Matthew Amy

Dalhousie University
Department of Mathematics and Statistics
6316 Coburg Road - PO BOX 15000 Halifax,
Nova Scotia B3H 4R2, Canada

Phone: (647) 746-1664
Email: matt.e.amy@gmail.com
Links: Google scholar, Github

Research Interests

Quantum computing, Programming languages, logic

Education

PhD. Computer Science, University of Waterloo, 2015–2019.
Supervisor: Michele Mosca.
Thesis: *Formal Methods in Quantum Circuit Design*.
GPA 4.00.

M.Math. Computer Science (Quantum Information), University of Waterloo, 2011–2013.
Supervisor: Michele Mosca.
Thesis: *Algorithms for the Optimization of Quantum Circuits*.
GPA 3.78.

B.Math. Computer Science (Hons, Pure Mathematics minor) University of Waterloo, 2011.
Graduated with distinction on the Dean's honour list.
GPA 3.92.

Publications

Journal Papers

M. Amy, M. Mosca, *T-count optimization and Reed-Muller codes*. IEEE Transactions on Information Theory **65**(8), 2019. DOI: 10.1109/TIT.2019.2906374, arXiv:1601.07363.

N. Killoran, J. Izaac, N. Quesada, V. Bergholm, M. Amy, C. Weedbrook, *Strawberry Fields: A Software Platform for Photonic Quantum Computing*. Quantum, 2019. DOI: 10.22331/q-2019-03-11-129, arXiv:1804.03159.

M. Amy, P. Azimzadeh, M Mosca, *On the CNOT-complexity of CNOT-PHASE circuits*. Quantum Science and Technology, 2018. DOI: 10.1088/2058-9565/aad8ca, arXiv:1712.01859.

N. Abdessaied, M. Amy, R. Drechsler, M. Soeken, *Complexity of reversible circuits and their quantum implementations*. Theoretical Computer Science 618, 2016. DOI: 10.1016/j.tcs.2016.01.011.

M. Amy, D. Maslov, M. Mosca, *Polynomial-time T-depth Optimization of Clifford+T circuits via Matroid Partitioning*. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems **33**(10), 2014. DOI: 10.1109/TCAD.2014.2341953, arXiv:1303.2042.

M. Amy, D. Maslov, M. Mosca, M. Roetteler, *A meet-in-the-middle algorithm for fast synthesis of depth-optimal quantum circuits*. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems **32**(6), 2013. DOI: 10.1109/TCAD.2013.2244643, arXiv:1206.0758.

Conference Proceedings

M. Amy, *Type Systems for Quantum Metaprogramming*. Proceedings of the 11th International Conference on Reversible Computation (RC), 2019. DOI: 10.1007/978-3-030-21500-2_6, arXiv:1908.02644.

M. Amy, *Towards large-scale functional verification of universal quantum circuits*. Proceedings of the 15th International Conference on Quantum Physics and Logic (QPL), 2018. DOI: 10.4204/EPTCS.287.1.

M. Amy, J. Chen, N. Ross, *A finite presentation of CNOT-dihedral operators*. Proceedings of the 14th International Conference on Quantum Physics and Logic (QPL), 2017. DOI: 10.4204/EPTCS.266.5.

M. Amy, M. Roetteler, K. Svore, *Verified compilation of space-efficient reversible circuits*. Proceedings of the 29th International Conference on Computer Aided Verification, 2017. DOI: 10.1007/978-3-319-63390-9_1, arXiv:1603.01635.

M. Amy, O. Di Matteo, V. Gheorghiu, M. Mosca, A. Parent, J. Schanck, *Estimating the cost of generic quantum pre-image attacks on SHA-2 and SHA-3*. Proceedings of the 23rd Conference on Selected Areas in Cryptography (SAC), 2016. DOI:10.1007/978-3-319-69453-5_18, arXiv:1603.09383.

N. Abdessaied, M. Amy, M. Soeken, R. Drechsler, *Technology mapping of reversible circuits to Clifford+ T quantum circuits*. Proceedings of the IEEE International Symposium on Multi-Valued Logic (ISMVL), 2016. DOI:10.1109/ISMVL.2016.33.

Conference presentations

Type Systems for Quantum Metaprogramming. Reversible Computation, Lausanne, Switzerland 2019. Peer reviewed conference talk.

On the CNOT-complexity of CNOT-PHASE circuits. Theory of Quantum Computation, Communication and Cryptography, Sydney, Australia 2018. Peer reviewed conference talk.

Towards large-scale verification of universal quantum circuits. Theory of Quantum Computation, Communication and Cryptography, Sydney, Australia 2018. Poster presentation.

Towards large-scale verification of universal quantum circuits. Quantum Physics and Logic, Halifax, Canada 2018. Peer reviewed conference talk.

Verification in Quantum Computing. Design Automation for Quantum Computers, Irvine, 2017. Invited talk at ICCAD satellite workshop.

Verified compilation of space-efficient reversible circuits. Computer Aided Verification, Heidelberg, Germany 2017. Peer reviewed conference talk.

Estimating the cost of generic quantum pre-image attacks on SHA-2 and SHA-3. Selected Areas in Cryptography, St. Johns, Canada 2016. Peer reviewed conference talk.

T-count optimization and Reed-Muller codes. BIRS workshop on Quantum Computer Science, Banff, Canada 2016.

Verified compilation of space-efficient reversible circuits. BIRS workshop on Quantum Computer Science software demonstration, Banff, Canada 2016.

A meet-in-the-middle algorithm for fast synthesis of depth-optimal quantum circuits. 16th Workshop on Quantum Information Processing poster session, Beijing, China 2013. Poster presentation.

Awards

AARMS Postdoctoral Fellowship, 2019–2021. *Valued at $35,000.*

Best student paper, Quantum Physics and Logic, 2018.

NSERC Alexander Graham Bell Canada Graduate Scholarship (CGS), 2015–2017. *Valued at $70,000.*

President's Graduate Scholarship, University of Waterloo, 2015-2017. *Valued at $20,000.*

Mathematics Graduate Experience Award, University of Waterloo, 2015. *Valued at $1,000.*

Bell Graduate Scholarship, University of Toronto, 2014–2015. *Valued at $20,000.*

Ontario Graduate Scholarship (OGS), University of Toronto, 2013–2014. *Valued at $15,000.*

David R. Cheriton Graduate Scholarship, University of Waterloo, 2011–2013. *Valued at $20,000.*

Mathematics Graduate Experience Award, University of Waterloo, 2011. *Valued at $1,000.*

NSERC Undergraduate Student Research Award, University of Toronto, 2011. *Valued at $4,500.*

President's Scholarship, University of Waterloo, 2007–2008. *Valued at $2,000.*

Experience

Postdoctoral Fellow, Dalhousie University, Halifax, NS. November 2019–present.

- Ongoing research into path integral-based formal methods for quantum computing, particularly for applications to verification and optimization.
- Ongoing research into characterization of quantum circuit gate sets and presentations of operator groups.

Research software engineer (6 month contract), SoftwareQ, Waterloo, ON. May 2019–October 2019.

- Designed & developed a quantum computing software stack in C++. Software is open source (staq).
- Implemented advanced & improved versions of state-of-the-art circuit optimization and mapping algorithms.

Research assistant, University of Waterloo, Waterloo, ON. September 2015–May 2019.

- Developed a formal model of quantum circuits based on the Feynman path integral. Designed new optimization and verification methods using this model.
- Designed & implemented quantum circuit analysis toolkit in Haskell. Toolkit comprises circuit utilities and novel optimization/verification algorithms. Software is open source (Feynman).
- Published 9 academic papers and 2 patent applications.

Consulting software engineer, Xanadu AI, Toronto, ON. August 2017–November 2017.

- Consulted on the design & development of a continuous variable (CV) quantum programming stack (UI, compiler, simulators, etc.) in Python.
- Wrote a backend simulator for CV quantum circuits in Python/NumPy.

Software engineer (contract), Microsoft Research, Redmond, WA. January 2016–August 2018.

- Developing & maintaining formally verified reversible circuit compiler ReVerC.
- Added a garbage collector to ReVerC, along with machine-checked proofs of correctness. Uses abstract-interpretation techniques to scalably perform reversible garbage collection.

Summer intern, Microsoft Research, Redmond, WA. April 2015–July 2015.

- Developed a formally verified compiler from an imperative language to reversible circuits. Used the dependently typed programming language F* to write machine-checked proofs of correctness. Software is open-source (ReVerC).
- Wrote a model checker for reversible circuits/programs using BDDs in F#/.NET.

Research assistant, University of Toronto, Toronto, ON. September 2013–April 2015.

- Designed & implemented a compositional dependency analysis for concurrent, heap manipulating C programs in OCaml. Implemented as an algorithm in open-source project duet.
- Designed a synthesis algorithm for concurrency control in C programs. Algorithm is a complete procedure for eliminating bad traces by adding concurrency primitives.
- Worked on verification of probabilistic programs for low-power, error prone hardware.

Research assistant, University of Waterloo, Waterloo, ON. September 2011–August 2013.

- Designed & implemented a quantum circuit optimization algorithm in C++. Algorithm is developed as an abstract-interpretation of quantum circuits and uses matroid partitioning to optimize layout. Software is open-source on github (t-par).
- Designed & implemented a quantum circuit synthesizer based on meet-in-the-middle searching in C++. Numerous optimal quantum circuits have been found using this software. Software is open-source on github (mitms).

Undergraduate Research Assistant, University of Toronto, Toronto, ON. May 2011–August 2011.

- Implemented a program dependency analysis for concurrent C programs in OCaml.
- Developed a procedure summary based method for compositional, concurrent alias analysis.

Teaching

Instructional Assistant — *planning and leading tutorials, review sessions; holding office hours; marking.*

Programming Languages, University of Toronto, Winter 2014.

Mathematical Expression and Reasoning for Computer Science, University of Toronto, Fall 2013.

Logic and Computation, University of Waterloo, Fall 2011.

Teaching Assistant — *marking assignments and exams.*

Foundations of Sequential Programs, University of Waterloo, Fall 2016.

Introduction to Combinatorics, University of Waterloo, Fall 2010.

Calculus 1 for the Sciences, University of Waterloo, Winter 2010, Fall 2009.

Academic Service

Program Committees

Programming Languages for Quantum Computing (PLanQC), 2020.

Peer Review of Academic Articles

Communications in Mathematical Physics (CIMP), Quantum Physics & Logic (QPL), International Colloquium on Automata, Languages and Programming (ICALP), Programming Language Design and Implementation (PLDI), Quantum, Quantum Science and Technology (QST), IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD), Physical Review A (PRA), Workshop on Quantum Information Processing (QIP), Quantum Information Processing, Computer Physics Communications, Journal of Computer Science and Technology.

Leadership & Volunteer

Institute for Quantum Computing Student Mentorship Program, September 2012–September 2013.

Technical Skills

Programming languages: C/C++, Haskell, OCaml/F#, Python, Coq, F*

Operating systems: Linux, Windows

Other skills: LaTeX, git, Interactive theorem proving, Embedded & real-time systems programming