

# List of Publications

Joe Hurd

April 24, 2012

## Refereed Conference Papers

1. Joe Hurd. The OpenTheory standard theory library. In Mihaela Bobaru, Klaus Havelund, Gerard J. Holzmann, and Rajeev Joshi, editors, *Third International Symposium on NASA Formal Methods (NFM 2011)*, volume 6617 of *Lecture Notes in Computer Science*, pages 177–191. Springer, April 2011.
2. David Burke, Joe Hurd, John Launchbury, and Aaron Tomb. Trust relationship modeling for software assurance. In *Proceedings of the 7th International Workshop on Formal Aspects of Security & Trust (FAST 2010)*, September 2010.
3. Joe Hurd. Composable packages for higher order logic theories. In M. Aderhold, S. Autexier, and H. Mantel, editors, *Proceedings of the 6th International Verification Workshop (VERIFY 2010)*, July 2010.
4. Joe Hurd and Guy Haworth. Data assurance in opaque computations. In H. Jaap Van den Herik and Pieter Spronck, editors, *Advances in Computer Games, 12th International Conference (ACG 2009)*, volume 6048 of *Lecture Notes in Computer Science*, pages 221–231. Springer, May 2010.
5. Joe Hurd. OpenTheory: Package management for higher order logic theories. In Gabriel Dos Reis and Laurent Théry, editors, *PLMMS '09: Proceedings of the ACM SIGSAM 2009 International Workshop on Programming Languages for Mechanized Mathematics Systems*, pages 31–37. ACM, August 2009.
6. Joe Hurd. Proof pearl: The termination analysis of TERMINATOR. In Klaus Schneider and Jens Brandt, editors, *20th International Conference on Theorem Proving in Higher Order Logics: TPHOLs 2007*, volume 4732 of *Lecture Notes in Computer Science*, pages 151–156. Springer, September 2007.
7. Jianjun Duan, Joe Hurd, Guodong Li, Scott Owens, Konrad Slind, and Junxing Zhang. Functional correctness proofs of encryption algorithms. In Geoff Sutcliffe and Andrei Voronkov, editors, *Logic for Programming, Artificial Intelligence, and Reasoning, 12th International Conference (LPAR 2005)*, volume 3835 of *Lecture Notes in Artificial Intelligence*, pages 519–533. Springer, December 2005.
8. Joe Hurd. First-order proof tactics in higher-order logic theorem provers. In Myla Archer, Ben Di Vito, and César Muñoz, editors, *Design and Application of Strategies/Tactics in Higher Order Logics (STRATA 2003)*, number NASA/CP-2003-212448 in NASA Technical Reports, pages 56–68, September 2003.
9. Konrad Slind and Joe Hurd. Applications of polytypism in theorem proving. In David Basin and Burkhart Wolff, editors, *16th International Conference on Theorem Proving in Higher Order Logics: TPHOLs 2003*, volume 2758 of *Lecture Notes in Computer Science*, pages 103–119. Springer, September 2003.

10. Mike Gordon, Joe Hurd, and Konrad Slind. Executing the formal semantics of the Accellera Property Specification Language by mechanised theorem proving. In Daniel Geist and Enrico Tronci, editors, *Correct Hardware Design and Verification Methods (CHARME 2003)*, volume 2860 of *Lecture Notes in Computer Science*, pages 200–215. Springer, October 2003.
11. Joe Hurd. An LCF-style interface between HOL and first-order logic. In Andrei Voronkov, editor, *Proceedings of the 18th International Conference on Automated Deduction (CADE-18)*, volume 2392 of *Lecture Notes in Artificial Intelligence*, pages 134–138. Springer, July 2002.
12. Joe Hurd. A formal approach to probabilistic termination. In Víctor A. Carreño, César A. Muñoz, and Sofiène Tahar, editors, *15th International Conference on Theorem Proving in Higher Order Logics: TPHOLs 2002*, volume 2410 of *Lecture Notes in Computer Science*, pages 230–245. Springer, August 2002.
13. Joe Hurd. Predicate subtyping with predicate sets. In Richard J. Boulton and Paul B. Jackson, editors, *14th International Conference on Theorem Proving in Higher Order Logics: TPHOLs 2001*, volume 2152 of *Lecture Notes in Computer Science*, pages 265–280. Springer, September 2001.
14. Joe Hurd. Integrating Gandalf and HOL. In Yves Bertot, Gilles Dowek, André Hirschowitz, Christine Paulin, and Laurent Théry, editors, *Theorem Proving in Higher Order Logics, 12th International Conference, TPHOLs '99*, volume 1690 of *Lecture Notes in Computer Science*, pages 311–321. Springer, September 1999.

### Refereed Journal Articles

1. Joe Hurd, Annabelle McIver, and Carroll Morgan. Probabilistic guarded commands mechanized in HOL. *Theoretical Computer Science*, 346:96–112, November 2005.
2. Joe Hurd. Verification of the Miller-Rabin probabilistic primality test. *Journal of Logic and Algebraic Programming*, 50(1–2):3–21, May–August 2003. Special issue on Probabilistic Techniques for the Design and Analysis of Systems.
3. Joe Hurd. Congruence classes with logic variables. *Logic Journal of the IGPL*, 9(1):59–75, January 2001.

### Conference Proceedings

1. Joe Hurd and Tom Melham, editors. *18th International Conference on Theorem Proving in Higher Order Logics: TPHOLs 2005*, volume 3603 of *Lecture Notes in Computer Science*. Springer, August 2005.
2. Joe Hurd, Edward Smith, and Ashish Darbari. Theorem proving in higher order logics: Emerging trends proceedings. Technical Report PRG-RR-05-02, Oxford University Computing Laboratory, August 2005.

### Special Journal Issues

1. Richard Boulton, Joe Hurd, and Konrad Slind. Computer assisted reasoning: A Festschrift for Michael J. C. Gordon. *Special Issue of the Journal of Automated Reasoning*, 43(3):237–242, October 2009.

### Unrefereed Conference Papers

1. Sally A. Browning and Joe Hurd. Cryptol: The language of cryptanalysis (invited talk abstract). In Daniel J. Bernstein and Kris Gaj, editors, *Proceedings of the 5th Special-Purpose Hardware for Attacking Cryptographic Systems Workshop (SHARCS 2012)*, pages 57–59, March 2012.

2. Joe Hurd. Evaluation opportunities in mechanized theories (invited talk abstract). In D. McGuinness, A. Stump, G. Sutcliffe, and C. Tinelli, editors, *Proceedings of the Workshop on Evaluation Methods for Solvers and Quality Metrics for Solutions (EMS+QMS 2010)*, July 2010.
3. Joe Hurd, Magnus Carlsson, Sigbjorn Finne, Brett Letner, Joel Stanley, and Peter White. Policy DSL: High-level specifications of information flows for security policies. In *High Confidence Software and Systems: HCSS 2009*, May 2009.
4. Joe Hurd, Anthony Fox, Mike Gordon, and Konrad Slind. ARM verification (abstract). In *High Confidence Software and Systems: HCSS 2007*, May 2007.
5. Joe Hurd, Mike Gordon, and Anthony Fox. Formalized elliptic curve cryptography. In *High Confidence Software and Systems: HCSS 2006*, April 2006.
6. Joe Hurd. System description: The Metis proof tactic. In Christoph Benzmueller, John Harrison, and Carsten Schuermann, editors, *Empirically Successful Automated Reasoning in Higher-Order Logic*, pages 103–104. arXiv.org, December 2005.
7. Joe Hurd. First order proof for higher order theorem provers (abstract). In Christoph Benzmueller, John Harrison, and Carsten Schuermann, editors, *Empirically Successful Automated Reasoning in Higher-Order Logic*, pages 1–3. arXiv.org, December 2005.
8. Joe Hurd. Formal verification of chess endgame databases. In Joe Hurd, Edward Smith, and Ashish Darbari, editors, *Theorem Proving in Higher Order Logics: Emerging Trends Proceedings*, number PRG-RR-05-02 in Oxford University Computing Laboratory Research Reports, pages 85–100, August 2005.
9. Joe Hurd. Compiling HOL4 to native code. In Konrad Slind, editor, *TPHOLs 2004: Emerging Trends*, number UUCS-04 in School of Computing, University of Utah, September 2004.
10. Joe Hurd. Fast normalization in the HOL theorem prover. In Toby Walsh, editor, *Ninth Workshop on Automated Reasoning: Bridging the Gap between Theory and Practice*. The Society for the Study of Artificial Intelligence and Simulation of Behaviour, April 2002. An extended abstract.
11. Joe Hurd. HOL theorem prover case study: Verifying probabilistic programs. In Gethin Norman, Marta Kwiatkowska, and Dimitar Guelev, editors, *AVoCS 2002: Second Workshop on Automated Verification of Critical Systems*, number CSR-02-6 in University of Birmingham Technical Report, pages 83–92, April 2002.
12. Joe Hurd. Lightweight probability theory for verification. In Mark Aagaard, John Harrison, and Tom Schubert, editors, *TPHOLs 2000: Supplemental Proceedings*, number CSE-00-009 in Oregon Graduate Institute Technical Reports, pages 103–113, August 2000.

## Book Reviews

1. Joe Hurd. Book review: Rippling: Meta-level guidance for mathematical reasoning by A. Bundy, D. Basin, D. Hutter and A. Ireland. *Bulletin of Symbolic Logic*, 12(3):498–499, 2006.

## Technical Reports

1. Joe Hurd. Using inequalities as term ordering constraints. Technical Report 567, University of Cambridge Computer Laboratory, June 2003.

## Technical Manuals

1. Joe Hurd. *OpenTheory Article Format*, August 2010. Available for download at <http://gilith.com/research/opentheory/article.html>.
2. Joe Hurd. *The Probability Theories in hol98*, June 2000. Part of the documentation for the hol98 theorem prover.
3. Joe Hurd. *The Real Number Theories in hol98*, November 1998. Part of the documentation for the hol98 theorem prover.

## Unpublished Works

1. Joe Hurd. Embedding Cryptol in higher order logic. Available from the author's website, March 2007.
2. Joe Hurd. Formalizing elliptic curve cryptography in higher order logic. Available from the author's website, October 2005.

## Ph.D. Thesis

1. Joe Hurd. *Formal Verification of Probabilistic Algorithms*. PhD thesis, University of Cambridge, 2002.