

# Bibtex Entries for the ACL2 Workshops

Jared Davis

February 24, 2005

This file provides a list of bibtex entries which can be used to cite papers from the ACL2 workshops from within  $\LaTeX$ . If you see any errors in these entries please email me at [jared@cs.utexas.edu](mailto:jared@cs.utexas.edu).

## 1 ACL2 Workshop 2000

00-lusk-parallel[11]

ACL2 for Parallel Systems Software: A Progress Report

00-wilding-stobj[42]

Using a Single-Threaded Object to Speed a Verified Graph Pathfinder

00-sumners-bdds[54]

Correcness Proof of a BDD Manager in the Context of Satisfiability Checking

00-shumsky-sdl[44]

Developing a Framework for Simulation, Verification and Testing of SDL Specifications

00-manolios-pipeline[46]

Verification of Pipelined Machines in ACL2

00-sumners-stuttering[53]

An Incremental Stuttering Refinement Proof of a Concurrent Program in ACL2

00-reina-multiset[18]

Multiset Relations: A Tool for Proving Termination

00-goerigk[74]

Proving Preservation of Partial Correctness with ACL2: A Mechanical Compiler Source Level Correctness Proof

00-sawada-computed[34]

ACL2 Computed Hints: Extension and Practice

00-bulo-polynomial[17]  
Automatic Verification of Polynomial Rings: Fundamental Properties in ACL2

00-russinoff-chinese[7]  
A Mechanical Proof of the Chinese Remainder Theorem

00-manolios-partial[48]  
Partial Functions in ACL2

00-bailey-tarai[69]  
Knuth's Generalization of Takeuchi's Tarai Function: Preliminary Report

00-kaufmann-pipeline[40]  
Verification of Pipeline Circuits

## 2 ACL2 Workshop 2002

02-barrione-vhdl[51]  
A Framework for VHDL Combining Theorem Proving and Symbolic Simulation

02-caldwell-nuprl[24]  
Representing Nuprl Proof Objects in ACL2: toward a proof checker for Nuprl

02-sawada-sqrt[35]  
Formal Verification of Divide and Square Root Algorithms Using Series Calculation

02-gamboa-taylor[58]  
Taylor's Formula with Remainder

02-bulo-polynomial[16]  
Implementation in ACL2 of Well-Founded Polynomial Orderings

02-reina-terms[19]  
A Theory About First-Order Terms in ACL2

02-reina-dags[20]  
Progress Report: Term Dags Using Stobj

02-manolios-adding[49]  
Adding a Total Order to ACL2

02-sumners-sat[55]  
Checking ACL2 Theorems via SAT Checking

02-kaufmann-rewriting[41]  
Efficient Rewriting of Operations on Finite Structures in ACL2

02-cowles-primitive[28]  
Consistently Adding Primitive Recursive Definitions in ACL2

02-cowles-flat[29]  
Flat Domains and Recursive Equations in ACL2

02-martin-molecular[13]  
Molecular Computation Models in ACL2: a Simulation of Lipton's Experiment Solving SAT

02-martin-instantiation[12]  
A Generic Instantiation Tool and a Case Study: A Generic Multiset Theory.

02-ray-quicksort[66]  
Verification of an In-place Quicksort in ACL2

### **3 ACL2 Workshop 2003**

03-kaufmann-simplifying[39]  
A Tool for Simplifying Files of ACL2 Definitions

03-hendrix-matrices[27]  
Matrices in ACL2

03-manolios-ordinal[47]  
Ordinal Arithmetic in ACL2

03-sustik-dickson[43]  
Proof of Dickson's Lemma Using the ACL2 Theorem Prover via an Explicit Ordinal Mapping

03-gamboa-arrays[61]  
Using ACL2 Arrays to Formalize Matrix Algebra

03-gamboa-kalman[60]  
On the Verification of Synthesized Kalman Filters

03-matlin-encapsulation[45]  
Encapsulation for Practical Simplification Procedures

03-sumners-fairness[56]  
Fair Environment Assumptions in ACL2

03-toma-sha[8]  
SHA Formalization

03-greve-separation[5]  
A Separation Kernel Formal Security Policy

03-moore-tagging[23]  
Memory Taggings and Dynamic Data Structures

03-moore-assertions[22]  
Inductive Assertions and Operational Semantics

03-greve-typed[3]  
Typed ACL2 Records

03-greve-mbe[4]  
Using MBE to Speed a Verified Graph Pathfinder

03-liu-rockwell[15]  
A Solution to the Rockwell Challenge

03-song-security[68]  
Using ACL2 to Verify Security Properties of Specification-based Intrusion Detection Systems

03-al-sammamne-mathematica[14]  
Combining ACL2 and Mathematica for the Symbolic Simulation of Digital Systems

03-schmaltz-bus[32]  
Validation of a Parameterized Bus Architecture Model

03-gamboa-polymorphism[63]  
Polymorphism in ACL2

03-gamboa-literate[59]  
Writing Literate Proofs with XML Tools

03-ray-modelchecking[65]  
Certifying Compositional Model Checking Algorithms in ACL2

03-austel-types[70]  
Implementing Abstract Types in ACL2

## 4 ACL2 Workshop 2004

04-summers-invariant[57]  
Reducing Invariant Proofs to Finite Search via Rewriting

04-ray-partial[64]  
Attaching Efficient Executability to Partial Functions in ACL2

04-matthews-clock[31]  
Partial Clock Functions in ACL2

04-gameiro-interval[38]  
Formally Verifying an Algorithm Based on Interval Arithmetic for Checking Transversality

04-manolios-hard[50]  
A Suite of Hard ACL2 Theorems Arising in Refinement-Based Processor Verification

04-davis-sets[25]  
Finite Set Theory based on Fully Ordered Lists

04-roach-hats[67]  
Verifying Transformation Rules of the HATS High-Assurance Transformation System: An Approach

04-fisler-features[37]  
A Case Study in using ACL2 for Feature-Oriented Verification

04-sawada-vhdl[36]  
ACL2VHDL Translator: A Simple Approach to Fill the Semantic Gap

04-austel-typing[71]  
Adding a typing mechanism to ACL2

04-reina-unification[21]  
A Formally Verified Quadratic Unification Algorithm

04-legato-preconditions[73]  
Generic Theories as Proof Strategies: A Case Study for Weakest Precondition

Style Proofs

04-hunt-nonlinear[72]

Integrating Nonlinear Arithmetic into ACL2

04-greve-partitioning[6]

A Summary of Intrinsic Partitioning Verification

04-greve-enumeration[2]

Address Enumeration and Reasoning Over Linear Address Spaces

04-smith-bags[10]

An ACL2 Library for Bags (Multisets)

04-richards-common[52]

The Common Criteria, Formal Methods and ACL2

04-young-abstract[1]

Reverse Abstraction in ACL2

04-foss-gwv[26]

An Analysis of the GWV Security Policy

04-schmaltz-network[33]

A Functional Specification and Validation Model for Networks on Chip in the ACL2 Logic

04-toma-sha[9]

Verification of a Cryptographic Circuit: SHA-1 using ACL2

04-gamboa-axiomatic[62]

Axiomatic Events in ACL2(r): A Story of defun, defun-std, and encapsulate

04-cowles-tail[30]

Contributions to the Theory of Tail Recursive Functions

## References

- [1] Bill Young. Reverse Abstraction in ACL2. In *Fifth International Workshop on the ACL2 Theorem Prover and its Applications (ACL2-2004)*, November 2004.

- [2] David Greve. Address Enumeration and Reasoning Over Linear Address Spaces. In *Fifth International Workshop on the ACL2 Theorem Prover and its Applications (ACL2-2004)*, November 2004.
- [3] David Greve and Matthew Wilding. Typed ACL2 Records. In *Fourth International Workshop on the ACL2 Theorem Prover and Its Applications (ACL2-2003)*, July 2003.
- [4] David Greve and Matthew Wilding. Using MBE to Speed a Verified Graph Pathfinder. In *Fourth International Workshop on the ACL2 Theorem Prover and Its Applications (ACL2-2003)*, July 2003.
- [5] David Greve, Matthew Wilding, and W. Mark Vanfleet. A Separation Kernel Formal Security Policy. In *Fourth International Workshop on the ACL2 Theorem Prover and Its Applications (ACL2-2003)*, July 2003.
- [6] David Greve, Raymond Richards, and Matthew Wilding. A Summary of Intrinsic Partitioning Verification. In *Fifth International Workshop on the ACL2 Theorem Prover and its Applications (ACL2-2004)*, November 2004.
- [7] David M. Russinoff. A Mechanical Proof of the Chinese Remainder Theorem. Technical Report TR-00-29, The University of Texas at Austin, Department of Computer Sciences, November 2000. ACL2 Workshop 2000 Proceedings, Part A.
- [8] Diana Toma and Dominique Borrione. SHA Formalization. In *Fourth International Workshop on the ACL2 Theorem Prover and Its Applications (ACL2-2003)*, July 2003.
- [9] Diana Toma and Dominique Borrione. Verification of a Cryptographic Circuit: SHA-1 using ACL2. In *Fifth International Workshop on the ACL2 Theorem Prover and its Applications (ACL2-2004)*, November 2004.
- [10] Eric Smith, Serita Nelesen, David Greve, Matthew Wilding, and Raymond Richards. An ACL2 Library for Bags (Multisets). In *Fifth International Workshop on the ACL2 Theorem Prover and its Applications (ACL2-2004)*, November 2004.
- [11] Ewing Lusk and William McCune. ACL2 for Parallel Systems Software: A Progress Report. Technical Report TR-00-29, The University of Texas at Austin, Department of Computer Sciences, November 2000. ACL2 Workshop 2000 Proceedings, Part A.
- [12] F.J. Martín-Mateos, J.A. Alonso, M.J. Hidalgo, and J.L. Ruiz-Reina. A Generic Instantiation Tool and a Case Study: A Generic Multiset Theory. In *Third International Workshop on the ACL2 Theorem Prover and its Applications (ACL2-2002)*, April 2002.

- [13] F.J. Martín-Mateos, J.A. Alonso, M.J. Pérez-Jiménez, and F. Sancho-Caparrini. Molecular Computation Models in ACL2: a Simulation of Lipton's Experiment Solving SAT. In *Third International Workshop on the ACL2 Theorem Prover and its Applications (ACL2-2002)*, April 2002.
- [14] Ghiath Al Sammane, Dominique Borrione, Pierre Ostier, Julien Schmaltz, and Diana Toma. Combining ACL2 and Mathematica for the Symbolic Simulation of Digital Systems. In *Fourth International Workshop on the ACL2 Theorem Prover and Its Applications (ACL2-2003)*, July 2003.
- [15] Hanbing Liu. A Solution to the Rockwell Challenge. In *Fourth International Workshop on the ACL2 Theorem Prover and Its Applications (ACL2-2003)*, July 2003.
- [16] I. Medina-Bulo, F. Palomo-Lozano, and J. A. Alonso-Jiménez. Implementation in ACL2 of Well-Founded Polynomial Orderings. In *Third International Workshop on the ACL2 Theorem Prover and its Applications (ACL2-2002)*, April 2002.
- [17] I. Medina-Bulo, J.A. Alonso-Jiménez, and F. Palomo-Lozano. Automatic Verification of Polynomial Rings: Fundamental Properties in ACL2. Technical Report TR-00-29, The University of Texas at Austin, Department of Computer Sciences, November 2000. ACL2 Workshop 2000 Proceedings, Part A.
- [18] J.-L. Ruiz-Reina, J.-A. Alonso, M.-J. Hidalgo, and F.-J. Martín. Multiset Relations: A Tool for Proving Termination. Technical Report TR-00-29, The University of Texas at Austin, Department of Computer Sciences, November 2000. ACL2 Workshop 2000 Proceedings, Part A.
- [19] J.-L. Ruiz-Reina, J.-A. Alonso, M.-J. Hidalgo, and F.-J. Martín-Mateos. A Theory About First-Order Terms in ACL2. In *Third International Workshop on the ACL2 Theorem Prover and its Applications (ACL2-2002)*, April 2002.
- [20] J.-L. Ruiz-Reina, J.-A. Alonso, M.-J. Hidalgo, and F.-J. Martín-Mateos. Progress Report: Term Dags Using Stobjs. In *Third International Workshop on the ACL2 Theorem Prover and its Applications (ACL2-2002)*, April 2002.
- [21] J.-L. Ruiz Reina, J.-A. Alonso, M.-J. Hidalgo, and F.-J. Martín-Mateos. A Formally Verified Quadratic Unification Algorithm. In *Fifth International Workshop on the ACL2 Theorem Prover and its Applications (ACL2-2004)*, November 2004.
- [22] J Strother Moore. Inductive Assertions and Operational Semantics. In *Fourth International Workshop on the ACL2 Theorem Prover and Its Applications (ACL2-2003)*, July 2003.

- [23] J Strother Moore. Memory Taggings and Dynamic Data Structures. In *Fourth International Workshop on the ACL2 Theorem Prover and Its Applications (ACL2-2003)*, July 2003.
- [24] James L. Caldwell and John Cowles. Representing Nuprl Proof Objects in ACL2: toward a proof checker for Nuprl. In *Third International Workshop on the ACL2 Theorem Prover and its Applications (ACL2-2002)*, April 2002.
- [25] Jared Davis. Finite Set Theory based on Fully Ordered Lists. In *Fifth International Workshop on the ACL2 Theorem Prover and Its Applications (ACL2-2004)*, November 2004.
- [26] Jim Alves-Foss and Carol Taylor. An Analysis of the GWV Security Policy. In *Fifth International Workshop on the ACL2 Theorem Prover and its Applications (ACL2-2004)*, November 2004.
- [27] Joe Hendrix. Matricies in ACL2. In *Fourth International Workshop on the ACL2 Theorem Prover and Its Applications (ACL2-2003)*, July 2003.
- [28] John Cowles. Consistently Adding Primitive Recursive Definitions in ACL2. In *Third International Workshop on the ACL2 Theorem Prover and its Applications (ACL2-2002)*, April 2002.
- [29] John Cowles. Flat Domains and Recursive Equations in ACL2. In *Third International Workshop on the ACL2 Theorem Prover and its Applications (ACL2-2002)*, April 2002.
- [30] John Cowles and Ruben Gamboa. Contributions to the Theory of Tail Recursive Functions. In *Fifth International Workshop on the ACL2 Theorem Prover and its Applications (ACL2-2004)*, November 2004.
- [31] John Matthews and Daron Vroon. Partial Clock Functions in ACL2. In *Fifth International Workshop on the ACL2 Theorem Prover and Its Applications (ACL2-2004)*, November 2004.
- [32] Julien Schmaltz and Dominique Borrione. Validation of a Parameterized Bus Architecture Model. In *Fourth International Workshop on the ACL2 Theorem Prover and Its Applications (ACL2-2003)*, July 2003.
- [33] Julien Schmaltz and Dominique Borrione. A Functional Specification and Validation Model for Networks on Chip in the ACL2 Logic. In *Fifth International Workshop on the ACL2 Theorem Prover and its Applications (ACL2-2004)*, November 2004.
- [34] Jun Sawada. ACL2 Computed Hints: Extension and Practice. Technical Report TR-00-29, The University of Texas at Austin, Department of Computer Sciences, November 2000. ACL2 Workshop 2000 Proceedings, Part A.

- [35] Jun Sawada. Formal Verification of Divide and Square Root Algorithms Using Series Calculation. In *Third International Workshop on the ACL2 Theorem Prover and its Applications (ACL2-2002)*, April 2002.
- [36] Jun Sawada. ACL2VHDL Translator: A Simple Approach to Fill the Semantic Gap. In *Fifth International Workshop on the ACL2 Theorem Prover and Its Applications (ACL2-2004)*, November 2004.
- [37] Kathi Fisler and Brian Roberts. A Case Study in using ACL2 for Feature-Oriented Verification. In *Fifth International Workshop on the ACL2 Theorem Prover and Its Applications (ACL2-2004)*, November 2004.
- [38] Marcio Gameiro and Panagiotis Manolios. Formally Verifying an Algorithm Based on Interval Arithmetic for Checking Transversality. In *Fifth International Workshop on the ACL2 Theorem Prover and Its Applications (ACL2-2004)*, November 2004.
- [39] Matt Kaufmann. A Tool for Simplifying Files of ACL2 Definitions. In *Fourth International Workshop on the ACL2 Theorem Prover and Its Applications (ACL2-2003)*, July 2003.
- [40] Matt Kaufmann and David M. Russinoff. Verification of Pipeline Circuits. Technical Report TR-00-29, The University of Texas at Austin, Department of Computer Sciences, November 2000. ACL2 Workshop 2000 Proceedings, Part A.
- [41] Matt Kaufmann and Rob Summers. Efficient Rewriting of Operations on Finite Structures in ACL2. In *Third International Workshop on the ACL2 Theorem Prover and its Applications (ACL2-2002)*, April 2002.
- [42] Matthew Wilding. Using a Single-Threaded Object to Speed a Verified Graph Pathfinder. Technical Report TR-00-29, The University of Texas at Austin, Department of Computer Sciences, November 2000. ACL2 Workshop 2000 Proceedings, Part A.
- [43] Matyas Sustik. Proof of Dickson's Lemma Using the ACL2 Theorem Prover via an Explicit Ordinal Mapping. In *Fourth International Workshop on the ACL2 Theorem Prover and Its Applications (ACL2-2003)*, July 2003.
- [44] Olga Shumsky and Lawrence J. Henschen. Developing a Framework for Simulation, Verification and Testing of SDL Specifications. Technical Report TR-00-29, The University of Texas at Austin, Department of Computer Sciences, November 2000. ACL2 Workshop 2000 Proceedings, Part A.
- [45] Olga Shumsky Matlin and William McCune. Encapsulation for Practical Simplification Procedures. In *Fourth International Workshop on the ACL2 Theorem Prover and Its Applications (ACL2-2003)*, July 2003.

- [46] Panagiotis Manolios. Verification of Pipelined Machines in ACL2. Technical Report TR-00-29, The University of Texas at Austin, Department of Computer Sciences, November 2000. ACL2 Workshop 2000 Proceedings, Part A.
- [47] Panagiotis Manolios and Daron Vroon. Ordinal Arithmetic in ACL2. In *Fourth International Workshop on the ACL2 Theorem Prover and Its Applications (ACL2-2003)*, July 2003.
- [48] Panagiotis Manolios and J Strother Moore. Partial Functions in ACL2. Technical Report TR-00-29, The University of Texas at Austin, Department of Computer Sciences, November 2000. ACL2 Workshop 2000 Proceedings, Part A.
- [49] Panagiotis Manolios and Matt Kaufmann. Adding a Total Order to ACL2. In *Third International Workshop on the ACL2 Theorem Prover and its Applications (ACL2-2002)*, April 2002.
- [50] Panagiotis Manolios and Sudarshan K. Srinivasan. A Suite of Hard ACL2 Theorems Arising in Refinement-Based Processor Verification. In *Fifth International Workshop on the ACL2 Theorem Prover and Its Applications (ACL2-2004)*, November 2004.
- [51] Philippe Georgelin, Dominique Borrione, and Pierre Ostier. A Framework for VHDL Combining Theorem Proving and Symbolic Simulation. In *Third International Workshop on the ACL2 Theorem Prover and its Applications (ACL2-2002)*, April 2002.
- [52] Raymond Richards, David Greve, and Matthew Wilding. The Common Criteria, Formal Methods and ACL2. In *Fifth International Workshop on the ACL2 Theorem Prover and its Applications (ACL2-2004)*, November 2004.
- [53] Rob Sumners. An Incremental Stuttering Refinement Proof of a Concurrent Program in ACL2. Technical Report TR-00-29, The University of Texas at Austin, Department of Computer Sciences, November 2000. ACL2 Workshop 2000 Proceedings, Part A.
- [54] Rob Sumners. Correctness Proof of a BDD Manager in the Context of Satisfiability Checking. Technical Report TR-00-29, The University of Texas at Austin, Department of Computer Sciences, November 2000. ACL2 Workshop 2000 Proceedings, Part A.
- [55] Rob Sumners. Checking ACL2 Theorems via SAT Checking. In *Third International Workshop on the ACL2 Theorem Prover and its Applications (ACL2-2002)*, April 2002.
- [56] Rob Sumners. Fair Environment Assumptions in ACL2. In *Fourth International Workshop on the ACL2 Theorem Prover and Its Applications (ACL2-2003)*, July 2003.

- [57] Rob Sumners and Sandip Ray. Reducing Invariant Proofs to Finite Search via Rewriting. In *Fifth International Workshop on the ACL2 Theorem Prover and Its Applications (ACL2-2004)*, November 2004.
- [58] Ruben A. Gamboa and Brittany Middleton. Taylor’s Formula with Remainder. In *Third International Workshop on the ACL2 Theorem Prover and its Applications (ACL2-2002)*, April 2002.
- [59] Ruben Gamboa. Writing Literate Proofs with XML Tools. In *Fourth International Workshop on the ACL2 Theorem Prover and Its Applications (ACL2-2003)*, July 2003.
- [60] Ruben Gamboa, John Cowles, and Jeff Van Baalen. On the Verification of Synthesized Kalman Filters. In *Fourth International Workshop on the ACL2 Theorem Prover and Its Applications (ACL2-2003)*, July 2003.
- [61] Ruben Gamboa, John Cowles, and Jeff Van Baalen. Using ACL2 Arrays to Formalize Matrix Algebra. In *Fourth International Workshop on the ACL2 Theorem Prover and Its Applications (ACL2-2003)*, July 2003.
- [62] Ruben Gamboa, John Cowles, and Nadya Kuzmina. Axiomatic Events in ACL2(r): A Story of defun, defun-std, and encapsulate. In *Fifth International Workshop on the ACL2 Theorem Prover and its Applications (ACL2-2004)*, November 2004.
- [63] Ruben Gamboa and Mark Patterson. Polymorphism in ACL2. In *Fourth International Workshop on the ACL2 Theorem Prover and Its Applications (ACL2-2003)*, July 2003.
- [64] Sandip Ray. Attaching Efficient Executability to Partial Functions in ACL2. In *Fifth International Workshop on the ACL2 Theorem Prover and Its Applications (ACL2-2004)*, November 2004.
- [65] Sandip Ray, John Matthews, and Mark Tuttle. Certifying Compositional Model Checking Algorithms in ACL2. In *Fourth International Workshop on the ACL2 Theorem Prover and Its Applications (ACL2-2003)*, July 2003.
- [66] Sandip Ray and Rob Sumners. Verification of an In-place Quicksort in ACL2. In *Third International Workshop on the ACL2 Theorem Prover and its Applications (ACL2-2002)*, April 2002.
- [67] Steve Roach and Fares Fraij. Verifying Transformation Rules of the HATS High-Assurance Transformation System: An Approach. In *Fifth International Workshop on the ACL2 Theorem Prover and Its Applications (ACL2-2004)*, November 2004.
- [68] Tao Song, Jim Alves-Foss, Calvin Ko, Cui Zhang, and Karl Levitt. Using ACL2 to Verify Security Properties of Specification-based Intrusion Detection Systems. In *Fourth International Workshop on the ACL2 Theorem Prover and Its Applications (ACL2-2003)*, July 2003.

- [69] Tom Bailey and John Cowles. Knuth's Generalization of Takeuchi's Tarai Function: Preliminary Report. Technical Report TR-00-29, The University of Texas at Austin, Department of Computer Sciences, November 2000. ACL2 Workshop 2000 Proceedings, Part A.
- [70] Vernon Austel. Implementing Abstract Types in ACL2. In *Fourth International Workshop on the ACL2 Theorem Prover and Its Applications (ACL2-2003)*, July 2003.
- [71] Vernon Austel. Adding a typing mechanism to ACL2. In *Fifth International Workshop on the ACL2 Theorem Prover and Its Applications (ACL2-2004)*, November 2004.
- [72] Warren A. Hunt, Jr., Robert Bellarmine Krug, and J Moore. Integrating Nonlinear Arithmetic into ACL2. In *Fifth International Workshop on the ACL2 Theorem Prover and its Applications (ACL2-2004)*, November 2004.
- [73] Wilfred Legato. Generic Theories as Proof Strategies: A Case Study for Weakest Precondition Style Proofs. In *Fifth International Workshop on the ACL2 Theorem Prover and its Applications (ACL2-2004)*, November 2004.
- [74] Wolfgang Goerigk. Proving Preservation of Partial Correctness with ACL2: A Mechanical Compiler Source Level Correctness Proof. Technical Report TR-00-29, The University of Texas at Austin, Department of Computer Sciences, November 2000. ACL2 Workshop 2000 Proceedings, Part A.