding

Fatemeh Arbabjolfaei
Department of Electrical and Computer Engineering
University of California, San Diego
La Jolla, CA, 92093
farbabjo@ucsd.edu

Young-Han Kim
Department of Electrical and Computer Engineering
University of California, San Diego
La Jolla, CA, 92093
yhk@ucsd.edu

Full text available at: http://dx.doi.org/10.1561/0100000094
Editorial Scope

Topics

Foundations and Trends® in Communications and Information Theory publishes survey and tutorial articles in the following topics:

- Coded modulation
- Coding theory and practice
- Communication complexity
- Communication system design
- Cryptology and data security
- Data compression
- Data networks
- Demodulation and Equalization
- Denoising
- Detection and estimation
- Information theory and statistics
- Information theory and computer science
- Joint source/channel coding
- Modulation and signal design
- Multiuser detection
- Multiuser information theory
- Optical communication channels
- Pattern recognition and learning
- Quantization
- Quantum information processing
- Rate-distortion theory
- Shannon theory
- Signal processing for communications
- Source coding
- Storage and recording codes
- Speech and Image Compression
- Wireless Communications

Information for Librarians

Foundations and Trends® in Communications and Information Theory, 2018, Volume 14, 4 issues. ISSN paper version 1567-2190. ISSN online version 1567-2328. Also available as a combined paper and online subscription.
# Contents

1 Introduction 2  
1.1 Motivation 2 
1.2 Formal Definition of the Problem 5 
1.3 Objectives and the Organization 10  
1.A Capacity Region Under Average Error Probability Criterion 11  
1.B Proof of Lemma 1.1 12 
1.C Proof of Lemma 1.2 13 

2 Mathematical Preliminaries 16  
2.1 Directed Graphs 16 
2.2 Graph Coloring 17 
2.3 Perfect Graphs 19 
2.4 Graph Products 20 
2.5 Information Measures 21 

3 Multiletter Characterizations of the Capacity 23  
3.1 Confusion Graphs 23 
3.2 Capacity via Confusion Graphs 26 
3.3 Capacity via Random Coding 29 

4 Structural Properties of Index Coding Capacity 32  
4.1 Generalized Lexicographic Products 32
4.2 Special Cases ........................................ 34
4.3 Capacity of a Generalized Lexicographic Product .... 38
4.4 Proof of the Converse for Theorem 4.1 ............ 43

5 Performance Bounds .................................. 45
5.1 MAIS Bound ...................................... 45
5.2 Polymatroidal Bound ............................ 47
5.3 Information Inequalities and Index Coding ........ 53
5.4 Proof of Proposition 5.1 ....................... 59
5.5 Proof of Proposition 5.3 ....................... 60
5.6 Proof of Proposition 5.6 ....................... 61

6 Coding Schemes .................................... 66
6.1 MDS Codes ...................................... 66
6.2 Clique Covering .................................... 68
6.3 Fractional Clique Covering ...................... 70
6.4 Local Clique Covering .......................... 71
6.5 Partial Clique Covering ......................... 73
6.6 Recursive Codes .................................. 75
6.7 General Linear Codes .......................... 77
6.8 Linear Codes Based on Interference Alignment .... 82
6.9 Flat Coding ...................................... 86
6.10 Composite Coding .............................. 89
6.11 Proof of Proposition 6.5 ...................... 98
6.12 Analysis of Error Probability for Composite Coding 100
6.13 Proof of Proposition 6.12 ..................... 101

7 Criticality .............................................. 104
7.1 A Sufficient Condition .......................... 104
7.2 Necessary Conditions ............................ 110

8 Index Coding Problems with Known Capacity ...... 114
8.1 Problems with Broadcast Rate of Two ............ 114
8.2 Problems with Very Small Capacity ............. 116
8.3 Perfect Graphs .................................... 118
8.4 Locally Acyclic Graphs .......................... 119
8.5 Symmetric Neighboring Side Information .................. 121
8.6 Problems with Small Number of Messages .............. 122

9 Capacity Approximation .................................................. 130
  9.1 Ramsey Numbers ......................................................... 130
  9.2 Approximate Capacity for Some Classes of Problems .... 134
  9.A Proof of Theorem 9.1 ..................................................... 140

10 Index Coding and Network Coding ................................. 141
  10.1 Multiple Unicast Network Coding ............................... 141
  10.2 Relationship Between Index Coding and Network Coding . 143
  10.A Proof of Lemma 10.1 .................................................... 149
  10.B Proof of Lemma 10.2 .................................................... 150

11 Index Coding, Distributed Storage, and Guessing Games ...... 151
  11.1 Locally Recoverable Distributed Storage Problem .......... 151
  11.2 Guessing Games on Directed Graphs ............................ 155
  11.3 Equivalence of Distributed Storage and Guessing Games . 158
  11.4 Complementarity of Index Coding and Distributed Storage 159

12 Further Reading .............................................................. 163
  12.1 Beyond Multiple Unicast .............................................. 163
  12.2 Noisy Broadcast .......................................................... 164
  12.3 Distributed Servers ..................................................... 166
  12.4 Security and Privacy ................................................... 167

Acknowledgments ............................................................... 169

References ..................................
ABSTRACT

Index coding is a canonical problem in network information theory that studies the fundamental limit and optimal coding schemes for broadcasting multiple messages to receivers with different side information. The index coding problem provides a simple yet rich model for several important engineering tasks such as satellite communication, content broadcasting, distributed caching, device-to-device relaying, and interference management. This monograph aims to provide a broad overview of this fascinating subject, focusing on the simplest form of multiple-unicast index coding. A unified treatment on coding schemes based on graph-theoretic, algebraic, and information-theoretic approaches is presented. Although the problem of characterizing the optimal communication rate is open in general, several bounds and structural properties are established. The relationship to other problems such as network coding and distributed storage is also discussed.
1

Introduction

1.1 Motivation

We open our discussion with a simple example. Consider the wireless communication system consisting of one server and three receivers, as depicted in Figure 1.1. The server has three distinct messages $x_1, x_2,$ and $x_3$. Receiver $i \in \{1, 2, 3\}$ is interested in message $x_i$ and has some of the other messages as side information. In particular, receiver 1 has message $x_2$ as side information, receiver 2 has $x_1$ and $x_3$, and receiver 3 has $x_1$. The server wishes to communicate all the messages to their designated receivers using the minimum possible number of broadcast transmissions.

The most naive strategy for the server to achieve this goal is to send one message at a time, which takes overall three transmissions. Alternatively, if the server transmits two coded messages $x_1 + x_2$ and $x_3$ (assuming that the messages can be represented in an alphabet with well-defined addition), then each receiver can recover its desired message using the received coded messages and its side information. Indeed, receiver 1 can recover $x_1$ from the received message $x_1 + x_2$ and its side information $x_2$. Similarly, receiver 2 can recover $x_2$ from $x_1 + x_2$ and $x_1$. Receiver 3 can trivially recover $x_3$. This simple example
1.1. **Motivation**

![Diagram of index coding example with three receivers.](image)

**Figure 1.1:** An index coding example with three receivers.

illustrates that sending *coded messages* may decrease the number of broadcast transmissions.

Generalizing our initial example, we study the communication problem depicted in Figure 1.2, which is commonly referred to as *index coding*. In this canonical problem in network information theory, a server has a tuple of \( n \) messages

\[
x^n := (x_1, \ldots, x_n)
\]

and broadcasts a coded message \( y \) generated from \( x^n \) to \( n \) receivers. Each receiver \( i \in [n] := \{1, 2, \ldots, n\} \) wishes to recover the message \( x_i \) from \( y \) and a set of other messages

\[
x(A_i) := (x_j, j \in A_i), \quad A_i \subseteq [n] \setminus \{i\}
\]

it already has as side information. Assuming that the side information sets \( A_1, \ldots, A_n \) are known prior to the communication, we are interested in devising a coding scheme that exploits the side information at the receivers and broadcasts the messages reliably with the minimum amount of transmissions.

The index coding problem was introduced by Birk and Kol [26, 27] in the context of satellite communication. Related formulations were studied earlier by Celebiler and Stette [40], Wyner, Wolf, and
Introduction

Figure 1.2: The index coding problem.

Willems [157, 161], and Yeung [163]. The term “index coding” is due to Bar-Yossef, Birk, Jayram, and Kol [22], who compared the index coding problem to the problem of zero-error source coding with side information studied by Witsenhausen [158] and contrasted the fact that in the index coding problem the receiver wishes to recover a single component of the source, the index of which is unknown to the sender. Hence, as for compound channels [28, 54, 159], the sender can proactively encode its transmission and broadcast to the receiver in all possible configurations [49]. In addition to satellite communication, index coding has applications in diverse areas such as multimedia distribution [117], interference management [83], coded caching [106, 84], and distributed computing [96]. This problem is also closely related to many other important problems such as network coding [125, 62, 60], locally recoverable distributed storage [111, 132, 13], guessing games on directed graphs [125, 167, 13], matroid theory [62], and zero-error capacity of channels [135]. Due to this significance, the index coding problem has been broadly studied over the past two decades. Tools from various disciplines including graph theory, coding theory, and information theory have been utilized to propose numerous nontrivial coding schemes [26, 104, 23, 44, 117, 30, 8, 107, 83, 134, 7, 9, 153, 119, 82, 145, 150, 167], as well as performance bounds [165, 23, 56, 29, 18, 145].
1.2  Formal Definition of the Problem

We formulate the problem more precisely. A \((t_1, \ldots, t_n, r)\) index code is defined by

- \(n\) messages, where the \(i\)-th message \(x_i = (x_{i1}, \ldots, x_{it_i})\) takes values from \(\mathcal{X}^{t_i}\) for some common finite alphabet \(\mathcal{X}\),

- an encoder \(\phi : \prod_{i=1}^{n} \mathcal{X}^{t_i} \to \mathcal{X}^r\) that maps the message \(n\)-tuple \(x^n\) to an index \(y = (y_1, \ldots, y_r) \in \mathcal{X}^r\), and

- \(n\) decoders, where the decoder at receiver \(i \in [n]\), \(\psi_i : \mathcal{X}^r \times \prod_{j \in A_i} \mathcal{X}^{t_j} \to \mathcal{X}^{t_i}\), maps the received index \(y = \phi(x^n)\) and the side information \(x(A_i)\) back to \(x_i\).

Thus, for every \(x^n \in \prod_{i=1}^{n} \mathcal{X}^{t_i}\),

\[\psi_i(\phi(x^n), x(A_i)) = x_i, \quad i \in [n].\]

A \((t, \ldots, t, r)\) code will be written simply as a \((t, r)\) code.

Suppose that \(\mathcal{X}\) is an alphabet over which linear operations are well-defined, for example, a finite field \(\mathbb{F}_q\) or a ring (see, for example, [48]). If the encoder of a code is a linear function of \(x^n = (x_{11}, \ldots, x_{1t_1}, \ldots, x_{nt_n}) = (x_{11}, \ldots, x_{1t_1}, \ldots, x_{nt_1}, \ldots, x_{nt_n})\) and the decoders are also linear functions of \(x^n\) (and \(y = (y_1, \ldots, y_r)\)), then the code is referred to as a linear index code. If \(t_i = 1\) for all \(i \in [n]\), then the linear index code is said to be a scalar linear index code. Otherwise, the code is a vector linear index code.

As an example, for the 3-message index coding problem in Figure 1.1, a \((1,1,1,2)\) index code with \(\mathcal{X} = \mathbb{F}_2\), the encoder defined by

\[y_1 = x_1 + x_2 \quad \text{and} \quad y_2 = x_3,\]

and the decoders defined by

\[x_1 = y_1 + x_2, \quad x_2 = y_1 + x_3, \quad \text{and} \quad x_3 = y_2,\]

where in both cases the addition operations are in \(\mathbb{F}_2\), is a scalar linear code.
A tuple \((R_1, \ldots, R_n) \in \mathbb{R}_{\geq 0}^n\) of nonnegative real numbers is said to be an achievable rate tuple for the index coding problem if there exists a \((t_1, \ldots, t_n, r)\) index code such that
\[ R_i \leq \frac{t_i}{r}, \quad i \in [n]. \]
The capacity region \(\mathcal{C}\) of the index coding problem is defined as the closure of the set of all achievable rate tuples. The ultimate goal of studying the index coding problem is to characterize the capacity region of a general index coding problem and develop a simple coding scheme that achieves or approximates the capacity region.

**Remark 1.1.** Our definition of capacity region, with the stringent requirement of perfect, zero-error recovery of the messages, should be distinguished from the more common definition of vanishing-error capacity region in network information theory that allows for arbitrarily small probability of error. It can be shown, however, that these two capacity regions coincide; see Appendix 1.A for details.

The definition of the capacity region depends on the alphabet \(X\) on which the messages are defined and one may well denote it by \(\mathcal{C}_X\) to emphasize this dependence. As we will prove in Appendix 1.B, however, the choice of \(X\) is irrelevant to the actual capacity region itself.

**Lemma 1.1.** For any two finite alphabets \(X\) and \(X'\),
\[ \mathcal{C}_X = \mathcal{C}_{X'}. \]
Consequently, we assume without loss of generality that \(X = \mathbb{F}_2\) for a general index code and consequently that the base of logarithm is 2 throughout, unless specified otherwise.

By limiting our attention to linear codes, we can similarly define linearly achievable rate tuple and linear capacity region \(\mathcal{L}\). In contrast to the capacity region, the linear capacity region of the index coding problem may depend on the chosen alphabet \(X\) and indeed does so [104] (see Section 6.7).

The capacity region, linear or nonlinear, is closed by definition. Based on the standard time-sharing argument (see, for example, [61, Sec. 4.4]), it can be readily checked to be convex.
1.2. Formal Definition of the Problem

In many cases, it is convenient to focus on a single performance metric instead of a multidimensional region. Let \( \mu = (\mu_1, \ldots, \mu_n) \in \mathbb{R}_{\geq 0}^n \) be a tuple of nonnegative real numbers. The \( \mu \)-directed capacity of the index coding problem is defined as

\[
C(\mu) = \max\{R : R\mu \in \mathcal{C}\}.
\]

Remark 1.2. The capacity region can be written in terms of \( \mu \)-directed capacities as

\[
\mathcal{C} = \bigcup_{\mu}(R_1, \ldots, R_n) : R_i \leq C(\mu)\mu_i, \ i \in [n]\}. \tag{1.1}
\]

Note that if \( \mu = c\mu' \) for some constant \( c \), then \( C(\mu)\mu = C(\mu')\mu' \) and thus in (1.1), it suffices to take the union only over normalized vectors, e.g., over \( \mu \) such that \( \sum_{i=1}^n \mu_i = n \).

The \( 1 \)-directed capacity of the index coding problem is referred to as the symmetric capacity (or the capacity in short), that is,

\[
C_{\text{sym}} = C(1) = \max\{R : (R, \ldots, R) \in \mathcal{C}\}.
\]

The symmetric capacity can be equivalently defined as

\[
C_{\text{sym}} = \sup_r \sup_{(t,r) \ \text{codes}} t = \lim_{r \to \infty} \sup_{(t,r) \ \text{codes}} t,
\]

where the equality between the supremum and the limit follows by Fekete’s lemma [69] and the superadditivity

\[
\sup_{(t,r_1+r_2) \ \text{codes}} t \geq \sup_{(t_1,r_1) \ \text{codes}} t_1 + \sup_{(t_2,r_2) \ \text{codes}} t_2.
\]

The reciprocal of the symmetric capacity,

\[
\beta = \frac{1}{C_{\text{sym}}},
\]

is referred to as the broadcast rate, which can be alternatively defined as

\[
\beta = \inf_t \inf_{(t,r) \ \text{codes}} r = \lim_{t \to \infty} \inf_{(t,r) \ \text{codes}} r. \tag{1.2}
\]
The linear broadcast rate is similarly defined as

\[
\lambda = \inf_{t} \inf_{(t,r) \text{ linear codes}} \frac{r}{t} = \lim_{t \to \infty} \inf_{(t,r) \text{ linear codes}} \frac{r}{t}.
\]

As with the linear capacity region \( \mathcal{L} \), the linear broadcast rate depends on the underlying alphabet \( \mathcal{X} \) and will be sometimes denoted \( \lambda_{\mathcal{X}} \) to emphasize this dependence. For any \( \mathcal{X} \), \( \beta \leq \lambda_{\mathcal{X}} \).

Note that the capacity region \( \mathcal{C} \) of the index coding problem includes the simplex \( \{(R_1, \ldots, R_n) : R_1 + \cdots + R_n = 1, R_i \geq 0, i \in [n]\} \) and is included in the hypercube \( \{(R_1, \ldots, R_n) : 0 \leq R_i \leq 1, i \in [n]\} \). Consequently, the capacity and the broadcast rate are bounded as \( \frac{1}{n} \leq C_{\text{sym}} \leq 1 \) and \( 1 \leq \beta \leq n \), respectively. Similar bounds hold for \( \mathcal{L} \) and \( \lambda \) as well.

Any instance of the index coding problem is fully determined by the side information sets \( A_1, \ldots, A_n \), and is represented compactly by a sequence \((i|A_i), i \in [n]\). For example, the 3-message index coding problem with \( A_1 = \{2\} \), \( A_2 = \{1, 3\} \), and \( A_3 = \{1\} \) in Figure 1.1 is represented as

\[(1|2), (2|1,3), (3|1).\]

Each instance of the index coding problem can be equivalently specified by a directed graph \( G = (V, E) \) with \( n \) vertices, referred to as the side information graph [27, 44]. Each vertex of \( G \) corresponds to a receiver (and its associated message) and there is a directed edge \( j \to i \) if and only if (iff) receiver \( i \) knows message \( x_j \) as side information, i.e., \( j \in A_i \) (see Figure 1.3). The reader is cautioned that in the literature the opposite convention is sometimes used to describe the availability of side information, in which there is a directed edge \( i \to j \) if \( j \in A_i \).

![Figure 1.3: The graph representation for the index coding problem with \( A_1 = \{2, 3\}, A_2 = \{1\}, \) and \( A_3 = \{1, 2\} \).](http://dx.doi.org/10.1561/0100000094)
1.2. Formal Definition of the Problem

Either way, the number of index coding problems with $n$ messages is $2^{n(n-1)}$, which blows up quickly with $n$. Even when we remove isomorphic (i.e., symmetric up to vertex relabeling) instances and concentrate on nonisomorphic instances, the number of such problems is equal to that of nonisomorphic directed graphs with $n$ vertices [151, Seq. A000273], which grows superexponentially. Throughout the monograph, we identify an instance of the index coding problem with its side information graph $G$ and often write “index coding problem $G$.” We also denote the broadcast rate and the capacity region of problem $G$ with $\beta(G)$ and $C(G)$, respectively, when this dependence is to be emphasized.

The index coding problem can be also formulated as a special case of the multiple-unicast network coding problem [2, 164]; see Section 10 for a self-contained description of the latter. For example, the index coding problem with $A_1 = \{2\}, A_2 = \{1, 3\}$, and $A_3 = \{1\}$ can be represented as a network coding problem depicted in Figure 1.4. In this network coding graph, each edge (solid line) represents a link of unit capacity and each vertex represents a node. There are three messages communicated from source nodes on the left to destination nodes on the right (depicted by dashed lines). Each source node is connected to the top left node, which encodes the messages into an index (coded message) and communicates it to the top right node (under the capacity constraint). The top right node is connected to each destination node and forwards (broadcasts) the index to all of them. The remaining edges connect source nodes and destination nodes directly according to the availability pattern of side information. The essence of each problem

![Network Coding Graph](image-url)
instance is captured by such direct connections between the source and destination nodes. If we consider the subgraph consisting of only source and destination nodes and overlap each source–destination pair, then we recover the side information graph in Figure 1.3.

1.3 Objectives and the Organization

As mentioned earlier, our main objectives in studying the index coding problem are to characterize the capacity region for a general index coding instance in a computable expression and to develop the coding scheme that can achieve it. Despite their simplicity, these two closely related questions are extremely difficult and precise answers to them, after twenty years of vigorous investigation, are still in terra incognita. There are, nonetheless, many elegant results that shed light on the fundamental challenges in multiple-unicast network communication and expose intriguing interplay between coding theory, graph theory, and information theory. This monograph thus aims to provide a concise survey of these results in a unified framework.

To facilitate the development of this framework, the rest of the monograph is organized as follows. Section 2 reviews some known results in graph theory that will be recalled frequently throughout. Our main story starts with Section 3, which presents a few noncomputable characterizations of the capacity of a general index coding problem in graph-theoretic and information-theoretic expressions. As a main application of these characterizations, we present basic structural properties of index coding capacity in Section 4. The next two sections develop upper and lower bounds on the capacity. In Section 5, we establish a few capacity upper bounds and the relationships among them. In Section 6, we develop several coding schemes based on algebraic, graph-theoretic, and information-theoretic tools along with the corresponding lower bounds on the capacity. Section 7 is devoted to the notion of criticality, namely, whether the side information graph cannot be reduced without lowering the capacity, and presents necessary and sufficient conditions for an index coding problem to be critical. In Section 8, we combine the results in Sections 4 through 7 to characterize the capacity of several classes of the index coding problem. The capacity
1.A Capacity Region Under Average Error Probability Criterion

Approximation results beyond these classes of problems are presented in Section 9. The next two sections explore the connection between index coding and other related problems. In Section 10, we relate index coding to the well-known multiple-unicast network coding problem. In Section 11, we present the intriguing duality between index coding, locally recoverable distributed storage, and guessing games. We conclude our discussion in Section 12 by pointing out numerous variations and extensions of the basic index coding problem presented thus far. Some technical proofs are relegated to the end of each section.

1.A Capacity Region Under Average Error Probability Criterion

Let $X_i$ and $\hat{X}_i$ be random variables representing the $i$-th message and its estimate, respectively. Suppose that $(X_1, \ldots, X_n)$ is uniformly distributed over $\mathcal{X}_1 \times \cdots \times \mathcal{X}_n$, i.e., the messages are uniformly distributed and independent of each other. A rate tuple $(R_1, \ldots, R_n)$ is said to be vanishing-error achievable if for every $\epsilon > 0$, there exists a $(t_1, \ldots, t_n, r)$ code with $R_i \leq t_i/r, i \in [n]$, such that the average probability of error

$$P_e = P\{(\hat{X}_1, \ldots, \hat{X}_n) \neq (X_1, \ldots, X_n)\} \leq \epsilon. \quad (1.3)$$

Equivalently, a rate tuple $(R_1, \ldots, R_n)$ is vanishing-error achievable if there exists a sequence of $([rR_1], \ldots, [rR_n], r)$ index codes such that the average probability of error $P_e$ converges to 0 as $r \to \infty$. The vanishing-error capacity region $\mathcal{C}^*$ of the index coding problem is the closure of the set of all vanishing-error achievable rate tuples $(R_1, \ldots, R_n)$.

For a general network communication problem, the vanishing-error capacity region and the (zero-error) capacity region are not the same \cite{59, 154}. For a network with a single sender that broadcasts multiple messages, however, these two regions can be shown to be identical \cite{156} (see also \cite[Problem 8.11]{61}), which was rediscovered by Chan and Grant \cite{42}, and Langberg and Effros \cite{92} in the context of index coding and single-sender network coding problems.

**Lemma 1.2.** For any index coding problem, $\mathcal{C} = \mathcal{C}^*$. 
The proof is delegated to Appendix 1.C. One can similarly define \textit{vanishing-error linearly achievability}. The \textit{vanishing-error linear capacity region} $\mathcal{L}^*$ is then defined to be the closure of the set of all vanishing-error achievable rate tuples, which is also the same as the (zero-error) linear capacity region.

**Lemma 1.3.** For any $\mathcal{X} = \mathbb{F}_q$, $\mathcal{L} = \mathcal{L}^*$.

To prove Lemma 1.3, we establish the following stronger result.

**Lemma 1.4.** For any linear index code, if the probability of error $P_e < 1/2$, then $P_e = 0$.

**Proof.** Let $t_\Sigma = \sum_{i=1}^n t_i$. Every linear encoder $\phi$ is specified by a matrix $\Phi \in \mathbb{F}_q^{r \times t_\Sigma}$ such that $y = \phi(x^n) = \Phi x^n$. Assume by contradiction that $0 < P_e < 1/2$. Since the probability of error is nonzero, there exist distinct $\tilde{x}^n, \tilde{z}^n \in \mathbb{F}_q^{t_\Sigma}$ such that $\Phi \tilde{x}^n = \Phi \tilde{z}^n$ and $\tilde{x}(A_i) = \tilde{z}(A_i)$ for some $i \in [n]$, or equivalently, $\Phi e^n = 0$ and $e(A_i) = 0$, where $e^n = \tilde{x}^n - \tilde{z}^n$.

Now for every $x^n$, since the code is linear, there exists $z^n = x^n + e^n$ for which $\Phi x^n = \Phi z^n$ and $x(A_i) = z(A_i)$ for some $i$. Therefore, at most one of $x^n$ and $z^n$ can be recovered correctly and consequently the average probability of error $P_e \geq 1/2$, which contradicts the assumption.  

We are now ready to prove Lemma 1.3. Clearly $\mathcal{L} \subseteq \mathcal{L}^*$. Thus, it suffices to show that $\mathcal{L}^* \subseteq \mathcal{L}$. Let $(R_1, \ldots, R_n)$ be a vanishing error linearly achievable rate tuple. Then, by definition, there exists a sequence of $([rR_1], \ldots, [rR_n], r)$ index codes for which (1.3) is satisfied. Therefore, there exists a sufficiently large $r$ such that the error probability of the index code $([rR_1], \ldots, [rR_n], r)$ is less than 1/2. By Lemma 1.4, the error probability of this code is zero and thus, $(R_1, \ldots, R_n)$ is also a (zero-error) linearly achievable rate tuple. Hence, we have $\mathcal{L}^* \subseteq \mathcal{L}$, which completes the proof.

1.B Proof of Lemma 1.1

Let $I$ and $I'$ be index coding instances defined over finite alphabets $\mathcal{X}$ and $\mathcal{X}'$, respectively, and let $\mathcal{A}$ and $\mathcal{A}'$ be the associated sets of achievable rate tuples. We consider two cases.
1.C. Proof of Lemma 1.2

Case 1. \( \log_{|\mathcal{X}|} |\mathcal{X}'| \) is a rational number, i.e., \( \log_{|\mathcal{X}|} |\mathcal{X}'| = a/b \) for some \( a, b \in \mathbb{N} \). To show that the capacity regions are equal, it suffices to show \( \mathcal{A} = \mathcal{A}' \). Suppose that \( \mathbf{R} = (R_1, \ldots, R_n) \in \mathcal{A} \). Then, by definition, there exists a \((t, r) = (t_1, \ldots, t_n, r)\) code for problem \( I \) such that \( R_i \leq t_i/r, \; i \in [n] \). Repeat the \((t, r)\) code \( a \) times to construct an \((at, ar)\) index code for problem \( I \). Since the two instances are both defined on the same set of side information, and \( |\mathcal{X}|^a = |\mathcal{X}'|^b \), this leads to a \((bt, br)\) code for problem \( I' \). Therefore, \( \mathbf{R} \in \mathcal{A}' \), and thus \( \mathcal{A} \subseteq \mathcal{A}' \).

By similar steps we can show \( \mathcal{A}' \subseteq \mathcal{A} \), which completes the proof.

Case 2. \( \log_{|\mathcal{X}|} |\mathcal{X}'| \) is irrational. First, we show that \( \mathcal{A}' \subseteq \mathcal{C}_X \). Suppose that \( R \in \mathcal{A}' \). Then, by definition, there exists a \((t, r)\) index code for problem \( I' \) such that \( R_i \leq t_i/r, \; i \in [n] \). For any \( b \in \mathbb{N} \) sufficiently large, there exists \( a \in \mathbb{N} \) such that \( a/b < \log_{|\mathcal{X}|} |\mathcal{X}'| < (a + 1)/b \). Construct a \((bt, br)\) index code for problem \( I' \) by repeating the \((t, r)\) code \( b \) times. Since \( |\mathcal{X}|^a < |\mathcal{X}'|^b < |\mathcal{X}'|^{a+1} \) and the two problems are defined on the same set of side information, a \((at, (a+1)r)\) code for problem \( I \) can be constructed from the \((bt, br)\) code for problem \( I' \). Letting \( b \to \infty \) (and hence \( a \to \infty \)) proves that \( \mathbf{R} \in \mathcal{C}_X \), and thus \( \mathcal{A}' \subseteq \mathcal{C}_X \). Since \( \mathcal{C}_X \) is closed, we have \( \mathcal{C}_{X'} \subseteq \mathcal{C}_X \). By similar steps we can show \( \mathcal{C}_X \subseteq \mathcal{C}_{X'} \), which completes the proof.

1.C. Proof of Lemma 1.2

We adapt Telatar’s simplification of the classical proof by Willems [156] on the invariance of the broadcast channel capacity region under the average and maximal error probability criteria that appeared in [61, Problem 8.11].

It is trivial to see that \( \mathcal{C} \subseteq \mathcal{C}^* \). We thus prove the other direction. Let \( (R_1, \ldots, R_n) \subseteq \mathcal{C}^* \). Then for every \( \epsilon > 0 \), there exists a sequence of \((t_1, \ldots, t_n, r)\) codes with \( t_i = \lceil rR_i \rceil, \; i \in [n] \), such that the average probability of error \( P_e \leq \epsilon \) for \( r \) sufficiently large. Assume without loss of generality that \( R_i > 0, \; i \in [n] \). (Otherwise, the message \( x_i \) of zero rate \( R_i = 0 \) is fixed and can be ignored.) We will identify the set \( \{0, 1\}^t \) of all \( t \)-bit sequences with the set \( \{2^t\} = \{1, \ldots, 2^t\} \) of integers throughout. Then the set of codewords of the \((t_1, \ldots, t_n, r)\) index code
can be expressed as

\[ \mathcal{C} = \{ \phi(x^n) \in [2^r] : x^n \in [2^{l_1}] \times \cdots \times [2^{l_n}] \}, \]

which will be referred to as the codebook. For each message tuple \( x^n \), we define its probability of error as

\[ P_e(x^n) = P\{X^n \neq \hat{X}^n | X^n = x^n \}. \quad (1.4) \]

Note that \( P_e(x^n) \) is either 0 or 1 for any index code. We say that a codeword \( \phi(x^n) \) is said to be “bad” if the corresponding \( P_e(x^n) = 1 \).

Since the average probability of error is

\[ \epsilon = \frac{1}{2^{t_\Sigma}} \sum_{x^n} P_e(x^n), \]

there are \( 2^{t_\Sigma} \epsilon \) “bad” codewords \( \phi(x^n) \), where \( t_\Sigma = \sum_{i=1}^n t_i \). Randomly and independently permute the messages \( x_1, \ldots, x_n \) to generate a new codebook \( \overline{\mathcal{C}} \) that consists of codewords \( \phi(\pi_1(x_1), \ldots, \pi(x_n)) \), where \( \pi_1, \ldots, \pi_n \) denote the independent random permutations.

We now proceed with the multicoding technique by Marton [108] originally developed for broadcast channels. We partition the codebook \( \overline{\mathcal{C}} \) into subcodebooks \( \overline{\mathcal{C}}(x'_1, \ldots, x'_n) \) for a new set of message tuples \((x'_1, \ldots, x'_n) \in [2^{l_1}/r^2] \times \cdots \times [2^{l_n}/r^2] \), each subcodebook consisting of \( r^2 \times \cdots \times r^2 = r^{2n} \) codewords of length \( r \). We will show that there exists a new encoder \( \phi'(x'_1, \ldots, x'_n) \) that maps each message tuple \((x'_1, \ldots, x'_n) \) to some codeword in the corresponding subcodebook \( \overline{\mathcal{C}}(x'_1, \ldots, x'_n) \), so that every codeword \( \phi'(x'_1, \ldots, x'_n) \) is “good” (= not “bad”) and hence distinguishable from the rest with zero error. Since the rate of the new code is \( R'_i = (t_i - 2 \log r)/r = ([rR_i] - 2 \log r)/r \), which converges to the original rate \( R_i \) as \( r \to \infty \), there is no asymptotic rate loss for achieving the zero error probability. Details on the existence of \( \phi'(x'_1, \ldots, x'_n) \) are as follows.

First note that every subcodebook has the same distribution as the set

\[ \{ \phi(\pi_1(x_1), \ldots, \pi_n(x_n)) : x_1, \ldots, x_n \in [r^2] \}. \]

The probability that all \( r^{2n} \) codewords in this set are “bad” is upper bounded by the probability that all \( r^2 \) “diagonal” codewords, that is,
all codewords in
\[ \{ \phi(\pi_1(x), \ldots, \pi_n(x)) : x \in [r^2] \}, \]
are “bad.” Since the permutations are independent and there are \( 2^{t \Sigma} \epsilon \) “bad” codewords, the probability that all “diagonal” codewords are “bad” is upper bounded by
\[
\frac{2^{t \Sigma} \epsilon}{\prod_{i=1}^{n} 2^{t_i}} \cdot \frac{2^{t \Sigma} \epsilon - 1}{\prod_{i=1}^{n} (2^{t_i} - 1)} \cdot \frac{2^{t \Sigma} \epsilon - 2}{\prod_{i=1}^{n} (2^{t_i} - 2)} \cdots \frac{2^{t \Sigma} \epsilon - (r^2 - 1)}{\prod_{i=1}^{n} (2^{t_i} - (r^2 - 1))}
\leq \left( \prod_{i=1}^{n} \frac{2^{t_i}}{2^{t_i} - (r^2 - 1)} \right)^{r^2} \epsilon^{r^2},
\]
which is further upper bounded by \( (2 \epsilon)^{r^2} \) for \( r \) sufficiently large (since \( 2^{t_i} / (2^{t_i} - (r^2 - 1)) \to 1 \) as \( r \to \infty \)).

Next, since every subcodebook has the same distribution, the expected number of subcodebooks for which all of their constituent codewords are “bad” is upper bounded by
\[
\frac{2^{t \Sigma}}{r^{2n} (2 \epsilon)^{r^2}},
\]
which is the product of the number of all subcodebooks and the probability bound of \( (2 \epsilon)^{r^2} \) we computed above. Since this bound tends to zero as \( r \to \infty \), there exists at least one permutation tuple \( (\pi_1, \ldots, \pi_n) \) such that every subcodebook has at least one codeword that is “good.” Hence, we can define the new encoder \( \phi'(x'_1, \ldots, x'_n) \) that maps each message tuple \( (x'_1, \ldots, x'_n) \in [2^{t_1} / r^2] \times \cdots \times [2^{t_n} / r^2] \) to a “good” codeword in the subcodebook \( \overline{C}(x'_1, \ldots, x'_n) \). This completes the proof of Lemma 1.2.
References


Full text available at: http://dx.doi.org/10.1561/0100000094


References


References


References


References


References


References


