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: Prof. R.K. Shayamasundar.
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

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

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. "Best of 2016" by ACM Computing Reviews, 2016 for paper number 7 in the publications list.
2. Young Researcher Award, National University of Singapore, 2012.
3. "Best paper award" at the 42nd ACM Symposium on Theory of Computing (STOC) 2010 for paper number 16 in the publications list.
4. IBM Distinguished Dissertation Award, 2005.
5. TAA-Sasken Best Thesis Award, 2005-2006.

Professional Activities

Editorial Membership

1. Journal of Computer and System Sciences (JCSS), May 2016 onwards.

Program Committee Membership

1. Annual conference on Quantum Information Processing (QIP), 2018, 2016, 2014.
2. IARCS annual conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS), 2017, 2012.
3. Annual conference on the Theory of Quantum Communications, Computation and Cryptography (TQC), 2017, 2010.
4. International Colloquium on Automata, Languages and Programming (ICALP), 2016.
5. International Symposium on Theoretical Aspects of Computer Science (STACS), 2016.
6. Annual conference on Theory and Applications of Models of Computation (TAMC), 2016, 2015 (co-Chair), 2013.
7. International Symposium on Algorithms and Computation (ISAAC), 2014.

Teaching

1. CS6234, "Advanced Algorithms", Spring 2012, Spring 2013, Spring 2014, Spring 2016.
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.

Cont'd

Journal publications

1. "Quantum communication using coherent rejection sampling." Physical Review Letters (PRL), Vol. 119, Issue 12 - 22 September 2017.
(With Anurag Anshu and Vamsi Krishna Devabathini.)

2. "A generalized quantum Slepian-Wolf." IEEE Transactions of Information Theory (IEEE-TIT), 2018. To appear. Contributed talk at the 17th Asian Quantum Information Science Conference (AQIS) 2017.
(With Anurag Anshu and Naqueeb Ahmad Warsi.)

3. "A one-shot achievability result for quantum state redistribution." IEEE Transactions of Information Theory (IEEE-TIT), 2018. To appear.
(With Anurag Anshu and Naqueeb Ahmad Warsi.)

4. "Multipartite Quantum Correlation and Communication." Computational Complexity (CC), Volume 26 Issue 1, Pages 199-228, March 2017.
(With Zhaohui Wei, Penghui Yao and Shengyu Zhang.)

5. "New One Shot Quantum Protocols with Application to Communication Complexity." IEEE Transactions of Information Theory (IEEE-TIT), Volume: 62, Issue: 12, Dec. 2016.
(With Anurag Anshu, Priyanka Mukhopadhyay, Ala Shayeghi and Penghui Yao.)

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

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

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

9. "The space complexity of recognizing well-parenthesized expression." IEEE Transactions on Information Theory (IEEE-TIT), vol. 60:10, pp.1-23, 2014.
(With Ashwin Nayak.)

10. "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.
(With Somshubhro Bandyopadhyay, Jonathan Oppenheim and Christopher Perry.)

Journal publications

11. "Efficient protocols for generating bipartite classical distributions and quantum states." IEEE Transactions on Information Theory (IEEE-TIT), vol. 59(8), pp. 5171-5178, 2013.
(With Yaoyun Shi, Zhaohui Wei and Shengyu Zhang.)

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

13. "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.

14. "The influence lower bound via query elimination." Theory of Computation (ToC), Volume 7, Article 10 pp. 147-153, 2011.
(With Shengyu Zhang.)

15. "The communication complexity of correlation." IEEE Transactions on Information Theory (IEEE-TIT), 56(1), pp. 438-449, 2010.
(With Prahladh Harsha, David McAllester and Jaikumar Radhakrishnan.)

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

17. "QIP = PSPACE." Invited to the Journal of the ACM (JACM). Published as Article no. 30, Volume 58, Issue 6, December 2011. Research highlight in Communications of the ACM (CACM), Vol. 53 No. 12, 2010.
(With Zhengfeng Ji, Sarvagya Upadhyay and John Watrous.)

18. "On the power of a unique quantum witness." Theory of Computation (ToC), Volume 8, Article 17, pp. 375-400, 2012.
(With Iordanis Kerenidis, Greg Kuperberg, Miklos Santha, Or Sattath and Shengyu Zhang.)

19. "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.
(With Alexandra Kolla, Gatis Midrijanis and Ben W. Reichardt.)

20. "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.
(With Richard Cleve and Dmitry Gavinsky.)

Journal publications

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

22. "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.)

23. "A separation between divergence and Holevo information for ensembles." 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.)

24. "New binding-concealing trade-offs for quantum string commitment." Journal of Cryptology (JoC), 2008, Vol. 21 (4), pp. 579-592.

25. "Communication complexity of remote state preparation with entanglement." In Quantum Information and Computation (QIC), Vol.6 No.4&5 pp. 461-464, 2006.

26. "Better lower bounds for locally decodable codes." In Random Structures and Algorithms, pp. 358-378, 2005.
(With Amit Deshpande, Satyanarayana V. Lokam, Jaikumar Radhakrishnan and Kavitha Telikapalli.)

27. "A direct sum theorem in communication complexity via message compression." Invited to a special issue of Theoretical Computer Science (TCS) on ICALP 2003.
(With Jaikumar Radhakrishnan and Pranab Sen.)

Refereed conference publications

1. "A composition theorem for randomized query complexity." In proceedings of The 37rd Foundations of Software Technology and Theoretical Computer Science (FSTTCS), 2017.
(With Anurag Anshu, Dmitry Gavinsky, Srijita Kundu, Troy Lee, Priyanka Mukhopadhyay, Miklos Santha and Swagato Sanyal.)

2. "Separating quantum communication and approximate rank." In proceedings of the 32th IEEE Conference on Computational Complexity (CCC), LIPIcs, pp. 24:1-24:33, 2017.
(With Anurag Anshu, Shalev Ben-David, Ankit Garg, Robin Kothari and Troy Lee).

3. "Extension Complexity of Independent Set Polytopes." In proceedings of The 57th Annual IEEE Symposium on Foundations of Computer Science (FOCS), pp. 565-572, 2016.
(With Mika Göös and Thomas Watson.)

4. "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.
(With Anurag Anshu, Aleksandrs Belovs, Shalev Ben-David, Mika Göös, Robin Kothari, Troy Lee and Miklos Santha.)

5. "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.
(With Prahladh Harsha and Jaikumar Radhakrishnan.)

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

7. "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. Listed among "best of 2016" by ACM Computing Reviews.
(With Lila Fontes, Iordanis Kerenidis, Mathieu Laurière, Sophie Laplante, Jérémie Roland.)

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

9. "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.
(With Attila Pereszlényi, Penghui Yao.)

Cont'd

Refereed conference publications

10. "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.
(With Prahladh Harsha.)

11. "Efficient protocols for generating bipartite classical distributions and quantum states." In proceedings of the ACM-SIAM Symposium on Discrete Algorithms (SODA), pp. 1503-1512, 2013.
(With Yaoyun Shi, Zhaohui Wei and Shengyu Zhang.)

12. "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.
(With Attila Perészlenyi and Penghui Yao.)

13. "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.
(With Penghui Yao.)

14. "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.
(With Hartmut Klauck and Shengyu Zhang.)

15. "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.
(With Hartmut Klauck.)

16. "QIP = PSPACE." In proceedings of The 42nd ACM Symposium on Theory of Computing (STOC), pp. 573-582, 2010. Recipient of the best paper award.
(With Zhengfeng Ji, Sarvagya Upadhyay and John Watrous.)

17. "On the power of a unique quantum witness." In proceedings of the 1st Annual Conference on Innovations in Theoretical Computer Science (ITCS), pp. 470-481, 2010.
(With Iordanis Kerenidis, Greg Kuperberg, Miklos Santha, Or Sattath and Shengyu Zhang.)

18. "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.
(With Sarvagya Upadhyay and John Watrous.)

19. "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.
(With Hartmut Klauck.)

Cont'd

Refereed conferene publications

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

22. "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.
(With Ashwin Nayak and Yi Su.)

23. "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.
(With Hartmut Klauck and Ashwin Nayak.)

24. "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.)

25. "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.)

26. "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.)

27. "Better lower bounds for locally decodable codes." 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.)

28. "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.)

29. "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.
(With Jaikumar Radhakrishnan and Pranab Sen.)

30. "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.)

Cont'd

Manuscripts

1. "Quantifying resource in catalytic resource theory." 2017. ArXiv:1708.00381.
   (With Anurag Anshu and Min-Hsiu Hsieh.)

2. "Lifting randomized query complexity to randomized communication complexity." 2017. ArXiv:1703.07521.
   (Anurag Anshu, Naresh B.Goud, Srijita Kundu and Priyanka Mukhopadhyay.)

3. "A hypothesis testing approach for communication over entanglement assisted compound quantum channel." 2017. ArXiv:1706.08286.
   (With Anurag Anshu and Naqueeb Ahmad Warsi.)

4. "Parallel device-independent quantum key distribution." 2017. ArXiv:1703.05426.
   (With Carl A. Miller and Yaoyun Shi.)

5. "A unified approach to source and message compression." 2017. ArXiv:1707.03619.
   (With Anurag Anshu and Naqueeb Ahmad Warsi.)

6. "One-shot measurement compression with quantum side information using shared randomness." 2017. ArXiv:1703.02342.
   (Anurag Anshu and Naqueeb Ahmad Warsi.)

7. "One-shot entanglement assisted classical and quantum communication over noisy quantum channels: A hypothesis testing and convex split approach." 2017. arXiv:1702.01940.
   (Anurag Anshu and Naqueeb Ahmad Warsi.)

8. "Smooth min-max relative entropy based bounds for one-shot classical and quantum state redistribution." 2017. ArXiv:1702.02396.
   (With Anurag Anshu and Naqueeb Ahmad Warsi.)

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

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

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

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

Manuscripts

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

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

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