Ben W. Reichardt Curriculum Vitae, October 2010

Personal *Address:* Computer Science / 200 University Ave W / Waterloo ON N2L 3G1
Telephone: 415-683-0805, 519-888-4567 x38616
Internet: breic@iqc.ca / www.cs.uwaterloo.ca/~breic

Education 2006 Ph.D. in Computer Science, University of California, Berkeley
2001 B.S. in Mathematics, with Distinction & Dept. Honors, Stanford University

Experience

Assistant Professor University of Waterloo: School of Computer Science and Institute for Quantum Computing, 2008 –

Postdoctoral fellow California Institute of Technology
Institute for Quantum Information, 2006 – 2008

Academic service

- Conference program committee: Quantum Information Processing (QIP) 2009, '08, Theory of Quantum Computation, Communication and Cryptography (TQC) '09
- Journal referee: SICOMP, TCS, J. Phys. A, Phys. Rev. Lett., Phys. Rev. A, QIC
- Conference referee: FOCS, STOC, ICALP, QIP, ICS, CATS

Invited conference talks

2010 American Physical Society (APS) March Meeting
Quantum Information Processing (QIP)
2008 Workshop on Quantum Algorithms & Complexity Theory (WQACT)
Quantum Information Processing (QIP)
2007 Asian Conference on Quantum Information Science (AQIS)
Mathfest
2006 Quantum Information Processing (QIP)
NIST Workshop on Trapped Ion Quantum Computing
2004 Bay Area Theory Symposium (BATS)

Refereed conference papers

- Foundations of Computer Science (FOCS) 2009, 2007, 2006
- Symposium on Theory of Computation (STOC) '08, '04
- Symposium on Discrete Algorithms (SODA) '11 (x2)
- International Conference on Automata, Languages and Programming (ICALP) '06
- Quantum Information Processing (QIP) '09, '07
- Workshop on Selected Areas in Cryptography (SAC) '02

Grants, awards and fellowships

- 2009 Five-year Natural Sciences and Engineering Research Council of Canada (NSERC) Discovery Grant, C$29,000/year (Principal investigator)
- 2009 Three-year US Army Research Office (ARO) grant, US$200K/year (8 PIs)
- 2009 MITACS grant C$173,000 (10 PIs)
- 2001 Awarded National Science Foundation & DOD NDSEG Graduate Fellowships
- 2001 Phi Beta Kappa
- 1997 Member U.S. Physics Olympiad Team, and National Merit Scholar

Research interests

Quantum algorithms, Fault-tolerant quantum computation, Quantum information theory, Geometry of minimal surfaces, Cryptanalysis

Teaching

2010 AMATH871 / CO681 / CS667 / PHYS767 / QIC710 Quantum Information Processing
CS 768 Advanced Topics in Fault-Tolerant Quantum Computing, U. Waterloo
2009 CS 360 Introduction to the Theory of Computation, U. Waterloo
2007 Guest lecturer, CS 294-2 Quantum Computation, UC Berkeley
(two lectures on fault tolerance)
2006 Guest lecturer, CS 294-5 Great Algorithms, UC Berkeley
(Shor's factoring algorithm, Grover search)
2005 T.A., Chem./CS/Phys. 191, Quantum Information Theory, UC Berkeley

Seminars and other talks

2010 Caltech, NIST
2009 UC Berkeley, U. New Mexico, Perimeter Institute, U. Waterloo, Inst. for Advanced Study (Princeton), Caltech, MIT, Canadian Inst. for Advanced Research (CIFAR), Kavli Inst. for Theoretical Physics (KITP), HRL Laboratories
2008 National University of Singapore, UC Berkeley, UC Davis, U. Waterloo, U. Southern California (USC)
2007 USC, NEC Labs, U. Waterloo
2006 MIT, UC Berkeley, U. New Mexico, ARO/NSA/DTO Quantum Algorithms program review
2005 Caltech, UC Berkeley, U. Toronto, U. Waterloo, NIST, Bell Labs, CIFAR, DARPA Quantum Information Science and Technology (QuIST) program review
2004 Quantum computation and information theory @ Banff International Research Station

Ben W. Reichardt October 2010

Publication List

2011 1. Reflections for quantum query complexity: The general adversary bound is tight for every boolean function
B. Reichardt
Accepted to Symp. on Discrete Algorithms (SODA) 2011, arXiv:1005.1601, 13 pages.

2. Faster quantum algorithm for evaluating game trees
B. Reichardt
Accepted to Symp. on Discrete Algorithms (SODA) 2011, arXiv:0907.1623, 25 pages.

2010 3. Approximating Turaev-Viro 3-manifold invariants is universal for quantum computation
G. Alagic, S. Jordan, R. Koenig, B. Reichardt
Accepted to *Phys. Rev. A*, 2010. arXiv:1003.0923 [quant-ph], 4 pages.

4. Quantum computation with Turaev-Viro codes
R. Koenig, G. Kuperberg, B. Reichardt
Accepted to *Annals of Physics*, 2010. arXiv:1002.2816 [quant-ph], 53 pages.

5. Span programs and quantum query algorithms
B. Reichardt
Technical Report TR10-110, Electronic Colloqium on Computational Complexity, 2010, 34 pages. Submitted to *JACM*.

6. Least span program witness size equals the general adversary lower bound
B. Reichardt
Technical Report TR10-075, Electronic Colloqium on Computational Complexity, 2010, 18 pages. Submitted to *SICOMP*.

7. Any AND-OR formula of size N can be evaluated in time $N^{1/2+o(1)}$ on a quantum computer
A. Ambainis, A. Childs, B. Reichardt, R. Špalek, S. Zhang
In *Proc. 48th IEEE Foundations of Computer Science (FOCS)*, 2007, 19 pages
FOCS 2007 special issue of *SIAM Journal on Computing* **39**(6):2513-2530, 2010.

8. Span-program-based quantum algorithm for evaluating formulas
B. Reichardt, R. Špalek
In *Proc. 40th ACM Symp. on Theory of Computing (STOC)*, 2008, pages 103-112.
Accepted pending revisions to *Theory of Computing*, 2010. arXiv:0710.2630, 42 pages

2009 9. Span programs and quantum query complexity: The general adversary bound is nearly tight for every boolean function
B. Reichardt
arXiv:0904.2759 [quant-ph], 2009, 70 pages
Extended abstract in *Proc. 50th IEEE Foundations of Computer Science (FOCS)*, 2009, pages 544-551.

10. Error-detection-based quantum fault-tolerance threshold
B. Reichardt
Algorithmica, **55**(3):517-556, 2009

11. Quantum universality by distilling certain one- and two-qubit states with stabilizer operations
B. Reichardt
Quantum Information and Computation **9**:1030-1052, 2009, arXiv: quant-ph/0608085

12. On parallel composition of zero-knowledge proofs with black-box quantum simulators
R. Jain, A. Kolla, G. Midrijānis, B. Reichardt
Quantum Information and Computation **9**:513-532, 2009, arXiv: quant-ph/0607211

13. Exact entanglement renormalization for string-net models
R. Koenig, B. Reichardt, G. Vidal
Physical Review B **79**, 195123, 2009, arXiv:0806.4583 [cond-mat.str-el], 6 pages

14. Span-program-based quantum algorithm for evaluating unbalanced formulas
B. Reichardt
arXiv:0907.1622 [quant-ph], 2009, 28 pages.

2008 15. Proof of the Double Bubble Conjecture in $\mathbf{R}^n$
B. Reichardt
Journal of Geometric Analysis **18**(1):172-191, 2008
arXiv:0705.1601 [math.MG], DOI 10.1007/s12220-007-9002-y

"Fault-tolerant quantum computation" & "Quantum search" (with Lov Grover)
Articles in *Encyclopedia of Algorithms*, M.-Y. Kao (ed.), Springer, 2008.

2007 16. Every NAND formula of size N can be evaluated in time $N^{1/2+o(1)}$ on a quantum computer
A. Childs, B. Reichardt, R. Špalek, S. Zhang
arXiv: quant-ph/0703015, 2007, 14 pages

2006 17. Error-detection-based quantum fault-tolerance against discrete Pauli noise
B. Reichardt
Ph.D. thesis, University of California, Berkeley, 2006, 195 pages, arXiv: quant-ph/0612004

18. Postselection threshold against biased noise
B. Reichardt
In *Proc. 47th IEEE Foundations of Computer Science (FOCS)*, 2006, pages 420-428
arXiv: quant-ph/0608018

19. Fault-tolerance threshold for a distance-three quantum code
B. Reichardt
In Proc. Int. Conf. on Automata, Languages and Programming (ICALP) '06,
LNCS 4051, 2006, pages 50-61, arXiv: quant-ph/0509203

2005 20. Quantum universality from magic states distillation applied to CSS codes
B. Reichardt
Quantum Information Processing **4**:251-264, 2005, arXiv: quant-ph/0411036

21. Quantum error correction of systematic errors using a quantum search framework
B. Reichardt, L. Grover
Physical Review A **72**:042326, 2005, 5 pages, arXiv: quant-ph/0506242

2004 22. The quantum adiabatic optimization algorithm and local minima
B. Reichardt
In *Proc. 36th ACM Symp. on Theory of Computing (STOC)*, 2004, pages 502-510.

23. Improved ancilla preparation scheme increases fault-tolerance threshold
B. Reichardt
arXiv: quant-ph/0406025, 2004, 4 pages

2003 24. Proof of the Double Bubble Conjecture in $\mathbf{R}^4$ and certain higher dimensional cases
B. Reichardt, C. Heilmann, Y. Lai, A. Spielman
Pacific Journal of Mathematics **208**(2):347-366, 2003

2002 25. Markov truncated differential cryptanalysis of Skipjack
B. Reichardt, D. Wagner
In *Proc. 9th Selected Areas in Cryptography (SAC)*, LNCS 2595, 2002, pages 110-128

Selected Talks

2010 A semi-definite program for quantum query complexity
2nd Barriers in Computational Complexity Workshop, Princeton 8/28/10

Span programs and optimal quantum query algorithms
Invited talk, American Physical Society (APS) March Meeting 2010, Portland 3/15/10

Equivalent quantum computer models, for algorithms and implementations
National Institute of Standards and Technology (NIST) 2/17/10

Span programs and quantum algorithms
Invited talk, Quantum Information Processing (QIP) 2010, Zurich 1/19/10

2009 Span programs & quantum algorithms
HRL Labs 12/10/09

Faster quantum algorithm for evaluating game trees
Caltech 11/17/09

Span programs & quantum algorithms
MIT 11/09/09

Span programs and quantum query complexity: The general adversary bound is nearly tight for every boolean function
Foundations of Computer Science (FOCS) 2009 10/27/09

Span programs and quantum query algorithms
Institute for Advanced Study, Princeton 9/29/09

Span programs and quantum query algorithms
Kavli Institute for Theoretical Physics (KITP), Santa Barbara 9/18/09

Span programs and quantum query complexity
Waterloo Combinatorics & Optimization Dept. Tutte Seminar 8/14/09

Quantum algorithms based on span programs: The general adversary bound is nearly tight for quantum query complexity
CIFAR Quantum Information Processing Meeting 5/25/09

Quantum algorithms based on span programs: The general adversary bound is nearly tight for quantum query complexity
UNM 4/16/09

Semi-definite programs for span programs
UC Berkeley quantum lunch seminar 3/6/09

2008 Quantum algorithm for evaluating span programs
WQACT 2008, Singapore

Exact entanglement renormalization for string-net models
IQC colloquium, University of Waterloo 10/06/08

Span-program-based quantum algorithm for formula evaluation
Symp. on Theory of Computing (STOC) 2008, Victoria, BC

Making quantum computers fault tolerant
USC 4/9/08

Making quantum computers fault tolerant
UC Davis 3/17/08

Research directions in quantum computing
UC Berkeley BNNI 3/14/08

Making quantum computers fault tolerant
UC Berkeley BNNI 3/13/08

Formula evaluation using a quantum computer, and Factories for quantum fault tolerance
University of Waterloo 2/11/08

Span-program-based quantum algorithm for evaluating formulas
UC Berkeley 2/1/08

Span-program-based quantum algorithm for formula evaluation
Invited talk, Quantum Information Processing (QIP) 2008

2007 Span-program-based quantum algorithm for evaluating formulas
NEC/Rutgers Quantum Computation Group seminar 10/25/07

Any AND-OR formula of size N can be evaluated in time N^{1/2+o(1)} on a quantum computer
Foundations of Computer Science (FOCS) 2007

Quantum algorithms for formula evaluation
Invited talk, Asian Conference on Quantum Information Science (AQIS) 2007, Kyoto

Proof of the Double Bubble Conjecture in R^n
Mathfest 2007, San Jose

Any AND-OR formula of size N can be evaluated in time N^{1/2+o(1)} on a quantum computer
NEC Labs 7/07

Error-detection-based quantum fault tolerance

Perimeter Institute FTQC 2 Workshop, Waterloo 6/07

Error-detection-based quantum fault tolerance against discrete Pauli noise
USC 5/31/07

Universality by distillation
Quantum Information Processing (QIP) 2007, Brisbane

2006 Postselection threshold against biased noise
Foundations of Computer Science (FOCS) 2006, Berkeley

A probabilistic mixing lemma and quantum fault tolerance
UC Berkeley Theory Lunch 9/13/06

Fault-tolerance threshold for a distance-three quantum code
ICALP 2006, Venice 7/10/06

Quantum fault tolerance against probabilistic Pauli noise
UC Berkeley Theory Seminar dissertation talk 5/15/06

Techniques for fault-tolerant quantum error correction
UC Berkeley quantum seminar 3/14/06

Techniques for fault-tolerant quantum error correction
NIST Boulder Workshop on Trapped Ion Quantum Computing 2006

Rigorous fault-tolerance thresholds
Invited talk, Quantum Information Processing (QIP) 2006, Paris

2005 Fault-tolerance threshold for a distance-three quantum code
CIAR QIP program meeting invited talk 12/08/05

Threshold for a distance three Steane quantum code
Caltech 10/05

Quantum universality from magic states distillation applied to CSS codes
IQC, University of Waterloo 6/21/05

Quantum algorithms, complexity, and robustness
DARPA Quantum Information Science and Technology (QuIST) program review, St. Augustine, FL 4/05

Improved “magic states” distillation for quantum universality
Toronto Quantum Information Seminar 2/4/05

Fault-tolerant universality from fault-tolerant stabilizer operations and noisy ancillas
ARDA program review invited talk, Bell Labs 1/20/05

Recent schemes for increasing the fault-tolerance threshold
Invited talk, Bay Area Theory Symposium, Berkeley 12/10/05

2004 Improved magic states distillation for quantum universality
Quantum computing seminar, UC Berkeley 9/28/04

Recent schemes for increasing the fault-tolerance threshold
Banff International Research Station (BIRS) Workshop on Quantum Computation and Information Theory 9/25/04

2002 Markov truncated differential cryptanalysis of Skipjack
Selected Areas in Cryptography (SAC) 2002, St. John's, Newfoundland 8/15/02