Computational Complexity

Seventeenth Annual IEEE Conference

Sponsored by

The IEEE Computer Society Technical Committee on Mathematical Foundations of Computing

In cooperation with

ACM-SIGACT and EATCS

May 21–24, 2002

Montréal, Canada

ELECTRONIC REGISTRATION

Electronic registration is possible through:
http://www.crm.umontreal.ca/CCC.

You can also fill the registration form below and return the form by mail or fax.

ADVANCE REGISTRATION FORM

Last name _____

First name _____

Affiliation _____

Mailing address _____

_____

_____

EMail address _____

Telephone _____

Special dietary needs _____

Membership number
(ACM, SIGACT, EATCS or IEEE) _____

Method of Payment

☐ Check Enclosed

We accept only checks drawn on Canadian or US banks. Make checks payable to "Centre de recherches mathématiques" *Do not send cash or money orders*

☐ VISA ☐ MasterCard

Credit Card Number _____

Exp. Date _____

Name on Card _____

Signature _____

Payment computation

Registration fee	$ _____
Extra proceedings (each $40US or $65CDN)	$ _____
Extra banquet tickets (each $60US or $95CDN)	$ _____
Total	$ _____
STOC discount ($15US or $25CDN)	$ _____
Net Total	$ _____

Registration Fee (In US Dollars)

	Advance†	Late
Members‡*	$ 250US	$ 340US
Nonmembers*	$ 310US	$ 380US
Students+	$ 55US	$ 75US

Registration Fee (In CDN Dollars)

	Advance†	Late
Members‡*	$ 395CDN	$ 480CDN
Nonmembers*	$ 490CDN	$ 600CDN
Students+	$ 85CDN	$ 120CDN

*The registration fee includes a copy of the proceedings, the reception, the banquet, and one lunch.

+The registration fee includes a copy of the proceedings, the reception, and one lunch.

†The advance registration deadline is April 15.

‡ACM, EATCS, IEEE, or SIGACT members.

Extra proceedings/banquet tickets

Extra proceedings are $40US or $65CDN. Extra banquet tickets are $60US or $95CDN. Both will also be available for sale on site.

STOC discount

If you register to both CCC 2002 and STOC 2002, then a discount of$15US ($25CDN if paying in CDN) is applied to each of your two registration fees.

Conference homepage

Information about this year's conference is available on the Web at

http://www.crm.umontreal.ca/CCC

Information about the Computational Complexity conference is available at

http://www.cs.utep.edu/longpre/complexity.html.

Conference registration

Conference registration is through this year's conference web site. Reimbursement in full (minus handling expenses) can be obtained on cancellations received before April 1st. Additional cancellation fee of $100US thereafter until May 15 will apply. No reimbursement thereafter.

If you're sending the form by mail, send to

CCC 2002
Centre de recherches mathématiques
Université de Montréal
C.P. 6128, succ. Centre-ville
Montréal (Québec) CANADA
H3C 3J7

or FAX to: 514 343-2254.

Lodging

Lodging for the conference will be at:

- Résidences de l'Université de Montréal, 2350, boul. Edouard-Montpetit, Montréal, Québec, Canada, H3T 1J4

  Rate: $40.26 CDN per night. 514 343-6531.

A block of rooms has been reserved at the residences for our conference. The registration web site has a PDF form that needs to be faxed or sent in. If calling directly, be sure to mention "Computational Complexity Conference". The room price above includes tax (about 15%). Reservation requests received after April 26 2002, referred to as the cut-off date, will be accepted on a space available basis.

You can also stay at the STOC 2002 Hotel and commute by subway. Our conference web site contains other choices for alternative lodging closer to the Complexity conference site.

Conference Information

Location For the first day of the conference, which is joint with STOC 02, the sessions will be held at the Windham Hotel, 1255 Jeanne Mance Street. This is downtown Montreal, close to subway stations "Place des Arts" and "Place d'Armes".
The next days, sessions will held in room 1140 of the Pavillon André-Aisenstadt, Université de Montréal Campus. Attendants can find a large variety of restaurants for lunch and dinner in the neighborhood just west of campus, about 10 minutes walk from the conference site.
A parking pass can be obtained on site for $9CDN per day, and allows parking at the residences and anywhere else on campus. Street parking is very difficult.
Mid-may is very pleasant in Montreal, and you can expect day temperatures in the 60 to 70F range.

Social Program *Tuesday evening:* Reception starting at 7pm, in Pavillon André-Aisenstadt. Room number to be posted at the entrance of the building. *Wednesday evening:* Business meeting, starting at 9pm, in Pavillon André-Aisenstadt., *Thursday afternoon:* Rump session at 2 p.m. *Thursday evening:* There will be a banquet at 7 p.m. at Restaurant Hélène de Champlain, 200, Tour de l"Isle, Ile Ste-Hélène.

Getting There

By airplane: You will most probably arrive at Dorval Airport. (Some chartered flights arrive in Mirabel airport, an airport 40 km further away.) From Dorval airport, you can reach the campus of the University by taxi, for about $25CDN plus tip. You can also take the shuttle to downtown bus terminal, for $11CDN. The bus terminal is close to subway station Berri-Uqam. Subway is called "Metro" in Montreal. Subway fares are $2.25CDN, $9CDN for 6 tickets, or $14CDN for a Monday to Sunday weekly pass. Transfer (for free) from the orange line to the blue line. Get off at Edouard-Montpetit for the residences, or at Université de Montréal for the conference site. Subway maps are posted in the stations and directions are easy to follow. Check the subway map at
http://www.stcum.qc.ca/English/metro/a-mapmet.htm.

By other means

The train station also connects to the subway system. For information on arriving by car, please consult the conference website (the residences web site has detailed information.)

Messages & Additional Information

Messages for attendees can be sent to phone 514-343-7501, fax 514-343-2254. Electronic messages can be sent to
CRM@CRM.UMontreal.ca.

Complexity Abstracts

Each year, brief abstracts on current research on topics covered by the conference are made available electronically a week before the conference. Submission is open to all. May 16 is the submission deadline. For details of submissions format send email to abstract@cs.umd.edu or contact the Abstracts Editor: William Gasarch; Dept. of Comp. Sci.; Univ. of Maryland at College Park; College Park, Maryland, 20742, Email: gasarch@cs.umd.edu.

Acknowledgments

Sponsors The conference is sponsored by the IEEE Computer Society Technical Committee for Mathematical Foundations of Computing in cooperation with ACM, SIGACT and EATCS. Support was provided by Centre de recherches mathématiques and Département d'informatique et de recherche opérationelle (Université de Montréal) and MITACS.

Local Arrangements Pierre McKenzie, U. Montréal, Denis Thérien, McGill

Program Committee Anne Condon (Chair), Harry Buhrman, Sam Buss, Jin-Yi Cai, Sophie Laplante, Dieter van Melkebeek, Amit Sahai, Michael Saks, John Watrous.

Conference Committee Lance Fortnow (Chair), Manindra Agrawal, Luc Longpré, Jack Lutz, Pierre McKenzie, Toni Pitassi, Alexander Razborov, Madhu Sudan.

PROGRAM

Tuesday sessions are joint with STOC 2002, and will be in the Windham hotel. All other sessions will

be in room 1140 of the Pavillon André-Aisenstadt, Université de Montréal Campus.

TUESDAY

SESSION 1 (Joint with STOC 2002)
Chair: Sam Buss (UCSD)

8:30–8:55 *Relations between Average Case Complexity and Approximation Complexity*, Uriel Feige (Weizmann Institute)

8:55–9:20 *Vertex Cover on 4-regular Hypergraphs is Hard to Approximate Within 2-epsilon*, Jonas Holmerin (Royal Inst. Tech., Stockholm)

9:20–9:40 *Resolution Lower Bounds for the Weak Pigeon Hole Principle*, Ran Raz (Weizmann Institute)

9:45–10:10 *Hard Examples for Bounded Depth Frege*, Eli Ben-Sasson (Hebrew U.)

10:10–10:30 Break

SESSION 2 (Joint with STOC 2002)
Chair: Anne Condon (UBC)

10:30–10:55 *Improved Cryptographic Hash Functions with Worst-case/Average-case Connection*, Daniele Micciancio (UCSD)

10:55–11:20 *Algorithmic Derandomization via Complexity Theory*, D. Sivakumar (IBM Almaden)

11:20–11:50 *Pseudo-Random Generators for all Hardnesses*, Christopher Umans (Microsoft Research)

11:50–1:00 Lunch (provided)

SESSION 3 (Joint Session with STOC 2002)
Chair: Michael Saks (Rutgers U. and Microsoft)

1:00–1:25
Randomness Conductors and Constant-Degree Lossless Expanders, Michael Capalbo (IAS, Princeton), Omer Reingold (AT&T Labs), Salil Vadhan (Harvard), and Avi Wigderson (IAS, Princeton and Hebrew U.)

1:25–1:50 *Expanders from Symmetric Codes*, Roy Meshulam (Technion) and Avi Wigderson (IAS, Princeton)

1:50–2:15 *The Complexity of Approximating the Entropy*, Tugkan Batu (U. Penn), Sanjoy Dasgupta (AT&T Research), Ravi Kumar (IBM Almaden), and Ronitt Rubinfeld (NEC)

2:15–2:40 *Time-Space Tradeoffs Multiparty Communication Complexity and Nearest Neighbor Problems*, Paul Beame (U. Washington) and Erik Vee (U. Washington)

2:40–3:20 *On Communication over an Entanglement-Assisted Quantum Channel*, Ashwin Nayak (Caltech) and Julia Salzman (Princeton)

3:00–3:20 Break

SESSION 4 (Joint Session with STOC 2002)
Chair: Sam Buss (UCSD)

3:20–3:45 *Hardness Amplification Within NP*, Ryan O'Donnell (MIT)

3:45–4:10 *3-MANIFOLD KNOT GENUS is NP-complete*, Ian Agol (U. Illinois), Joel Hass (UC Davis), and William P. Thurston (UC Davis)

4:10–4:35 *On the Power of Unique 2-Prover 1-Round Games*, Subhash Khot (Princeton U.)

4:35–5:00 *Learnability Beyond AC0*, Jeffrey C. Jackson (Duquesne U.), Adam R. Klivans (MIT) and Rocco A. Servedio (Harvard)

7:00 Reception, Pavillon André-Aisenstadt.

WEDNESDAY

SESSION 5 Chair: Sophie Laplante (U. Paris-Sud)

9:00–9:30 *Resolution Lower Bounds for Perfect Matching Principles*, Alexander A. Razborov (IAS, Princeton and Steklov Math. Inst.)

9:30–10:00 *Resolution width-size trade-offs for the Pigeon-Hole Principle*, Stefan Dantchev (BRICS)

10:00–10:30 *The inapproximability of lattice and coding problems with preprocessing*, Uriel Feige (Weizmann Institute), Daniele Micciancio (UCSD)

10:30–11:00 *Sampling short lattice vectors and the*

closest lattice vector problem, Miklos Ajtai (IBM Almaden), Ravi Kumar (IBM Almaden), and D. Sivakumar (IBM Almaden)

11-11:30 Break

Invited talk 1 Chair: Harry Buhrman (CWI)

11:30–12:45 *The History of Complexity*, Lance Fortnow (NEC)

SESSION 6 Chair: Michael Saks (Rutgers U. and Microsoft)

2:00–2:30 *The Correlation Between Parity and Quadratic Polynomials Mod 3*, Frederic Green (Clark U.)

2:30–3:00 *Functions that have read-twice, constant width, branching programs are not necessarily testable*, Eldar Fischer (Technion) and Ilan Newman (U. Haifa)

3:00–3:30 *On the Complexity of Integer Multiplication in Branching Programs with Multiple Tests and in Read-Once Branching Programs with Limited Nondeterminism*, Philipp Woelfel (U. Dortmund)

3:30–4:00 Break

SESSION 7 Chair: John Watrous (U. Calgary)

4:00–4:30 *Information Theory Methods in Communication Complexity*, Ziv Bar-Yossef (UC Berkeley) and T.S. Jayram (IBM Almaden) and Ravi Kumar (IBM Almaden) and D. Sivakumar (IBM Almaden)

4:30–5:00 *Extracting Quantum Entanglement (General Entanglement Purification Protocols)*, Andris Ambainis (IAS, Princeton), Adam Smith (MIT) and Ke Yang (CMU)

5:00–5:30 *Algebras of minimal rank over perfect fields*, Markus Bläser (U. Lübeck)

9:00 Business meeting

THURSDAY

Invited talk 2 Chair: Sam Buss (UCSD)

9:00–10:15 *Mixing* Peter Winkler (Bell Labs)

10:15–10:45 Break

SESSION 8 Chair: Dieter van Melkebeek (U. Wisconsin)

10:45–11:15 *Pseudorandomness and Average-Case Complexity with Uniform Reductions*, Luca Trevisan (UC Berkeley) and Salil Vadhan (Harvard)

11:15–11:45 *Pseudo-random Generators and Structure of Complete Degrees*, Manindra Agrawal (IIT Kanpur)

11:45–12:15 *Decoding Concatenated Codes using Soft Information*, Venkatesan Guruswami (UC Berkeley) and Madhu Sudan (MIT)

2:00 Rump session

7:00 Banquet

FRIDAY

Survey talk 1 Chair: Jin-Yi Cai (U. Wisconsin)

9:00–10:15 John Watrous (U. Calgary) *Arthur and Merlin in a Quantum World*

10:15–10:45 Break

SESSION 9: Chair: Amit Sahai (Princeton)

10:45–11:15 *Streaming Computation of Combinatorial Objects*, Ziv Bar-Yossef (UC Berkeley) and Omer Reingold (AT&T Labs) and Ronen Shaltiel (Weizmann Institute) and Luca Trevisan (UC Berkeley)

11:15–11:45 *Lower Bounds for Linear Locally Decodable Codes and Private Information Retrieval*, Oded Goldreich (Weizmann University) and Howard Karloff (AT&T Labs) and Leonard Schulman (Caltech) and Luca Trevisan (UC Berkeley)

11:45–12:15 *Better Lower Bounds for Locally Decodable Codes*, Amit Deshpande (Chennai Math. Inst., India) and Rahul Jain (Tata Inst. Fund. Res., Mumbai) and T Kavita (Tata Inst. Fund. Res., Mumbai), Satyanarayana V. Lokam (U. Michigan) and Jaikumar Radhakrishnan (Tata Inst. Fund. Res., Mumbai)

12:15–12:45 *Universal Arguments and their Applications*, Boaz Barak (Weizmann Institute) and Oded Goldreich (Weizmann Institute)