Kristina Sojakova

Contact Information

INRIA Paris, France
Email: kristina.sojakova@inria.fr

Research Interests

Privacy and security, (homotopy) type theory, categorical logic, programming languages.

Current Research

I use insights from type theory and programming languages to develop novel ways of formally reasoning about the security of cryptographic protocols. Together with Joshua Gancher at Cornell I designed a calculus, called Interactive Probabilistic Dependency Logic (IPDL), for specifying and reasoning about distributed probabilistic computations. Central to the logic is the observation that a cryptographic proof is often fundamentally about removing a dependency (such as removing a message from a ciphertext); following this insight, we make dependency a first-class citizen in the logic. This makes our logic, implemented in the proof assistant Coq, particularly suitable for reasoning about certain kinds of distributed cryptographic protocols.

I am a coauthor of the Homotopy Type Theory book written during the Special Year on Univalent Foundations at the Institute for Advanced Study in Princeton. Homotopy type theory is a new branch of mathematics that investigates a deep and exciting connection between Martin-Löf's dependent type theory and the mathematical fields of abstract homotopy theory, algebraic topology, and higher category theory. In homotopy type theory, we can use geometric intuition to guide us in formulating new concepts in type theory and, conversely, use type-theoretic machinery to verify and often simplify existing mathematical proofs.

In my dissertation, which won the Distinguished Dissertation Award from Carnegie Mellon University, I investigated the properties of higher inductive types, which are a generalization of ordinary inductive types. They allow us to characterize many important geometric and categorical objects, such as the sphere $\mathbf{S}^n$, torus, a limit, etc., by an induction principle. I showed that this induction principle is equivalent to the universal property of being a *homotopy-initial algebra*. This extends an earlier analogous result for the type of well-founded trees (Martin-Löf's W-types), which was joint work with Steve Awodey and Nicola Gambino, and generalizes the well-known result by Peter Dybjer which states that certain inductive types in an extensional type theory can be characterized as initial algebras. Similarly to initiality, the chief significance of homotopy-initiality lies in its simplicity: the induction principle, which involves dependent types, can be rather complicated to state and use even for higher inductive types with relatively simple data, such as the torus. Homotopy-initiality, on the other hand, only involves a universal property with respect to non-dependent types, which makes it significantly easier to work with in a categorical setting.

Work and Education

INRIA Paris, France (July 2020 - present)
Starting Researcher position. Team Prosecco (Programming Securely with Cryptography).

Cornell University, USA (Dec 2017 - June 2020)
Postdoctoral Associate position. Supervisor: Greg Morrisett.

Appalachian State University, USA (June 2016 - Dec 2017)
Postdoctoral Researcher position. Supervisor: Patricia Johann.

Carnegie Mellon University, USA (Aug 2010 - Aug 2016)
Ph.D., Computer Science.
Advisors: Frank Pfenning, Steve Awodey.

Institute for Advanced Study, USA (Sep 2012 - May 2013)
Special Year on the Univalent Foundations of Mathematics.

Jacobs University Bremen, Germany (Sep 2006 - Jun 2010)
BSc. in Mathematics, MSc. in Computer Science.
Member of President's List for outstanding academic achievements.

Awards

Distinguished Dissertation Award (2016)
Winner of the School of Computer Science Distinguished Dissertation Award at Carnegie Mellon University.

Publications

- K. Sojakova, F. van Doorn, E. Rijke. Sequential Colimits in Homotopy Type Theory. To appear in *Logic in Computer Science (LICS 2020)*.
- K. Sojakova, P. Johann. A General Framework for Relational Parametricity. In *Logic in Computer Science (LICS 2018)*, pp. 869–878. ACM 2018.
- S. Awodey, N. Gambino, K. Sojakova. Homotopy-Initial Algebras in Type Theory. *Journal of The ACM (JACM 2017)*, v. 63(6), pp. 51:1–51:45, 2017.
- K. Sojakova. The Equivalence of The Torus and The Product of Two Circles in Homotopy Type Theory. *ACM Transactions on Computational Logic (TOCL 2016)*, v. 17(4), pp. 29:1–29:19, 2016.
- K. Sojakova. Higher Inductive Types as Homotopy-Initial Algebras. In *Symposium on Principles of Programming Languages (POPL 2015)*, pp. 31–42. ACM 2015.
- The Univalent Foundations Program. Homotopy Type Theory – Univalent Foundations of Mathematics. Univalent Foundations Project, 2013. Author of chapters 4 and 5.
- F. Rabe, K. Sojakova. Logical Relations for a Logical Framework. *ACM Transactions on Computational Logic (TOCL 2013)*, v. 14(4), pp. 32:1–32:34, 2013.
- S. Awodey, N. Gambino, K. Sojakova. Inductive Types in Homotopy Type Theory. In *Logic in Computer Science (LICS 2012)*, pp. 95–104. IEEE Computer Society 2012.
- M. Codescu, F. Horozal, M. Kohlhase, T. Mossakowski, F. Rabe, K. Sojakova. Towards Logical Frameworks in the Heterogeneous Tool Set Hets. In *Recent Trends in Algebraic Development Techniques (WADT 2010)*, pp.139–159. Springer 2010.
- K. Sojakova, F. Rabe. Translating a Dependently-Typed Logic to First-Order Logic. In *Recent Trends in Algebraic Development Techniques (WADT 2008)*, pp. 326–341. Springer 2008.

Theses

Doctoral Thesis: Higher Inductive Types in Homotopy Type Theory
I formulated and investigated a class of higher inductive types I called W-quotients, which generalize Martin-Löf's well-founded trees to a higher-dimensional setting. I showed that a propositional variant of W-quotients, whose computational behavior is determined up to a higher equality, is characterized by the universal property of being a homotopy-initial algebra. Furthermore, I showed that a number of other higher inductive types of interest arise as special cases of W-quotients, thereby inheriting an analogous characterization in terms of homotopy-initiality. Based on these results, I contend that W-quotients may play the same role in the higher dimensional setting as Martin-Löf's W-types do for ordinary inductive types: that of a simple, well-studied class of (higher) inductive types, which subsumes most of the other (higher) inductive types of interest as special cases. Accompanied by formalization in the Coq proof assistant and resulted in publications in the proceedings of *LICS 2012* and *POPL 2015*, and in *JACM 2017*.

Master Thesis: Mechanical Verification of Logic Translations
Developed a theory of logical relations for the Edinburgh Logical Framework and used it to mechanically verify logic translations in the Twelf logical framework. Resulted in a publication in *TOCL 2016*.

Bachelor Thesis: Translating Dependently-Typed Logic to First-Order Logic
Developed the translation in the model-theoretic framework of institutions and implemented it in a multi-logic algebraic specification tool set Hets, using the Haskell programming language. Resulted in a publication in the proceedings of *WADT 2008*.

Invited Talks

Initial Algebras in Homotopy Type Theory. *Workshop on Polynomial Functors*, 2021.
Higher Inductive Types in Homotopy Type Theory. *TypeLevel Summit*, 2019.
Higher Inductive Types as Homotopy-Initial Algebras. *Joint Mathematics Meetings*, 2018.

Service

- Panels: *NSF Small Formal Methods/Programming Languages Panel 2020.*
- Committees: *LICS 2021*, *MFPS 2020*, *LFMTP 2019*, *LFMTP 2017*
- Reviewing: *FOSSACS 2019*, *TYPES 2019*, *FOSSACS 2018*, *TOCL 2018*, *LICS 2017*, *FOSSACS 2017*, *LFCS 2013*

Teaching

Summer School on Homotopy Type Theory (Aug 2019)
Course on formalization of homotopy type theory using the Coq proof assistant.

Semantics of Programming Languages Teaching Assistant (Jan 2015 - May 2015)
Core graduate course at Carnegie Mellon University.

Principles of Imperative Computation Teaching Assistant (June 2012)
Intensive entry-level summer course at Carnegie Mellon University.

English Language Instructor (Sep 2005 - Aug 2006)
Taught private as well as corporate clients, both individuals and groups. Lessons were heavily communication-based.

Computer Science Teacher (Feb 2005 - Jun 2005)
Taught an intensive high-school computer science course, grades 10-12.

References

Greg Morrisett, Dean and Vice Provost, Cornell University, *greg.morrisett@cornell.edu*
Frank Pfenning, Professor, Carnegie Mellon University, *fp@cs.cmu.edu*
Steve Awodey, Professor, Carnegie Mellon University, *awodey@cmu.edu*
Thierry Coquand, Professor, University of Gothenburg, *coquand@chalmers.se*
Robert Harper, Professor, Carnegie Mellon University, *rwh@cs.cmu.edu*

Computer Skills

Coq, Twelf, Haskell, LaTeX.

Memberships

Mensa International