Joe Hurd

http://www.gilith.com/
joe@galois.com
+1 503 626 6616 ext. 152

Experience

Formal Methods Engineer 2007–present
Galois, Inc. Portland, OR, USA

Engineering and business roles in high assurance software research. Business tasks include proposal writing, hiring, budgeting and project management. Engineering work includes development of automatic static analysis tools for C and Android, designing a policy language to model information flow across security domains, and formal verification of elliptic curve cryptography.

Fellow in Computation 2003–2007
Magdalen College Oxford University, UK

Research in formal verification techniques, focusing on deploying advanced proof techniques as automatic tactics in interactive theorem provers. Teaching experience includes Ph.D. examination, lecturing and advising at the graduate and undergraduate level, small group teaching, interviewing students.

Postdoctoral Research Associate 2001–2003
Computer Laboratory Cambridge University, UK

Research in *Fully Expansive Proof and Algorithmic Verification*: using a higher order logic theorem prover as a platform to implement a verifying compiler from Property Specification Language (PSL) assertions to Verilog hardware monitors. Teaching experience includes undergraduate lecturing, small group teaching and advising final year projects.

Education

- Oxford University, 2004. M.A.
- Cambridge University, 2002. Ph.D. in Computer Science
  Dissertation: *Formal Verification of Probabilistic Algorithms*.
- Cambridge University, 1997. Masters in Mathematics
- Cambridge University, 1996. B.A. (Hons) in Mathematics

Selected Publications

- 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.
- 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.

- 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.
- 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.
- Joe Hurd, Annabelle McIver, and Carroll Morgan. Probabilistic guarded commands mechanized in HOL. *Theoretical Computer Science*, 346:96–112, November 2005.
- 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.
- 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.
- 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.
- 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.
- 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.
- 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.
- 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.
- 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.

Professional Service

Conferences Organized *TTVSI 2008* and *TPHOLs 2005*; serve on the Program Committees of *TPHOLs/ITP* and related workshops; and review papers for many formal verification conferences and journals.

Speaking Invited speaker at *SSV 2010* and workshops of *FLoC 2010* and *LPAR 2005*; and regularly present my research at international conferences and seminars in academia and industry.

Development *OpenTheory*, a package management system for logical theories; *Metis*, an open source automatic theorem prover; and have contributed many theories and proof tools to the *HOL4* interactive theorem prover. All these systems are open source.