

J Strother Moore

Employment

Admiral B. R. Inman Professor of Computing Theory, 1997–present

Department Chair, 2001–present

Department of Computer Sciences,
University of Texas at Austin.

Chief Scientist, 1987–1996

1987–Present: Founder and Member of Board of Directors;
Computational Logic, Inc.,
1717 West Sixth Street, Suite 290, Austin, TX.

Gottesman Family Centennial Professor, 1985–1988

Associate Professor, 1981–84;
Department of Computer Sciences,
University of Texas at Austin.

Staff Scientist, 1981

Senior Research Mathematician, 1979–81
Research Mathematician, 1976–78
Computer Science Laboratory
SRI International, Menlo Park, CA.

Research Mathematician, 1973–76

Computer Science Laboratory,
Xerox Palo Alto Research Center, Palo Alto, CA.

Research Fellow, 1973

Programmer, 1971–72
Department of Computational Logic,
University of Edinburgh, Edinburgh, Scotland.

Education

Ph.D. Computational Logic, University of Edinburgh, Edinburgh, Scotland, 1973 (Supervisor: R. M. Burstall).

Bachelor of Science, Mathematics, Massachusetts Institute of Technology, Cambridge, Massachusetts, 1970.

Honors

- National Academy of Engineering, 2007
- ACM Fellow, 2006
- 2005 ACM Software System Award (with R. S. Boyer and M. Kaufmann for the Boyer-Moore theorem prover)
- Lecturer, Marktoberdorf International Summer School, 2004
- Lecturer, Marktoberdorf International Summer School, 2002
- 1999 Herbrand Award, Conference on Automated Deduction (with R. S. Boyer)
- 1991 elected Fellow of the American Association for Artificial Intelligence
- 1991 Current Prize in Automatic Theorem Proving by the American Mathematical Society (with R. S. Boyer)
- Lecturer, Marktoberdorf International Summer School, 1988
- John McCarthy Prize for Program Verification (with R. S. Boyer), 1983.
- Member of the Editorial Board of the *Journal of Automated Reasoning and Formal Methods in System Design*
- IBM Chaire Internationale d'Informatique, Universite de Liege, Belgium, 1980.

Books

- A8.** *Computer-Aided Reasoning: An Approach*, with M. Kaufmann and P. Manolios, Kluwer Academic Publishers, Boston, 2000.
- A7.** *Computer-Aided Reasoning: ACL2 Case Studies*, with M. Kaufmann and P. Manolios (Eds.), Kluwer Academic Publishers, Boston, 2000.
- A6.** *A Computational Logic Handbook*, with R. S. Boyer, Academic Press, London, 1997. Second Edition.

- A5. *Piton: A Mechanically Verified Assembly Level Language*, Kluwer Academic Publishers, Dordrecht, The Netherlands 1996.
- A4. *Special Issue on System Verification, Journal of Automated Reasoning*, (Ed.), **5**, 4, 1989.
- A3. *A Computational Logic Handbook*, with R. S. Boyer, Academic Press, New York, 1988.
- A2. *The Correctness Problem in Computer Science*, with R. S. Boyer (Eds.), Academic Press, London, 1981.
- A1. *A Computational Logic*, with R. S. Boyer, Academic Press, New York, 1979.

Reviewed Articles

- B59. “Rewriting with Equivalence Relations in ACL2,” with B. Brock and M. Kaufmann, *Journal of Automated Reasoning*, **40**(4), pp. 293–306, May, 2008.
- B58. “Efficient Execution in an Automated Reasoning Environment,” with D. Greve, M. Kaufmann, P. Manolios, S. Ray, J. L. Ruiz-Reina, R. Sumners, D. Vroon, and M. Wilding, *Journal of Functional Programming*, **17**(01), pp. 15–46, January, 2008.
- B57. “Integrating CCG analysis into ACL2,” with M. Kaufmann, P. Manolios, J S. Moore, and D. Vroon, *Proceedings of The Eighth International Workshop on Termination (part of FLoC 2006)*, pp. 64–68, 2006.
- B56. “Integrating External Deduction Tools with ACL2.” with M. Kaufmann, S. Ray, and E. Reeber, Proceedings of the 6th International Workshop on the Implementation of Logics (IWIL 2006) (C. Benzmueller, 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/>. Expanded version to appear in the *Journal of Applied Logic*.
- B55. “A Mechanical Analysis of Program Verification Strategies,” with S. Ray, W. A. Hunt, J. Matthews, *Journal of Automated Reasoning*, 2007 (to appear).
- B54. “Verification Condition Generation via Theorem Proving,” with J. Matthews, S. Ray, and D. Vroon, *Proceedings of the 13th International Conference on Logic for Programming (LPAR 2006)*, M. Hermann and A. Voronkov (Eds.), Springer-Verlag, November, 2006.
- B53. “Double Rewriting for Equivalential Reasoning in ACL2,” with M. Kaufmann, *Proceedings of the ACL2 Workshop 2006* P. Manolios and M. Wilding (Eds.), ACM Digital Library, August, 2006.

- B52.** “Proof Pearl: Dijkstra’s Shortest Path Algorithm Verified with ACL2,” with Q. Zhang, *TPHOLS 2005*, J. Hurd and T. Melham (Eds.), Springer Lecture Notes in Computer Science, **3603**, pp. 373–384, 2005.
- B51.** “Meta Reasoning in ACL2,” with W. A. Hunt, M. Kaufmann, R. B. Krug, E. W. Smith, *TPHOLS 2005*, J. Hurd and T. Melham (Eds.), Springer Lecture Notes in Computer Science, **3603**, pp. 163–178, 2005.
- B50.** “Java Program Verification via a JVM Deep Embedding in ACL2,” with H. Liu, *TPHOLS 2004*, K. Slind, A. Bunker, and G. Gopalakrishnan (Eds.), Springer Lecture Notes in Computer Science, **3223**, pp. 184–200, 2004.
- B49.** “Some Key Research Problems in Automated Theorem Proving for Hardware and Software Verification,” with M. Kaufmann, *Spanish Royal Academy of Science (RACSAM)*, **98**(1), pp. 181–196, 2004.
- B48.** “Proof Styles in Operational Semantics,” with S. Ray, *Formal Methods in Computer-Aided Design (FMCAD 2004)*, A. J. Hu and A. K. Martin (Eds.), Springer Lecture Notes in Computer Science, **3312**, pp. 67–81, 2004.
- B47.** “Inductive Assertions and Operational Semantics,” *CHARME 2003*, D. Geist (Ed.), Springer Verlag LNCS 2860, pp. 289–303, 2003.
- B46.** “Linear and Non-Linear Arithmetic in ACL2,” with R. Krug and W. A. Hunt, *CHARME 2003*, D. Geist (Ed.), Springer Verlag LNCS 2860, pp. 319–333, 2003.
- B45.** “Memory Taggings and Dynamic Data Structures,” *ACL2 Workshop 2003*, M. Kaufmann, W. A. Hunt, Jr., and J. S. Moore (Eds.), Boulder, Co., July, 2003.
- B44.** “Executable JVM Model for Analytical Reasoning: A Study,” with H. Liu, *ACM SIGPLAN 2003 Workshop on Interpreters, Virtual Machines and Emulators*, San Diego, CA, June 12, 2003.
- B43.** “Proving Theorems about Java and the JVM with ACL2,” in *Models, Algebras and Logic of Engineering Software*, M. Broy and M. Pizka (Eds.), IOS Press, Amsterdam, pp. 227–290, 2003.
- B42.** “The Apprentice Challenge,” with G. Porter, *ACM TOPLAS*, **24**(3), pp. 1–24, May, 2002.
- B41.** “A Computational Logic for Applicative Common LISP,” with M. Kaufmann, *A Companion to Philosophical Logic*, D. Jacquette (Ed.), Blackwell Publishing, Oxford, pp. 724–741, 2002.

- B40.** “A Grand Challenge Proposal for Formal Methods: A Verified Stack,” *Formal Methods at the Crossroads: from Panacea to Foundational Support, 10th Anniversary Colloquium of UNU/IIST, the International Institute for Software Technology of The United Nations University*, B. K. Aichernig and T. Maibaum (Eds.), Springer-Verlag LNCS 2757, pp. 161–172, 2003.
- B39.** “On the Desirability of Mechanizing Computational Proofs,” with P. Manolios, *Information Processing Letters*, **77**(2-4), February, 2001, pp. 173–179.
- B38.** “Finite Set Theory in ACL2,” in *Proceedings of TPHOLs 2001*, R. J. Boulton and P. B. Jackson (Eds.), Springer-Verlag LNCS 2152, pp. 313–328, 2001.
- B37.** “Partial Functions in ACL2,” with P. Manolios, *Journal of Automated Reasoning*, Kluwer, 31(2), pp. 107-127, 2003.
- B36.** “An Executable Formal Java Virtual Machine Thread Model,” with G. Porter, *Proceedings of Java Virtual Machine Research and Technology Symposium*, USENIX, April, 2001.
- B35.** “Rewriting for Symbolic Execution of State Machine Models,” in *Proceedings of CAV 01*, G. Berry, H. Comon, and A. Finkel (Eds.), Springer-Verlag LNCS 2102, pp. 411-422, 2001.
- B34.** “Towards a Mechanically Checked Theory of Computation: The ACL2 Project,” in J. Minker, ed., *Logic and Artificial Intelligence*, pp. 545–575, Kluwer, 2000.
- B33.** “Single-Threaded Objects in ACL2,” with R. S. Boyer, S. Krishnamurthi, C. R. Ramakrishnan (Eds.) *PADL 2002*, LNCS 2257, pp. 9–27, 2002.
- B32.** “Proving Theorems about Java-like Byte Code,” in E.-R. Olderog and B. Steffen (Eds.) *Correct System Design – Recent Insights and Advances*, LNCS 1710, pp. 139–162, 1999.
- B31.** “Structured Theory Development for a Mechanized Logic,” with M. Kaufmann, *Journal of Automated Reasoning*, **26**(2), pp. 161–203, 2001.
- B30.** “A Mechanically Checked Proof of a Comparator Sort Algorithm,” with B. Brock, in C. A. R. Hoare, D. Harel, and M. Broy (Eds.) *Engineering Theories of Software Intensive Systems*, Springer NATO Science Series, **195**, pp. 141–175, 2005.
- B29.** “A Mechanically Checked Proof of a Multiprocessor Result via a Uniprocessor View,” *Formal Methods in System Design*, **14**(2), March, 1999, pp. 213–228.
- B28.** “Symbolic Simulation: An ACL2 Approach,” in G. Gopalakrishnan and P. Windley (Eds.) *Proceedings of the Second International Conference on Formal Methods in Computer-Aided Design (FMCAD’98)*, Springer-Verlag LNCS 1522, pp. 334–350, November, 1998.

- B27.** “An ACL2 Proof of Write Invalidate Cache Coherence,” in A. J. Hu and M. Y. Vardi (Eds.) *Computed Aided Verification: 10th International Conference, CAV ’98*, Springer-Verlag LNCS 1427, pp. 29–38, 1998.
- B26.** “Mechanized Formal Reasoning about Programs and Computing Machines,” with R. S. Boyer, in R. Veroff (Ed.) *Automated Reasoning and Its Applications: Essays in Honor of Larry Wos*, MIT Press, 1996.
- B25.** “ACL2 Theorems about Commercial Microprocessors,” with B. Brock and M. Kaufmann. In M. Srivas and A. Camilleri (Eds.) *Proceedings of Formal Methods in Computer-Aided Design (FMCAD’96)*, Springer-Verlag, pp. 275–293, 1996.
- B24.** “A Mechanically Checked Proof of the Correctness of the Kernel of the AMD5_K86 Floating-Point Division Algorithm,” with T. Lynch and M. Kaufmann, *IEEE Trans. Comp.*, **47**(9), pp. 913–926, Sep. 1998.
- B23.** “An Industrial Strength Theorem Prover for a Logic Based on Common Lisp,” with M. Kaufmann, *IEEE Transactions on Software Engineering*, **23**(4), April, 1997, pp. 203–213.
- B22.** “The Boyer-Moore Theorem Prover and Its Interactive Enhancement,” with R. S. Boyer and M. Kaufmann. In *Computers and Mathematics with Applications*, **5**(2) (1995) 27–62.
- B21.** “A Formal Model of Asynchronous Communication and Its Use in Mechanically Verifying a Biphase Mark Protocol.” In *Formal Aspects of Computing*, **6**(1) (1994) 60–91.
- B20.** “Introduction to the OBDD Algorithm for the ATP Community.” In *Journal of Automated Reasoning*, **6**(1) (1994) 33–45.
- B19.** “Functional Instantiation in First Order Logic,” with R. S. Boyer, D. M. Goldschlag, and M. Kaufmann. In V. Lifschitz, (Ed.), *Artificial Intelligence and Mathematical Theory of Computation: Papers in Honor of John McCarthy*, Academic Press, 1991, pp. 7–26.
- B18.** “MJRTY – A Fast Majority Vote Algorithm,” with R. S. Boyer. In R. S. Boyer (Ed.), *Automated Reasoning: Essays in Honor of Woody Bledsoe, Automated Reasoning Series*, Kluwer Academic Publishers, Dordrecht, The Netherlands, 1991, pp. 105–117.
- B17.** “The Use of a Formal Simulator to Verify a Simple Real Time Control Program,” with R. S. Boyer and M. W. Green, in W. H. J. Feijen, A. J. M. van Gasteren, D. Gries, and J. Misra” (Eds.), *Beauty is Our Business: A Birthday Salute to Edsger W. Dijkstra*, Springer-Verlag Texts and Monographs in Computer Science, 1990, pp. 54–66.
- B16.** “Special Issue on System Verification,” with W. R. Bevier, W. A. Hunt, and W. D. Young. *Journal of Automated Reasoning*, **5**(4) (1989) 461–492.

- B15.** “A Mechanically Verified Language Implementation.” In *Journal of Automated Reasoning*, **5**(4) (1989) 461–492.
- B14.** “The Addition of Bounded Quantification and Partial Functions to A Computational Logic and Its Theorem Prover,” with R. S. Boyer. In *Journal of Automated Reasoning*, **4**(2) (1988) 117–172.
- B13.** “Integrating Decision Procedures into Heuristic Theorem Provers: A Case Study of Linear Arithmetic”, with R. S. Boyer. In *Machine Intelligence*, **11**, Oxford University Press, 1988.
- B12.** “Program Verification,” with R. S. Boyer. *Journal of Automated Reasoning*, **1**(1) (1985) 17–23.
- B11.** “A Mechanical Proof of the Turing Completeness of PURE LISP,” with R. S. Boyer. In W. W. Bledsoe and D. W. Loveland, (Eds.), *Contemporary Mathematics*, **29**, *Automated Theorem Proving: After 25 Years*, American Mathematical Society, Providence, Rhode Island, 1984, pp. 133–168.
- B10.** “Proof-Checking, Theorem-Proving, and Program Verification,” with R. S. Boyer. In W. W. Bledsoe and D. W. Loveland, (Eds.), *Contemporary Mathematics*, **29**, *Automated Theorem Proving: After 25 Years*, American Mathematical Society, Providence, Rhode Island, 1984, pp. 119–132.
- B9.** “A Mechanical Proof of the Unsolvability of the Halting Problem,” with R. S. Boyer. *Journal of the Association for Computing Machinery*, **31**(3) (1984) 441–458.
- B8.** “Proof Checking the RSA Public Key Encryption Algorithm,” with R. S. Boyer. *American Mathematical Monthly*, **91**(3) (1984) 181–189.
- B7.** “A Verification Condition Generator for FORTRAN,” with R. S. Boyer. In R. S. Boyer and J S. Moore, (Eds.), *The Correctness Problem in Computer Science*, Academic Press, London, 1981.
- B6.** “Metafunctions: Proving Them Correct and Using Them Efficiently as New Proof Procedures,” with R. S. Boyer. In R. S. Boyer and J S. Moore, (Eds.), *The Correctness Problem in Computer Science*, Academic Press, London, 1981.
- B5.** “A Mechanical Proof of the Termination of Takeuchi’s Function,” *Information Processing Letters*, **9**(4) (1979) 176–181.
- B4.** “A Fast String Searching Algorithm,” with R. S. Boyer. *Communications of the Association for Computing Machinery*, **20**(10) (1977) 762–772.
- B3.** “Introducing Iteration into the Pure LISP Theorem-Prover.” *IEEE Transactions on Software Engineering*, **SE-1**(3) (1975) 328–338.

- B2.** “Proving Theorems about LISP Functions,” with R. S. Boyer. *Journal of the Association for Computing Machinery*, **22**(1) (1975) 129–144.
- B1.** “The Sharing of Structure in Theorem-proving Programs,” with R. S. Boyer. In B. Meltzer and D. Michie, (Eds.), *Machine Intelligence*, **7**, Edinburgh University Press, 1972, pp. 101–116.

Other Publications

- C23** “String Searching over Small Alphabets,” with M. Sustik, TR-07-62, Department of Computer Sciences, University of Texas at Austin, December, 2007.
- C22** “Maintaining the ACL2 Theorem Proving System,” with M. Kaufmann. Invited talk. *Proceedings of the FLoC’06 Workshop on Empirically Successful Computerized Reasoning, 3rd International Joint Conference on Automated Reasoning*, (G. Sutcliffe, R. Schmidt, and S. Schulz, eds.), CEUR Workshop Proceedings, **192**, Seattle, August, 2006.
- C21.** “Interactive Symbolic Visualization of Semi-automatic Theorem Proving,” with C. Bajaj, S. Khandelwal, V. Siddavanahalli, Technical Report TR-03-37, Department of Computer Sciences, University of Texas at Austin, August 2003.
- C20.** “University-Industry Sponsored Research Agreements,” with L. Snyder and P. A. Bernstein, CRA Best Practices Memo, July, 2003.
- C19.** “Model Language for Patent and Licensing Agreements for Industrially Sponsored University Research in Information Technology,” CRA Best Practices Memo (supporting material), June, 2003.
- C18.** “Design Goals of ACL2,” with M. Kaufmann. CLI Technical Report 101, Computational Logic, Inc., 1717 West Sixth Street, Suite 290, Austin, TX 78703, 1994.
- C17.** “Should We Begin a Standardization Process for Interface Logics?,” with M. Kaufmann. CLI Technical Report 72, Computational Logic, Inc., 1717 West Sixth Street, Suite 290, Austin, TX 78703, 1992.
- C16.** “Mechanically Verified Hardware Implementing an 8-Bit Parallel IO Byzantine Agreement Processor.” NASA CR-189588, 1992.
- C15.** “The Mechanical Verification of a FORTRAN Square Root Program,” with R. S. Boyer. CSL Report, SRI International, 1981.
- C14.** “Text Editing Primitives – The TXDT Package.” Technical Report CSL-81-2, Xerox Palo Alto Research Center, 1981.

- C13.** “Program Verification: An Approach to Reliable Hardware and Software,” with L. Lamport. *Transactions of the American Nuclear Society, American Nuclear Society*, **35** (1980) 252–253.
- C12.** “A Theorem-Prover for Recursive Functions,” with R. S. Boyer. *Software Engineering Notes*, Association for Computing Machinery, **5**(3) (1980) 26–27.
- C11.** “The FORTRAN Verification System,” with R. S. Boyer. *Software Engineering Notes*, Association for Computing Machinery, **5**(3) (1980) 16–17.
- C10.** “A Statement of Position.” *Software Engineering Notes*, Association for Computing Machinery, **5**(3) (1980) 23–24.
- C9.** “A Theorem-Prover for Recursive Functions: A User’s Manual,” with R. S. Boyer. Technical Report CSL-91, Computer Science Laboratory, SRI International, 1979.
- C8.** “A Guided Tour Through a Working Theorem Prover.” *Proceedings of the Fourth Work shop on Artificial Intelligence*, Institut fur Informatik, Universitat Bonn, 1979, pp. 89–97.
- C7.** “A Lemma Driven Automatic Theorem Prover for Recursive Function Theory,” with R. S. Boyer. *Proceedings of the 5th International Joint Conference on Artificial Intelligence*, 1977, pp. 511–519.
- C6.** “The INTERLISP Virtual Machine Specification.” Technical Report CSL-76-5, Xerox Palo Alto Research Center, 1976.
- C5.** “Primitive Recursive Program Transformation,” with R. S. Boyer and R. E. Shostak. *Proceedings of the Third ACM Symposium on Principles of Programming Languages*, Association for Computing Machinery, Atlanta, 1976.
- C4.** “Automatic Proof of the Correctness of a Binary Addition Algorithm.” *SIGART Newsletter*, Association for Computing Machinery, **52** (1975) 13–14.
- C3.** “Computational Logic: Structure Sharing and Proof of Program Properties.” Ph.D. Thesis, Department of Computational Logic, University of Edinburgh, 1973.
- C2.** “The 77-Editor,” with R. S. Boyer and D. J. M. Davies. Technical Report 62, Department of Computational Logic, University of Edinburgh, 1973.
- C1.** “The GSS Package.” Technical Report 51, Department of Computational Logic, University of Edinburgh, 1972.