Jan Hoffmann

Carnegie Mellon University – Computer Science Department

+1 412 268 6309 • jhoffmann@cmu.edu • www.cs.cmu.edu/~janh

Research Interests

My research interests are in the intersection of *programming languages* and *formal methods* with a focus on *quantitative software analysis*. I am an expert on *static resource-usage analysis* and interested in applying quantitative methods to *security and privacy.*

Education

Ludwig-Maximilians-Universität and TU Munich **Munich**
Ph.D. in Computer Science *2008–2011*
Advisor: Prof. Martin Hofmann. Grade: magna cum laude.
Topic: Types with Potential: Polynomial Resource Bounds via Automatic Amortized Analysis.

Ludwig-Maximilians-Universität **Munich**
Diplom mit Auszeichnung (Master with Honors in Computer Science) *2001–2007*
Grade: 1.0 (best possible).
Major: Theoretical Computer Science. Minor subject: Mathematics.

Positions

Carnegie Mellon University **Pittsburgh**
Tenure-Track Assistant Professor *2015–present*
In the Computer Science Department of the School of Computer Science.

Yale University **New Haven**
Associate Research Scientist *2012–2015*
Topic: Quantitative Verification. Support: NSF VeriQ (PI) and DARPA HACMS (Key Personnel).

Yale University **New Haven**
Postdoctoral Associate *2011–2012*
In the group of Prof. Zhong Shao. Topic: Verification of Lock-Free Data Structures.
Support: DARPA HACMS (Key Personnel) and DARPA CRASH.

Microsoft Research **Cambridge, UK**
Research Intern *Feb. – Apr. 2011*
Mentors: Andrew Kennedy and Nick Benton. Topic: Operational Semantics in Coq.

Ludwig-Maximilians-Universität and TU Munich **Munich**
Research Assistant *2007–2011*
In the group of Prof. Martin Hofmann. Topic: Automatic Resource Bound Analysis.

University of California, San Diego **San Diego**
Master Thesis *Jan. – Jun. 2007*
Advisor: Prof. Samuel R. Buss. Topic: DLL Algorithms and Resolution Proofs.

Professional Activities

Organizer

19th Workshop on Logic and Computational Complexity (LCC'18) (Co-Chair with Erich Graedel) 2018
Dagstuhl Seminar *Resource Bound Analysis*, with M. Gaboardi, R. Wilhelm, and F. Zuleger 2017
LOLA 2016 - Syntax and Semantics of Low-Level Languages (Co-Chair with Marco Gaboardi) 2016
Annual PUMA Workshop, Venice, Italy. 2009

Guest Editor

Journal of Automated Reasoning, Special Issue *Automatic Resource Bound Analysis* 2015–present

Committee Member

Program Committee – European Symposium on Programming (ESOP'18) 2017
Program Committee – Joint Workshop on Developments in Implicit Computational Complexity and Foundational and Practical Aspects of Resource Analysis (DICE-FOPARA'17) 2017
Program Committee – Int. Conf. on Formal Structures for Computation and Deduction (FSCD'17) 2017
Program Committee – Conf. on Programming Language Design and Implementation (PLDI'17) 2016–2017
External Review Committee – Conference on Computer Aided Verification (CAV'16) 2016
Program Committee – Conf. on Found. of Software Science and Comp. Structures (FOSSACS'16) 2015
Program Committee – Developments in Implicit Computational Complexity (DICE'15) 2015
External Review Committee – Symposium on Principles of Programming Languages (POPL'15) 2014

External Reviewer: ESOP'17, Trans. Dependable Secure Comput; ESOP'14, Science of Comp. Prog. (2013), LICS'11, ESOP'10, PADL'10, CSL'10, POPL'09, ESOP'09.

University Service

Master Admission Committee – Computer Science Department, Carnegie Mellon University 2015-2016

Teaching and Mentoring

Current Students and Post-Docs

Chan Ngo, Post-Doc 2016–present
Ankush Das, PhD Student 2015–present
Quentin Carbonneaux, PhD Student (co-advised with Zhong Shao) 2013–present
Yue Niu, BS Student 2017–present
Benjamin Lichtman, BS Student (now Software Engineer at Microsoft) 2016–2017

Courses Taught

15-312: Principles of Programming Languages (with Bob Harper) Carnegie Mellon, Spring 2017
15-411/15-611: Compiler Design Carnegie Mellon, Fall 2016
Type-Based Resource Analysis Oregon PL Summer School, Summer 2016
15-819: Advanced Topics in Programming Languages: Resource Analysis Carnegie Mellon, Spring 2016
CPSC730: Advanced Formal Methods Topics (with Zhong Shao) Yale, Fall 2012
CPSP721: Advanced Programming Language Topics (with Zhong Shao) Yale, Spring 2012

Grants and Awards

Schmidt Sciences Grant

The Eric and Wendy Schmidt Fund for Strategic Innovation *2017–2018*
Title: *An Automated Algorithm Designer.* With Carl Kingsford, Nina Balcan, Mor Harchol-Balter, Guy Blelloch, Anupam Gupta, and Jan Hoffmann.

Google Research Award

Google Inc. *2016*
Title: *Automated Static Resource Regression Analysis.*

Dagstuhl Seminar (Organizer)

Schloss Dagstuhl *2016*
Title: *Resource Bound Analysis*. Date: July, 2017.
With Marco Gaboardi, Reinhard Wilhelm, and Florian Zuleger.

Research Contract (Principle Investigator)

DARPA STAC – Space/Time Analysis for Cybersecurity *2015–2019*
Title: *CURB: Calculating and Understanding Resource Bounds to Detect Space/Time Vulnerabilities.*
$6,230,090, 4 years, Award FA8750-15-C-0082 PIs: A. Loginov (GrammaTech),
T. Reps (U Wisconsin), J. Hoffmann (CMU) and Z. Shao (Yale); Yale/CMU component: $1,448,531.

Research Grant (Principal Investigator)

National Science Foundation (NSF) *2013–2016*

Title: *VeriQ: Formal Quantitative Software Verification in Realistic Application Scenarios.*
$449,721, 3 years, Award CCF-1319671, PIs: Zhong Shao and Jan Hoffmann.

Ph.D. Scholarship
DFG Research Training Group (Graduiertenkolleg) PUMA *2008–2011*
PUMA is a joint graduate school (doctoral training center) of LMU Munich and TU Munich.
It is supported by the German Research Foundation (DFG).

Foreign Education Scholarship
German National Academic Foundation (Studienstiftung) *2007*
For a six months' stay at University of California, San Diego.

Student Scholarship
German National Academic Foundation (Studienstiftung) *2005–2007*
For studying computer science at Ludwig-Maximilians-Universität Munich.

Software

Quantitative CompCert
A formally-verified C compiler that preserves quantitative properties *2013–present*
We modified Xavier Leroy's CompCert compiler and used the Coq Proof Assistant to prove the preservation of quantitative properties during compilation of C to x86 assembly. This enables the verification of stack-space bounds at the C level. This artifact was approved by the *PLDI'13 Artifact Evaluation Committee.* (Project Website)

C^{4}B
A compositional certified resource-bound analyzer for C programs *2013–present*
We designed and implemented a system for statically determining a symbolic bound on the resource usage of C programs. The system is based on a fully-automatic amortized resource analysis. (Project Website)

Resource Aware ML
A system for automatic derivation of resource bounds for functional programs *2009–present*
For my Ph.D., I designed and implemented a system that automatically derives polynomial resource bounds for functional programs at compile time. We are currently integrating the analysis systems with INRIA's OCaml compiler. (Project Website)

CertiKOS
A formally-verified hypervisor kernel *2012–2015*
In the DARPA HACMS and DARPA CRASH programs, we use the Coq Proof Assistant and the verified CompCert C compiler to implement and verify the realistic hypervisor kernel CertiKOS. (Project Website)

Publications

In Peer-Reviewed Conferences

1. B. Lichtman and J. Hoffmann.
   Arrays and References in Resource Aware ML.
   In *2nd International Conference on Formal Structures for Computation and Deduction (FSCD'17)*, 2017. PDF.

2. Q. Carbonneaux, J. Hoffmann, T. Reps, and Z. Shao.
   Automated Resource Analysis with Coq Proof Objects.
   In *29th International Conference on Computer-Aided Verification (CAV'17)*, 2017. PDF.

3. V. C. Ngo, M. Dehesa-Azuara, M. Fredrikson, and J. Hoffmann.
   Verifying and Synthesizing Constant-Resource Implementations with Types.
   In *38th IEEE Symposium on Security and Privacy (S&P '17)*, 2017. PDF.

4. A. Das and J. Hoffmann.
   ML for ML: Learning Cost Semantics by Experiment.
   In *23rd International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS'17)*, 2017. PDF.

5. E. Çiçek, G. Barthe, M. Gaboardi, D. Garg, and J. Hoffmann.
Relational Cost Analysis.
In *44th Symposium on Principles of Programming Languages (POPL'17)*, 2017. PDF.

6. J. Hoffmann, A. Das, and S.-C. Weng.
Towards Automatic Resource Bound Analysis for OCaml.
In *44th Symposium on Principles of Programming Languages (POPL'17)*, 2017. Artifact submitted and approved. PDF.

7. Q. Carbonneaux, J. Hoffmann, and Z. Shao.
Compositional Certified Resource Bounds.
In *36th Conference on Programming Language Design and Implementation (PLDI'15)*, 2015. Artifact submitted and approved. PDF.

8. J. Hoffmann and Z. Shao.
Automatic Static Cost Analysis for Parallel Programs.
In *24th European Symposium on Programming (ESOP'15)*, 2015. PDF.

9. J. Hoffmann and Z. Shao.
Type-Based Amortized Resource Analysis with Integers and Arrays.
In *12th International Symposium on Functional and Logic Programming (FLOPS'14)*, 2014. PDF.

10. Q. Carbonneaux, J. Hoffmann, T. Ramananandro, and Z. Shao.
End-to-End Verification of Stack-Space Bounds for C Programs.
In *35th Conference on Programming Language Design and Implementation (PLDI'14)*, 2014. Artifact submitted and approved. PDF.

11. G. Scherer and J. Hoffmann.
Tracking Data-Flow with Open Closure Types.
In *19th International Conference on Logic for Programming, Artificial Intelligence and Reasoning (LPAR'13)*, 2013. PDF.

12. H. Liang, J. Hoffmann, X. Feng, and Z. Shao.
Characterizing Progress Properties of Concurrent Objects via Contextual Refinements.
In *24th International Conference on Concurrency Theory (CONCUR'13)*, 2013. PDF.

13. J. Hoffmann, M. Marmar, and Z. Shao.
Quantitative Reasoning for Proving Lock-Freedom.
In *28th ACM/IEEE Symposium on Logic in Computer Science (LICS'13)*, 2013. PDF.

14. J. Hoffmann, K. Aehlig, and M. Hofmann.
Resource Aware ML.
In *24rd International Conference on Computer Aided Verification (CAV'12)*, 2012. PDF.

15. N. R. Krishnaswami, N. Benton, and J. Hoffmann.
Higher-Order Functional Reactive Programming in Bounded Space.
In *39th Symposium on Principles of Programming Languages (POPL'12)*, 2012. PDF.

16. J. Hoffmann, K. Aehlig, and M. Hofmann.
Multivariate Amortized Resource Analysis.
In *38th Symposium on Principles of Programming Languages (POPL'11)*, 2011. PDF.

17. J. Hoffmann and M. Hofmann.
Amortized Resource Analysis with Polymorphic Recursion and Partial Big-Step Operational Semantics.
In *8th Asian Symposium on Programming Languages (APLAS'10)*, 2010. PDF.

18. J. Hoffmann and M. Hofmann.
Amortized Resource Analysis with Polynomial Potential.
In *19th European Symposium on Programming (ESOP'10)*, 2010. PDF.

19. D. Baumeister, F. Brandt, F. A. Fischer, J. Hoffmann, and J. Rothe.
The Complexity of Computing Minimal Unidirectional Covering Sets.
In *Algorithms and Complexity, 7th International Conference (CIAC'10)*, 2010. PDF.

20. F. Brandt, M. Brill, F. A. Fischer, and J. Hoffmann.
The Computational Complexity of Weak Saddles.
In *Algorithmic Game Theory, Second International Symposium (SAGT'09)*, 2009. PDF.

In Peer-Reviewed Journals

21. J. Hoffmann and Z. Shao.
Type-Based Amortized Resource Analysis with Integers and Arrays.
J. Funct. Program., 2015. PDF.

22. D. Baumeister, F. Brandt, F. A. Fischer, J. Hoffmann, and J. Rothe.
The Complexity of Computing Minimal Unidirectional Covering Sets.
Theory of Computing Systems, 2013. PDF.

23. J. Hoffmann, K. Aehlig, and M. Hofmann.
Multivariate Amortized Resource Analysis.
ACM Trans. Program. Lang. Syst., 2012. PDF.

24. F. Brandt, M. Brill, F. A. Fischer, and J. Hoffmann.
The Computational Complexity of Weak Saddles.
Theory of Computing Systems, 2010. PDF.

25. F. Brandt, M. Brill, F. Fischer, P. Harrenstein, and J. Hoffmann.
Computing Shapley's Saddles.
ACM SIGecom Exchanges, 8, 2009. PDF.

26. J. Hoffmann.
Finding a Tree Structure in a Resolution Proof is NP-Complete.
Theoretical Computer Science, 410(21-23), 2009. PDF.

27. S. R. Buss, J. Hoffmann, and J. Johannsen.
Resolution Trees with Lemmas: Resolution Refinements that Characterize DLL Algorithms with Clause Learning.
Logical Methods in Computer Science, 4(4), 2008. PDF.

28. S. R. Buss and J. Hoffmann.
The NP-hardness of Finding a Directed Acyclic Graph for Regular Resolution.
Theoretical Computer Science, 396(1-3), 2008. PDF.

Theses

29. J. Hoffmann.
Types with Potential: Polynomial Resource Bounds via Automatic Amortized Analysis. PhD thesis, Ludwig-Maximilians-Universiät München, 2011. PDF.

30. J. Hoffmann.
Resolution Proofs and DLL-Algorithms with Clause Learning. Diploma Thesis, LMU München, 2007. PDF.

Other Papers

31. A. Das and J. Hoffmann.
Learning Cost Semantics for Modeling Running Time of OCaml Programs, 2016. Presented at Syntax and Semantics of Low-Level Languages (LOLA'16). PDF.

Talks

Resource Bound Analysis and Static Analysis
Invited talk at the 9th Working Conference on Verified Software: Theories, Tools, and Experiments (VSTTE '17); Heidelberg, Germany — July 2017

Towards Automatic Resource Bound Analysis for OCaml
Symposium on Principles of Programming Languages (POPL'17); Paris, France — January 2017

Resource Aware ML
Invited talk at the 5th South of England Regional Programming Language Seminar; Oxford; UK — January 2017
Invited talk at Max Planck Institute for Software Systems; Saarbrücken; Germany — June 2016

Automatic Resource Bound Analysis and Linear Optimization
Invited talk at the workshop *Beyond Worst-Case Analysis* at the Simons Institute; Berkeley; CA — November 2016

Static Analysis for Finding Space/Time Vulnerabilities
Invited talk at the CyLab Partners Conference; Pittsburgh; PA — September 2016

Type-Based Resource Analysis
Invited lecture at the Oregon Programming Languages Summer School); Eugene; OR — June 2016

Certified Resource Bounds in the CompCert Compiler
Invited talk at Mathematical Foundations of Programming Semantics (MFPS'16); Pittsburgh; PA — Mai 2016

Resource Aware Programming
Principles of Programming (PoP) Group Retreat; Seven Springs; PA — October 2015

Compositional Certified Resource Bounds
Conf. on Programming Language Design and Implementation (PLDI'15); Portland; OR — June 2015

Automatic Static Cost Analysis for Parallel Programs
European Symposium on Programming (ESOP'15); London; UK — April 2015

Formal Reasoning about Quantitative Properties of Software
Invited talk at University of Colorado Boulder; Boulder, CO — March 2015
Invited talk at Carnegie Mellon University; Pittsburgh, PA — February 2015
Invited talk at University of Illinois at Urbana-Champaign; Urbana-Champaign, IL — February 2015
Invited talk at University of Waterloo; Waterloo ON, Canada — January 2015
Invited talk at Heriot-Watt University; Edinburgh, UK — January 2015
Invited talk at TU Munich (Department of Computer Science); Munich, Germany — November 2014
Invited talk at Boston University; Boston MA — October 2014
Invited talk at Northeastern University; Boston MA — October 2014
Invited talk at MIT; Boston MA — April 2014
Invited talk at Harvard University; Boston MA — April 2014

Formal Verification of Quantitative Software Properties
Invited talk at TU Munich (Institute for Advanced Study); Munich, Germany — November 2014

End-to-End Verification of Stack-Space Bounds for C Programs
Workshop on Higher Order Computation: Types, Complexity, Applications; Paris, France — June 2014

Type-Based Amortized Resource Analysis with Integers and Arrays
Int. Symp. on Functional and Logic Programming (FLOPS'14); Kanasawa, Japan — June 2014

Tracking Data-Flow with Open Closure Types
Int. Conf. on Logic for Prog., Art. Intel. and Reasoning (LPAR'13); Stellenbosch, South Africa — December 2013

Characterizing Progress Properties of Concurrent Objects via Contextual Refinements
DARPA HACMS-CARS site visit; New Haven, CT — September 2013

Quantitative Reasoning for Proving Lock-Freedom

ACM/IEEE Symposium on Logic in Computer Science (LICS'13); New Orleans, LA — June 2013
Invited talk at University of Pennsylvania; Philadelphia, PA — February 2013
DARPA CRASH PI meeting; San Diego, CA — November 2012
DARPA CRASH-CertiKOS site visit; New Haven, CT — October 2012

Resource Aware ML
Int. Conf. on Computer Aided Verification (CAV'12); Berkeley, CA — July 2012

Polynomial Amortized Resource Analysis
DFG PUMA site visit; Munich, Germany — June 2012
Dissertation defense at LMU; Munich, Germany — October 2011

Higher-Order Functional Reactive Programming in Bounded Space
PUMA Workshop; Traunkirchen, Austria — October 2011

Multivariate Amortized Resource Analysis
Invited talk at Université Paris 7 - Denis Diderot; Paris, France — September 2011
Invited talk at UPENN; Philadelphia, PA — June 2011
Invited talk at Yale University; New Haven, CT — June 2011
Invited talk at IST Austria; Vienna, Austria — June 2011
Invited talk at Microsoft Research; Cambridge, UK — March 2011
Symposium on Principles of Programming Languages (POPL'11); Austin, TX — January 2011
PUMA Workshop; Szentendre, Hungary — October 2010

Amortized Resource Analysis with Polymorphic Recursion and Partial Big-Step Op. Sem.
Asian Symposium on Programming Languages (APLAS'10); Shanghai, China — November 2010

Analysing Sorting Algorithms in Resource Aware ML
Invited talk at University of Kassel; Kassel, Germany — November 2010

Automatic Amortized Resource Analysis
National DFG GK Workshop; Dagstuhl, Germany — June 2010

Amortized Resource Analysis with Polynomial Potential
European Symposium on Programming (ESOP'10); Cyprus — March 2010
PUMA Workshop; Venice, Italy — October 2009

A Purely-Functional SAT Solver
PUMA Kickoff Meeting; Spitzingsee, Germany — October 2008

DLL-Algorithms and Resolution Proofs
Fall School: Logic and Complexity; Prague, Czech Republic — September 2008

Languages

German: Native
English: Fluent
French: Elementary

References

Prof. Martin Hofmann, PhD
LMU München
Institut für Informatik
Oettingenstr. 67
80538 München, Germany
Email: hofmann@ifi.lmu.de
Phone: +49 (89) 2180 9341

Prof. Zhong Shao, PhD
Yale University
Department of Computer Science
51 Prospect St.
New Haven, CT 06511, USA
Email: zhong.shao@yale.edu
Phone: +1 (203) 432 6828

Prof. Andrew W. Appel, PhD
Princeton University
Department of Computer Science
35 Olden St.
Princeton, NJ 08540, USA
Email: appel@princeton.edu
Phone: +1 (609) 258 4627

Nick Benton, PhD
Microsoft Research
21 Station Road
Cambridge CB1 2FB, UK
Email: nick@microsoft.com
Phone: +44 (1223) 479700 (reception)

Frank Pfenning, Professor and Department Head
Carnegie Mellon University
Computer Science Department
5000 Forbes Avenue
Pittsburgh, PA 15213-3891, USA
Email: fp@cs.cmu.edu
Phone: +1 (412) 268-6343