

# Aleksey Nogin

# Curriculum Vitae

**Email:** aleksey@nogin.org

**Web:** <http://nogin.org/>

**Phone:** (805) 630-9415

**Mailing Address:** 645 Hampshire Rd Apt 129

Westlake Village, CA 91361-2340

**Citizenship:** USA

**Degrees** **Cornell University** **Ithaca, NY**

*Aug 2002* **Ph.D.** in Computer Science; **Minor** in Cognitive Studies

*May 2000* **M.S.** in Computer Science

**Moscow State University** **Moscow, Russia**

*Jun 1997* **Diploma with Honors**, Faculty of Mathematics and Mechanics, Division of Mathematics

**Major:** Mathematics, Applied Mathematics (Dept. of Mathematical Logic and Theory of Algorithms)

**Research Interests** Development, application, and theory of systems and tools for computer-aided programming language research and experimentation, computer-aided software engineering, and computer-aided reasoning and verification. Formal methods for reliable software design process. Development, application, and theory of interactive proof assistants and logical frameworks. Type theories, higher-order abstract syntax, and their applications.

## Research

**Experience** **HRL Laboratories, LLC** **Malibu, CA**

*8/2006–Present* **Research Staff Scientist**

**California Institute of Technology** **Pasadena, CA**

*9/2002–8/2006* **Postdoctoral Scholar / Senior Postdoctoral Scholar**

**Research Projects:** Computer-aided and formal software engineering based on the logical frameworks, including building reliable extensible compilers. Improving the software engineering capabilities of the MetaPRL formal toolkit. Foundations for practical syntax-based reasoning about properties of programming languages and languages with bindings, as well as for formal reasoning in the area of logical reflection in general. Formalizing the foundations of abstract algebra and number theory. Designing and implementing of the OMake build system. Designing serializability protocols for distributed filesystems.

*Jul–Aug 2000* Visitor with Prof. Jason Hickey

### MetaPRL Project

*Since 1999* **Coordinator and a Lead Developer.** MetaPRL is a formal methods programming toolkit that can be used as a computer-aided software engineering tool. It is also an interactive tactic-based theorem prover. It also implements a logical framework that allows its users to specify and work with different logical theories and formalisms. Finally, MetaPRL is a basis for a programming language research, experimentation and meta-reasoning toolkit that is currently being developed.

**Cornell University** **Ithaca, NY**

*9/1997–9/2002* **Research Assistant** with Prof. Robert Constable

**Ph.D. Dissertation:** *Theory and Implementation of an Efficient Tactic-Based Logical Framework*

**Research Projects:** Increased the logical speed of the MetaPRL system by two orders of magnitude. Came up with several methods of improving expressivity and making type theory formalization more usable in both automated and user-guided theorem proving.

*Mar–Apr 1997* Visitor with Prof. Robert Constable

*9/1992–6/1997* **Moscow State University** **Moscow, Russia**

*9/1995–6/1997* Laboratory for Logical Problems in Computer Science

*9/1994–6/1997* Department of Mathematical Logic and Theory of Algorithms; Advisor: Prof. Alexander Razborov

*May 1997* **Diploma Thesis:** *Improving the Efficiency of NuPRL Proofs*

**Related Experience**

Participated in creation of **three successful grant applications**:

- A recent MetaPRL-based grant by Laboratory for Computational Methods at Moscow State University (approximately 30 men-years worth of funding);
- NSF grant 0313354 “*ITR: Reliable Distributed Programming with Speculations*”;
- ONR/MURI grant N00014-01-1-0765 “*Building Interactive Digital Libraries of Formal Algorithmic Knowledge*”.

Co-organized a day-long tutorial “*Introduction to MetaPRL Theorem Prover*” given at the 16<sup>th</sup> International Conference on Theorem Proving in Higher Order Logics (TPHOLs 2003).

**Teaching Experience****California Institute of Technology****Pasadena, CA**

*Fall 2005* **Creator and Instructor**, undergraduate course “Language-Based Security”.

*June 2004* **Creator and Instructor**, course “Introduction into formal computer-aided reasoning and the MetaPRL theorem prover”, North American Summer School in Logic, Language and Information (NASSLI) 2004 at UCLA.

*Winter 2004* **Creator and Instructor**, graduate / advanced undergraduate course “Programming Language Semantics”.

*Spring 2003* **Creator and Instructor**, graduate / advanced undergraduate MetaPRL-based course “Type Theory and Formal Methods”.

**Cornell University****Ithaca, NY**

*Spring 2002* **TA**, undergraduate course “Structure and Interpretation of Computer Programs”.

*Fall 2000* **Instructor**, undergraduate course “Introduction to Unix”.

*Spring 1998* **TA**, undergraduate course “Structure and Interpretation of Computer Programs”.

*Fall 1997* **TA**, undergraduate course “Introduction to Theory of Computing (Honors)”.

**Publications**

2006

• Jason Hickey and Aleksey Nogin. Formal compiler construction in a logical framework. *Higher-Order and Symbolic Computation*, 19(2–3):197–230, September 2006.

• Jason Hickey and Aleksey Nogin. OMake: Designing a scalable build process. In Luciano Baresi and Reiko Heckel, editors, *Fundamental Approaches to Software Engineering, 9<sup>th</sup> International Conference, FASE 2006*, volume 3922 of *Lecture Notes in Computer Science*, pages 63–78. Springer, 2006. An extended version is available as California Institute of Technology technical report CaltechC-STR:2006.001.

• Jason Hickey, Aleksey Nogin, Xin Yu, and Alexei Kopylov. Mechanized meta-reasoning using a hybrid HOAS/de Bruijn representation and reflection. In John H. Reppy and Julia L. Lawall, editors, *Proceedings of the 11<sup>th</sup> ACM SIGPLAN International Conference on Functional Programming, ICFP 2006*, pages 172–183. ACM, 2006.

• Jason Hickey, Aleksey Nogin, Xin Yu, and Alexei Kopylov. Practical reflection for sequent logics. In *Proceedings of the International Workshop on Logical Frameworks and Meta-Languages: Theory and Practice (LFMTP’06)*, Electronic Notes in Theoretical Computer Science, 2006.

• Aleksey Nogin and Alexei Kopylov. Formalizing type operations using the “Image” type constructor. In *Proceedings of the 13<sup>th</sup> Workshop on Logic, Language, Information and Computation (WoLLIC 2006)*, volume 165 of *Electronic Notes in Theoretical Computer Science*, pages 121–132. Elsevier, 2006. Extended version was submitted to *Information and Computation Journal*.

2005

• Aleksey Nogin, Alexei Kopylov, Xin Yu, and Jason Hickey. A computational approach to reflective meta-reasoning about languages with bindings. In *MERLIN ’05: Proceedings of the 3rd ACM SIGPLAN workshop on Mechanized reasoning about languages with variable binding*, pages 2–12. ACM Press, 2005. An extended version is available as California Institute of Technology technical report CaltechCSTR:2005.003.

2004

• Jason Hickey and Aleksey Nogin. Extensible hierarchical tactic construction in a logical framework. In Konrad Slind, Annette Bunker, and Ganesh Gopalakrishnan, editors, *Proceedings of the 17<sup>th</sup> International Conference on Theorem Proving in Higher Order Logics (TPHOLs 2004)*, volume 3223 of *Lecture Notes in Computer Science*, pages 136–151. Springer-Verlag, 2004.

- Cristian Țăpuș, Aleksey Nogin, Jason Hickey, and Jerome White. A simple serializability mechanism for a distributed objects system. In David A. Bader and Ashfaq A. Khokhar, editors, *Proceedings of the 17<sup>th</sup> International Conference on Parallel and Distributed Computing Systems (PDCS-2004)*. International Society for Computers and Their Applications (ISCA), 2004.
- Nathaniel Gray, Jason Hickey, Aleksey Nogin, and Cristian Țăpuș. Building extensible compilers in a formal framework. A formal framework user’s perspective. In Konrad Slind, editor, *Emerging Trends. Proceedings of the 17<sup>th</sup> International Conference on Theorem Proving in Higher Order Logics (TPHOLs 2004)*, pages 57–70. University of Utah, 2004.
- 2003
  - Jason Hickey, Aleksey Nogin, Robert L. Constable, Brian E. Aydemir, Eli Barzilay, Yegor Bryukhov, Richard Eaton, Adam Granicz, Alexei Kopylov, Christoph Kreitz, Vladimir N. Krupski, Lori Lorigo, Stephan Schmitt, Carl Witty, and Xin Yu. MetaPRL — A modular logical environment. In David Basin and Burkhart Wolff, editors, *Proceedings of the 16<sup>th</sup> International Conference on Theorem Proving in Higher Order Logics (TPHOLs 2003)*, volume 2758 of *Lecture Notes in Computer Science*, pages 287–303. Springer-Verlag, 2003.
  - Jason Hickey, Aleksey Nogin, Adam Granicz, and Brian Aydemir. Compiler implementation in a formal logical framework. In *Proceedings of the 2003 workshop on Mechanized reasoning about languages with variable binding*, pages 1–13. ACM Press, 2003. Extended version of the paper is available as Caltech Technical Report caltechCSTR:2003.002.
  - Xin Yu, Aleksey Nogin, Alexei Kopylov, and Jason Hickey. Formalizing abstract algebra in type theory with dependent records. In David Basin and Burkhart Wolff, editors, *16<sup>th</sup> International Conference on Theorem Proving in Higher Order Logics (TPHOLs 2003)*. *Emerging Trends Proceedings*, pages 13–27. Universität Freiburg, 2003.
  - Yegor Bryukhov, Alexei Kopylov, Vladimir Krupski, and Aleksey Nogin. Implementing and automating basic number theory in MetaPRL proof assistant. In David Basin and Burkhart Wolff, editors, *16<sup>th</sup> International Conference on Theorem Proving in Higher Order Logics (TPHOLs 2003)*. *Emerging Trends Proceedings*, pages 29–39. Universität Freiburg, 2003.
  - Nathaniel Gray, Cristian Țăpuș, Aleksey Nogin, and Jason Hickey. Building reliable compilers with a formal methods framework. In Dr. Indrakshi Ray, editor, *The 14<sup>th</sup> International Symposium on Software Reliability Engineering (ISSRE 2003)*. *Supplementary Proceedings*, pages 319–320. Chillarege Press, 2003.
- 2002
  - Aleksey Nogin. *Theory and Implementation of an Efficient Tactic-Based Logical Framework*. PhD thesis, Cornell University, Ithaca, NY, August 2002.
  - Aleksey Nogin. Quotient types: A modular approach. In Victor A. Carreño, César A. Muñoz, and Sophièn Tahar, editors. *Proceedings of the 15<sup>th</sup> International Conference on Theorem Proving in Higher Order Logics (TPHOLs 2002)*, volume 2410 of *Lecture Notes in Computer Science*, pages 263–280. Springer-Verlag, 2002.
  - Aleksey Nogin and Jason Hickey. Sequent schema for derived rules. In Victor A. Carreño, César A. Muñoz, and Sophiène Tahar, editors. *Proceedings of the 15<sup>th</sup> International Conference on Theorem Proving in Higher Order Logics (TPHOLs 2002)*, volume 2410 of *Lecture Notes in Computer Science*, pages 281–297. Springer-Verlag, 2002.
- 2001
  - Alexei Kopylov and Aleksey Nogin. Markov’s principle for propositional type theory. In L. Fribourg, editor, *Computer Science Logic, Proceedings of the 10<sup>th</sup> Annual Conference of the EACSL*, volume 2142 of *Lecture Notes in Computer Science*, pages 570–584. Springer-Verlag, 2001.
  - Stephan Schmitt, Lori Lorigo, Christoph Kreitz, and Aleksey Nogin. JProver: Integrating connection-based theorem proving into interactive proof assistants. In *International Joint Conference on Automated Reasoning*, volume 2083 of *Lecture Notes in Artificial Intelligence*, pages 421–426. Springer-Verlag, 2001.
- 2000
  - Jason J. Hickey and Aleksey Nogin. Fast tactic-based theorem proving. In J. Harrison and M. Aagaard, editors, *Theorem Proving in Higher Order Logics: 13<sup>th</sup> International Conference, TPHOLs 2000*, volume 1869 of *Lecture Notes in Computer Science*, pages 252–266. Springer-Verlag, 2000.

- Aleksey Nogin. Writing constructive proofs yielding efficient extracted programs. In Didier Galmiche, editor, *Proceedings of the Workshop on Type-Theoretic Languages: Proof Search and Semantics*, volume 37 of *Electronic Notes in Theoretical Computer Science*. Elsevier Science Publishers, 2000.

1997 • Aleksey Nogin. Improving the efficiency of NuPRL proofs. Department of Computer Science TR97-1643, Cornell University, August 1997.

1995 • Aleksey Nogin. On Horn interpolation in linear logic. Mathematical Logic and Theoretical Computer Science TR 1995-11, Steklov Mathematical Institute, April 1995. In Russian.

## Online Publications

- Jason J. Hickey, Aleksey Nogin, *et al.* OMake Home Page. <http://omake.metaprl.org/>
- Jason Hickey, Aleksey Nogin, Alexei Kopylov, *et al.* MetaPRL Home Page. <http://metaprl.org/>
- Jason Hickey, Brian Aydemir, Yegor Bryukhov, Alexei Kopylov, Aleksey Nogin, and Xin Yu. A listing of MetaPRL theories. <http://metaprl.org/theories.pdf>
- Jason Hickey, Nathaniel Gray, Aleksey Nogin, Cristian Țăpuș, and Xin Yu. Introduction to MetaPRL Theorem Prover. Tutorial: Implementing FOL in MetaPRL. <http://files.metaprl.org/papers/tutorial1.pdf>
- Jason Hickey, Aleksey Nogin and Alexei Kopylov. MetaPRL User Guide. <http://metaprl.org/user-guide/default.html>
- Jason Hickey and Aleksey Nogin. MetaPRL System Description. <http://metaprl.org/system/default.html>
- Aleksey Nogin and Vladimir Krupski. MetaPRL Developer Guide. <http://metaprl.org/developer-guide/default.html>

- Talks**
- Sep 2005* 3rd ACM SIGPLAN workshop on Mechanized reasoning about languages with variable binding, Tallinn, Estonia
  - Mar 2005* CS Colloquium, Purdue University, West Lafayette, IN
  - Oct 2004* Microsoft Research, Redmond, WA
  - Sep 2004* Theorem Proving in Higher Order Logics, 17<sup>th</sup> International Conference, Park City, UT
  - Sep 2003* Seminar “Logical Problems in Computer Science”, Department of Mathematical Logic and Theory of Algorithms, Faculty of Mathematics and Mechanics, Moscow State University, Moscow, Russia
  - Apr 2003* Microsoft Research, Redmond, WA
  - Dec 2002* City University of New York Graduate Center, Computer Science Colloquium, New York, NY
  - Aug 2002* Theorem Proving in Higher Order Logics, 15<sup>th</sup> International Conference, Hampton, VA, *two talks*
  - Sep 2001* Computer Science Logic, 10<sup>th</sup> Annual Conference of the EACSL, Paris, France
  - Sep 2001* Logic Seminar Series, Department of Informatics of Saarland University and MPI Institute, Saarbrücken, Germany
  - Aug 2000* Theorem Proving in Higher Order Logics, 13<sup>th</sup> International Conference, Portland, OR
  - Jun 2000* Workshop on Type-Theoretic Languages: Proof Search and Semantics, Pittsburgh, PA
  - Mar 2000* Seminar “Logical Problems in Computer Science”, Department of Mathematical Logic and Theory of Algorithms, Faculty of Mathematics and Mechanics, Moscow State University, Moscow, Russia

## Academic and Community Service

- 2000–2006* Helped to set up and administer a 16×2-node cluster for Jason Hickey’s Mojave Group at Caltech
- Since 1996* Contributor to Open Source projects, including OCaml, Mozilla, and Red Hat Linux/Fedora Project
- 1997–2002* Set up and administered a department-wide CVS server. Administered Linux servers for the Cornell PRL group.
- 1995–1997* Set up and administered network, mail, and dial-up servers for the Youth Scientific Creativity Center.