Juraj Hromkovič

Communication Complexity and Parallel Computing

通信复杂性与并行计算

Springer-Verlag

世界图书出版公司

Juraj Hromkovič

Communication Complexity and Parallel Computing

With 40 Figures

Springer-Verlag
世界图书出版公司

书　　名：Communication Complexity and Parallel Computing
作　　者：J. Hromkovič
中 译 名：通信复杂性和并行计算
出 版 者：世界图书出版公司北京公司
印 刷 者：北京中西印刷厂
发　　行：世界图书出版公司北京公司（北京市朝阳门内大街 137 号　100010）
开　　本：1/32　850×1168　　印　张：11
出版年代：2000 年 6 月
书　　号：ISBN 7-5062-4736-4/ TP・58
版权登记：图字 01-1999-2439
定　　价：49.00 元

Prof. Dr. Juraj Hromkovič
Institut für Informatik und Praktische Mathematik
Universität Kiel
Olshausenstr. 40
D-24098 Kiel, Germany

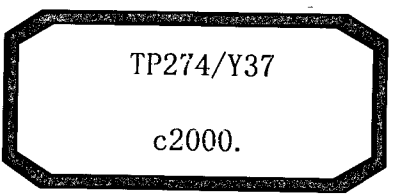
CR Subject Classification (1991): F.1.2-3, F.2.3, G.2.2, B.7.1, C.2.1, F.4.3

Library of Congress Cataloging-in-Publication Data

Hromkovič, Juraj, 1958-
Communication complexity and parallel computing / Juraj Hromkovič.
p. cm. -- (Texts in theoretical computer science)
Includes bibliographical references and index.
ISBN 3-540-57459-X (hardcover : alk. paper)
1. Parallel processing (Electronic computers) 2. Computational complexity. I. Title. II. Series.
QA76.58.H76 1997
005.2'75--dc21 96-29508
CIP

ISBN 3-540-57459-X Springer-Verlag Berlin Heidelberg New York

Texts in Theoretical Computer Science
An EATCS Series



Preface

The communication complexity of two-party protocols is an only 15 years old complexity measure, but it is already considered to be one of the fundamental complexity measures of recent complexity theory. Similarly to Kolmogorov complexity in the theory of sequential computations, communication complexity is used as a method for the study of the complexity of concrete computing problems in parallel information processing. Especially, it is applied to prove lower bounds that say what computer resources (time, hardware, memory size) are necessary to compute the given task. Besides the estimation of the computational difficulty of computing problems the proved lower bounds are useful for proving the optimality of algorithms that are already designed. In some cases the knowledge about the communication complexity of a given problem may be even helpful in searching for efficient algorithms to this problem.

The study of communication complexity becomes a well-defined independent area of complexity theory. In addition to a strong relation to several fundamental complexity measures (and so to several fundamental problems of complexity theory) communication complexity has contributed to the study and to the understanding of the nature of determinism, nondeterminism, and randomness in algorithmics. There already exists a non-trivial mathematical machinery to handle the communication complexity of concrete computing problems, which gives a hope that the approach based on communication complexity will be instrumental in the study of several central open problems of recent complexity theory.

This book presents the basic concepts in the study of communication complexity and in its application in proving lower bounds on distinct fundamental complexity measures. In the applications we focus on the complexity measures of realistic, parallel computing models like combinational (Boolean) circuits, VLSI circuits and interconnection networks. The book is written at a level accessible to advanced undergraduates and to graduate students. Since it gives a survey on the study of communication complexity and formulates a lot of research problems we expect it will also prove to be a reference for researchers in this area.

First of all I would like to thank Grzegorz Rozenberg and Arto Salomaa, who encouraged me to write this book, and to Burkhard Monien and Wolfgang Thomas for the good working atmosphere in Paderborn and Kiel during the work on the book. I am indebted to Ingeborg Mayer, Andrew Ross and Hans

Wössner of Springer-Verlag for their editorial help, comments and suggestions which essentially contributed to the quality of the presentation of the book.

I am grateful for the comments and materials received from several people, including Ivana Černá, Josef Gruska, Ivana Höltring, Oliver Matz, Dana Pardubská, Anna Slobodová, Ondrej Sýkora, Imrich Vrťo, Juraj Waczulík, and Avi Wigderson. Special thanks go to Martin Dietzfelbinger and Georg Schnitger for an intensive research cooperation, which during the work on the book led to the solutions of some open problems enabling to present a complete picture of some research directions on communication complexity in this book. I would like to thank Sebastian Seibert for carefully reading of the whole manuscript. I am indebted to Heidi Luca-Gottschalk, Oliver Matz, Walter Unger, and Thomas Wilke for the help with LaTeX and to Marion Küpper and Gerti Rosenfeld for typing some parts of the manuscript.

My deepest thanks go to Tanja, not only for carefully typing of several parts of this book.

Kiel, January 1997 Juraj Hromkovič

Texts in Theoretical Computer Science – An EATCS Series

J. L. Balcázar, J. Díaz, J. Gabarró
Structural Complexity I
2nd ed. (see also overleaf, Vol. 22)

M. Garzon
Models of Massive Parallelism
Analysis of Cellular Automata and Neural Networks

J. Hromkovič
Communication Complexity and Parallel Computing

A. Leitsch
The Resolution Calculus

A. Salomaa
Public-Key Cryptography
2nd ed.

K. Sikkel
Parsing Schemata
A Framework for Specification and Analysis of Parsing Algorithms

Monographs in Theoretical Computer Science – An EATCS Series

C. Calude
Information and Randomness
An Algorithmic Perspective

K. Jensen
Coloured Petri Nets
Basic Concepts, Analysis Methods and Practical Use, Vol. 1
2nd ed.

K. Jensen
Coloured Petri Nets
Basic Concepts, Analysis Methods and Practical Use, Vol. 2

A. Nait Abdallah
The Logic of Partial Information

Former volumes appeared as EATCS Monographs on Theoretical Computer Science

Vol. 5: W. Kuich, A. Salomaa
Semirings, Automata, Languages

Vol. 6: H. Ehrig, B. Mahr
Fundamentals of Algebraic Specification 1
Equations and Initial Semantics

Vol. 7: F. Gécseg
Products of Automata

Vol. 8: F. Kröger
Temporal Logic of Programs

Vol. 9: K. Weihrauch
Computability

Vol. 10: H. Edelsbrunner
Algorithms in Combinatorial Geometry

Vol. 12: J. Berstel, C. Reutenauer
Rational Series and Their Languages

Vol. 13: E. Best, C. Fernández C.
Nonsequential Processes
A Petri Net View

Vol. 14: M. Jantzen
Confluent String Rewriting

Vol. 15: S. Sippu, E. Soisalon-Soininen
Parsing Theory
Volume I: Languages and Parsing

Vol. 16: P. Padawitz
Computing in Horn Clause Theories

Vol. 17: J. Paredaens, P. DeBra, M. Gyssens, D. Van Gucht
The Structure of the Relational Database Model

Vol. 18: J. Dassow, G. Páun
Regulated Rewriting in Formal Language Theory

Vol. 19: M. Tofte
Compiler Generators
What they can do, what they might do, and what they will probably never do

Vol. 20: S. Sippu, E. Soisalon-Soininen
Parsing Theory
Volume II: LR(k) and LL(k) Parsing

Vol. 21: H. Ehrig, B. Mahr
Fundamentals of Algebraic Specification 2
Module Specifications and Constraints

Vol. 22: J. L. Balcázar, J. Díaz, J. Gabarró
Structural Complexity II

Vol. 24: T. Gergely, L. Úry
First-Order Programming Theories

R. Janicki, P. E. Lauer
Specification and Analysis of Concurrent Systems
The COSY Approach

O. Watanabe (Ed.)
Kolmogorov Complexity and Computational Complexity

G. Schmidt, Th. Ströhlein
Relations and Graphs
Discrete Mathematics for Computer Scientists

S. L. Bloom, Z. Ésik
Iteration Theories
The Equational Logic of Iterative Processes

Springer and the environment

At Springer we firmly believe that an international science publisher has a special obligation to the environment, and our corporate policies consistently reflect this conviction.
We also expect our business partners – paper mills, printers, packaging manufacturers, etc. – to commit themselves to using materials and production processes that do not harm the environment. The paper in this book is made from low- or no-chlorine pulp and is acid free, in conformance with international standards for paper permanency.

Springer

Table of Contents

1. Introduction

1.1 Motivation and Aims

Parallel data processing has become a reality. Large numbers of processors (computers) cooperating to compute a given task have brought an essential speed-up of classical sequential computations. Many computing problems requiring too much time to be solved in real time by sequential machines can be computed in parallel very quickly. Because there are many computing tasks requiring a real-time solution in industry, the investigation of parallel computing is becoming one of the central parts of theoretical computer science and computer engineering. In the theory the study ranges from the study of abstract parallel computing models (complexity measures) and limits to parallel computations (classification of computing problems in two classes: problems that allow quick parallel solution by using a realistic number of processors and problems for which no efficient parallel algorithm exists) to the development of parallel programming languages, communication algorithms for different parallel architectures, and automatic design of VLSI circuits.

This book is devoted to the abstract theory of parallel complexity measures, where one tries to measure the computational difficulty of a computing problem as an inherent property of the problem. We are mainly interested in proving some lower bounds that say what computer resources (time, hardware, memory size) are necessary to compute the given task (problem). The lower bound proofs are usually connected with a detailed analysis of the given computing problems and so they provide knowledge about the nature of the problem. Besides the classification of the computational difficulty of the computing problems the proved lower bounds may be usefull in searching for efficient algorithms for the problem as well as for proving the optimality of algorithms that are already designed.

This book concentrates on only one complexity measure – communication complexity of two-party protocols. Informally, a *two-party protocol* (shortly, *protocol*) is a computing model consisting of two abstract computers C_I and C_{II} with unlimited power. In this book we call C_I the first (left) computer and C_{II} the second (right) computer (see Figure 1.1).

At the beginning one considers that an input w is divided in a balanced way between C_I and C_{II} (for instance, C_I has the first half of the input w and C_{II} obtains the second half of w). The aim is to compute the output for the

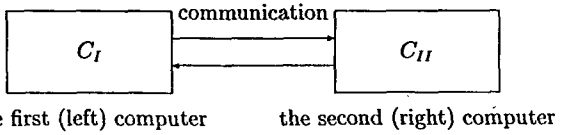


Fig. 1.1. The model of two-party communication protocols

given input w. To achieve this aim C_I and C_{II} are allowed to communicate by exchanging some binary messages. The communication complexity of the computation on w is the sum of the lengths of all messages exchanged between C_I and C_{II}. The communication complexity of a protocol computing a finite problem is the maximum of the communication complexities over all inputs of the problem.

Some natural questions arise: Why write a book about one complexity measure only? Why study a simple model, where the parallelism is restricted to two computers only? The reason is that this communication complexity is useful for parallel computing in a similar way as Kolmogorov complexity has been shown to be useful for the study of sequential computations. The communication complexity measure is so close to a lot of realistic parallel (and even sequential) complexity measures that it can be used as method for proving lower bounds on the complexity measures of fundamental computing models like VLSI circuits, combinatorial circuits, interconnection networks, Turing machines, etc. Moreover, it enables one to achieve new results in the principal topic of theoretical computer science dealing with the comparison of the computational power of deterministic, nondeterministic, and probalistic computations.

The main aim of this book is to provide an overview of the study of communication complexity and its application to parallel computing. The book is written for students as an introduction to this topic as well as for use by researchers interested in working in this area. For these reasons the book includes a lot of exercises of varying difficulty as well as the formulations of research (open) problems of interest.

More precisely, the central aims of the book are the following.

(i) To fix the formalism in the definition of two-party protocols (note that a few distinct formalisms have been considered so far in the literature) and to define several versions of communication complexity depending on the partitions of the input, because different applications require consideration of different sets of input partitions.

(ii) To give an overview of the basic theoretical properties of the communication complexity measure.

(iii) To give an overview of the methods for proving lower bounds on the communication complexity of concrete computing problems. This part is of most interest because the lower bounds on the communication complexity of concrete problems are applied to get lower bounds on the complexity measures of realistic models of parallel computations.

(iv) To give an overview of the main results concerning nondeterministic and probabilistic protocols and their communication complexity. For communication complexity one can establish results that people try but fail to establish for time complexity of sequential computations. For instance, nondeterminism and Monte Carlo probabilism can be much more powerful than determinism for two-party protocols, but deterministic communication complexity is polynomially related to Las Vegas communication complexity.

(v) To give an overview of the use of communication complexity for proving lower bounds on different complexity measures of distinct computing models. The main emphasis is placed on the relation between communication complexity and area-time complexity measures of distinct circuit models.

Recently, a lot of results about communication complexity have appeared in the literature. We are not able to present all of them. The ones chosen for presentation in this book are explained very carefully and their proofs usually contain more details than their counterparts in the journal or proceedings publications. Some of the results from the literature are formulated in the exercises or mentioned in the bibliographical remarks only. Because the central idea of the book is to give methods for proving lower bounds on parallel complexity measures by applying communication complexity, the overviews connected with the aims (iii) and (v) above are more exhaustive than the other ones. The book does not contain any result connected with relativized communication complexity classes and oracles, whose study represents a research direction in communication complexity theory too.

Proving non-trivial lower bounds on the complexity of concrete computing problems and especially the development of mathematical proof methods enabling one to achieve them is probably one of the few central topics of recent theoretical computer science. The reason why we are not able to solve the P versus NP question, which is perhaps the single most important problem of theoretical computer science, is the lack of powerful lower bounds methods in complexity theory. The two-party communication protocol model has enabled us to prove a sequence of important lower bounds and so to contribute essentially to complexity theory. This model provides several lower bound techniques based on information theoretic arguments and is elegant in use. There already exists non-trivial mathematical machinery to handle the communication complexity of concrete problems. From these reasons we hope that the approach based on communication protocols will be instrumental in solving further important open