Matt Kaufmann

Senior Research Scientist
Dept. of Computer Science, Univ. of Texas at Austin

2203 Euclid Avenue, Austin, TX 78704
(512) 443-9212
Born: 12/9/52; married; no children
U.S. Citizen

Education

Ph.D., Mathematics, June, 1978
University of Wisconsin, Madison, Wisconsin

M.A., Mathematics, December, 1974
University of Wisconsin, Madison, Wisconsin

S.B., Mathematics, June, 1973
Massachusetts Institute of Technology

Honors

Co-winner (with Robert S. Boyer and J Strother Moore) of the 2005 ACM Software System Award.

Support Activities

Have served on program committees, Ph.D. committees, and NSF panels; reviewed papers; served as conference/workshop (co-)chair; maintained mailing lists; etc. Details available upon request.

Employment History

Senior Research Scientist, December 2005 – present
Dept. of Computer Sciences, University of Texas, Austin, Texas

Senior Member of the Technical Staff, August 1999 – November 2005
Advanced Micro Devices, Inc., Austin, Texas

Senior Systems Engineer, August 1997 – August 1999
EDS, Inc., CIO Services, Austin, Texas

Senior Individual Contributor, August 1995 – August 1997
Motorola, Inc., Austin, Texas

Senior Computing Research Scientist, September 1987 – August 1995
Computational Logic, Inc., Austin, Texas

Research Scientist, August 1986 – August 1987
Institute for Computing Science, University of Texas, Austin, Texas

Adjunct Associate Professor: Spring 1988, Fall 1989, and Fall 1994
Departments of Mathematics (1988, 89) and Philosophy (1994)
University of Texas, Austin, Texas

Research Scientist, October 1985 – June 1986
Associate Research Scientist, June 1984 – October 1985
Austin Research Center
Burroughs Corporation, Austin, Texas

Assistant Professor, August 1978 – May 1984 (on leave 9/82 – 5/83)
Department of Mathematics
Purdue University, West Lafayette, Indiana

Visiting Assistant Professor, September 1982 – May 1983
Department of Mathematics
University of Connecticut, Storrs, Connecticut

Teaching Assistant, August 1973 – May 1978
Department of Mathematics
University of Wisconsin, Madison, Wisconsin

Summary of Experience

Tool Development:

Co-author (with J Moore) of the ACL2 theorem proving system. Also contribute actively to the ACL2 community through the ACL2 Workshop, the acl2-help mailing list, the Univ. of Texas ACL2 seminar, and serving on Ph.D. committees.

Other formal verification tools

- Wrote many tools based on ACL2: some recently, for example, a program transformation tool based on simplification (ongoing, 2017); and some decades ago, for example, a symbolic execution tool for ACL2 (early to mid 1990s).
- Enhanced Motorola's Verilog/DSL model-checker and compiler

- Built numerous extensions to the Boyer-Moore "Nqthm" prover
- Designed and implemented a prototype verification system for a subset of Common Lisp that includes macros and imperative features
- With Bob Boyer, developed a modification of the Boyer-Moore theorem prover to use as a verification tool for the applicative language SASL

Translators

- At AMD, co-developed a language and tools for representing state-machine HDL descriptions in ACL2
- Wrote internal Motorola translator from one commercial hardware design language to another
- Wrote translators for several small hardware design languages
- Wrote translator from Nqthm to ACL2

Other tools

- At AMD, wrote sophisticated C++ multi-processor memory model and did associated simulation debug
- Became AMD expert on routing tables and developed several pertinent tools
- Wrote heuristics-based tool at AMD for analyzing certain collected Northbridge transaction data
- At AMD, developed and ran a "smart" tool that finds classes of syntax bugs in rtl
- Wrote tool for finding dead code in RTL
- Developed numerous enhancements of EDS analysis tool for COBOL, Cogen 2000^{TM}. In particular, implemented data flow, type propagation, and test instrumentation. Also developed regression test capability.
- Wrote assembler for Motorola CAP processor (assisted by Bishop Brock)
- Co-authored/applied a course-grained parallel "dispatcher"
- Developed and documented an enhanced Lisp tracing facility
- Implemented the PODEM algorithm for generating tests for faults in circuits

Applications of automated reasoning tools:

Formally verified the correctness of a SAT proof-checker, used for example in SAT Competition 2017 and in verifying "World's Largest Math Proof" (194 terabytes, 8,651 CPU hours).

Contributed to x86 ISA modeling project at UT Austin.

Used ACL2 on several projects at AMD

Using ACL2, specified and verified expression replacement rules used by EDS tool Cogen 2000 for Year 2000 remediation

Created, with J Moore, a mechanically-checked proof of correctness of the floating-point division algorithm for the AMD K5 microprocessor

Co-authored a simplified 60x (Power PC) bus protocol specification and verification

Improved ACL2 integer libraries

Contributed to FM9001 chip verification

Assisted in Piton assembler proof

Developed and published correctness proof for a generalization algorithm

Co-developed Ada subset semantics and did corresponding program verification

Verified SASL (lazy functional language) programs

Instructional, support, and tech transfer activities:

At AMD, in collaboration with others, developed theory and ran tools pertaining to routing of packets, including x86 assembly and writing descriptions for BIOS guide. (See also related item about routing, above, under "Tool Development / Other Tools.")

Made extensive comments on AMD protocol documentation

Maintained rules documents for Year 2000 COBOL renovations performed by EDS CIO Services

Assisted internal Motorola customers in use of formal verification and translator tools

Developed tutorial materials for the Boyer-Moore theorem prover

By invitation, twice visited the Mathematics Reasoning group IRST (Trento, Italy)

Gave short courses in Lisp and theorem proving for hardware verification at Boeing Corp., Motorola GSG (Phoenix), and UT Year of Programming

Taught mathematics courses and performed other instructional activities, first as teaching assistant and then as faculty member at Purdue and (later) at UT Austin

Other technical activities:

At AMD, implemented C++ northbridge-related checkers and did associated simulation debug

Participated in evaluations of formal and semi-formal tools external to AMD

Wrote scripts in support of Motorola's model checker, for example to support regression testing and tool release

Participated in comparisons of theorem provers

Evaluated TRW's "Deductive Theory Manager" and documented findings

Served by invitation on NSF Committee of Visitors, July, 1996

Served on committees (program, dissertation, ...), refereed papers, did proposal writing, gave invited talks

Contributed to Nqthm *functional instantantiation* capability

Developed a formal logic and model theory for the programming language SASL

Co-developed improved compilation algorithm for SASL

Ran experiments to analyze potential speedup for concurrent execution of SASL programs

Pure mathematics research included over 20 papers (some co-authored) in Mathematical Logic

Selected Publications

NOTE: *A complete list of invited talks, approximately 90 publications, and 30 other documents may be found in the long version of this resume, which however also omits Motorola internal documents and approximately 50 internal notes from Computational Logic, Inc.*

Efficient, Verified Checking of Propositional Proofs (with Marijn Heule, Warren Hunt, Jr., and Nathan Wetzler). Accepted, ITP 2017; to appear LNCS 10499, Springer International Publishing, 2017.

Efficient Certified RAT Verification (with Luís Cruz-Filipe, Marijn Heule, Warren Hunt, and Peter Schneider-Kamp). Proceedings CADE 26 - 26th International Conference on Automated Deduction, Gothenburg, Sweden, August 6-11, 2017, Leonardo de Moura, editor, pp. 220–236. `https://doi.org/10.1007/978-3-319-63046-5_14`.

Iterated Ultrapowers for the Masses (with Ali Enayat and Zachiri McKenzie). *Archive for Mathematical Logic*, Springer. URL `http://link.springer.com/article/10.1007/`

s00153-017-0592-1 (Springer Open Access). Preliminary version: URL http://arxiv.org/abs/1702.03487.

Industrial Hardware and Software Verification with ACL2 (with Warren A. Hunt, Jr., J Strother Moore, and Anna Slobodova). To appear, *Philosophical Transactions of the Royal Society*.

Rough Diamond: An Extension of Equivalence-based Rewriting (with J Strother Moore). *Proceedings of ITP 2014, 5th Conference on Interactive Theorem Proving,* Gerwin Klein and Ruben Gamboa, editors. LNCS 8558 pp. 537-542, Springer International Publishing, 2014. DOI 10.1007/978-3-319-08970-6_35. URL http://dx.doi.org/10.1007/978-3-319-08970-6_35.

Simulation and Formal Verification of x86 Machine-Code Programs that make System Calls (with Shilpi Goel, Warren A. Hunt, Jr., and Soumava Ghosh). *Proceedings of Formal Methods in Computer-Aided Design (FMCAD'14)*, October, 2014. URL http://www.cs.utexas.edu/users/hunt/FMCAD/FMCAD14/proceedings/18_goel.pdf.

A Parallelized Theorem Prover for a Logic with Parallel Execution (with David L. Rager and Warren A. Hunt, Jr.). *Proceedings of ITP 2013, 4th Conference on Interactive Theorem Proving.* S. Blazy, C. Paulin-Mohring, and D. Pichardie (Eds.), LNCS 7998, pp. 435-450, Springer-Verlag Berlin Heidelberg 2013.

A Formal Model of a Large Memory that Supports Efficient Execution (with Warren A. Hunt, Jr.). *Proceedings of Formal Methods in Computer-Aided Design (FMCAD'12)* (G. Cabodi and S. Singh, editors). ACM Digital Library, URL http://www.cs.utexas.edu/users/hunt/FMCAD/FMCAD12/fmcad2012.pdf, pp. 60-67, 2012.

Interactive Theorem Proving: First International Conference, ITP 2010, Edinburgh, Scotland, July 2010 (co-editor with Lawrence Paulson). LNCS 6172, Springer, 2010 (eBook at URL http://dx.doi.org/10.1007/978-3-642-14052-5).

The Right Tools for the Job: Correctness of Cone of Influence Reduction Proved Using ACL2 and HOL4 (with M. Gordon and S. Ray). *Journal of Automated Reasoning*, Volume 47, Number 1, Springer, 2011, pp. 1–16, DOI 10.1007/s10817-010-9169-y.

Integrating External Deduction Tools with ACL2 (with J S. Moore, Sandip Ray, and Erik Reeber). *Journal of Applied Logic* (Special Issue: Empirically Successful Computerized Reasoning), Volume 7, Issue 1, March 2009, pp. 3–25. Also published online (DOI 10.1016/j.jal.2007.07.002). Preliminary version in: *Proceedings of the 6th International Workshop on the Implementation of Logics (IWIL 2006)* (C. Benzmller, B. Fischer, and G. Sutcliffe, editors), CEUR Workshop Proceedings Vol. 212, Phnom Penh, Cambodia, pp. 7-26, November 2006. http://ceur-ws.org/Vol-212/.

An Integration of HOL and ACL2 (with Michael J.C. Gordon, Warren A. Hunt, Jr., and James Reynolds). *Proceedings of Formal Methods in Computer-Aided Design (FMCAD'06)* (A. Gupta and P. Manolios, editors). IEEE Computer Society Press, pp. 153-160, November,

2006.

Efficient Execution in an Automated Reasoning Environment (with David A. Greve, Panagiotis Manolios, J Strother Moore, Sandip Ray, José Luis Ruiz-Reina, Rob Sumners, Daron Vroon, and Matthew Wilding). Journal of Functional Programming, Volume 18, Issue 01, January 2008, Cambridge University Press. Long version is available as Technical Report TR-06-59, Department of Computer Sciences, University of Texas at Austin, URL `http://www.cs.utexas.edu/ftp/pub/techreports/tr06-59.pdf`.

Rewriting with Equivalence Relations in ACL2 (with Bishop Brock and J Strother Moore). *Journal of Automated Reasoning* 40 (2008), pp. 293-306. Also published online (DOI `10.1007/s10817-007-9095-9`).

Meta Reasoning in ACL2 (with Warren Hunt, Robert Krug, J Moore and Eric Smith). TPHOLs 2005, ed. J. Hurd and T. F. Melham, LNCS 3603, Springer-Verlag, Berlin, 2005, pp. 163-178.

Formal Verification of Floating-Point RTL at AMD using the ACL2 Theorem Prover (David Russinoff, Matt Kaufmann, Eric Smith, Robert Sumners). 17th IMACS World Congress: Scientific Computation, Applied Mathematics and Simulation. July, 2005. Available from URL `http://www.russinoff.com/papers/paris.pdf`.

Verification of Pipeline Circuits (with David M. Russinoff). Proceedings ACL2 Workshop 2000, Oct. 2000. Available at URL `http://www.cs.utexas.edu/users/moore/acl2/workshop-2000/final/russinoff-kaufmann/paper.pdf`.

Computer-Aided Reasoning: An Approach (with P. Manolios and J Moore). Kluwer Academic Publishers, June, 2000.

Computer-Aided Reasoning: ACL2 Case Studies (editor, and contributed an article; with co-editors P. Manolios and J Moore). Kluwer Academic Publishers, June, 2000.

Structured Theory Development for a Mechanized Logic (with J Moore). *Journal of Automated Reasoning* 26, no. 2 (2001) 161-203.

Nonstandard Analysis in ACL2 (with Ruben Gamboa). *Journal of Automated Reasoning* 27(4), 323-351, 2001.

Verification of Year 2000 Conversion Rules Using the ACL2 Theorem Prover. *Software Tools for Technology Transfer* 3, no. 1 (September 2000), 13-19.

Design Constraints In Symbolic Model Checking (with Andrew Martin and Carl Pixley). In: *Computer Aided Verification: 10th International Conference* (proceedings, CAV'98 Vancouver, BC, Canada, June 28 - July 2, 1998). ed. Alan J. Hu and Moshe Y. Vardi, LNCS 1427, Springer-Verlag, 1998.

Intertwined Development and Formal Verification of a 60x Bus Model (with Carl Pixley). ICCD'97. pp. 25-30, October, 1997.

An Industrial Strength Theorem Prover for a Logic Based on Common Lisp (with J Moore). *IEEE Transactions on Software Engineering 23*, no. 4, April 1997, 203–213.

Formal Verification of FIRE: A Case Study (with Jae-Young Jang, Carl Pixley, and Shaz Qadeer). In: *Proceedings of Design Automation Conference (DAC)*, 1997.

A Mechanically Checked Proof of the AMD5$_K$86^{TM} Floating-Point Division Program (with J Moore and T. Lynch). *IEEE Trans. Computers* 47, no. 9 (1998), pp. 913–926.

Interaction with the Boyer-Moore Theorem Prover: A Tutorial Study Using the Arithmetic-Geometric Mean Theorem (with Paolo Pecchiari). *Journal of Automated Reasoning* 16, no. 1-2 (1996) 181-222.

The Boyer-Moore Theorem Prover and Its Interactive Enhancement (with Robert S. Boyer and J Strother Moore), *Computers and Mathematics with Applications,* Vol. 29, No. 2, pp. 27-62, 1995.

An Extension of the Boyer-Moore Theorem Prover to Support First-Order Quantification, *Journal of Automated Reasoning*, Vol. 9, No. 3., December 1992, pp. 355-372.

An interactive enhancement to the Boyer-Moore Theorem Prover. In: *Proc. 9th Intl. Conf. on Automated Deduction* (CADE-9, Argonne, Illinois, 23-26 May 1988), ed. E. Lusk and R. Overbeek, LNCS 310, Springer-Verlag, Berlin, 1988, pp. 735-736.

Remarks on Weak Notions of Saturation in Models of Peano Arithmetic (with J. Schmerl). *Journal of Symbolic Logic* 52 (1987), pp. 129-148.

The Quantifier "There Exist Uncountably Many" and Some of Its Relatives, in: *Model-Theoretic Logics* (J. Barwise and S. Feferman, editors), Springer-Verlag, 1985, pp. 123-176.

On Random Models of Finite Power and Monadic Logic (with S. Shelah). *Discrete Mathematics* 54 (1985), pp. 285-293.

The Strength of Nonstandard Methods in Arithmetic (with C.W. Henson and H.J. Keisler). *J. Symbolic Logic* 49 (1984), pp. 1039-1058.

Blunt and Topless End Extensions of Models of Set Theory. *J. Symbolic Logic* 48 (1983), pp. 1053-1071.

Filter logics: Filters on ω_1. *Ann. Math. Logic* 20 (1980), pp. 155-200.

Stationary Logic (with J. Barwise and M. Makkai). *Ann. Math. Logic* 13 (1978), pp. 171-224.

A Rather Classless Model. *Proceedings Amer. Math. Soc.* 62 (1977), pp. 330-333.

— — —

Last revised: October 10, 2017