

**Lower Bounds for Probabilistic Communication Complexity
and for the Depth of Monotone Boolean Circuits**

Thesis submitted for the Degree

"Doctor of Philosophy"

by Ran Raz

Submitted to the Senate of the Hebrew University

in 1992

This work was carried out under the supervision of

Professor Michael Ben-Or and Professor Avi Wigderson

Contents

I. Introduction.	1
I.1 Communication complexity and boolean circuits.	5
I.2 Probabilistic communication complexity.	8
I.3 Universal boolean relations.	11
I.4 Problems of graph connectivity.	14
I.5 The Matching function and the Clique function.	16
II. Uniform ways of behavior of big sets of paths and cuts in graphs.	17
II.1 The deviation from uniformity of a low-information probabilistic measure.	20
II.2 The paths-cuts graph structure.	22
II.3 The behavior of a big set of cuts, under projection.	30
II.4 More about the behavior of big sets of cuts.	33
III. The probabilistic communication complexity	
of the monotone boolean relation R_{stc}^m .	37
III.1 A preparatory lemma.	44
III.2 The main lemma.	73
III.3 A lower bound for a deterministic protocol with mistakes.	75
III.4 A lower bound for a probabilistic protocol.	80
IV. More about the st-connectivity function in graphs.	81
IV.1 A lower bound for a semi-monotone computation of the st-connectivity function.	81
V. The depth of monotone computations of the Clique and the Matching functions.	87
V.1 A lower bound for the Matching function.	88
V.2 Additional results.	95

Introduction

"Communication Complexity" is an area of research dealing with the quantity of information that two players have to transfer between them, in order to compute a value of a given two input function. In the beginning each player knows only the value of his own input. The research in the area had been originated by Yao [Y] and had been continued in many works, the main point of interest being: to establish lower bounds for the communication complexity in different cases.

The logical scheme of "boolean circuits" is a model of computation which has been investigated for some decades. In this model the input is a string of binary digits (bits) and the computation is performed by logical gates. The output is also a string of bits and in many cases it is assumed that the output is only one bit long. Two important parameters which characterize a boolean circuit are: its size and its depth. The size of a boolean circuit is defined as: The number of gates in it. The depth of the circuit is the maximal distance between its input and its output. One of the main directions of research in the area, is establishing lower bounds for the size and the depth of circuits computing certain functions. Such bounds give immediate bounds for all the other computation models, and this includes the Turing machine model. So far there are very few successes in this direction. The basic questions in the area are still open. In particular, the best known lower bounds for an explicit function are: $\Omega(n)$ for the size and $\Omega(\log n)$ for the depth, and this does not amount to anything.

It had been easier to find lower bounds in weaker computation models. One of these models is the computation model of "monotone boolean circuits". A monotone circuit is a circuit which computes a monotone boolean function using only AND and OR gates. The first results giving lower bounds for monotone circuits, appeared in Razborov [R1] [R2], who gave super-polynomial bounds for the size of circuits computing certain functions. [AB] using the same approach obtained exponential

bounds for the size of those circuits. Exponential bounds were also obtained by Andreev [A].

There is a surprising connection between the research areas of: "lower bounds for communication complexity" and "lower bounds for the depth of boolean circuits", discovered by Karchmer and Wigderson [KW]. [KW] deals with communication complexity of relations, i.e. problems in communication complexity in which the set of all possible outputs for a given input is of magnitude possibly larger than one. The connection is given by a reduction which matches every boolean function f with a communication complexity problem R_f , and every monotone function f with a communication complexity problem R_f^m . The communication complexity of R_f is equal to the minimal depth of a boolean circuit computing f . The communication complexity of R_f^m is equal to the minimal depth of a monotone circuit computing f . This connection between those two areas was used in [KW] to prove an $\Omega(\log^2 n)$ lower bound for the depth of monotone boolean circuit computing the st -connectivity function in graphs. This function gets a graph as an input and decides whether it contains a path between two special vertices in it.

A very natural question to ask, about a connection between areas, is whether the connection is a tool that gives a different understanding of the problem, or only a different presentation of it. The proof, given in [KW], does not resolve this question, because it can be translated very easily to a proof that does not use communication complexity at all.

The problems R_f and R_f^m , that we have mentioned, are deterministic problems, but in the area of communication complexity we always look on the probabilistic case also.

Another natural question about the connection, we have been talking about, is: Could the area of probabilistic communication complexity help us with the understanding of

boolean circuits ?

This work studies the relations between the research of communication complexity, and the research of the depth of boolean circuits. It tries to answer affirmatively the two questions we have asked, and to give some lower bounds in both areas.

In the area of "communication complexity" research, a lot of effort is made developing new tools, and the results are less important. In the area of "boolean circuits" research the opposite is true, the results are very important and we try to obtain better and better lower bounds. In these two points this work tries to contribute.

Chapter I of the work is an introduction that gives a review and some definitions. Chapters II, III and IV deal with the st -connectivity function in graphs, and with some related communication complexity problems:

Chapter III looks at the communication complexity problem R_f^m , related to the st -connectivity function in graphs, and proves for this problem an $\Omega(\log^2 n)$ probabilistic lower bound, which generalizes the deterministic lower bound of [KW].

Chapter IV uses the same tools and gives a lower bound for the depth of computation of the st -connectivity function by a semi-monotone boolean circuit, which means: a circuit in which we allow negations of only a limited number of input variables. In particular it is proven that every NC1 circuit, which computes this function, uses the negations of at least a constant percentage of the input variables. Every circuit that uses less than a constant percentage of the input variables is not NC1.

Chapter III and IV use the same tools and require some useful lemmas which are proven in Chapter II. All these lemmas deal with uniform ways of behavior of big sets. Some of the lemmas have also a value of their own.

Chapter V is an independent part which proves lower bound for the depth of monotone circuits computing some functions of graphs. Among these functions are the **Matching** function and the **Clique** function. The proof goes through a number of reductions, that together reduce the probabilistic communication complexity problem of

Disjointness to these functions. For this problem, which is a classical problem in communication complexity, there is a linear lower bound [KS]. These bounds give lower bounds of $\Omega(n)$ in terms of the vertex number, and improve lower bounds of $\Omega(\log^2 n)$ for the Matching function [R2], and $\Omega(n^{1/3})$ for the Clique function [AB], derived from the related bounds for the size. (The $\Omega(n^{1/3})$ bound for the Clique function was till now the best known lower bound for any explicit function). The $\Omega(n)$ bounds are also the upper bounds.

From these bounds we get additional results. One of these results, which is derived from the bound for the Matching function, is the existence of a gap between the depth of the monotone computation, and the depth of the non monotone computation. This gap is shown to be exponential.

All the parts of this work try to contribute to the understanding of the connection between "communication complexity" and "depth of boolean circuits", and to show the possibility of using tools and results from the area of "probabilistic communication complexity", in order to get lower bounds for the depth of circuits.