Department of Electrical and Computer Engineering
University of Waterloo
200 University Ave. W., Waterloo, ON, N2L 3G1
Canada
☎ *+1 (519) 888-4567 x36616*
✉ *arie.gurfinkel@uwaterloo.ca*
arieg.bitbucket.org
office: DC2536

Arie Gurfinkel

Research Interests

Automated reasoning about software systems, especially model-checking, and software engineering methodologies supporting it.

Design, development, and verification of Cyber-Physical Systems and Real-Time Embedded Systems. Software Certification of safety critical systems.

Education

2007 **Ph.D., Computer Science**, *University of Toronto*, Toronto.
Dissertation *Model-Checking with Many Values* (Adviser: Prof. M. Chechik)

2003 **M.Sc., Computer Science**, *University of Toronto*, Toronto.
Dissertation *Multi-Valued Symbolic Model-Checking: Fairness, Counter-Examples, Running Time* (Adviser: Prof. M. Chechik)

2000 **B.Sc., Computer Science**, *University of Toronto*, Toronto.

Employment

2016 – Present **Associate Professor**, *Electrical & Computer Engineering, University of Waterloo*, Waterloo.

2015 – 2016 **Principle Researcher (MTS A)**, *Software Engineering Institute, Carnegie Mellon University*, Pittsburgh.
Lead research and development in the areas of verification, analysis, and certification of software systems.

2011 – 2015 **Senior Researcher (MTS B)**, *Software Engineering Institute, Carnegie Mellon University*, Pittsburgh.
Develop tools and techniques for verification, analysis, and certification of software systems.

2011 – 2015 **Research Scientist (Assistant Professor)**, *Computer Science Department, Carnegie Mellon University*, Pittsburgh.
Courtesy appointment hosted by Prof. Edmund Clarke.

2006 – 2010 **Researcher (MTS C)**, *Software Engineering Institute, Carnegie Mellon University*, Pittsburgh.
Develop tools and techniques for verification, analysis, and certification of software systems.

Summer 2005 **Intern**, *IBM CAS*, Toronto.
Dynamic and static analysis of webservices, and integration of software model-checker YASM with Eclipse IDE.

Honors and Awards

2015 Best paper award at the International Conference on Formal Methods in Computer-Aided Design (FMCAD).

2015 Gold and Silver at the 4th International Competition on Software Verification (SV-COMP).

2014 Software Engineering Institute (SEI) Leading and Advancing AJ Staff Award.

2014 Silver and Bronze at the 3rd International Competition on Software Verification (SV-COMP).

2013 Gold and Bronze at the 2nd International Competition on Software Verification (SV-COMP).

2004 IBM Ph.D. Fellowship.

2003 – 2005 NSERC Postgraduate Scholarship, *(PGS B)*.

2001 – 2002 Ontario Graduate Scholarship.

2000 – 2001 University of Toronto Fellowship.

Service

Co-Chair International Conference on Formal Methods for Computer-Aided Design, *2018*.

Workshop on Verification and Synthesis for Software Evolution, *2016*.

7th Working Conference on Verified Software: Theories, Tools, and Experiments (VSTTE), *2015*.

1st Artifact Evaluation Committee of 27th International Conference on Computer Aided Verification (CAV-ART), *2015*.

2nd International Workshop on Horn Clauses for Verification and Synthesis (HCVS), *2015*.

Tool Demonstration at 29th IEEE/ACM International Conference on Automated Software Engineering (ASE-TOOLS), *2014*.

5th International Workshop on the State of the Art in Automated Software Engineering Research, *2014*.

Quantified Reasoning Session at the 4th International Congress on Mathematical Software (ICMS), *2014*.

Program Committee 41th International Conference on Software Engineering (ICSE), *2019*.

30th International Conference on Computer Aided Verification (CAV), *2018*.

23rd International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS), *2018*.

40th International Conference on Software Engineering (ICSE), *2018*.

The 8th International Conference on Ambient Systems, Networks and Technologies (ANT), *2017*.

Software Verification and Testing (SAC-SVT), *2017*.

24th International SPIN Symposium on Model Checking of Software (SPIN), *2017*.

9th NASA Formal Methods Symposium (NFM), *2017*.

43nd ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL), *2016*.

Formal Methods in Computer-Aided Design (FMCAD), *2016*.

International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC), *2016*.

21th International Symposium on Formal Methods, *2016*.

3rd Workshop on Horn Clauses for Verification and Synthesis, *2016*.

22nd International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS), *2016*.

17th International Conference on Verification, Model Checking, and Abstract Interpretation (VMCAI), *2016*.

Software Verification and Testing track of the 31st ACM/SIGAPP Symposium on Applied Computing (SAC-SVT), *2016*.

8th NASA Formal Methods Symposium (NFM), *2016*.

27th International Conference on Computer Aided Verification (CAV), *2015*.

30th IEEE/ACM International Conference on Automated Software Engineering (ASE), *2015*.

20th International Symposium on Formal Methods, *2015*.

21st International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS), *2015*.

4th International Competition on Software Verification (SV-COMP), *2015*.

10th Ershov Informatics Conference (PSI), *2015*.

International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC), *2015*.

The Sixth Workshop on Tools for Automatic Program Analysis, *2015*.

29th IEEE/ACM International Conference on Automated Software Engineering (ASE), *2014*.

6th NASA Formal Methods Symposium (NFM), *2014*.

6th Working Conference on Verified Software: Theories, Tools, and Experiments (VSTTE), *2014*.

Fifth International Symposium on Games, Automata, Logics and Formal Verification (GandALF), *2014*.

International Symposium on Model Checking of Software (SPIN), *2014*.

FormaliSE: FME Workshop on Formal Methods in Software Engineering, *2014*.

9th Ershov Informatics Conference (PSI), *2014*.

3rd International Competition on Software Verification (SV-COMP), *2014*.

25th International Conference on Computer Aided Verification (CAV), *2013*.

28th IEEE/ACM International Conference on Automated Software Engineering (ASE), *2013*.

5th Working Conference on Verified Software: Theories, Tools, and Experiments (VSTTE), *2013*.

20th International Static Analysis Symposium (SAS), *2013*.

IFIP Joint International Conference on Formal Techniques for Distributed Systems (FORTE/FMOODS), *2013*.

2nd International Competition on Software Verification (SV-COMP), *2013*.

FormaliSE: FME Workshop on Formal Methods in Software Engineering, *2013*.

27th IEEE/ACM International Conference on Automated Software Engineering (ASE), *2012*.

Third International Symposium on Games, Automata, Logics, and Formal Verification, *2012*.

Asian Symposium on Programming Languages and Systems, *2012*.

26th IEEE/ACM International Conference on Automated Software Engineering (ASE), *2011*.

Annual International Conference on Computer Science and Software Engineering, *2009*.

Annual International Conference on Computer Science and Software Engineering, *2008*.

The 19th International Conference on Concurrency Theory (CONCUR), *2008*.

Referee Many conferences and journals including International Conference on Concurrency Theory (CONCUR), International Conference on Fundamental Approaches to Software Engineering (FASE), International Conference on Verification, Model Checking, and Abstract Interpretation (VMCAI), The Annual ACM Symposium on Theory of Computing (STOC), IFIP International Conference on Theoretical Computer Science (TCS), International Conference on Computer Aided Verification (CAV), Annual IEEE Symposium on Logic in Computer Science (LICS), International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS), International Conference on Formal Methods in Computer-Aided Design (FMCAD), Formal Methods in System Design (FMSD), Theoretical Computer Science, Software Tools for Technology Transfer, and many others.

Panel National Science Foundation, *2017*.

National Science Foundation, *2015*.

National Science Foundation, *2014*.

National Science Foundation, *2012*.

Teaching

2018 ECE653: Software Testing, Quality Assurance, and Maintenance, *University of Waterloo*.

2018 ECE453/CS447: Software Testing, Quality Assurance, and Maintenance, *University of Waterloo*.

2017 ECE650: Tools and Methods for Software Engineering, *University of Waterloo*.

2017 ECE653: Software Testing, Quality Assurance, and Maintenance, *University of Waterloo*.

2014 15-414/614: Bug Catching: Automated Program Verification (with Prof. Edmund Clarke and Sagar Chaki), *Carnegie Mellon University*.

2012 15-414/614: Bug Catching: Automated Program Verification (with Prof. Edmund Clarke and Sagar Chaki), *Carnegie Mellon University*.

2011 15-414: Bug Catching: Automated Program Verification and Testing (with Prof. Edmund Clarke and Sagar Chaki), *Carnegie Mellon University*.

Journal Publications

[1] A. Komuravelli, A. Gurfinkel, and S. Chaki. "SMT-based model checking for recursive programs". In: *Formal Methods in System Design* 48.3 (2016).

[2] S. Chaki, A. Gurfinkel, and O. Strichman. "Regression verification for multi-threaded programs (with extensions to locks and dynamic thread creation)". In: *Formal Methods in System Design* 47.3 (2015).

[3] A. Gurfinkel, T. Kahsai, and J. A. Navas. "Algorithmic logic-based verification". In: *SIGLOG News* 2.2 (2015).

[4] H. Chockler, A. Gurfinkel, and O. Strichman. "Beyond vacuity: towards the strongest passing formula". In: *Formal Methods in System Design (FMSD)* 43.3 (2013).

[5] N. Ghafari, A. Gurfinkel, N. Klarlund, and R. J. Trefler. "Reachability Problems in Piecewise FIFO Systems". In: *ACM Transactions on Computational Logic (TOCL)* 13.1 (2012).

[6] A. Gurfinkel and M. Chechik. "Robust Vacuity for Branching Temporal Logic". In: *ACM Transactions on Computational Logic (TOCL)* 13.1 (2012).

[7] S. Chaki and A. Gurfinkel. "Automated assume-guarantee reasoning for omega-regular systems and specifications". In: *Innovations in Systems and Software Engineering (ISSE)* 7.2 (2011).

[8] O. Wei, A. Gurfinkel, and M. Chechik. "On the consistency, expressiveness, and precision of partial modeling formalisms". In: *Information and Computatiion* 209.1 (2011).

[9] A. Gurfinkel and S. Chaki. "Combining predicate and numeric abstraction for software model checking". In: *International Journal on Software Tools for Technology Transfer (STTT)* 12.6 (2010).

[10] J. Simmonds, J. Davies, A. Gurfinkel, and M. Chechik. "Exploiting resolution proofs to speed up LTL vacuity detection for BMC". In: *International Journal on Software Tools for Technology Transfer (STTT)* 12.5 (2010).

[11] M. Chechik and A. Gurfinkel. "A framework for counterexample generation and exploration". In: *International Journal on Software Tools for Technology Transfer (STTT)* 9.5-6 (2007).

[12] M. Chechik, A. Gurfinkel, B. Devereux, A. Y. C. Lai, and S. M. Easterbrook. "Data structures for symbolic multi-valued model-checking". In: *Formal Methods in System Design (FMSD)* 29.3 (2006).

[13] M. Chechik, B. Devereux, S. M. Easterbrook, and A. Gurfinkel. "Multi-valued symbolic model-checking". In: *ACM Transactions Software Engineering and Methodology (TOSEM)* 12.4 (2003).

[14] A. Gurfinkel, M. Chechik, and B. Devereux. "Temporal Logic Query Checking: A Tool for Model Exploration". In: *IEEE Transactions on Software Engineering (TSE)* 29.10 (2003).

Conference Publications

[1] A. Katis, G. Fedyukovich, H. Guo, A. Gacek, J. Backes, A. Gurfinkel, and M. W. Whalen. "Validity-Guided Synthesis of Reactive Systems from Assume-Guarantee Contracts". In: *Tools and Algorithms for the Construction and Analysis of Systems - 24th International Conference, TACAS 2018, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2018, Thessaloniki, Greece, April 14-20, 2018, Proceedings, Part II*. Vol. 10806. Lecture Notes in Computer Science. 2018.

[2] H. Bourbouh, P. Garoche, C. Garion, A. Gurfinkel, T. Kahsai, and X. Thirioux. "Automated analysis of Stateflow models". In: *LPAR-21, 21st International Conference on Logic for Programming, Artificial Intelligence and Reasoning, Maun, Botswana, May 7-12, 2017*. Vol. 46. EPiC Series in Computing. 2017.

[3] A. Gurfinkel and A. Ivrii. "K-induction without unrolling". In: *2017 Formal Methods in Computer Aided Design, FMCAD 2017, Vienna, Austria, October 2-6, 2017*. 2017.

[4] A. Gurfinkel and J. A. Navas. "A Context-Sensitive Memory Model for Verification of C/C++ Programs". In: *Static Analysis - 24th International Symposium, SAS 2017, New York, NY, USA, August 30 - September 1, 2017, Proceedings*. Vol. 10422. Lecture Notes in Computer Science. 2017.

[5] M. Marescotti, A. Gurfinkel, A. E. J. Hyvärinen, and N. Sharygina. "Designing parallel PDR". In: *2017 Formal Methods in Computer Aided Design, FMCAD 2017, Vienna, Austria, October 2-6, 2017*. 2017.

[6] Y. Vizel, A. Gurfinkel, S. Shoham, and S. Malik. "IC3 - Flipping the E in ICE". In: *Verification, Model Checking, and Abstract Interpretation - 18th International Conference, VMCAI 2017, Paris, France, January 15-17, 2017, Proceedings*. Vol. 10145. Lecture Notes in Computer Science. 2017.

[7] A. Albarghouthi, I. Dillig, and A. Gurfinkel. "Maximal specification synthesis". In: *Proceedings of the 43rd Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL 2016, St. Petersburg, FL, USA, January 20 - 22, 2016*. 2016.

[8] A. Champion, A. Gurfinkel, T. Kahsai, and C. Tinelli. "CoCoSpec: A Mode-Aware Contract Language for Reactive Systems". In: *Software Engineering and Formal Methods - 14th International Conference, SEFM 2016, Held as Part of STAF 2016, Vienna, Austria, July 4-8, 2016, Proceedings*. Vol. 9763. Lecture Notes in Computer Science. 2016.

[9] G. Fedyukovich, A. Gurfinkel, and N. Sharygina. "Property Directed Equivalence via Abstract Simulation". In: *Computer Aided Verification - 28th International Conference, CAV 2016, Toronto, ON, Canada, July 17-23, 2016, Proceedings, Part II*. Vol. 9780. Lecture Notes in Computer Science. 2016.

[10] A. Gurfinkel, S. Shoham, and Y. Meshman. "SMT-based Verification of Parameterized Systems". In: *Proceedings of the 2016 24th ACM SIGSOFT International Symposium on Foundations of Software Engineering*. FSE 2016. Seattle, WA, USA, 2016.

[11] C. Urban, A. Gurfinkel, and T. Kahsai. "Synthesizing Ranking Functions from Bits and Pieces". In: *Tools and Algorithms for the Construction and Analysis of Systems - 22nd International Conference, TACAS 2016, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2016, Eindhoven, The Netherlands, April 2-8, 2016, Proceedings*. Vol. 9636. Lecture Notes in Computer Science. 2016.

[12] N. Bjørner and A. Gurfinkel. "Property Directed Polyhedral Abstraction". In: *Verification, Model Checking, and Abstract Interpretation - 16th International Conference, VMCAI 2015, Mumbai, India, January 12-14, 2015. Proceedings*. Vol. 8931. Lecture Notes in Computer Science. 2015.

[13] N. Bjørner, A. Gurfinkel, K. L. McMillan, and A. Rybalchenko. "Horn Clause Solvers for Program Verification". In: *Fields of Logic and Computation II - Essays Dedicated to Yuri Gurevich on the Occasion of His 75th Birthday*. Vol. 9300. Lecture Notes in Computer Science. 2015.

[14] G. Fedyukovich, A. Gurfinkel, and N. Sharygina. "Automated Discovery of Simulation Between Programs". In: *Logic for Programming, Artificial Intelligence, and Reasoning - 20th International Conference, LPAR-20 2015, Suva, Fiji, November 24-28, 2015, Proceedings*. Vol. 9450. Lecture Notes in Computer Science. 2015.

[15] A. Gurfinkel and A. Ivrii. "Pushing To The Top". In: *Formal Methods in Computer-Aided Design, FMCAD 2015, Austin, Texas, September, 2015*. 2015.

[16] A. Gurfinkel, T. Kahsai, A. Komuravelli, and J. A. Navas. "The SeaHorn Verification Framework". In: *Computer Aided Verification - 27th International Conference, CAV 2015, San Francisco, CA, USA, July 18-24, 2015, Proceedings, Part I*. Vol. 9206. Lecture Notes in Computer Science. 2015.

[17] A. Gurfinkel, T. Kahsai, and J. A. Navas. "SeaHorn: A Framework for Verifying C Programs (Competition Contribution)". In: *Tools and Algorithms for the Construction and Analysis of Systems - 21st International Conference, TACAS 2015, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2015, London, UK, April 11-18, 2015. Proceedings*. Vol. 9035. Lecture Notes in Computer Science. 2015.

[18] A. Komuravelli, N. Bjørner, A. Gurfinkel, and K. L. McMillan. "Compositional Verification of Procedural Programs using Horn Clauses over Integers and Arrays". In: *Formal Methods in Computer-Aided Design, FMCAD 2015, Austin, Texas, September, 2015*. 2015.

[19] Y. Vizel, A. Gurfinkel, and S. Malik. "Fast Interpolating BMC". In: *Computer Aided Verification - 27th International Conference, CAV 2015, San Francisco, CA, USA, July 18-24, 2015, Proceedings, Part I*. Vol. 9206. Lecture Notes in Computer Science. 2015.

[20] S. Chaki, A. Gurfinkel, and N. Sinha. "Efficient verification of periodic programs using sequential consistency and snapshots". In: *Formal Methods in Computer-Aided Design, FMCAD 2014, Lausanne, Switzerland, October 21-24, 2014*. 2014.

[21] G. Fedyukovich, A. Gurfinkel, and N. Sharygina. "Incremental Verification of Compiler Optimizations". In: *NASA Formal Methods - 6th International Symposium, NFM 2014, Houston, TX, USA, April 29 - May 1, 2014. Proceedings*. Vol. 8430. Lecture Notes in Computer Science. 2014.

[22] P. Garoche, A. Gurfinkel, and T. Kahsai. "Synthesizing Modular Invariants for Synchronous Code". In: *Proceedings First Workshop on Horn Clauses for Verification and Synthesis, HCVS 2014, Vienna, Austria, 17 July 2014*. Vol. 169. EPTCS. 2014.

[23] A. Gurfinkel and A. Belov. "FrankenBit: Bit-Precise Verification with Many Bits - (Competition Contribution)". In: *Tools and Algorithms for the Construction and Analysis of Systems - 20th International Conference, TACAS 2014, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2014, Grenoble, France, April 5-13, 2014. Proceedings*. Vol. 8413. Lecture Notes in Computer Science. 2014.

[24] A. Gurfinkel, A. Belov, and J. Marques-Silva. "Synthesizing Safe Bit-Precise Invariants". In: *Tools and Algorithms for the Construction and Analysis of Systems - 20th International Conference, TACAS 2014, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2014, Grenoble, France, April 5-13, 2014. Proceedings*. Vol. 8413. Lecture Notes in Computer Science. 2014.

[25] A. Gurfinkel and Y. Vizel. "DRUPing for interpolates". In: *Formal Methods in Computer-Aided Design, FMCAD 2014, Lausanne, Switzerland, October 21-24, 2014*. 2014.

[26] A. Ivrii, A. Gurfinkel, and A. Belov. "Small inductive safe invariants". In: *Formal Methods in Computer-Aided Design, FMCAD 2014, Lausanne, Switzerland, October 21-24, 2014*. 2014.

[27] W. Jin, C. Cohen, J. Gennari, C. Hines, S. Chaki, A. Gurfinkel, J. Havrilla, and P. Narasimhan. "Recovering C++ Objects From Binaries Using Inter-Procedural Data-Flow Analysis". In: *Proceedings of the 3rd ACM SIGPLAN Program Protection and Reverse Engineering Workshop 2014, PPREW 2014, January 25, 2014, San Diego, CA*. 2014.

[28] A. Komuravelli, A. Gurfinkel, and S. Chaki. "SMT-Based Model Checking for Recursive Programs". In: *Computer Aided Verification - 26th International Conference, CAV 2014, Held as Part of the Vienna Summer of Logic, VSL 2014, Vienna, Austria, July 18-22, 2014. Proceedings*. Vol. 8559. Lecture Notes in Computer Science. 2014.

[29] Y. Li, A. Albarghouthi, Z. Kincaid, A. Gurfinkel, and M. Chechik. "Symbolic optimization with SMT solvers". In: *The 41st Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL '14, San Diego, CA, USA, January 20-21, 2014*. 2014.

[30] Y. Vizel and A. Gurfinkel. "Interpolating Property Directed Reachability". In: *Computer Aided Verification - 26th International Conference, CAV 2014, Held as Part of the Vienna Summer of Logic, VSL 2014, Vienna, Austria, July 18-22, 2014. Proceedings*. Vol. 8559. Lecture Notes in Computer Science. 2014.

[31] A. Albarghouthi, A. Gurfinkel, Y. Li, S. Chaki, and M. Chechik. "UFO: Verification with Interpolants and Abstract Interpretation - (Competition Contribution)". In: *Tools and Algorithms for the Construction and Analysis of Systems - 19th International Conference, TACAS 2013, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2013, Rome, Italy, March 16-24, 2013. Proceedings*. Vol. 7795. Lecture Notes in Computer Science. 2013.

[32] N. Bjørner, A. Gurfinkel, K. Korovin, and O. Lahav. "Instantiations, Zippers and EPR Interpolation". In: *LPAR 2013, 19th International Conference on Logic for Programming, Artificial Intelligence and Reasoning, December 12-17, 2013, Stellenbosch, South Africa, Short papers proceedings*. Vol. 26. EPiC Series. 2013.

[33] S. Chaki, A. Gurfinkel, S. Kong, and O. Strichman. "Compositional Sequentialization of Periodic Programs". In: *Verification, Model Checking, and Abstract Interpretation, 14th International Conference, VMCAI 2013, Rome, Italy, January 20-22, 2013. Proceedings*. Vol. 7737. Lecture Notes in Computer Science. 2013.

[34] S. Chaki, A. Gurfinkel, and O. Strichman. "Verifying periodic programs with priority inheritance locks". In: *Formal Methods in Computer-Aided Design, FMCAD 2013, Portland, OR, USA, October 20-23, 2013*. 2013.

[35] A. Gurfinkel, S. F. Rollini, and N. Sharygina. "Interpolation Properties and SAT-Based Model Checking". In: *Automated Technology for Verification and Analysis - 11th International Symposium, ATVA 2013, Hanoi, Vietnam, October 15-18, 2013. Proceedings*. Vol. 8172. Lecture Notes in Computer Science. 2013.

[36] A. Komuravelli, A. Gurfinkel, S. Chaki, and E. M. Clarke. "Automatic Abstraction in SMT-Based Unbounded Software Model Checking". In: *Computer Aided Verification - 25th International Conference, CAV 2013, Saint Petersburg, Russia, July 13-19, 2013. Proceedings*. Vol. 8044. Lecture Notes in Computer Science. 2013.

[37] S. Sapra, M. Minea, S. Chaki, A. Gurfinkel, and E. M. Clarke. "Finding Errors in Python Programs Using Dynamic Symbolic Execution". In: *Testing Software and Systems - 25th IFIP WG 6.1 International Conference, ICTSS 2013, Istanbul, Turkey, November 13-15, 2013, Proceedings*. Vol. 8254. Lecture Notes in Computer Science. 2013.

[38] A. Albarghouthi, A. Gurfinkel, and M. Chechik. "Craig Interpretation". In: *Static Analysis - 19th International Symposium, SAS 2012, Deauville, France, September 11-13, 2012. Proceedings*. Vol. 7460. Lecture Notes in Computer Science. 2012.

[39] A. Albarghouthi, A. Gurfinkel, and M. Chechik. "From Under-Approximations to Over-Approximations and Back". In: *Tools and Algorithms for the Construction and Analysis of Systems - 18th International Conference, TACAS 2012, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2012, Tallinn, Estonia, March 24 - April 1, 2012. Proceedings*. Vol. 7214. Lecture Notes in Computer Science. 2012.

[40] A. Albarghouthi, A. Gurfinkel, and M. Chechik. "Whale: An Interpolation-Based Algorithm for Inter-procedural Verification". In: *Verification, Model Checking, and Abstract Interpretation - 13th International Conference, VMCAI 2012, Philadelphia, PA, USA, January 22-24, 2012. Proceedings*. Vol. 7148. Lecture Notes in Computer Science. 2012.

[41] A. Albarghouthi, Y. Li, A. Gurfinkel, and M. Chechik. "Ufo: A Framework for Abstraction- and Interpolation-Based Software Verification". In: *Computer Aided Verification - 24th International Conference, CAV 2012, Berkeley, CA, USA, July 7-13, 2012 Proceedings*. Vol. 7358. Lecture Notes in Computer Science. 2012.

[42] S. Chaki, A. Gurfinkel, and O. Strichman. "Regression Verification for Multi-threaded Programs". In: *Verification, Model Checking, and Abstract Interpretation - 13th International Conference, VMCAI 2012, Philadelphia, PA, USA, January 22-24, 2012. Proceedings*. Vol. 7148. Lecture Notes in Computer Science. 2012.

[43] W. Jin, S. Chaki, C. Cohen, A. Gurfinkel, J. Havrilla, C. Hines, and P. Narasimhan. "Binary Function Clustering Using Semantic Hashes". In: *11th International Conference on Machine Learning and Applications, ICMLA, Boca Raton, FL, USA, December 12-15, 2012. Volume 1*. 2012.

[44] S. Ben-David, M. Chechik, A. Gurfinkel, and S. Uchitel. "CSSL: a logic for specifying conditional scenarios". In: *SIGSOFT/FSE'11 19th ACM SIGSOFT Symposium on the Foundations of Software Engineering (FSE-19) and ESEC'11: 13rd European Software Engineering Conference (ESEC-13), Szeged, Hungary, September 5-9, 2011*. 2011.

[45] S. Chaki, C. Cohen, and A. Gurfinkel. "Supervised learning for provenance-similarity of binaries". In: *Proceedings of the 17th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, San Diego, CA, USA, August 21-24, 2011*. 2011.

[46] S. Chaki, A. Gurfinkel, and O. Strichman. "Time-bounded analysis of real-time systems". In: *International Conference on Formal Methods in Computer-Aided Design, FMCAD '11, Austin, TX, USA, October 30 - November 02, 2011*. 2011.

[47] A. Gurfinkel, S. Chaki, and S. Sapra. "Efficient Predicate Abstraction of Program Summaries". In: *NASA Formal Methods - Third International Symposium, NFM 2011, Pasadena, CA, USA, April 18-20, 2011. Proceedings*. Vol. 6617. Lecture Notes in Computer Science. 2011.

[48] A. Albarghouthi, A. Gurfinkel, O. Wei, and M. Chechik. "Abstract Analysis of Symbolic Executions". In: *Computer Aided Verification, 22nd International Conference, CAV 2010, Edinburgh, UK, July 15-19, 2010. Proceedings*. Vol. 6174. Lecture Notes in Computer Science. 2010.

[49] S. Chaki and A. Gurfinkel. "Automated Assume-Guarantee Reasoning for Omega-Regular Systems and Specifications". In: *Second NASA Formal Methods Symposium - NFM 2010, Washington D.C., USA, April 13-15, 2010. Proceedings*. Vol. NASA/CP-2010-216215. NASA Conference Proceedings. 2010.

[50] H. Chockler, A. Gurfinkel, and O. Strichman. "Variants of LTL Query Checking". In: *Hardware and Software: Verification and Testing - 6th International Haifa Verification Conference, HVC 2010, Haifa, Israel, October 4-7, 2010. Revised Selected Papers*. Vol. 6504. Lecture Notes in Computer Science. 2010.

[51] A. Gurfinkel and S. Chaki. "Boxes: A Symbolic Abstract Domain of Boxes". In: *Static Analysis - 17th International Symposium, SAS 2010, Perpignan, France, September 14-16, 2010. Proceedings*. Vol. 6337. Lecture Notes in Computer Science. 2010.

[52] I. Ozkaya, J. A. D. Pace, A. Gurfinkel, and S. Chaki. "Using Architecturally Significant Requirements for Guiding System Evolution". In: *14th European Conference on Software Maintenance and Reengineering, CSMR 2010, 15-18 March 2010, Madrid, Spain*. 2010.

[53] S. Chaki, A. Gurfinkel, and O. Strichman. "Decision diagrams for linear arithmetic". In: *Proceedings of 9th International Conference on Formal Methods in Computer-Aided Design, FMCAD 2009, 15-18 November 2009, Austin, Texas, USA*. 2009.

[54] S. Chaki, J. A. D. Pace, D. Garlan, A. Gurfinkel, and I. Ozkaya. "Towards engineered architecture evolution". In: *ICSE Workshop on Modeling in Software Engineering, MiSE 2009, Vancouver, BC, Canada, May 17-18, 2009*. 2009.

[55] N. Ghafari, A. Gurfinkel, and R. J. Trefler. "Verification of Parameterized Systems with Combinations of Abstract Domains". In: *Formal Techniques for Distributed Systems, Joint 11th IFIP WG 6.1 International Conference FMOODS 2009 and 29th IFIP WG 6.1 International Conference FORTE 2009, Lisboa, Portugal, June 9-12, 2009. Proceedings*. Vol. 5522. Lecture Notes in Computer Science. 2009.

[56] O. Wei, A. Gurfinkel, and M. Chechik. "Mixed Transition Systems Revisited". In: *Verification, Model Checking, and Abstract Interpretation, 10th International Conference, VMCAI 2009, Savannah, GA, USA, January 18-20, 2009. Proceedings*. Vol. 5403. Lecture Notes in Computer Science. 2009.

[57] H. Chockler, A. Gurfinkel, and O. Strichman. "Beyond Vacuity: Towards the Strongest Passing Formula". In: *Formal Methods in Computer-Aided Design, FMCAD 2008, Portland, Oregon, USA, 17-20 November 2008*. 2008.

[58] A. Gurfinkel and S. Chaki. "Combining Predicate and Numeric Abstraction for Software Model Checking". In: *Formal Methods in Computer-Aided Design, FMCAD 2008, Portland, Oregon, USA, 17-20 November 2008*. 2008.

[59] A. Gurfinkel, O. Wei, and M. Chechik. "Model Checking Recursive Programs with Exact Predicate Abstraction". In: *Automated Technology for Verification and Analysis, 6th International Symposium, ATVA 2008, Seoul, Korea, October 20-23, 2008. Proceedings*. Vol. 5311. Lecture Notes in Computer Science. 2008.

[60] T. E. Hart, K. Ku, A. Gurfinkel, M. Chechik, and D. Lie. "Augmenting Counterexample-Guided Abstraction Refinement with Proof Templates". In: *23rd IEEE/ACM International Conference on Automated Software Engineering (ASE 2008), 15-19 September 2008, L'Aquila, Italy*. 2008.

[61] T. E. Hart, K. Ku, A. Gurfinkel, M. Chechik, and D. Lie. "PtYasm: Software Model Checking with Proof Templates". In: *23rd IEEE/ACM International Conference on Automated Software Engineering (ASE 2008), 15-19 September 2008, L'Aquila, Italy*. 2008.

[62] M. Chechik, M. Gheorghiu, and A. Gurfinkel. "Finding Environment Guarantees". In: *Fundamental Approaches to Software Engineering, 10th International Conference, FASE 2007, Held as Part of the Joint European Conferences, on Theory and Practice of Software, ETAPS 2007, Braga, Portugal, March 24 - April 1, 2007, Proceedings*. Vol. 4422. Lecture Notes in Computer Science. 2007.

[63] N. Ghafari, A. Gurfinkel, N. Klarlund, and R. J. Trefler. "Algorithmic Analysis of Piecewise FIFO Systems". In: *Formal Methods in Computer-Aided Design, 7th International Conference, FMCAD 2007, Austin, Texas, USA, November 11-14, 2007, Proceedings*. 2007.

[64] M. Gheorghiu, A. Gurfinkel, and M. Chechik. "Finding State Solutions to Temporal Logic Queries". In: *Integrated Formal Methods, 6th International Conference, IFM 2007, Oxford, UK, July 2-5, 2007, Proceedings*. Vol. 4591. Lecture Notes in Computer Science. 2007.

[65] J. Simmonds, J. Davies, A. Gurfinkel, and M. Chechik. "Exploiting Resolution Proofs to Speed Up LTL Vacuity Detection for BMC". In: *Formal Methods in Computer-Aided Design, 7th International Conference, FMCAD 2007, Austin, Texas, USA, November 11-14, 2007, Proceedings*. 2007.

[66] A. Gurfinkel and M. Chechik. "Why Waste a Perfectly Good Abstraction?" In: *Tools and Algorithms for the Construction and Analysis of Systems, 12th International Conference, TACAS 2006 Held as Part of the Joint European Conferences on Theory and Practice of Software, ETAPS 2006, Vienna, Austria, March 25 - April 2, 2006, Proceedings*. Vol. 3920. Lecture Notes in Computer Science. 2006.

[67] A. Gurfinkel, O. Wei, and M. Chechik. "Systematic Construction of Abstractions for Model-Checking". In: *Verification, Model Checking, and Abstract Interpretation, 7th International Conference, VMCAI 2006, Charleston, SC, USA, January 8-10, 2006, Proceedings*. Vol. 3855. Lecture Notes in Computer Science. 2006.

[68] A. Gurfinkel, O. Wei, and M. Chechik. "Yasm: A Software Model-Checker for Verification and Refutation". In: *Computer Aided Verification, 18th International Conference, CAV 2006, Seattle, WA, USA, August 17-20, 2006, Proceedings*. Vol. 4144. Lecture Notes in Computer Science. 2006.

[69] M. Chechik and A. Gurfinkel. "A Framework for Counterexample Generation and Exploration". In: *Fundamental Approaches to Software Engineering, 8th International Conference, FASE 2005, Held as Part of the Joint European Conferences on Theory and Practice of Software, ETAPS 2005, Edinburgh, UK, April 4-8, 2005, Proceedings*. Vol. 3442. Lecture Notes in Computer Science. 2005.

[70] M. Chechik and A. Gurfinkel. "Model-Checking Software Using Precise Abstractions". In: *Verified Software: Theories, Tools, Experiments, First IFIP TC 2/WG 2.3 Conference, VSTTE 2005, Zurich, Switzerland, October 10-13, 2005, Revised Selected Papers and Discussions*. Vol. 4171. Lecture Notes in Computer Science. 2005.

[71] A. Gurfinkel and M. Chechik. "How Thorough Is Thorough Enough?" In: *Correct Hardware Design and Verification Methods, 13th IFIP WG 10.5 Advanced Research Working Conference, CHARME 2005, Saarbrücken, Germany, October 3-6, 2005, Proceedings*. Vol. 3725. Lecture Notes in Computer Science. 2005.

[72] S. Nejati, A. Gurfinkel, and M. Chechik. "Stuttering Abstraction for Model Checkin". In: *Third IEEE International Conference on Software Engineering and Formal Methods (SEFM 2005), 7-9 September 2005, Koblenz, Germany*. 2005.

[73] O. Wei, A. Gurfinkel, and M. Chechik. "Identification and Counter Abstraction for Full Virtual Symmetry". In: *Correct Hardware Design and Verification Methods, 13th IFIP WG 10.5 Advanced Research Working Conference, CHARME 2005, Saarbrücken, Germany, October 3-6, 2005, Proceedings*. Vol. 3725. Lecture Notes in Computer Science. 2005.

[74] A. Gurfinkel and M. Chechik. "Extending Extended Vacuity". In: *Formal Methods in Computer-Aided Design, 5th International Conference, FMCAD 2004, Austin, Texas, USA, November 15-17, 2004, Proceedings*. Vol. 3312. Lecture Notes in Computer Science. 2004.

[75] A. Gurfinkel and M. Chechik. "How Vacuous Is Vacuous?" In: *Tools and Algorithms for the Construction and Analysis of Systems, 10th International Conference, TACAS 2004, Held as Part of the Joint European Conferences on Theory and Practice of Software, ETAPS 2004, Barcelona, Spain, March 29 - April 2, 2004, Proceedings*. Vol. 2988. Lecture Notes in Computer Science. 2004.

[76] M. Chechik and A. Gurfinkel. "TLQSolver: A Temporal Logic Query Checker". In: *Computer Aided Verification, 15th International Conference, CAV 2003, Boulder, CO, USA, July 8-12, 2003, Proceedings*. Vol. 2725. Lecture Notes in Computer Science. 2003.

[77] S. M. Easterbrook, M. Chechik, B. Devereux, A. Gurfinkel, A. Y. C. Lai, V. Petrovykh, A. Tafliovich, and C. D. Thompson-Walsh. "ChiChek: A Model Checker for Multi-Valued Reasoning". In: *Proceedings of the 25th International Conference on Software Engineering, May 3-10, 2003, Portland, Oregon, USA*. 2003.

[78] A. Gurfinkel and M. Chechik. "Generating Counterexamples for Multi-valued Model-Checking". In: *FME 2003: Formal Methods, International Symposium of Formal Methods Europe, Pisa, Italy, September 8-14, 2003, Proceedings*. Vol. 2805. Lecture Notes in Computer Science. 2003.

[79] A. Gurfinkel and M. Chechik. "Multi-Valued Model Checking via Classical Model Checking". In: *CONCUR 2003 - Concurrency Theory, 14th International Conference, Marseille, France, September 3-5, 2003, Proceedings*. Vol. 2761. Lecture Notes in Computer Science. 2003.

[80] A. Gurfinkel and M. Chechik. "Proof-Like Counter-Examples". In: *Tools and Algorithms for the Construction and Analysis of Systems, 9th International Conference, TACAS 2003, Held as Part of the Joint European Conferences on Theory and Practice of Software, ETAPS 2003, Warsaw, Poland, April 7-11, 2003, Proceedings*. Vol. 2619. Lecture Notes in Computer Science. 2003.

[81] M. Chechik, A. Gurfinkel, and B. Devereux. "ChiChek: A Multi-valued Model-Checker". In: *Computer Aided Verification, 14th International Conference, CAV 2002,Copenhagen, Denmark, July 27-31, 2002, Proceedings*. Vol. 2404. Lecture Notes in Computer Science. 2002.

[82] A. Gurfinkel, B. Devereux, and M. Chechik. "Model exploration with temporal logic query checking". In: *Proceedings of the Tenth ACM SIGSOFT Symposium on Foundations of Software Engineering 2002, Charleston, South Carolina, USA, November 18-22, 2002*. 2002.

[83] M. Chechik, B. Devereux, and A. Gurfinkel. "Model-Checking Infinite State-Space Systems with Fine-Grained Abstractions Using SPIN". In: *Model Checking Software, 8th International SPIN Workshop, Toronto, Canada, May 19-20, 2001, Proceedings*. Vol. 2057. Lecture Notes in Computer Science. 2001.

Invited Talks and Lectures

2018 Regression Verification of Multi-Threaded Programs, *Dagstuhl Seminar on Program Equivalence*.

2017 SeaHorn: Software Model Checking with SMT and AI, *Invited tutorial at Haifa Verification Conference (HVC)*.

Pushing to the Top with k-induction, *The Technion*.

A Context Sensitive Memory Model for Software Model Checking, *Tel-Aviv University*.

Solving Constrained Horn Clauses by Property Directed Reachability, *International Workshop on Horn Clauses for Verification and Synthesis (HCVS)*.

System Verification by Abstract Interpretation and Model Checking, *The Next 40 years of Abstract Interpretation Workshop at POPL*.

2016 Algorithmic Logic-based Verification with SeaHorn, *University of Washington*.

Algorithmic Logic-based Verification with SeaHorn, *Invited talk at the 4th Workshop on Software Correctness and Reliability*.

Algorithmic Logic-based Verification with SeaHorn, *Università della Svizzera Italiana*.

Algorithmic Logic-Based Verification: Parameterized Systems, *Tenth IFIP WG 1.9/2.15 Meeting on Verified Software*.

Career Management at a Research Lab, *Invited talk at 2nd International Verification Mentoring Workshop*.

Model Checking, *Invited tutorial at Dagstuhl Seminar on Synergies among Testing, Verification, and Repair for Concurrent Programs*.

Algorithmic Logic-Based Verification, *Dagstuhl Seminar on Synergies among Testing, Verification, and Repair for Concurrent Programs*.

2015 Algorithmic Logic-based verification with SeaHorn, *POPL 2016 PC Workshop*.

Algorithmic Logic-based verification with SeaHorn, *Invited tutorial at the International Symposium on Symbolic and Numeric Algorithms for Scientific Computing*.

Parametric Symbolic Reachability, *Dagstuhl Seminar on Information from Deduction: Models and Proofs*.

Interpolating Property Directed Reachability, *Invited talk at 3rd International Workshop on Interpolation: From Proofs to Applications*.

Building Program Verifiers from Compilers and Theorem Provers, *Lectures at the Fifth Summer School on Formal Techniques*.

The SeaHorn Verification Framework, *Invited talk at the 3rd International Workshop on Verification and Program Transformation*.

2014 Verifying Programs by Evolving (Under)-Approximations, *Invited talk at the 3rd International Workshop on Valid Strategies for Software Evolution*.

2013 Verifying Programs by Evolving (Under)-Approximations, *Bell Labs*.

Trust in Formal Methods Toolchains, *VeriSure: Verification and Assurance*.

Vinta: Combining Model Checking and Abstract Interpretation, *Microsoft Research Redmond*.

2013 UFO: From Under-approximations to Over-approximations and Back!, *CMACS Seminar, Carnegie Mellon University*.

Static Analysis of Real Time Embeded Systems with REK, *Dagstuhl Seminar on Certification: Theories and Tools*.

VINTA: Verification with INTerpolation and Abstract interpretation, *Università della Svizzera Italiana*.

2012 From Under-approximations to Over-approximations and Back!, *Microsoft Research Redmond*.

Time-Bounded Analysis of Real-Time Systems, *Laboratoire d'Informatique Algorithmique: Fondements et Applications (LIAFA), Université Paris Diderot - Paris 7*.

From Under-approximations to Over-approximations and Back!, *Università della Svizzera Italiana*.

2011 An Abstract Domain of Boxes, *Departmental Colloquium Series, University of Iowa*.

2008 Introduction to BMC, *Guest lecture at 15-414, Carnegie Mellon University*.

2007 Why Waste a Perfectly Good Abstraction?, *Specification and Verification Center (SVC) Seminar, Carnegie Mellon University*.

2006 Model Checking: From Hardware to Software, *Tutorial at 14th International Symposium on Formal Methods*.

Why Waste a Perfectly Good Abstraction?, *Microsoft Research Cambridge*.

2005 Software Model-Checking with YASM: A Tutorial, *Guest lecture at CSC2108, University of Toronto*.

2003 An Automata-Theoretic Approach to Branching Time Model-Checking, *Guest lecture at CSC2108, University of Toronto*.

Graduate Students

Spring 2018 **Matteo Marescotti**, *Intern, University of Waterloo*.
Distributed Property Directed Reachability

2017–Present **Jakub Kuderski**, *MSc, University of Waterloo*.
Memory Safety Verification with Software Model Checking

2017–Present **Rylo Ashmore**, *MSc, University of Waterloo*.
Local Verification of Distributed Systems (Co-Adviser: Prof. Richard Trefler)

Summer 2017 **Bernhard Gleiss**, *Intern, University of Waterloo*.
Better Generalization for IC3

2016–Present **Reza Babaee**, *PhD, University of Waterloo*.
Run-time Monitoring of Probabilistic Systems

Summer 2015 **Caterina Urban**, *Intern, Carnegie Mellon University*.
Synthesizing Ranking Functions from Bits and Pieces

2014–2015 **Grigory Fedyukovich**, *PhD, Università della Svizzera italiana (USI)*.
Automated Incremental Software Verification (Co-Adviser: Prof. Natasha Sharygina)

2012–2015 **Anvesh Komuravelli**, *PhD, Carnegie Mellon University*.
Abstraction in SMT-Based Model Checking (Co-Adviser: Prof. Edmund Clarke)

Summer 2012 **Soonho Kong**, *PhD, Carnegie Mellon University*.
Analyzing Real-Time Embedded Systems (Co-Adviser: Prof. Edmund Clarke)

2011–2013 **Yi Li**, *MSc, University of Toronto*.
Precise Transformers for Linear Arithmetic (Co-Adviser: Prof. Marsha Chechik)

2009–2014 **Aws Albarghouthi**, *PhD, University of Toronto*.
Software Verification with Interpolation (Co-Adviser: Prof. Marsha Chechik)

Summer 2010 **Samir Sapra**, *PhD, Carnegie Mellon University*.
Efficient Predicate Abstraction of Program Summaries (Co-Adviser: Prof. Edmund Clarke)

2006–2009 **Nagmeh Ghafari**, *PhD, University of Waterloo*.
Algorithmic Analysis of Infinite State Systems (Co-Adviser: Prof. Richard Trefler)

2003–2009 **Ou Wei**, *PhD, University of Toronto*.
Abstraction for Verification and Refutation (Co-Adviser: Prof. Marsha Chechik)

Undergraduate Students

Winter 2018 **Charles Lei**, *USRA, University of Waterloo*.
Executable Counterexamples for Software Model Checking

Winter 2018 **Yubo Han**, *USRA, University of Waterloo*.
Alias Analysis in LLVM

Funding

2017–2022 Automated Software Verification: Foundations and Applications, *NSERC Discovery*.

2016 IBM Faculty Award, *IBM*.

2015–2016 Property-Directed Test-case Generation, *SEI*.

2014-2017 Contract-based Compositional Verification for Outsourced Flight Critical Systems, *NASA*.

2013–2015 Verifying Evolving Software, *SEI*.

2010–2011 Regression Verification of Real-time Embedded Software, *SEI*.

References

Marsha Chechik
Professor
Dept. of Computer Science
University of Toronto
Toronto, Canada
✉ chechik@cs.toronto.edu
☎ +1 (416) 978-3820

Orna Grumberg
Professor
Computer Science Dept.
Technion – Israel Inst. of Technology
Haifa, Israel
✉ orna@cs.technion.ac.il
☎ +972 (4) 829-4327

Nikolaj Bjørner
Principal Researcher
Microsoft Research
Redmond, USA
✉ nbjorner@microsoft.com

Aarti Gupta
Professor
Dept. of Computer Science
Princeton University
Princeton, USA
✉ aartig@cs.princeton.edu
☎ +1 (609) 258-8017