CAMBRIDGE

Cambridge University Press
978-1-108-49798-5 — Communication Complexity
Anup Rao , Amir Yehudayoff
Frontmatter
More Information

Communication Complexity

Communication complexity is the mathematical study of scenarios where several parties need to communicate to achieve a common goal, a situation that naturally appears during computation. This introduction presents the most recent developments in an accessible form, providing the language to unify several disjointed research subareas. Written as a guide for a graduate course on communication complexity, it will interest a broad audience in computer science, from advanced undergraduates to researchers in areas ranging from theory to algorithm design to distributed computing.

Part I presents basic theory in a clear and illustrative way, offering beginners an entry into the field. Part II describes applications, including circuit complexity, proof complexity, streaming algorithms, extension complexity of polytopes, and distributed computing. Proofs throughout the text use ideas from a wide range of mathematics, including geometry, algebra, and probability. Each chapter contains numerous examples, figures, and exercises to aid understanding.

ANUP RAO is an associate professor at the School of Computer Science, University of Washington. He received his PhD in Computer Science from the University of Texas at Austin and was a researcher at the Institute for Advanced Study, Princeton. His research interests are primarily in theoretical computer science.

AMIR YEHUDAYOFF is Associate Professor of Mathematics at Technion – Israel Institute of Technology. He is interested in mathematical questions that are motivated by theoretical computer science and machine learning. He was a member of the Institute for Advanced Study in Princeton and served as the secretary of the Israel Mathematical Union. He has won several prizes, including the Cooper Prize and the Krill Prize for excellence in scientific research, and the Kurt Mahler Prize for excellence in mathematics.

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-1-108-49798-5 — Communication Complexity
Anup Rao , Amir Yehudayoff
Frontmatter
More Information

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-1-108-49798-5 — Communication Complexity
Anup Rao , Amir Yehudayoff
Frontmatter
More Information

Communication Complexity and Applications

Anup Rao
University of Washington

Amir Yehudayoff
Technion – Israel Institute of Technology

CAMBRIDGE
UNIVERSITY PRESS

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-1-108-49798-5 — Communication Complexity
Anup Rao , Amir Yehudayoff
Frontmatter
More Information

CAMBRIDGE
UNIVERSITY PRESS

University Printing House, Cambridge CB2 8BS, United Kingdom

One Liberty Plaza, 20th Floor, New York, NY 10006, USA

477 Williamstown Road, Port Melbourne, VIC 3207, Australia

314–321, 3rd Floor, Plot 3, Splendor Forum, Jasola District Centre,
New Delhi – 110025, India

79 Anson Road, #06–04/06, Singapore 079906

Cambridge University Press is part of the University of Cambridge.

It furthers the University's mission by disseminating knowledge in the pursuit of education, learning, and research at the highest international levels of excellence.

www.cambridge.org
Information on this title: www.cambridge.org/9781108497985
DOI: 10.1017/9781108671644

© Anup Rao and Amir Yehudayoff 2020

This publication is in copyright. Subject to statutory exception and to the provisions of relevant collective licensing agreements, no reproduction of any part may take place without the written permission of Cambridge University Press.

First published 2020

Printed in the United Kingdom by TJ International Ltd., Padstow Cornwall

A catalogue record for this publication is available from the British Library.

Library of Congress Cataloging-in-Publication Data
Names: Rao, Anup, 1980– author. | Yehudayoff, Amir, author.
Title: Communication complexity and applications / Anup Rao, Amir Yehudayoff.
Description: Cambridge ; New York, NY : Cambridge University Press, 2020. |
Includes bibliographical references and index.
Identifiers: LCCN 2019038156 (print) | LCCN 2019038157 (ebook) |
ISBN 9781108497985 (hardback) | ISBN 9781108671644 (epub)
Subjects: LCSH: Computational complexity.
Classification: LCC QA267.7 .R37 2020 (print) | LCC QA267.7 (ebook) |
DDC 511.3/52–dc23
LC record available at `https://lccn.loc.gov/2019038156`
LC ebook record available at `https://lccn.loc.gov/2019038157`

ISBN 978-1-108-49798-5 Hardback

Cambridge University Press has no responsibility for the persistence or accuracy of URLs for external or third-party internet websites referred to in this publication and does not guarantee that any content on such websites is, or will remain, accurate or appropriate.

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-1-108-49798-5 — Communication Complexity
Anup Rao , Amir Yehudayoff
Frontmatter
More Information

Dedicated to our families.

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-1-108-49798-5 — Communication Complexity
Anup Rao , Amir Yehudayoff
Frontmatter
More Information

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-1-108-49798-5 — Communication Complexity
Anup Rao , Amir Yehudayoff
Frontmatter
More Information

Contents

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE
Cambridge University Press
978-1-108-49798-5 — Communication Complexity
Anup Rao , Amir Yehudayoff
Frontmatter
More Information

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-1-108-49798-5 — Communication Complexity
Anup Rao , Amir Yehudayoff
Frontmatter
More Information

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-1-108-49798-5 — Communication Complexity
Anup Rao , Amir Yehudayoff
Frontmatter
More Information

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE
Cambridge University Press
978-1-108-49798-5 — Communication Complexity
Anup Rao , Amir Yehudayoff
Frontmatter
More Information

Preface

COMMUNICATION IS AN ESSENTIAL part of our lives and plays a central role in our technology. Communication complexity is a mathematical theory that addresses a basic question:

> If two or more parties want to compute something about the information they jointly possess, how long does their conversation need to be?

It provides a systematic framework for measuring, discussing, and understanding communication.

The fundamental nature of communication complexity leads to many deep connections with the study of *computation* in general. This is not surprising – it is hard to imagine a computing machine that does not include communicating components. Moreover, the costs associated with communication are often the most significant costs involved in carrying out the computation. For example, in the human brain, most of the mass consists of *white matter* rather than *gray matter*. It is the white matter that facilitates communication between different regions of the brain.

In the years following the basic definitions by Yao,[1] communication complexity has become a standard tool for identifying the limitations of computation. The theory is general enough that it captures something important about many computational processes, yet simple and elegant enough that beautiful ideas from a wide range of mathematical disciplines can be used to understand it. In this book, we guide the reader through the theory along a path that includes many exquisite highlights of mathematics – including from geometry, probability theory, matrix analysis, algebra, and combinatorics. We will apply the theory to discover basic truths about Boolean circuits, proofs, data structures, linear programs, distributed systems, and streaming algorithms. Communication complexity is simultaneously beautiful and widely applicable.

[1] Yao, 1979.

The main protagonist of our story is the *disjointness* problem. Here Alice and Bob each have access to their own set and want to figure out whether or not these sets are disjoint. For example, imagine that Alice and Bob want to know if there is a movie that they would both enjoy. Alice knows the collection of movies that she would like to see, and Bob knows the movies he would like to see. How long does their conversation need to be? Set disjointness appears in many applications

Two sets are disjoint if they have no common elements.

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE
Cambridge University Press
978-1-108-49798-5 — Communication Complexity
Anup Rao , Amir Yehudayoff
Frontmatter
More Information

of communication complexity, and it helps to illustrate many techniques applicable to understanding communication.

Our exposition is in two parts. The first part, entitled *Communication*, focuses on communication complexity per se. Here communication protocols are rigorously defined and the foundations of the theory are built. The second part, entitled *Applications*, uses the theory to derive conclusions about a variety of different models of computation. In the first part, disjointness serves as a litmus test to see how the ideas we develop are progressing. In the second part, results about disjointness help to determine the limits of other models of computation.

We intend to present the key ideas in the field in the most elegant form possible. This is a textbook of basic concepts, and not a survey of the latest research results. The reader is encouraged to discover the wider body of work that forms the theory of communication complexity by following the many references that are cited in the book.

Like this.

Each page of the book has a large margin, where one can find references to the relevant literature, diagrams, and additional explanations of arguments in the main text.

Acknowledgments

THANKS TO Noga Alon, Anil Ananthaswamy, Arkadev Chattopadhyay, Morgan Dixon, Yaniv Elchayani, Yuval Filmus, Abe Friesen, Mika Göös, Jeff Heer, Pavel Hrubeš, Weston Karnes, Guy Kindler, Vincent Liew, Venkatesh Medabalimi, Or Meir, Shay Moran, Aram Odeh, Rotem Oshman, Sebastian Pokutta, Kayur Patel, Sivaramakrishnan Natarajan Ramamoorthy, Cyrus Rashtchian, Thomas Rothvoß, Makrand Sinha, and Avi Wigderson for many contributions to this book.

We thank the National Science Foundation, the Israel Science Foundation, the Simons Institute for the Theory of Computing, the Technion-IIT, and the University of Washington for their support.

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE
Cambridge University Press
978-1-108-49798-5 — Communication Complexity
Anup Rao , Amir Yehudayoff
Frontmatter
More Information

Conventions and Preliminaries

In this section, we set up notation and recall some standard facts that are used throughout the book.

We mostly use standard notation. The reader is advised to only skim through this section, and come back to it when necessary.

Sets, Numbers, and Functions

$[a, b]$ denotes the set of real numbers x in the interval $a \leq x \leq b$. For a positive integer n, we use $[n]$ to denote the set $\{1, 2, \ldots, n\}$. Following the convention in computer science, we often refer to the numbers 0 and 1 as bits. All logarithms in this book are computed in base 2, unless otherwise specified.

bit = binary digit.

There is a natural identification between the subsets of $[n]$ and binary strings $\{0,1\}^n$. Every set $X \subseteq [n]$ corresponds to its indicator vector $x \in \{0,1\}^n$, defined by $x_i = 1$ if and only if $i \in X$ for all $i \in [n]$.

Given a vector $x = (x_1, x_2, \ldots, x_n)$, we write $x_{\leq i}$ to denote $(x_1, \ldots, x_i)$. We define $x_{<i}$ similarly. We write x_S to denote the projection of x to the coordinates specified by the set $S \subseteq [n]$.

A *function* $f : D \to R$ is an object that maps every element x in the set D to a unique element $f(x)$ of the set R. A Boolean function is a function that evaluates to a bit, namely $R = \{0, 1\}$.

D is the domain and R is the range of the function.

Given two functions f, g that map natural numbers to real numbers, we write $f(n) \leq O(g(n))$ if there are numbers $n_0, c > 0$, such that if $n > n_0$ then $f(n) \leq cg(n)$. We write $g(n) \geq \Omega(f(n))$ when $f(n) \leq O(g(n))$. We write $f(n) \leq o(g(n))$ if $\lim_{n\to\infty} \frac{f(n)}{g(n)} = 0$.

Graphs

A graph is a pair $G = (V, E)$, where V is a set and E is a collection of subsets of V of size 2. The elements of V are called vertices and the elements of E are called edges. The size of the graph G is the number of vertices in it. A clique $C \subseteq V$ in the graph is a subset of the vertices such that every subset of C of size 2 is an edge of the graph. An independent set $I \subseteq V$ in the graph is a set that does not contain any edges. A *path* in the graph is a sequence of vertices $v_1, \ldots, v_n$ such that $\{v_i, v_{i+1}\}$ is an edge for each i. A *cycle* is a path whose first and last vertices are the same. A cycle is called *simple* if all of its edges are distinct. A graph is said to be *connected* if there is a path between every two distinct vertices in the graph. A graph is called a *tree* if it is connected and

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE
Cambridge University Press
978-1-108-49798-5 — Communication Complexity
Anup Rao , Amir Yehudayoff
Frontmatter
More Information

has no simple cycles. The *degree* of a vertex in a graph is the number of edges it is contained in. A *leaf* in a tree is a vertex of degree one. Every tree has at least one leaf. It follows by induction on n that every tree of size n has exactly $n-1$ edges.

Probability

Throughout this book, we consider only finite probability spaces, or uniform distributions on compact sets of real numbers.

Let p be a probability distribution on a finite set Ω. That is, p is a function $p : \Omega \to [0,1]$ and $\sum_{a\in\Omega} p(a) = 1$. Let A be a random variable chosen according to p. That is, for each $a \in \Omega$, we have $\Pr[A = a] = \Pr_p[A = a] = p(a)$. We use the notation $p(a)$ to denote both the distribution of the variable A and the number $\Pr[A = a]$. The meaning is clear from the context. For example, if $\Omega = \{0,1\}^2$ and A is uniformly distributed in Ω, then $p(a)$ denotes the uniform distribution on Ω. However if $a = (0,0)$, then $p(a)$ denotes the number $1/4$. Random variables are denoted by capital letters (like A) and values they attain are denoted by lowercase letters (like a). An event $\mathcal{E}$ is a subset of Ω. The probability of the event $\mathcal{E}$ is $\Pr[\mathcal{E}] = \sum_{a\in\mathcal{E}} p(a)$. Events are denoted by calligraphic letters.

This notation is similar to how $f(x)$ is often used to refer to the function f, when x is a variable, and a fixed value when x is fixed. This notation makes many equations more succinct. We shall encounter complicated scenarios where there are several random variables with a complicated conditioning structure. In those cases, it is helpful to use as succinct a notation as possible.

Given a distribution on 4-tuples $p(a,b,c,d)$, we write $p(a,b,c)$ to denote the marginal distribution on the variables a,b,c (or the corresponding probability). We often write $p(ab)$ instead of $p(a,b)$, for conciseness of notation. We also write $p(a|b)$ to denote either the distribution of A conditioned on the event $B = b$, or the number $\Pr[A = a|B = b]$. In the preceding example, if $B = A_1 + A_2$, and $b = 1$, then $p(a|b)$ denotes the uniform distribution on $\{(0,1),(1,0)\}$ when a is a free variable. When $a = (0,1)$ then $p(a|b) = 1/2$.

Given $g : \Omega \to \mathbb{R}$, we write $\mathbb{E}_{p(a)}[g(a)]$ to denote the expected value of $g(a)$ with respect to p. So, $\mathbb{E}_{p(a)}[g(a)] = \sum_{a\in\Omega} p(a)g(a)$.

The *statistical distance*, also known as *total variational distance*, between two probability distributions $p(a)$ and $q(a)$ is defined to be

$$|p-q| = \frac{1}{2}\sum_a |p(a)-q(a)| = \max_{\mathcal{E}} p(\mathcal{E}) - q(\mathcal{E}),$$

The proof of the second equality is a good exercise.

where the maximum is taken over all events $\mathcal{E}$. For example, if p is uniform on $\Omega = \{0,1\}^2$ and q is uniform on $\{(0,1),(1,0)\} \subset \Omega$, then when a is a free variable $|p(a)-q(a)|$ denotes the statistical distance between the distributions, which is $1/2$, and when $a = (0,0)$, we have $|p(a)-q(a)| = 1/4$.

We sometimes write $p(x) \overset{\epsilon}{\approx} q(x)$ to indicate that $|p(x)-q(x)| \le \epsilon$. Suppose A, B are two random variables in a probability space p. For ease of notation, we write $p(a|b) \overset{\epsilon}{\approx} p(a)$ *for average* b to mean that

$$\mathop{\mathbb{E}}_{p(b)}\left[|p(a|b)-p(a)|\right] \le \epsilon.$$

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE
Cambridge University Press
978-1-108-49798-5 — Communication Complexity
Anup Rao , Amir Yehudayoff
Frontmatter
More Information

Some Useful Inequalities

Markov

Suppose X is a nonnegative random variable, and $\gamma > 0$ is a number. Markov's inequality bounds the probability that X exceeds γ in terms of the expected value of X:

$$\mathbb{E}[X] > p(X > \gamma) \cdot \gamma \Rightarrow p(X > \gamma) < \frac{\mathbb{E}[X]}{\gamma}.$$

Concentration

A sum of independently distributed bits concentrates around its expectation. Namely, the value of the sum is close to its expected value with high probability. The Chernoff-Hoeffding bound controls this concentration. Suppose $X_1, \ldots, X_n$ are independent identically distributed bits. Let $\mu = \mathbb{E}\left[\sum_{i=1}^{n} X_i\right]$. The bound says that for any $0 < \delta < 1$,

$$\Pr\left[\left|\sum_{i=1}^{n} X_i - \mu\right| > \delta\mu\right] \leq e^{-\delta^2\mu/3}.$$

When $\delta \geq 1$, the following bound applies

$$\Pr\left[\sum_{i=1}^{n} X_i > (1+\delta)\mu\right] \leq e^{-\delta\mu/3}.$$

The *binomial coefficient* $\binom{n}{k}$ is the number of subsets of $[n]$ of size k.

These bounds give estimates on binomial coefficients. The idea is to consider $X_1, \ldots, X_n$ that are uniformly distributed and independent random bits. For a number $0 \leq a \leq n/2$, we have

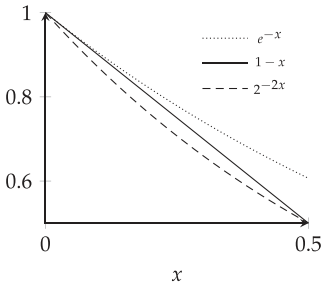
$$\sum_{k \in [n] : |k - n/2| > a} \binom{n}{k} \leq 2^n \cdot e^{-\frac{2a^2}{3n}}.$$

The following upper bounds on binomial coefficients is also useful: for all $k \in [n]$,

$$\binom{n}{k} \leq \frac{2^{n+1}}{\sqrt{\pi n}}.$$

Approximations

We will often need to approximate linear functions with exponentials. The following inequalities are useful: $e^{-x} \geq 1 - x$ for all real x, and $1 - x \geq 2^{-2x}$ when $0 \leq x \leq 1/2$.



Cauchy-Schwartz Inequality

The Cauchy-Schwartz inequality says that for two vectors $x, y \in \mathbb{R}^n$, their inner product is at most the products of their norms.

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE
Cambridge University Press
978-1-108-49798-5 — Communication Complexity
Anup Rao , Amir Yehudayoff
Frontmatter
More Information

$$\left|\sum_{i=1}^{n} x_i y_i\right| = |\langle x, y\rangle| \le \|x\| \cdot \|y\| = \sqrt{\sum_{i=1}^{n} x_i^2} \cdot \sqrt{\sum_{i=1}^{n} y_i^2}.$$

Convexity

A function $f : [a, b] \to \mathbb{R}$ is said to be *convex* if

$$\frac{f(x) + f(y)}{2} \ge f\left(\frac{x+y}{2}\right),$$

for all x, y in the domain. It is said to be concave if

$$\frac{f(x) + f(y)}{2} \le f\left(\frac{x+y}{2}\right).$$

Some convex functions: $x^2, e^x, x \log x$. Some concave functions: $\log x$, $\sqrt{x}$. Note that f is convex if and only if $-f$ is concave.

One can often prove that a function is convex by showing that its second derivative is nonnegative on the domain.

Jensen's inequality says if a function f is convex, then

$$\mathbb{E}\left[f(X)\right] \ge f(\mathbb{E}\left[X\right]),$$

for any random variable $X \in [a, b]$. Similarly, if f is concave, then

$$\mathbb{E}\left[f(X)\right] \le f(\mathbb{E}\left[X\right]).$$

In this book, we often say that an inequality follows *by convexity* when we mean that it can be derived by applying Jensen's inequality to a convex or concave function.

A consequence of Jensen's inequality is the Arithmetic-Mean Geometric-Mean inequality:

$$\frac{\sum_{i=1}^{n} a_i}{n} \ge \left(\prod_{i=1}^{n} a_i\right)^{1/n},$$

which can be proved using the concavity of the log function:

$$\log\left(\frac{\sum_{i=1}^{n} a_i}{n}\right) \ge \frac{\sum_{i=1}^{n} \log a_i}{n} = \log\left(\prod_{i=1}^{n} a_i^{1/n}\right).$$

Try to prove the Cauchy-Schwartz inequality using convexity.

Basic Facts from Algebra

A few places in this book require knowledge about polynomials and finite fields. We cannot give a comprehensive introduction to these topics here, but we state some basic facts that are relevant to this book.

A *field* $\mathbb{F}$ is a set containing 0 and 1 that is endowed with the operations of addition, multiplication, subtraction, and division. If $a, b \in \mathbb{F}$, then $a + b, ab, a - b$ must also be elements of $\mathbb{F}$, and a/b is an element of $\mathbb{F}$ as long as $b \neq 0$. We require that $a - a = 0$ for all $a \in \mathbb{F}$, and

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE
Cambridge University Press
978-1-108-49798-5 — Communication Complexity
Anup Rao , Amir Yehudayoff
Frontmatter
More Information

$a/a = 1$ for all $a \neq 0$. Several other requirements should be met, like commutativity and distributivity.

The simplest example of a field is the field of *rational numbers*. In applications, however, it is often useful to consider fields that have a finite number of elements. The simplest example of a finite field is a prime field. For a prime number p, there is a unique field $\mathbb{F}_p$ containing the p elements $0, 1, 2, \ldots, p-1$. These numbers can be added, subtracted, and multiplied modulo p to get the corresponding field operations. One can define division as well, using the property that p is prime. See Figure 1 for an example.

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

/	1	2	3	4
0	0	0	0	0
1	1	3	2	4
2	2	1	4	3
3	3	4	1	2
4	4	2	3	1

Figure 1 The addition, multiplication, and division tables of $\mathbb{F}_5$.

Vector Spaces

Given a field $\mathbb{F}$, the set $\mathbb{F}^n$ can be viewed as a vector space over $\mathbb{F}$. The elements of $\mathbb{F}^n$ are called vectors. Addition of vectors is defined coordinate-wise, so $(v+w)_i = v_i + w_i$, for all i, and multiplication by a scalar $c \in \mathbb{F}$ is defined as $c \cdot (v_1, v_2, \ldots, v_n) = (cv_1, cv_2, \ldots, cv_n)$, for $c \in \mathbb{F}$.

Linear combinations of vectors are taken using scalar coefficients from the field $\mathbb{F}$. The usual notions of dimension, linear dependence, and linear independence make sense here. A subspace V of $\mathbb{F}^n$ is a set that is closed under additions and multiplications by scalars. Given a subspace $V \subseteq \mathbb{F}$, we define its dual subspace

$$V^\perp = \left\{ w \in \mathbb{F}^n : \sum_{i=1}^{n} v_i w_i = 0 \text{ for all } v \in V \right\}.$$

The following fact is useful: If $V \subseteq \mathbb{F}^n$ is a subspace, the sum of the dimensions of V and $V^\perp$ is always exactly n.

Polynomials

A *polynomial* over the variables $X_1, X_2, \ldots, X_n$ is an expression of the form

$$aX_1X_2X_3^2 + bX_3X_7^3X_5 - cX_1X_4^4.$$

It is a linear combination of monomials, where the coefficients a, b, c are elements of a field. Every polynomial corresponds to a function that can be computed by evaluation, and every function $f : \mathbb{F}^n \to \mathbb{F}$ can be described by a polynomial.

A polynomial is called *multilinear* if every monomial is a product of distinct variables. For example: the polynomial

$$X_1X_2X_3 + 3X_3X_7X_5 - 2X_1X_4$$

is multilinear, and the polynomial X_1^2 is not. A useful fact is that every function $f : \{0,1\}^n \to \mathbb{F}$ can be *uniquely* represented as multilinear polynomial of n variables with coefficients from $\mathbb{F}$.

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-1-108-49798-5 — Communication Complexity
Anup Rao , Amir Yehudayoff
Frontmatter
More Information

© in this web service Cambridge University Press www.cambridge.org