

Rahul Jain

Curriculum Vitae

- Position** Assistant Professor, Department of Computer Science
Principal Investigator, Centre for Quantum Technologies
National University of Singapore
- Contact Information** S15-04-01, 3 Science Drive 2, Singapore 117543.
Telephone: +65 8180 6872.
Fax: +65 6516 6897.
Email: rahul@comp.nus.edu.sg
Homepage: <https://www.comp.nus.edu.sg/~rahul>
- Education** Ph.D. (Computer Science), Tata Institute of Fundamental Research, Mumbai 400005, India, 1998 – 2003.
Thesis Adviser: Jaikumar Radhakrishnan.
Thesis title: *Information Theoretic Problems in Computational Complexity Theory*.
Recipient of the IBM Distinguished Dissertation Award, 2005.
Recipient of the TAA-Sasken Best Thesis Award, 2005 – 2006.
B.Tech. (Electrical and Electronics Engineering), Indian Institute of Technology, Mumbai 400076, India, 1993 – 1997.
- Research Interests** Information Theory, Quantum Computation, Cryptography, Communication Complexity, Computational Complexity Theory.
- Professional Experience**
1. Assistant Professor, Department of Computer Science, and Principal Investigator, Centre for Quantum Technologies, National University of Singapore, from November 2008 onwards.
 2. Post doctoral research fellow in Computer Science department and Institute for Quantum Computing, University of Waterloo, ON, Canada, from May 2006 to October 2008.
 3. Post doctoral research fellow in Computer Science department of University of California at Berkeley, California, USA, from September 2004 to April 2006.
 4. Worked as Algorithms Consultant with Cadence Design Systems, NOIDA, U.P. India, from January 2004 to August 2004.
 5. Worked as Software Engineer in Verifone India Private Limited, Bangalore, India from August 1997 to July 1998.

Awards

1. Best paper award at the 42nd ACM Symposium on Theory of Computing (STOC) 2010.
2. IBM Distinguished Dissertation Award, 2005.
3. TAA-Sasken Best Thesis Award, 2005-2006.
4. National Talent Search Contest Scholarship by Central Board for Secondary Education, Government of India, 1991.
5. State Science Quiz scholarship by Council for Science Education, Government of Madhya Pradesh (India), 1989.

Professional Activities

Program Committee: TQC2010, the fifth Conference on the Theory of Quantum Communications, Computation and Cryptography, University of Leeds, 13th-15th April, 2010.

Refereeing for journals: SIAM Journal of Computing, Physical Review Letters, Quantum Information and Computation, Physical Review A, Journal of Physics A: Mathematical and Theoretical, International Journal of Quantum Information.

Refereeing for conferences: ACM Symposium on Theory of Computing, IEEE Conference on Foundations of Computer Science, IEEE Conference on Computational Complexity, International Colloquium on Automata Languages and Programming.

Supervision

1. Graduate students : Attila Pereszlenyi and Penghui Yao.
2. Interns : T. Varun Theja, Summer 2011; Praneeth Srikanti and Savin Goel, Summer 2010; Arpit Goel, Summer 2009; Ansis Rosmanis and Yi Su, University of Waterloo, Summer 2007.

Teaching

1. CS3230, "Design and Analysis of Algorithms", Fall, 2011.
2. CS6209, "Topics in Cryptography", Winter, 2011.
3. CS3231, "Theory of Computation", Fall 2010.
4. CS3231, "Theory of Computation" (jointly with Sanjay Jain), Winter 2010.
5. CS6285, "Foundations of Cryptography", Winter, 2009.
6. QT5198, Seminar Module offered in Centre for Quantum Technologies, Winter 2009.
7. Linear Algebra, University of Waterloo, Winter 2006.

Publications

1. “A parallel approximation algorithm for positive semidefinite programming.” In proceedings of the 52nd Annual IEEE Symposium on Foundations of Computer Science (FOCS), 2011, to appear. Also at arXiv:1104.2502.
(With Penghui Yao)
2. “The influence lower bound via query elimination.” Theory of Computation (ToC), 2011, to appear. Also at arXiv:1102.4699, ECCC-TR11-033.
(With Shengyu Zhang)
3. “Resource requirements of private quantum channels and consequence for oblivious remote state preparation.” Journal of Cryptology (JoC), 2010, DOI: 10.1007/s00145-010-9076-8. Also at quant-ph/0507075.
4. “Optimal Direct Sum Results for Deterministic and Randomized Decision Tree Complexity.” Information Processing Letter (IPL), 110 (2010), pp. 893-897. Also at arXiv:1004.0105.
(With Hartmut Klauck and Miklos Santha)
5. “Depth-Independent Lower bounds on Communication Complexity of Read-Once Boolean Functions.” In proceedings of the 16th Annual International Computing and Combinatorics Conference (COCOON), 2010. Lecture Notes in Computer Science, 2010, Volume 6196/2010, 54-59. Also at arXiv:0908.4453.
(With Hartmut Klauck and Shengyu Zhang)
6. “The Partition Bound for Classical Communication Complexity and Query Complexity.” In proceedings of the 25th IEEE Conference on Computational Complexity (CCC), 2010, pp. 247-258. Also at arXiv:0910.4266.
(With Hartmut Klauck)
7. “QIP = PSPACE.” In proceedings of The 42nd ACM Symposium on Theory of Computing (STOC), pp. 573-582, 2010. Recipient of the best paper award. Invited to the Journal of the ACM, to appear. Research highlight in Communications of the ACM, Vol. 53 No. 12, 2010. Also at arXiv:0907.4737.
(With Zhengfeng Ji, Sarvagya Upadhyay and John Watrous.)
8. “On the power of a unique quantum witness.” In proceedings of the 1st Annual Conference on Innovations in Computer Science (ICS), pp. 470-481, 2010.
(With Iordanis Kerenidis, Greg Kuperberg, Miklos Santha, Or Sattath and Shengyu Zhang.)
9. “Two-message quantum interactive proofs are in PSPACE.” In proceedings of the 50th Annual Symposium on Foundations of Computer Science (FOCS), 2009, pp. 534-543. Also at arXiv:0905.1300.
(With Sarvagya Upadhyay and John Watrous.)

Publications

10. “New Results in the Simultaneous Message Passing Model.” In proceedings of the 24th IEEE Conference on Computational Complexity (CCC), 2009, pp. 369-378. Also at arXiv:0902.3056.
(With Hartmut Klauck.)
11. “Parallel approximation of non-interactive zero-sum quantum games.” In proceedings of the 24th IEEE Conference on Computational Complexity (CCC), 2009, pp. 243-253. Also at arXiv:0808.2775.
(With John Watrous.)
12. “On parallel composition of zero-knowledge proofs with black-box quantum simulators.” Quantum Information and Computation (QIC), 2009, Vol.9, No.5 and 6, pp. 0513-0532. Also at quant-ph/0607211.
(With Alexandra Kolla, Gatis Midrijanis and Ben W. Reichardt.)
13. “Entanglement-Resistant Two-Prover Interactive Proof Systems and Non-Adaptive Private Information Retrieval Systems.” Quantum Information and Computation (QIC), 2009, Vol.9 No.7 and 8, pp. 0648-0656. Also at arXiv:0707.1729.
(With Richard Cleve and Dmitry Gavinsky.)
14. “New bounds on classical and quantum one-way communication complexity.” Theoretical Computer Science (TCS), Elsevier, 2009, (410) pp. 2463-2477.
(With Shengyu Zhang.)
15. “A separation between divergence and Holevo information for ensembles.” In proceedings of The 5th Annual Conference on Theory and Applications of Models of Computation (TAMC), 2008, pp 526-541. Invited to a special issue of Mathematical Structures in Computer Science (MSCS) on TAMC 2008. Also at arXiv:0712.3867.
(With Ashwin Nayak and Yi Su.)
16. “Direct product theorems for communication complexity via subdistribution bounds.” In proceedings of The 40th ACM Symposium on Theory of Computing (STOC), 2008, pp 599-608. Also at ECCC report number TR07-064.
(With Hartmut Klauck and Ashwin Nayak.)
17. “New binding-concealing trade-offs for quantum string commitment.” Journal of Cryptology (JoC), 2008, Vol. 21 (4), pp. 579-592. Also at quant-ph/0506001.
18. “Teleportation of Quantum States, **1993; Bennett, Brassard, Crepeau, Jozsa, Peres, Wootters.” Contributed article on invitation to Encyclopedia of Algorithms, 2008.

Publications

19. “A new information-theoretic property about quantum states with an application to privacy in quantum communication.” *Journal of the ACM (JACM)*, 2009, Volume 56, Issue 6, Article No.: 33.
(With Jaikumar Radhakrishnan and Pranab Sen.)
Many results in the above paper appeared previously in:
“Privacy and interaction in quantum communication complexity and a theorem about the relative entropy of quantum states.” In proceedings of 43rd IEEE Symposium on Foundations of Computer Science (FOCS), 2002, pp. 429-438.
(With Jaikumar Radhakrishnan and Pranab Sen.)
20. “The communication complexity of correlation.” In proceedings of 22nd IEEE Conference on Computational Complexity (CCC), pp. 10-23, 2007.
(With Prahladh Harsha, David McAllester and Jaikumar Radhakrishnan.)
21. “Communication complexity of remote state preparation with entanglement.” In *Quantum Information and Computation (QIC)*, Vol.6 No.4&5 pp. 461-464, 2006. Also at quant-ph/0504008.
22. “Prior entanglement, message compression and privacy in quantum communication.” In proceedings of 20th IEEE Conference on Computational Complexity (CCC), pp. 285-296, 2005.
(With Jaikumar Radhakrishnan and Pranab Sen.)
23. “Better lower bounds for locally decodable codes.” In *Random Structures and Algorithms*, pp. 358-378, 2005. Extended abstract In proceedings of 17th IEEE Conference on Computational Complexity (CCC), pp. 184-193, 2002.
(With Amit Deshpande, Satyanarayana V. Lokam, Jaikumar Radhakrishnan and Kavitha Telikapalli.)
24. “A direct sum theorem in communication complexity via message compression.” In proceedings of 30th International Colloquium on Automata, Languages and Programming (ICALP), 2003, pp. 300-315. Invited to a special issue of *Theoretical Computer Science (TCS)* on ICALP 2003. Also at cs.CC/0304020.
(With Jaikumar Radhakrishnan and Pranab Sen.)
25. “The quantum communication complexity of the pointer chasing problem: the bit version.” In proceedings of 22nd conference on the Foundations of Software Technology and Theoretical Computer Science (FSTTCS), 2002, pp. 218-229.
(With Jaikumar Radhakrishnan and Pranab Sen.)
26. “A lower bound for bounded round quantum communication complexity of set disjointness.” In proceedings of 44th IEEE Symposium on Foundations of Computer Science (FOCS), 2003, pp. 220-229. Also at quant-ph/0303138.
(With Jaikumar Radhakrishnan and Pranab Sen.)

Manuscripts

1. “A short proof of the quantum Substate Theorem.” 2011. At arXiv:1103.6067.
(With Ashwin Nayak)
2. “New strong direct product results in communication complexity.” 2010. At arXiv:1010.0522 , arXiv:1010.0846, ECCC-TR11-024.
3. “The space complexity of recognizing well-parenthesized expression.” 2010. At arXiv:1004.3165.
(With Ashwin Nayak)
4. “Accessible versus Holevo information for a binary random variable.” 2006. At quant-ph/0603278.
(With Ashwin Nayak.)
5. “An approach from classical information theory to lower bounds for smooth codes.” 2007. At cs.CR/0607042.
6. “Distinguishing sets of quantum states.” 2005. At arXiv:quant-ph/0506205.

Invited Talks

1. “Communication complexity : Lower bound methods and the Direct Sum/Direct Product questions.”
Invited talk at the 2nd Annual Mysore Park Workshop in Theoretical Computer Science: Algorithms and Complexity, May, 2011.
2. “New strong direct product results in communication complexity.”
Invited talk at the 2nd Annual Mysore Park Workshop in Theoretical Computer Science: Algorithms and Complexity, May, 2011.
3. “QIP=PSPACE.”
Invited talk at Microsoft Research India, May 2009.
Invited talk at the 13th Workshop on Quantum Information Processing, ETH Zurich, Switzerland, January, 2010.
4. “A lower bound for bounded round quantum communication complexity of set disjointness.”
Invited talk at Workshop on Quantum Information Processing, Institute of Quantum Computing, University of Waterloo, Canada, November, 2003.
Invited talk at Workshop on Quantum information processing, Centrum voor Wiskunde en Informatica , Amsterdam, The Netherlands, June, 2003.
5. “Privacy and interaction in quantum communication complexity and a theorem about the relative entropy of quantum states.”
Invited talk at Workshop on Quantum Information Processing at Mathematical Sciences Research Institute, Berkeley, USA, December, 2002.

References

1. Richard Cleve
David R. Cheriton School of Computer Science
University of Waterloo
200 University Avenue West
Waterloo, Ontario, Canada N2L 3G1.
email: cleve@cs.uwaterloo.ca
2. Ashwin Nayak
Dept. of Combinatorics and Optimization (MC 4034), Faculty of Mathematics
University of Waterloo
200 University Avenue West
Waterloo ON N2L 3G1, Canada.
email: anayak@math.uwaterloo.ca
3. Jaikumar Radhakrishnan
School of Technology and Computer Science
Tata Institute of Fundamental Research
Homi Bhabha Road, Colaba
Mumbai 400005, India.
email: jaikumar@tcs.tifr.res.in
4. Pranab Sen
School of Technology and Computer Science
Tata Institute of Fundamental Research
Homi Bhabha Road, Colaba
Mumbai 400005, India.
email: pranab.sen.73@gmail.com
5. Umesh Vazirani
Department of Computer Science
University of California
Berkeley, CA 94720, USA.
email: vazirani@cs.berkeley.edu
6. Andrew Yao
Center for Advanced Study
Tsinghua University
Beijing 100084, China
email: andrewcyao@tsinghua.edu.cn