Some Contributions of the Study of Abstract Communication Complexity to Other Areas of Computer Science

Juraj Hromkovič
Department of Computer Science I (Algorithms and Complexity), RWTH Aachen, 52056 Aachen, Germany

The aim of this survey is to present some contribution of the study of two-party communication protocols to other areas of computer science. Here, we concentrate on the applications of communication complexity for the study of several fundamental computing models, for the comparison of the power of deterministic, and probabilistic computations, and for the development of some kind of secure communication protocols in the practice

1. INTRODUCTION

The communication complexity of two-party protocols has been introduced by Abelson [1] and Yao [13] in 1978-1979. The initial goal was to develop a method for proving lower bounds on the complexity of distributed and parallel computations, with a special emphasis on VLSI computations.

Informally, a **two-party (communication) protocol** consists of two computers C_I and C_{II} computing a function[1] $f : X \times Y \to Z$ in the following way. At the beginning C_I obtains an input $x \in X$ and C_{II} obtains an input $y \in Y$. Then C_I and C_{II} communicate according to the protocol by exchanging binary messages until one of them knows the result $f(x, y)$. The complexity of the computation on input (x, y) is the sum of the lengths of messages exchanged. The complexity of the protocol is the maximum of the complexities over all inputs from $X \times Y$. The **communication complexity of f, $cc(f)$**, is the complexity of the best protocol for f.

A protocol is one-way if, for every input, C_I sends only one message to C_{II} and after that C_{II} determines the result based on its input and the received message. The **one-way communication complexity of f, $cc_1(f)$**, is the complexity of the best one-way protocol for f.

In the 20 years of its existence communication complexity has brought much more than one has expected at the beginning in the early eighties. Communication

[1] Usually f is considered to be a Boolean function, i.e., $Z = \{0, 1\}$

This work was supported by grant No. 95/5305/277 of the Slovak Grant Agency.

complexity has established itself as a subarea of complexity theory due to the well developed mathematical machinery to approximately determine the communication complexity of concrete computing problems (see, for instance [2; 3; 4; 6; 7; 9]).

The main contributions of two-party communication complexity may be divided into the following three main streams:

(1) The study of the relation between communication complexity and other complexity measures of fundamental computing models. In this way communication complexity becomes a very successful method for proving lower bounds in many subareas of complexity theory.
(2) The comparison of the power of determinism, nondeterminism and randomness has been successful for communication complexity. This has essentially contributed to the understanding of the nature of the fundamental modes of computation.
(3) New concepts for communication protocols have been developed with significant applications especially in cryptography.

The next three sections provide more details on the influence and the contributions of communication complexity study to other areas of computer science.

2. CONTRIBUTIONS TO THE STUDY OF OTHER COMPUTING MODELS

Analogous to the applications of Kolmogorov complexity in the theory of sequential computations, communication complexity has been developed as a method for the study of the complexity of concrete computing tasks, especially (but not only) in parallel information processing. Mainly, it has been applied to prove lower bounds on required computer resources (i.e, time, hardware, memory size, etc.) in order to compute a given task. For several computing models the method based on communication complexity is the most successful one among the lower bound methods used for these models.

The following, not exhaustive list shows fundamental complexity measures for which communication complexity has been used to prove lower bounds:

—VLSI circuits
  —trade-offs of area and time (also for three-dimensional circuits)
  —area complexity
  —area and other complexity measures of multilective VLSI circuits
—Boolean circuits
  —depth of general Boolean circuits and monotone Boolean circuits
  —combinational complexity of (multilective) planar Boolean circuits and circuits with sublinear separators
  —area complexity of Boolean circuits
  —combinational complexity of unbounded fan-in circuits
  —length of Boolean formulae
—Complexity trade-offs for interconnection networks with different topologies
—Size of finite automata
—Time and space complexity of Turing machines
—Size of linear programs

—Size of distinct models of branching programs
—Depth of decision trees
—Data structure problems.

To illustrate the progress covered by the above list we mention two specific contributions. The first superlinear lower bound on the size of planar Boolean circuits computing a specific Boolean function and the first superpolylogarithmic lower bounds on the depth of monotone Boolean circuits have been established.

The big success of communication complexity application should not to be surprising because we have information transfer in all computing models (for instance, between two parts of input data , between some parts (processors) of a parallel computing model, between two time moments, etc.). So, you can cut hardware, time, or both in your computing model, and then apply lower bounds on the communication complexity of your computing problem. In this way you have a lower bound on the information transfer that must be realized in the computing model considered in order to compute the given task. The appropriate choice of the cut is crucial for obtaining good lower bounds.

One of the perspectives is to extend the applications for proving lower bounds for multilective and/or non-oblivious computing models. This is one of the hardest tasks of special importance in complexity theory. The recent results show that using Ramsey theory and communication complexity over overlapping (not disjoint) partitions of inputs one has good chances to achieve progress in this hard topic too.

3. NONDETERMINISTIC AND RANDOMIZED COMPUTATIONS

One of the central principal questions of current theoretical computer science is which computational power have nondeterministic and randomized computations, especially in the comparison with the deterministic one. The fundamental questions about polynomial time computations (like P versus NP, P versus ZPP, P versus R) are long-stated open problems. For communication complexity the research has been successful and the relation between determinism, nondeterminism and randomness has been fixed. This has essentially contributed to the understanding of the nature of randomness and nondeterminism. Some of the main results are the following ones:

(1) There are exponential gaps between
—determinism and Monte Carlo randomness
—nondeterminism and bounded error probabilism.
(2) Deterministic communication can be bounded by at most twice the product of nondeterministic communication of the language and its complement. This implies an at most quadratic gap between determinism and Las Vegas randomization. A language having this quadratic gap has been found.
(3) There is a linear gap between determinism and Las Vegas randomness for one-way communication complexity.
(4) $O(\log n)$ random bits are sufficient to reach the full power of randomized communication for Las Vegas and Monte Carlo (error-bounded) protocols.
(5) In contrast to 4. there exist high thresholds on the amount of nondeterminism (for some computing problems the deterministic communication complexity is

almost the same as the nondeterministic one until one does not consider a large number (for instance, $\sqrt{n}$) of nondeterministic guesses).

Because communication complexity is strongly related to other computing models there are several consequences of the results above. To mention at least one of them let us consider finite automata whose size is related to one-way communication complexity. Applying (3) one obtains an at most quadratic gap (in the number of states) between deterministic finite automata and Las Vegas ones. This is the first proof of a polynomial relation between determinism and Las Vegas randomization for a uniform computing model. One of the main research perspectives in this area is to try to extend the obtained results and methods in order to understand the possible difference between deterministic computation and randomized computation for further computing models.

Completely another contribution is the fact that two-party communication protocols may be used to generate sequences of pseudo-random bits of high quality.

4. PRIVATE COMMUNICATION

A lot of effort has been done in order to achieve a secure communication[2] between two parties in cryptography. In communication complexity theory the following question has been considered. For which functions $f : X \times Y \rightarrow Z$ one can communicate in such a way, that after the communication the following situation appears:

(1) Both C_I and C_{II} know $f(x, y)$ for the given input x of C_I and y of C_{II}.
(2) C_I has no information about y, except for information one can learn knowing only x and $f(x, y)$.
(3) C_{II} has no information about x, except for information one can learn knowing only y and $f(x, y)$.

This formulation of security has clearly a new dimension. To be protected against adversaries is not sufficient, one wants protection against the counterpart in communication too. It is really surprising how many practically interesting functions may be evaluated in this way. For instance, a randomized private protocol for the following task may be constructed.

C_I knows a number x and C_{II} knows a number y. After the communication both C_I and C_{II} know whether $x < y$ or not, but no additional information about the input of the counterpart in communication. Popular variants of this problems are for instance: two people want to find out who is older without disclosing any other information about their ages or two millionaires want to find out who is richer without disclosing any information about their wealth.

One can expect that we shall learn still a lot of surprising protocols in the study of private communication.

5. CONCLUSION

There are several hundreds papers devoted to the study of communication protocols. The previous chapters have presented some of the reasons why we believe that the concept of communication protocols may be very fruitful for the theory and the

[2]protected against adversaries

practice in computer science. More detailed information can be found especially in two monographs [6; 4]. While [4] is mainly devoted to the topic of section 2, [6] preferably deals with the topic of section 3. Further interesting partial overviews can be found in [5; 8; 7; 10; 11; 12].

REFERENCES

[1] Ableson, H.: Lower bound on information transfer in distributed computations, Proc. *19th IEEE FOCS*, IEEE 1978, pp. 151-158.

[2] Aho, A.V., Ullman, J.D., Yannakakis, M.: On notions of informations transfer in VLSI circuits, Proc. *15th ACM STOC*, ACM 1983, pp.133-139.

[3] Dietzfelbinger, M., Hromkovič, J., Schnitger, G.: A comparison of two lower bounds methods for communication complexity, *Theoretical Computer Science* 168 (1996), 39-51.

[4] Hromkovič, J.: *Communication Complexity and Parallel Computing*, Springer 1997, 336p.

[5] Hromkovič. J.: Communication complexity and lower bounds on multilective computations. Unpublished manuscript, RWTH Aachen 1998. (extended abstract of a part of this paper in Proc. *MFCS '98, Lecture Notes in Computer Science 1450*, Springer 1998, pp. 789-797.)

[6] Kushilevitz, E., Nisan, N.: *Communication Complexity*, Cambridge University Press 1997.

[7] Lovász, L.: Communication Complexity. A Survey., In: *Paths, Flows and VLSI Layout* (Korte, Lovász, Promel and Schrijver, eds.), Springer 1990, pp. 235-266.

[8] Lengauer, Th.: VLSI Theory, In: *Handbook of Theoretical Computer Science*, Vol. A, Algorithms and Complexity, Elsevier 1990, pp. 835-868.

[9] Nisan, N., Wigderson, A.: On rank versus communication complexity, *Combinatorica 15* (1995), 557-565.

[10] Orlitsky, A., El Gamal, A.: Communication Complexity, In: *Complexity in Information Theory* (Y. Abu-Mostafa, ed.), Springer-Verlag 1988.

[11] Ullman, J.D.: *Computational Aspects of VLSI*, Computer Science Press 1994.

[12] Wigderson, A.: Information theoretic reasons for computational difficulty or communication complexity for circuit complexity, Proc. *Int. Congress of Mathematicians 1990*, Japan, pp.1537-1548.

[13] Yao, A.C.: Some complexity questions related to distributive computing, Proc. *11th ACM STOC*, ACM 1979, pp. 209-213.

[14] Yao, A.C.: How to generate and exchange secrets, Proc. *27th IEEE FOCS*, IEEE 1986, pp.162-167.