הקרן הלאומית למדע
المؤسّسة الإسرائيلية للعلوم
Israel Science Foundation

Application for an International Cooperation

Prof. Nadia Polikarpova is an associate professor at the Department of Computer Science and Engineering of the University of California, San Diego. She has developed and built Synquid, a state-of-the-art synthesis tool, and now focuses on cross-cutting concerns in software applications that can benefit from synthesis methods.

Description of the intended collaboration
In this project, synthesis is a viable and vital part. Prof. Polikarpova is an expert in the field, as well as a leading scholar of formal methods from her years under the supervision of Prof. Bertrand Meyer at ETH, Zurich. We will research scalability of synthesis algorithms and how to enhance it. We will construct benchmark suites for synthesis of functional programs, along the same lines of the ones that have been developed for imperative ones, throughout the last several years, by Prof. Rajeev Alur, Dr. Sumit Gulwani, Dr. Rishabh Singh, and others (known as the SyGuS benchmarks).

Complementary contributions and synergy
My skills come from the world of logic, first-order and type theory. My part will be in applying synthesis procedures in settings where program refinement requires automation to make the derivation succinct, *i.e.*, have fewer steps. Inevitably a scalability wall will bit hit, at which point the underlying synthesis algorithm will have to be revised or completely restructured. Prof. Polikarpova's experience with building synthesis engines and tuning them for performance will make a tremendous help in improving these methods. Driven by a concrete need, I am certain we can work together to obtain speedups that make the method feasible and suitable for an interactive setting. Prof. Polikarpova's work on rich types will provide the background for integrating resource-aware types as a metric in our tools.

Potential future collaboration beyond the current project period
Prof. Polikarpova's work on rich specifications in Haskell is grounds for more synthesis projects involving students from both institutes.

Itemized budget

- Travel expenses Israel–San Diego: 38,000 NIS for the entire grant period

Nadia Polikarpova

UCSD CSE
9500 Gilman Drive
La Jolla, CA 92093

Email: npolikarpova@eng.ucsd.edu
Homepage: cseweb.ucsd.edu/~npolikarpova/

Research interests

My research interests are in *program verification*, *program synthesis*, and *software security*. In particular, I am interested in building practical tools and techniques that make it easier for programmers to construct reliable software.

Research positions

Assistant Professor Sep 2017–present
University of Califoria, San Diego

Postdoctoral Associate Dec 2014–Aug 2017
Massachusetts Institute of Technology (Cambridge, MA)
Advisor: Armando Solar-Lezama

Research Intern May–Aug 2011
Microsoft Research (Redmond, WA)
Mentor: Michał Moskal

Education

PhD, Computer Science Sept 2008–Jul 2014
ETH Zurich (Switzerland)
Thesis: *Specified and Verified Reusable Components*
Advisor: Bertrand Meyer

MSc, Applied Mathematics and Informatics Sept 2006–May 2008
SPbSU ITMO (Saint-Petersburg, Russia)
Thesis: *Dynamic Assertion Inference in a Programming Language with Design by Contract Support (Eiffel Case Study)*
Advisor: Anatoly Shalyto
Co-advisor: Ilinca Ciupa (ETH Zurich)
Grade: 5 / 5

BEng, Applied Mathematics and Informatics Sept 2002–May 2006
SPbSU ITMO (Saint-Petersburg, Russia)
Thesis: *Object-oriented approach to modeling and specification of entities with complex behavior*
Advisor: Danil Shopyrin
Grade: 5 / 5

Projects

Synquid main author
Program synthesis from refinement types
`https://bitbucket.org/nadiapolikarpova/synquid`

AutoProof co-author
An automated verifier for programs that manipulate complex object structures
`http://comcom.csail.mit.edu/autoproof`

EiffelBase2 main author
A fully verified container library
`https://github.com/nadia-polikarpova/eiffelbase2`

Boogaloo main author
A symbolic execution engine for Boogie
`https://bitbucket.org/nadiapolikarpova/boogaloo`

Dafny contributor
Program Verifier for Functional Correctness
`http://research.microsoft.com/en-us/projects/dafny`

CITADEL main author
Dynamic invariant inference meets Desing-by-Contract
`http://people.csail.mit.edu/polikarn/citadel/`

Publications

International conferences

P12. J. P. Inala, N. Polikarpova, X. Qiu, B. S. Lerner, and A. Solar-Lezama. *Synthesis of Recursive ADT Transformations*. 23rd International Conference on Tools and Algorithms for the Construction and Analysis of Systems (**TACAS**), Uppsala, Sweden, April 2017

P11. N. Polikarpova, I. Kuraj, and A. Solar-Lezama. *Program synthesis from polymorphic refinement types*. 37th ACM SIGPLAN Conference on Programming Language Design and Implementation (**PLDI**), Santa Barbara, CA, June 2016

P10. N. Polikarpova, J. Tschannen, and C. A. Furia. *A Fully Verified Container Library*. 20th International Symposium on Formal Methods (**FM**), Oslo, Norway, June 2015, **best paper award**

P9. J. Tschannen, C. A. Furia, M. Nordio, and N. Polikarpova. *AutoProof: Auto-active Functional Verification of Object-oriented Programs*. 21st International Conference on Tools and Algorithms for the Construction and Analysis of Systems (**TACAS**), London, UK, April 2015

P8. N. Polikarpova, J. Tschannen, C. A. Furia, and B. Meyer. *Flexible Invariants Through Semantic Collaboration*. 19th International Symposium on Formal Methods (**FM**), Singapore, May 2014

P7. N. Polikarpova, C. A. Furia, and S. West. *To Run What No One Has Run Before*. Fourth International Conference on Runtime Verification (**RV**), Rennes, France, September 2013

P6. N. Polikarpova, C. A. Furia, Y. Pei, Y. Wei, and B. Meyer. *What Good Are Strong Specifications?* 35th International Conference on Software Engineering (**ICSE**), San Francisco, CA, May 2013

P5. K. R. M. Leino and N. Polikarpova. *Verified calculations*, Verified Software: Theories, Tools and Experiments (**VSTTE**), Atherton, CA, May 2013

P4. N. Polikarpova N and M. Moskal. *Verifying implementations of security protocols by refinement*. Verified Software: Theories, Tools and Experiments (**VSTTE**), Philadelphia, PA, January 2012

P3. P. Müller, N. Shankar, G. T. Leavens, T. Ridge, T. Tuerk, V. Klebanov, M. Ulbrich, B. Weiß, K. R. M. Leino, R. Chapman, R. Monahan, N. Polikarpova, D. Bronish, R. Arthan, E. Alkassar, E. Cohen, M. Hillebrand, S. Tobies, B. Jacobs, F. Piessens, and J. Smans. *The 1st Verified Software Competition: Experience Report*. 17th International Symposium on Formal Methods (**FM**), Limerick, Ireland, June 2011, **best paper award**

P2. N. Polikarpova, C. Furia, and B. Meyer. *Specifying Reusable Components*. Verified Software: Theories, Tools and Experiments (**VSTTE**), Edinburgh, UK, August 2010

P1. N. Polikarpova, I. Ciupa, and B. Meyer. *A comparative study of programmer-written and automatically inferred contracts*. 18th International Conference on Software Testing and Analysis (**ISSTA**), Chicago, IL, July 2009

Papers in Submission

S1. N. Polikarpova, J. Yang, S. Itzhhaky, and A. Solar-Lezama. *Type-Driven Repair for Information Flow Security*. In Submission.

National conferences

N2. N. Polikarpova, V. Tochilin, and A. Shalyto. *Applying Genetic Programming to Implementation of Systems with Complex behavior* (in Russian). IV International Theoretical and Practical Conference "Integrated Models and Soft Computing in Artificial Intelligence", Kolomna, Russia, May 2007

N1. N. Polikarpova. *Object-oriented approach to modeling and specification of entities with complex behavior*. Software Engineering Conference in Russia (**SEC(R)**), Moscow, Russia, November 2006

Books

B1. N. Polikarpova and A. Shalyto. *Automata-based Programming* (in Russian). Piter, 2009

Teaching

Lecturer

Program Synthesis (graduate)	UCSD, Fall 2017

Teaching assistant

Java and C# in depth	ETH Zurich, 2010, 2014
Introduction to Programming	ETH Zurich, 2008–2013
Software Architecture	ETH Zurich, 2009

Guest Lecturer

Foundations of Program Analysis	MIT, 2015
Software Verification	ETH Zurich, 2009–2013
Software Architecture	ETH Zurich, 2011
Eiffel: Analysis, Design and Programming	ETH Zurich, 2009

Mentoring

Isaac Grosof. *Symmetry Reduction in Synquid*, Undergraduate Advanced Project, MIT, May 2016

Severin Kozak. *A Front-End for Synquid*, Undergraduate Research Project, MIT, November 2015

Tobias Kiefer. *Model-Based Contracts for C#*, Bachelor Thesis, ETH Zurich, October 2012

Elena Mokhon. *Model-Based Contracts for C# collections*, Master Thesis, ETH Zurich and Tver State University (Russia), April 2011

Flaviu Roman. *Improving Relevancy of Dynamically-Inferred Contracts in Eiffel*, Master Thesis, ETH Zurich and Technical University of Cluj-Napoca (Romania), June 2009

Awards

Best Paper Awards: Formal Methods 2015, Formal Methods 2011.

ACM SIGSOFT Recognition of Services Award in appreciation for the contribution as a Deputy General Chair of ESEC/FSE 2013.

Talks

Refinement Types for Program Verification and Synthesis

Tutorial at PLDI'17 (with Ranjit Jhala and Niki Vazou)	June 2017

Type-Driven Program Synthesis and Repair

University of California San Diego (invited seminar)	Jun 2016
Microsoft Research Redmond (invited seminar)	Aug 2016
University of Pennsylvania (invited seminar)	Oct 2016

Program Synthesis with Synquid

MIT Programming Languages Offsite (tutorial)	May 2016

Programs Synthesis from Refinement Types

Kyoto University (invited seminar)	Mar 2015
Shonan Meeting	Mar 2015
MIT (ExCAPE PI meeting)	Jun 2015
Microsoft Research Redmond (invited seminar)	Aug 2015
IBM PL Day	Nov 2015
University of Washington (invited seminar)	Jan 2016
University of Toronto (invited seminar)	Jan 2016
University of Waterloo (invited seminar)	Jan 2016
McMaster University (invited seminar)	Jan 2016
Dagstuhl seminar	Apr 2016
CMU (invited seminar)	Apr 2016
University of Pennsylvania (ExCAPE PI meeting)	May 2016

A Fully Verified Container Library

Shonan Meeting	Sep 2015

Program verification and synthesis

Women's Technology Program, MIT	Jul 2015

Developing Verified Programs with Dafny

MIT Programming Languages Offsite (tutorial)	May 2015

Practical Techniques for Auto-Active Verification

Yale University (postdoc interview talk)	Jun 2014
Rice University (postdoc interview talk)	Jun 2014
CMU (postdoc interview talk)	Jun 2014
MIT (postdoc interview talk)	Jul 2014
Imperial College London (postdoc interview talk)	Jul 2014
Microsoft Research Cambridge (invited seminar)	Jul 2014
EPFL (postdoc interview talk)	Jul 2014

EiffelBase2: strong contracts for design and verification

Workshop "Eiffel at 25", ETH Zurich	Nov 2010

Specifying reusable components with model-based contracts

IFIP WG 2.3 meeting 50, Lachen (Switzerland)	Mar 2010

Summer Schools, Seminars, and Competitions

Rising Stars: An academic career workshop for women. CMU, USA. Oct 30–Nov 1, 2016.

Dagstuhl seminar on Language Based Verification Tools for Functional Programs. Schloss Dagstuhl, Germany. Mar 28–Apr 1, 2016.

Shonan Meeting on Semantics and Verification of Object-Oriented Languages. Shonan village, Japan. Sep 21–25, 2015.

4th VerifyThis Verification Competition. London, UK. Apr 12, 2015.

Shonan Meeting on Static Analysis Meets Runtime Verification. Shonan village, Japan. Mar 16–19, 2015.

Workshop on Software Correctness and Reliability. Zurich, Switzerland. Oct 3–4, 2014.

VSCOMP'14 Verified Software Competition. Jun 14–15, 2014.

Dagstuhl seminar on Evaluating Software Verification Systems: Benchmarks and Competitions. Schloss Dagstuhl, Germany. Apr 22–25, 2014.

Workshop on Software Correctness and Reliability. Zurich, Switzerland. Oct 4–5, 2013.

LASER summer school on Innovative Languages for Software Engineering. Elba, Italy. Sep 2–8, 2012.

VSCOMP'12 Verified Software Competition (**bronze medal**). Nov 8–10, 2011.

1st VerifyThis Verification Competition. Turin, Italy. Oct 4, 2011.

LASER summer school on Tools for Practical Software Verification. Elba, Italy. Sep 4–10, 2011.

LASER summer school on Empirical Software Engineering. Elba, Italy. Sep 5–11, 2010.

VSCOMP'10 Verified Software Competition. Edinburgh, Scotland. Aug, 2010

SICSA Summer School on Formal Reasoning & Representation of Complex Systems. Edinburgh, Scotland. Aug 14–15, 2010.

LASER summer school on Concurrency and Correctness. Elba, Italy. Sep 7–13, 2008.

Professional Activities

Program Co-chair, iFM'17

Program Committee member: OOPSLA'18, POPL'18, CAV'17, APLAS'16, FTfJP'16, SYNT'16, VSTTE'16, TAP'16, iFM'16, FESCA'16, VMCAI'16, PSI'15, FTfJP'15, FESCA'15, RV'14, FESCA'14

Artifact Evaluation Committee member: POPL 2017, ESEC/FSE 2015

Journal reviewer: ACM Transactions on Programming Languages and Systems, Journal of Functional Programming, Formal Aspect of Computing

Tutorials chair and **Proceedings chair**, RV 2014

Deputy general chair, ESEC/FSE 2013

Publicity chair: LASER Summer School 2011–2014, SEAFOOD 2010