Rahul Jain

Curriculum Vitae

Position
Associate 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.
B.Tech. (Electrical and Electronics Engineering), Indian Institute of Technology, Mumbai, India, 1993-1997.

Research Interests

Information Theory, Quantum Computation, Cryptography, Communication Complexity, Computational Complexity Theory.

Professional Experience

1. Associate Professor, Department of Computer Science, and Principal Investigator, Center for Quantum Technologies, National University of Singapore, from July 2013 onwards.
2. Assistant Professor, Department of Computer Science, and Principal Investigator, Center for Quantum Technologies, National University of Singapore, from November 2008 to June 2013.
3. Post doctoral research fellow in Computer Science department and Institute for Quantum Computing, University of Waterloo, ON, Canada, from May 2006 to October 2008.
4. Post doctoral research fellow in Computer Science department of University of California at Berkeley, California, USA, from September 2004 to April 2006.
5. Worked as Algorithms Consultant with Cadence Design Systems, NOIDA, U.P. India, from January 2004 to August 2004.
6. Worked as Software Engineer in Verifone India Private Limited, Bangalore, India from August 1997 to July 1998.

Awards

1. Young Researcher Award, National University of Singapore, 2012.
2. Best paper award at the 42nd ACM Symposium on Theory of Computing (STOC) 2010.
3. IBM Distinguished Dissertation Award, 2005.
4. TAA-Sasken Best Thesis Award, 2005-2006.
5. National Talent Search Contest Scholarship by Central Board for Secondary Education, Government of India, 1991.
6. State Science Quiz scholarship by Council for Science Education, Government of Madhya Pradesh (India), 1989.

Professional Activities

Program Committee Membership

1. The 12th annual conference on the theory of quantum communications, computation and cryptography (TQC), 2017.
2. The 42nd international colloquium on automata, languages, and programming (ICALP), Rome, Italy, July 2016.
3. The 33rd international symposium on theoretical aspects of computer science (STACS), Orléans, France, February 17 - 20, 2016.
4. (co-Chair) The 12th annual conference on theory and applications of models of computation (TAMC), Singapore, 18-20 May 2015.
5. The 25th international symposium on algorithms and computation (ISAAC), December 15-17, 2014, Jeonju, Korea.
6. The 17th annual conference on quantum information processing (QIP), Barcelona, Spain, February 03-07, 2014.
7. The 10th annual conference on theory and applications of models of computation (TAMC). Hong Kong, China, 20-22 May 2013.
8. IARCS annual conference on foundations of software technology and theoretical computer science (FSTTCS). Hyderabad, India, December 15-17, 2012.
9. The fifth annual conference on the theory of quantum communications, computation and cryptography (TQC). University of Leeds, 13th-15th April, 2010.

Cont'd

Teaching

1. CS6234, "Advanced Algorithms", Spring 2012, Spring 2013, Spring 2014.
2. CS3230, "Design and Analysis of Algorithms", Fall 2011, Fall 2012, Fall 2014.
3. CS3230-R, "Design and Analysis of Algorithms-Research", Spring 2011, Spring 2012, Spring 2013.
4. CS6209, "Topics in Cryptography", Spring 2011.
5. CS3231, "Theory of Computation", Fall 2010, Spring 2010.
6. CS6285, "Foundations of Cryptography", Spring 2009.
7. QT5198, Seminar Module offered in the Centre for Quantum Technologies, Spring 2009.
8. Linear Algebra, University of Waterloo, Spring 2006.

Supervision

1. Graduate students: Srijita Kundu, Anurag Anshu, Priyanka Mukhopadhyay, Attila Pereszlényi (graduated Jan. 2015), Penghui Yao (graduated Nov. 2013) .
2. Undergraduate students: Zhou Jun (2012-13).

Service

1. Member of the IT Committee at the Centre for Quantum Technologies, NUS, January 2009 onwards.
2. Member of the Academic Committee at the Centre for Quantum Technologies, NUS, January 2009 onwards.

Publications

1. "A new operational interpretation of relative entropy and trace distance between quantum states." IEEE Transactions of Information Theory (IEEE-TIT), 2016. To appear. ArXiv:1404.1366.
   (With Anurag Anshu, Priyanka Mukhopadhyay, Ala Shayeghi, Penghui Yao.)

2. "Extension Complexity of Independent Set Polytopes." In proceedings of The 57th Annual IEEE Symposium on Foundations of Computer Science (FOCS), pp. 565-572, 2016. ECCC:TR16-070.
   (With Mika G$\acute{o}\acute{o}$s and Thomas Watson.)

3. "Separations in communication complexity using cheat sheets and information complexity." In proceedings of The 57th Annual IEEE Symposium on Foundations of Computer Science (FOCS), pp. 555-564, 2016. ArXiv:1605.01142.
   (With Anurag Anshu, Aleksandrs Belovs, Shalev Ben-David, Mika G$\acute{o}\acute{o}$s, Robin Kothari, Troy Lee and Miklos Santha.)

4. "Partition bound is quadratically tight for product distributions." In proceedings of The 43rd International Colloquium on Automata, Languages, and Programming (ICALP), pp. 135:1-135:13, 2016. ECCC-TR15-199.
   (With Prahladh Harsha and Jaikumar Radhakrishnan.)

5. "Multipartite Quantum Correlation and Communication Complexities." Computational Complexity (CC), pp. 1-30, 2016. ArXiv:1405.6015.
   (With Zhaohui Wei, Penghui Yao, Shengyu Zhang.)

6. "Information-theoretic approximations of the nonnegative rank." Computational Complexity (CC), pp. 1-51, 2016. ECCC-TR13-158
   (With Gbor Braun, Troy Lee, Sebastian Pokutta.)

7. "Communication tasks with infinite quantum-classical separation." Phys. Rev. Lett. (PRL) 115, 030504, July 2015. ArXiv:1407.8217.
   (With Christopher Perry, Jonathan Oppenheim.)

8. "Relative discrepancy does not separate information and communication complexity." In proceedings of The 42nd International Colloquium on Automata, Languages, and Programming (ICALP 2015), vol. 9134, LNCS, pp. 506-516, 2015.
   (With Lila Fontes, Iordanis Kerenidis, Mathieu Laurière, Sophie Laplante, Jérémie Roland.)

9. "New strong direct product results in communication complexity." Journal of the ACM (JACM), volume 62 Issue 3, Article No. 20, June 2015.

Publications

10. "The space complexity of recognizing well-parenthesized expression." IEEE Transactions on Information Theory (IEEE IT), vol. 60:10, pp.1-23, 2014. ArXiv:1004.3165, ECCC-TR10-071.
(With Ashwin Nayak.)

11. "Input/Output Streaming Complexity of Reversal and Sorting." In proceedings of the 18th International Workshop on Randomization and Computation (RANDOM), pp. 654-668, 2014. ArXiv:1309.0647.
(With Nathanaël François, Frédéric Magniez.)

12. "A parallel repetition theorem for entangled two-player one-round games under product distributions." In proceedings of 29th IEEE Conference on Computational Complexity (CCC), pp. 209 - 216, 2014. ArXiv:1311.6309.
(With Attila Pereszlényi, Penghui Yao.)

13. "Conclusive exclusion of quantum states." Physical Review A. vol. 89(2), pp. 22336-22349, 2014. Contributed talk at the 13th Asian Quantum Information Science Conference (AQIS) 2013. At arXiv:1306.4683.
(With Somshubhro Bandyopadhyay, Jonathan Oppenheim and Christopher Perry.)

14. "A strong direct product theorem for the Tribes function via the smooth-rectangle bound." In proceedings of the 33rd Foundations of Software Technology and Theoretical Computer Science (FSTTCS), pp. 141-152, 2013. ArXiv:1302.0275.
(With Prahladh Harsha.)

15. "Efficient protocols for generating bipartite classical distributions and quantum states." IEEE Transactions on Information Theory, vol. 59(8), pp. 5171-5178, 2013.
In proceedings of the ACM-SIAM Symposium on Discrete Algorithms (SODA), pp. 1503-1512, 2013. ArXiv:1203.1153.
(With Yaoyun Shi, Zhaohui Wei and Shengyu Zhang.)

16. "A direct product theorem for bounded-round public-coin randomized communication complexity." In proceedings of The 53rd Annual IEEE Symposium on Foundations of Computer Science (FOCS), pp. 167-176, 2012. ArXiv:1201.1666.
(With Attila Perészlenyi and Penghui Yao.)

17. "Short proofs of the quantum Substate Theorem." IEEE Transactions on Information Theory (IEEE IT), Volume: 58(6), pp. 3664-3669, 2012.
(With Ashwin Nayak.)

18. "Resource requirements of private quantum channels and consequence for oblivious remote state preparation." Journal of Cryptology (JoC), Volume 25, Issue 1, pp. 1-13, 2012. Also at quant-ph/0507075.

Publications

19. "A parallel approximation algorithm for positive semidefinite programming." In proceedings of the 52nd Annual IEEE Symposium on Foundations of Computer Science (FOCS), pp. 463-471, 2011. ArXiv:1104.2502.
(With Penghui Yao.)

20. "The influence lower bound via query elimination." Theory of Computation (ToC), Volume 7, Article 10 pp. 147-153, 2011. ArXiv:1102.4699, ECCC-TR11-033.
(With Shengyu Zhang.)

21. "The communication complexity of correlation." IEEE Transactions on Information Theory, 56(1), pp. 438-449, 2010.
Extended abstract in proceedings of 22nd IEEE Conference on Computational Complexity (CCC), pp. 10-23, 2007.
(With Prahladh Harsha, David McAllester and Jaikumar Radhakrishnan.)

22. "Optimal Direct Sum Results for Deterministic and Randomized Decision Tree Complexity." Information Processing Letter (IPL), 110 (2010), pp. 893-897. ArXiv:1004.0105.
(With Hartmut Klauck and Miklos Santha.)

23. "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. ArXiv:0908.4453.
(With Hartmut Klauck and Shengyu Zhang.)

24. "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.)

25. "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. Published as Article no. 30, Volume 58, Issue 6, December 2011. Research highlight in Communications of the ACM, Vol. 53 No. 12, 2010. ArXiv:0907.4737.
(With Zhengfeng Ji, Sarvagya Upadhyay and John Watrous.)

26. "On the power of a unique quantum witness." Theory of Computation (ToC), Volume 8, Article 17, pp. 375-400, 2012.
Extended abstract 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.)

27. "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. ArXiv:0905.1300.
(With Sarvagya Upadhyay and John Watrous.)

Cont'd

Publications

28. "New Results in the Simultaneous Message Passing Model via Information theoretic techniques." In proceedings of the 24th IEEE Conference on Computational Complexity (CCC), 2009, pp. 369-378. ArXiv:0902.3056.
(With Hartmut Klauck.)

29. "Parallel approximation of non-interactive zero-sum quantum games." In proceedings of the 24th IEEE Conference on Computational Complexity (CCC), 2009, pp. 243-253. ArXiv:0808.2775.
(With John Watrous.)

30. "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.)

31. "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. ArXiv:0707.1729.
(With Richard Cleve and Dmitry Gavinsky.)

32. "New bounds on classical and quantum one-way communication complexity." Theoretical Computer Science (TCS), Elsevier, 2009, (410) pp. 2463-2477.
(With Shengyu Zhang.)

33. "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.)

34. "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. Published as Lecture Notes in Computer Science Volume 4978, 2008, pp 526-541.
(With Ashwin Nayak and Yi Su.)

35. "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.)

36. "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.

Cont'd

Publications

37. "Teleportation of Quantum States, **1993; Bennett, Brassard, Crepeau, Jozsa, Peres, Wootters." Contributed article on invitation to Encyclopedia of Algorithms, 2008.

38. "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.)

39. "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.

40. "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.)

41. "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.)

42. "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.)

43. "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.)

44. "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.)

Manuscripts

1. "Separating quantum communication and approximate rank." 2016. ArXiv:1611.05754.
   (With Anurag Anshu, Shalev Ben-David, Ankit Garg, Robin Kothari, Troy Lee.)

2. "Near optimal bounds on quantum communication complexity of single-shot quantum state redistribution." 2014. ArXiv:1410.3031.
   (With Anurag Anshu, Vamsi Krishna Devabathini)

3. "A quadratically tight partition bound for classical communication complexity and query complexity." 2014. ArXiv:1401.4512.
   (With Nisheeth K. Vishnoi, Troy Lee.)

4. "A strong direct product theorem in terms of the smooth rectangle bound." 2012. ArXiv:1209.0263.
   (With Penghui Yao)

5. "A parallel approximation algorithm for mixed packing and covering semidefinite programs." 2012. ArXiv:1201.6090.
   (With Penghui Yao)

6. "Accessible versus Holevo information for a binary random variable." 2006. At quant-ph/0603278.
   (With Ashwin Nayak.)

7. "An approach from classical information theory to lower bounds for smooth codes." 2007. At cs.CR/0607042.

8. "Distinguishing sets of quantum states." 2005. ArXiv:quant-ph/0506205.

9. "A super-additivity inequality for channel capacity of classical-quantum channels." 2005. ArXiv:quant-ph/0507088.