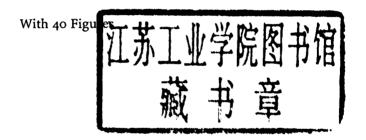
Juraj Hromkovič

# Communication Complexity and Parallel Computing 通信复杂性与并行计算

Springer-Verlag 冯界图出出版公司 Juraj Hromkovič

## Communication Complexity and Parallel Computing



Springer-Verlag 必果例よ业版公司 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

世界图书出版公司北京公司已获得 Springer-Verlag 授权在中国 大陆独家重印发行。 Prof. Dr. Juraj Hromkovič Institut für Informatik und Praktische Mathematik Universität Kiel Olshausenstr. 40 D-24098 Kiel, Germany

### Series Editors

Prof. Dr. Wilfried Brauer Institut für Informatik, Technische Universität München Arcisstrasse 21, D-80333 München, Germany

Prof. Dr. Grzegorz Rozenberg Institute of Applied Mathematics and Computer Science University of Leiden, Niels-Bohr-Weg 1, P.O. Box 9512 2300 RA Leiden, The Netherlands

Prof. Dr. Arto Salomaa Data City Turku Centre for Computer Studies FIN-20520 Turku, Finland

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.
QA76.59.H76 1997
005.2'75--dc21
96-29508
```

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

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer-Verlag. Violations are liable for prosecution under the German Copyright Law.

© Springer-Verlag Berlin Heidelberg 1997 Printed in Germany

The use of registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and therefore free for general use.

This reprint has been authorized by Springer-Verlag (Berlin/Heidelberg/New York) for sale in the People's Republic of China only and not for export therefrom.

Reprinted in China by Beijing World Publishing Corporation, 2000

### Texts in Theoretical Computer Science An EATCS Series

Editors: W. Brauer G. Rozenberg A. Salomaa

Advisory Board: G. Ausiello M. Broy S. Even J. Hartmanis N. Jones T. Leighton M. Nivat C. Papadimitriou D. Scott

TP274/Y37

c2000.

### **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 Vrto, 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
and 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.



### **Table of Contents**

1	Intro	oductio	n	1.
	1.1	Motiva	ation and Aims	1
	1.2		ept and Organization	4
	1.3	How t	o Read the Book	6
2	Con	nmunica	ation Protocol Models	7
	2.1	Basic	Notions	7
		2.1.1	Introduction	7
		2.1.2	Alphabets, Words, and Languages	7
		2.1.3	Boolean Functions and Boolean Matrices	11
		2.1.4	Representation of Computing Problems	16
		2.1.5	Exercises	20
	2.2	Comn	nunication Complexity According to a Fixed Partition	23
		2.2.1	Definitions	23
		2.2.2	Methods for Proving Lower Bounds	30
		2.2.3	Theoretical Properties of Communication Complexity	
			According to a Fixed Partition	53
		2.2.4	Exercises	57
		2.2.5	Research Problems	59
	2.3	Comm	nunication Complexity	60
		2.3.1	Introduction	60
		2.3.2	Definitions	61
		2.3.3	Lower Bound Methods	62
		2.3.4	Theoretical Properties of Communication Complexity	70
		2.3.5	Communication Complexity and Chomsky Hierarchy	77
		2.3.6	Exercises	82
		2.3.7	Research Problems	83
	2.4	One-V	Way Communication Complexity	83
		2.4.1	Introduction	83
		2.4.2	Definitions	84
		2.4.3	Methods for Proving Lower Bounds	86
		2.4.4	Communication Complexity Versus One-way	
			Communication Complexity	92
		2.4.5	Exercises	95
		2.4.6	Research Problems	96

### viii Table of Contents

	2.5	Nondeterministic Communication Complexity and			
		Rando	omized Protocols	97	
		2.5.1	Introduction	97	
		2.5.2	Nondeterministic Protocols	98	
		2.5.3	Lower Bounds on Nondeterministic Communication		
			Complexity	105	
		2.5.4	Deterministic Protocols Versus Nondeterministic		
		•	Protocols	109	
		2.5.5	Randomized Protocols	115	
		2.5.6	Randomness Versus Nondeterminism and Determinism .	123	
		2.5.7	Exercises	127	
		2.5.8	Research problems	130	
	2.6	An Im	proved Model of Communication Protocols	131	
		2.6.1	Introduction	131	
		2.6.2	Definitions	132	
		2.6.3	Lower Bound Methods	135	
		2.6.4	Communication Complexity Versus s-communication		
			Complexity	139	
		2.6.5	Some Properties of s-communication Complexity	140	
		2.6.6	Exercises	143	
		2.6.7	Problems	144	
	2.7	Biblio	graphical Remarks	144	
3		lean Ci		151	
	3.1	Introd	luction	151	
	3.2		tions and Fundamental Properties	152	
		3.2.1	Introduction	152	
		3.2.2	Boolean Circuit Models	152	
		3.2.3	Fundamental Observations	159	
		3.2.4	Exercises	163	
	3.3	Lower	Bounds on the Area of Boolean Circuits	164	
		3.3.1	Introduction	164	
		3.3.2	Definitions	164	
		3.3.3	Lower Bounds on the Area Complexity Measures	167	
		3.3.4	A Comparison of two Area Complexity Measures	173	
		3.3.5	Three-Dimensional Layout	179	
		3.3.6	Exercises	182	
		3.3.7	Problems	184	
	3.4	Topole	ogy of Circuits and Lower Bounds	185	
		3.4.1	Introduction	185	
		3.4.2	Separators	185	
		3.4.3	Lower Bounds on Boolean Circuits with a Sublinear		
			Separator	192	

		3.4.4	Circuit Structures for Which Communication	
			Complexity Does Not Help	196
		3.4.5	Planar Boolean Circuits	200
		3.4.6	Exercises	215
		3.4.7	Problems	217
	3.5	Lower	Bounds on the Size of Unbounded Fan-in Circuits	217
		3.5.1	Introduction	217
		3.5.2	Method of Communication Complexity of	
			Infinite Bases	218
		3.5.3	Unbounded Fan-in Circuits with Sublinear	
			Vertex-Separators	222
		3.5.4	Exercises	224
		3.5.5	Problems	225
	3.6	Lower	Bounds on the Depth of Boolean Circuits	225
		3.6.1	Introduction	225
		3.6.2	Monotone Boolean Circuits	226
		3.6.3	Communication Complexity of Relations	229
		3.6.4	Characterizations of Circuit Depth by the	
			Communication Complexity of Relations	231
		3.6.5	Exercises	236
		3.6.6	Research Problems	237
	3.7	Biblio	graphical Remarks	237
4			its and Interconnection Networks	241
	4.1		uction	241
	4.2		tions	242
		4.2.1	Introduction	242
		4.2.2	A VLSI circuit Model	242
		4.2.3	Complexity Measures	247
		4.2.4	Probabilistic Models	250
		4.2.5	Exercises	251
	4.3		Bounds on VLSI Complexity Measures	252
		4.3.1	Introduction	252
		4.3.2	Lower Bounds on Area Complexity	252
		4.3.3	Lower Bounds on Tradeoffs of Area and Time	254
		4.3.4	VLSI circuits with Special Communication Structures	258
		4.3.5	Exercises	263
		4.3.6	Problems	264
	4.4		onnection Networks	264
		4.4.1	Introduction	264
		4.4.2	A Model of Interconnection Networks	265
		4.4.3	Separators and Lower Bounds	266
		4.4.4	Exercises	270
		4.4.5	Problems	270

### x Table of Contents

	4.5	Multile	ective VLSI circuits
		4.5.1	Introduction and Definitions
		4.5.2	Multilectivity Versus Semilectivity 27
		4.5.3	Lower Bounds on Multilective VLSI programs 27
		4.5.4	Exercises
		4.5.5	Problems
	4.6	Bibliog	graphical Remarks
5	Sequ	ential (	Computations
	5.1		uction
	5.2		Automata
		5.2.1	Introduction
		5.2.2	Definitions
		5.2.3	One-Way Communication Complexity and
			Lower Bounds on the Size of Finite Automata 28
		5.2.4	Uniform Protocols 28
		5.2.5	Exercises
		5.2.6	Research Problems
	5.3	Turing	Machines
		5.3.1	Introduction
		5.3.2	Time Complexity of Classical Turing Machines 29
		5.3.3	Sequential Space and Time-Space Complexity 29
		5.3.4	Exercises
		5.3.5	Research Problems
	5.4	Decisio	on Trees and Branching Programs
		5.4.1	Introduction
		5.4.2	Definitions
		5.4.3	Capacity of Branching Programs
		5.4.4	Lower Bounds on the Depth of Decision Trees 30
		5.4.5	Exercises
		5.4.6	Research Problems
	5.5	Bibliog	graphical Remarks
Re	feren	ces .	
	1		90

### 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

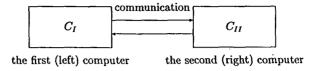


Fig. 1.1. The model of two-party communication protocols

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