42nd IEEE Symposium on Foundations of Computer Science

Proceedings

42nd IEEE Symposium on Foundations of Computer Science

October 14 – 17, 2001
Las Vegas, Nevada, USA

Sponsored by
IEEE Computer Society Technical Committee on
Mathematical Foundations of Computing

IEEE COMPUTER SOCIETY

Los Alamitos, California
Washington • Brussels • Tokyo

IEEE Computer Society Order Number PR01390
ISBN 0-7695-1390-5
ISBN 0-7695-1391-3 (case)
ISBN 0-7695-1392-1 (microfiche)
ISSN Number 0272-5428

Additional copies may be ordered from:

IEEE Computer Society
Customer Service Center
10662 Los Vaqueros Circle
P.O. Box 3014
Los Alamitos, CA 90720-1314
Tel: + 1-714-821-8380
Fax: + 1-714-821-4641
E-mail: cs.books@computer.org

IEEE Service Center
445 Hoes Lane
P.O. Box 1331
Piscataway, NJ 08855-1331
Tel: + 1-732-981-0060
Fax: + 1-732-981-9667
http://shop.ieee.org/store/
customer-service@ieee.org

IEEE Computer Society
Asia/Pacific Office
Watanabe Bldg., 1-4-2
Minami-Aoyama
Minato-ku, Tokyo 107-0062
JAPAN
Tel: + 81-3-3408-3118
Fax: + 81-3-3408-3553
tokyo.ofc@computer.org

Editorial production by Bob Werner
Cover art production by Alex Torres
Printed in the United States of America by VictorGraphics, Inc.

IEEE COMPUTER SOCIETY

Proceedings

42nd IEEE Symposium on Foundations of Computer Science

FOCS 2001

Foreword

The papers in these proceedings were presented at the 42nd Annual Symposium on Foundations of Computer Science (FOCS 2001) sponsored by the IEEE Technical Committee on Mathematical Foundations of Computing. The conference was held in Las Vegas, Nevada, October 14-17, 2001.

The program committee consisted of Susanne Albers (Dortmund and Freiburg), James Aspnes (Yale), Moses Charikar (Google and Princeton), Bernard Chazelle (Princeton and NECI), Cynthia Dwork (Compaq SRC), David Eppstein (UC Irvine), Jon Kleinberg (Cornell), Daniele Micciancio (UC San Diego), Peter Bro Miltersen (Aarhus), Moni Naor (Weizmann, Stanford and IBM Almaden), Ran Raz (Weizmann and IAS), Dana Ron (Tel-Aviv), Alistair Sinclair (UC Berkeley), D. Sivakumar (IBM Almaden), Madhu Sudan (MIT), and Salil Vadhan (Harvard).

The program committee met on June 29-30, 2001 and selected 63 papers from 214 submitted (one was withdrawn). The submissions were reviewed as carefully as time permitted, but they were not formally refereed. It is expected that many of them will appear in a more polished and complete form in scientific journals in the future. In addition to the regular program, the committee also invited three tutorial lectures from Christos Papadimitriou, Piotr Indyk and Madhu Sudan.

The committee selected two papers to jointly receive the Machtey Award for the best student-authored paper. These were "Almost Tight Upper Bounds for Vertical Decompositions in Four Dimensions", by Vladlen Koltun from Tel-Aviv University and "How to Go Beyond The Black-Box Simulation Barrier", by Boaz Barak from the Weizmann Institute of Science. The committee noted with pleasure that there were many excellent candidates for this award.

The committee wishes to thank all those who submitted papers for consideration, as well as those external reviewers who helped evaluate the submissions. A list of the latter individuals appears under the heading "Reviewers." The program committee also wishes to thank Steven Tate for running the electronic submission server and Bob Werner for the productions of these proceedings.

Moni Naor
Program Committee Chair

Program Committee

Chair of the IEEE Technical Committee on Mathematical Foundations of Computing
Prabhakar Raghavan, Verity

Local Arrangement and Finance Chairs
Lawrence L. Larmore and Wolfgang Bein (University of Nevada at Las Vegas)

Program Committee Chair
Moni Naor (Weizmann Institute, Stanford University and IBM Almaden)

Program Committee Members
Susanne Albers
James Aspnes
Moses Charikar
Bernard Chazelle
Cynthia Dwork
David Eppstein
Jon Kleinberg
Daniele Micciancio
Peter Bro Miltersen
Moni Naor
Ran Raz
Dana Ron
Alistair Sinclair
D. Sivakumar
Madhu Sudan
Salil Vadhan

Machtey Award

"Almost Tight Upper Bounds for Vertical Decompositions in Four Dimensions"
Vladlen Koltun

and

"How to Go Beyond the Black-Box Simulation Barrier"
Boaz Barak

Reviewers

Andris Ambainis
Ziv Bar-Yossef
Marshall Bern
Michel Abdalla
Pankaj Agarwal
Dorit Aharonov
Noga Alon
Stephen Alstrup
Matthew Andrews
Sanjeev Arora
Hagit Attiya
Yossi Azar
Paul Beame
Shai Ben-David
Rachel Ben-Eliyahu
Dan Boneh
Gerth Brodal
Nader Bshouty
Mike Burrows
Jin-Yi Cai
Ran Canetti
Timothy Chan
Isaac Chuang
Richard Cleve
Edith Cohen
Richard Cole
Wim Van Dam
Jim Demmel
Martin Dyer
Guy Even
Shimon Even
Rolf Fagerberg
Lisa Fleischer
Lance Fortnow
Gudmund S. Frandsen
Lance Fortnow
Nir Friedman
Naveen Garg
Leszek Gasieniec
Ricard Gavalda
Sally Goldman
Oded Goldreich
Catherine Greenhill
Xin Guo
David Guijarro
Anupam Gupta
Vassos Hadzilacos
Xin He
Lisa Hellerstein
Monika Henzinger
Tom Henzinger
Maurice Herlihy
Alejandro Hevia
Mark Huber
Russell Impagliazzo
Adam Kalai
Kyriakos Kalorkoti
Haim Kaplan
Bruce Kapron
Julia Kempe
Valerie King
Guy Kortsarz
Robert Krauthgamer
Michael Krivelevich
Ravi Kumar
Ming Li
Yehuda Lindell
Ami Litman
Peter Maass
Mohammad Mahdian
Madhav Marathe
Dieter van Melkebeek
Neri Merhav
Sara Miner
Nina Mishra
John Mitchell
Joe S. B. Mitchell
Michael Mitzenmacher
David Mount
Seffi Naor
Ashwin Nayak
Christos Papadimitriou
David Parkes
Boaz Patt-Shamir
David Peleg
Yuval Peres
Avi Pfeffer
Benny Pinkas
Toni Pitassi
Yuval Rabani
Jaikumar Radhakrishnan
Venkatesh Raman
Satish Rao
Theis Rauhe
Alexander Razborov
Amir Ronen
Ronny Roth
Tim Roughgarden
Ronitt Rubinfeld
Alex Russell
Boris Ryabko
Alex Samorodnitsky
Rob Schapire
Leonard Schulman
Rocco Servedio
David Shmoys
Amin Shokrollahi
Dan Simon
Michiel Smid
Aravind Srinivasan
Martin Strauss
Bernd Sturmfels
Benny Sudakov
Eva Tardos
Amnon Ta-Shma
Gadi Taubenfeld
Jayram Thathachar
Mikkel Thorup
Andrew Tomkins
Luca Trevisan
Moshe Vardi
Steve Vavasis
Umesh Vazirani
Martin Vetterli
Eric Vigoda
Berthold Voecking
Van Vu
David Wagner
John Watrous
Rolf Wanka
Bogdan Warinschi
Avi Wigderson
David Williamson
Peter Winkler
Yunhong Zhou
David Zuckerman
Uri Zwick

Contents

42nd IEEE Symposium on Foundations of Computer Science — FOCS 2001

Session 2
Chair: Cynthia Dwork

Session 3
Chair: Jon Kleinberg

Session 4
Chair: Ran Raz

Session 5
Chair: David Eppstein

Session 6
Chair: D. Sivakumar

Session 7
Chair: Susanne Albers

Session 8
Chair: Peter Bro Miltersen

Session 9
Chair: Moses Charikar

Session 10
Chair: Moni Naor

Session 11
Chair: James Aspnes

Session 12
Chair: Daniele Micciancio

Tutorials Day

Tutorial 1

Game Theory and Mathematical Economics:
A Theoretical Computer Scientist's Introduction

CHRISTOS H. PAPADIMITRIOU
Computer Science Dept.
U.C. Berkeley
christos@cs.berkeley.edu

August 8, 2001

Abstract

There has been recently increasing interaction between Game Theory and, more generally, Economic Theory, with Theoretical Computer Science, mainly in the context of the Internet. This paper is an invitation to this important fronteer.

1 Introduction

During the past decade the crucial role of computation in the world's economy has been made explicit, while the complex economic nature of certain novel computational artifacts such as the Internet also became apparent. During the same time, and probably not by coincidence, there has been much intellectual activity in the interface between Computer Science and Economics, especially the more mathematically inclined sectors of the respective research communities. The purpose of this paper is to give to researchers in Theoretical Computer Science a glimpse into this exciting field and some of its literature.

Understanding the literature and world outlook of Game and Economic Theory is in my opinion a thoroughly worthwhile challenge.[1] [37] and [14] are excellent introductions to Game Theory; see also [24] for another point of view, and the handbook [1] for a much more extensive and complete exposition (including a chapter on computational issues by Nati Linial). A very well-written and comprehensive introduction to the more general subject of Mathematical Economics is [29], and see also [23] for a less mathematical, but by no mean less sophisticated, book; both of these books also contain extensive treatments of Game Theory. For a recent survey of the interface with Computer Science see [38]; see also the home page of the graduate course [39] for more references as well as lecture notes on certain subjects covered here.

2 Nash Equilibrium

Game Theory, founded by von Neumann and Morgenstern [49], studies the behavior of rational economic agents in mathematically well-defined competitive situations called *games*. A game consists of two or more *players*, each with a set of *strategies*, and for each combination of strategies there is a numerical *payoff* for each player; players know this setup, are rational (and aware of each other's rationality...), and seek to maximize their payoffs. How do players act in such situations? The predominant "concept of rationality" here is the *Nash equilibrium*, a distribution on each player's strategy space (that is, a randomized play), the expected payoff of which no player can improve by changing the distribution. The classical result stating that all finite games have a Nash equilib-

[1] To quote [38], "Game Theory's sharp but pointedly faithful modeling, twisted cleverness, and unexpected depth make it quite akin to our field; but this may also be deceptive, since Game Theory is also characterized by a cohesive and complex research tradition and a defiantly original point of view and norms that are hard to get accustomed to."

rium already suggests a most important open problem of an algorithmic nature: Given a game (say, the matrix of the payoffs — the problem is open even in the case of two players), find a Nash equilibrium in polynomial time. See [40] for a complexity-theoretic treatment of this and related problems (including a discussion why they are most likely *not* NP-hard) as well as of the combinatorics that underlie them, and see [2] for the latest; see [17] for lower bounds in restricted models, and [3] for a simplex-like algorithm that solves the 2-player case (unfortunately, in exponential time, albeit establishing the existence of a rational Nash equilibrium). To quote again from [38], this problem may be, together with factoring, "*the most important concrete open question on the boundary of P today*" (emphasis of the original).

The concept of Nash equilibrium is by no means uncontroversial as a definition of rationality; see [12] for a recent criticism à propos the Internet. On the other hand, when compared with "socially optimum play" (the combination of strategies that maximizes the sum of payoffs) the Nash equlibrium arguably captures the extent to which the lack of centralized control (and unity of interest and purpose) degrades the performance of a system. A recent sequence of papers studying this "price of anarchy" [22, 44, 28, 43] is reminiscent of the beginnings of the on-line algorithms literature more than a decade ago —an attempt to capture degradation due to uncertainty about the future.

3 Mechanisms and Auctions

If Game Theory strives to map competitive situations to individual behavior, the object of Mechanism Design is the inverse: Given desired norms of behavior by a set of agents (where the key complication is that these norms depend on parameters known only to each individual agent), design a game in which the desired outcome is the only rational behavior by the agents. The simple classical (and surprisingly canonical) example here is an *auction* of an indivisible item by sealed bids. The basic idea due to Vickrey (refined and generalized by Clarke and Groves, and hence known as "CGV mechanism") is that the highest bidder wins, but pays an amount equal to the amount bid *by the second-highest bidder*. It is easy to see that all players are thus encouraged to reveal their true valuation of the item (whereas otherwise they might get involved in speculatively second-guessing other bidders), and the item goes to the bidder with the highest valuation —exactly as was desired. The rich interface of this field with Computation was first explored in [34, 31], while its thorny interaction with approximation was pointed out in [35]; see also [16] for an efficient generalized shortest-path algorithm that solves an interesting problem related to Internet routing suggested in [34]. For a recent survey of mechanism design and auctions from the standpoint of distributed AI see [45].

Auctions are, of course, a much-studied subject in Economics (see for example the survey in [20]), and game-theoretic considerations and tools are central. The subject acquired an important computational dimension by the combined advent of electronic auctions over the Internet, as well as of the auction for wireless spectrum by the FCC, in which one bids for whole sets of indivisible items. Such auctions are now called *combinatorial auctions*, and present much mathematical and computational challenge — see the extensive survey by [4]. Determining the winners of such an auction, so as to maximize total income for the auctioneer, is a weighted set packing problem, and therefore intractable and poorly approximable, see [47, 26, 45] for results along these lines as well as remedies; linear programming techniques are often of use [32, 42]. With so many items (sets) to bid on, even the notation for communicating bids is worthy of study — but the problem has, in some plausible sense, provably exponential communication complexity [33]. A further complication comes from the mechanism design aspects of the problem [51].

Even single-item auctions present novel challenges if the auctioned item is a piece of information ("digital good," that is, with zero reproduction cost). If the item is to be broadcast on the Internet with possibly significant transmission costs and potential buyers are to submit sealed bids for it, then the mechanism design is a little more complex, and issues of distributed computation interfere [9, 19]. When bids in an auction arrive one after the other and the auctioneer's decisions must be made on the fly, then we have a challenging genre of on-line problem, see [15], and [25] for the non-digital case.