

MICHAŁ JAN MOSKAL

CURRICULUM VITAE, VERSION 3.0

Brabanstr. 20
52070 Aachen
Germany



Tel.: +48 691 20 22 33 (Poland)
+49 15207845785 (Germany)
E-Mail: michal.moskal@nemerle.org
Home page: <http://nemerle.org/~malekith/>
<http://research.microsoft.com/~moskal/>
Born: January 30, 1981
Citizenship: Polish

Education

Sep 1996–May 2000 Second High School in Kędzierzyn-Koźle, mathematics–informatics profile.
Oct 2000–Jul 2005 Wrocław University, Wrocław. Mathematics and Computer Science Department, Computer Science Institute. MSc studies. Received the Ministry of The National Education and Sport scholarship during 2003–2005.
Jun 2005–Jan 2010 PhD studies at the same place. My advisor is prof. Leszek Pacholski.

Employment

May 31–Aug 18 2006 Internship at Microsoft Research, Redmond, WA. Improving the Zap theorem prover on program verification queries (up to two orders of magnitude faster, during three months). Work supervised by Madan Musuvathi, Shuvendu Lahiri and Rustan Leino.
Feb 19–Jul 6 2007 Internship at University College, Dublin. Designing and implementing ESC/Java2 sorted prover back-end; integrating Fx7 prover with ESC/Java2. Work supervised by Joseph R. Kiniry.
Jul 16–Dec 23 2007 Internship at Microsoft Research, Redmond, WA. Aximatization of the C semantics in the VCC compiler. Work supervised by Wolfram Schulte, Rustan Leino and Nikolaj Bjørner.
Jan 14 2008–now European Microsoft Innovation Center, Aachen, Germany. Still working on the VCC project. My managers are Thomas Santen and Wolfram Schulte.

Languages Polish, English, basics of German.

Professional Interests

Program verification and Satisfiability Modulo Theories (automated theorem proving for verification).

Programming languages and type theory.

Publications

Sep 2009 **HOL-Boogie: An interactive prover-backend for the Verifying C Compiler.**

- Sascha Böhme, Michał Moskał, Wolfram Schulte, Burkhart Wolff.*
Journal of Automated Reasoning, 2009, to appear.
On plugging Isabelle/HOL as a proof engine for VCC.
- Aug 2009 **VCC: A Practical System for Verifying Concurrent C.**
Ernie Cohen, Markus Dahlweid, Mark Hillebrand, Dirk Leinenbach, Michał Moskał, Thomas Santen, Wolfram Schulte, Stephan Tobies.
22nd International Conference on Theorem Proving in Higher Order Logics (TPHOLs 2009). (LNCS 5674).
General system description. Wolfram’s invited talk.
- Aug 2009 **Programming with Triggers.**
Michał Moskał.
Satisfiability Modulo Theories workshop 2009, Montreal. To appear.
E-matching triggers are described as a logic programming language. Common triggering patterns and experience report about using SMT for real-world verification.
- Jun 2009 **A Precise Yet Efficient Memory Model For C.**
Ernie Cohen, Michał Moskał, Wolfram Schulte, Stephan Tobies.
4th International Workshop on Systems Software Verification (SSV2009).
On a typed memory model, which allows to reason about C programs as if they were written in a type-safe object-oriented language.
- May 2009 **VCC: Contract-based Modular Verification of Concurrent C.**
Markus Dahlweid, Michał Moskał, Thomas Santen, Wolfram Schulte, Stephan Tobies.
Research demo at ICSE 2009.
- Feb 2009 **A Practical Verification Methodology for Concurrent Programs.**
Ernie Cohen, Michał Moskał, Wolfram Schulte, Stephan Tobies.
Microsoft Research Tech. Report MSR-TR-2009-15.
The main methodology paper. Still has ongoing work on it.
- Jul 2008 **Vx86: x86 Assembler Simulated in C Powered by Automated Theorem Proving.**
Stefan Maus, Michał Moskał, Wolfram Schulte.
12th International Conference on Algebraic Methodology and Software Technology, AMAST 2008 (LNCS 5140).
How to verify x86 assembly by “emulating” it in C.
- Oct 2007 **Rocket-fast proof checking for SMT solvers.**
Michał Moskał.
14th International Conference Tools and Algorithms for the Construction and Analysis of Systems, TACAS 2008.
On using term rewriting as an efficient proof engine.
- Sep 2007 **Edit & Verify.**
Radu Grigore, Michał Moskał.
First-order Theorem Proving workshop 2007, Liverpool, UK.
During incremental program verification we get many similar formulas, that need to be proven. We show how to simplify the new ones with respect to the old ones, that are already proven.
- Aug 2007 **Reachability Analysis for Annotated Code .**
Mikolas Janota, Radu Grigore, Michał Moskał.
Specification and Verification of Component-Based Systems, 2007, Cavtat, Croatia.
On smoke-testing soundness of assumptions in program annotations.
- Jul 2007 **Fx7 or In Software, It Is All About Quantifiers .**
Michał Moskał.

Satisfiability Modulo Theories Competition 2007, Berlin.

Fx7 system description, the solver was second in the AUFLIA division.

Jul 2007

E-Matching for Fun and Profit.

Michał Moskał, Jakub Łopuszański, Joseph R. Kiniry.

Satisfiability Modulo Theories workshop 2007, Berlin. Later in Vol. 198, Issue 2 of Electronic Notes in Theoretical Computer Science, Elsevier.

E-matching is used in quantifier instantiation in SMT solvers.

Jun 2004-2005

Type Inference with Deferral.

Michał Moskał.

MSc thesis, University of Wrocław, Poland.

About type inference for nominal type systems with subtyping, parametric polymorphism and overloading. Submitted on June 27th, 2005.

Languages and Verification

Oct 2000

Kelpie. An object oriented, somewhat inspired by C++ language. It was thought as tool to write RPG games. Compiler and virtual machine. Written in C. GPL.

Sep 2001

Ksi. Lispy in syntax, C-ish in semantics, 1:1 interface to the trees used internally in the GNU Compiler Collection (GCC). Compiler is a front end for GCC. Maintained until October 2003. Written in C. GPL.

Nov 2001

Gont¹. Language with C-like syntax, parametric polymorphism, type inference, garbage collection and higher order functions. Targets Ksi and C (in fact a common subset of C and C--). Written in Gont (first stage compiler was once written in OCaml). Bootstrapped in Summer 2002. BSD.

Dec 2002

ET version 2. An interpreter for a language invented by Zdzisław Szławiński. The language has a strong normalization property, a type system and syntax similar to ML, semantics given by λ_2 translation. It also has interesting connections with the proof theory. BSD.

Jan 2003–Jul 2007

Nemerle². A functional and object-oriented language for the .NET platform. Project leader. In March 2004 the project was awarded a grant by Microsoft Research³.

Dec 2005–Jul 2007

Fx7⁴ – Satisfiability Modulo Theories solver, using an embed SAT solver. The solver was second in the AUFLIA division of the 2007 SMT competition.

Jul 2007–now

VCC⁵, a sound verifier for concurrent C using automatic SMT solving. Main developer, first at Microsoft Research and then at the European Microsoft Innovation Center. VCC supports ownership and modular reasoning about concurrency, including the primitives. It is used to formally verify a large chunk of operating-system level code — the Microsoft Hypervisor.

Private Interests

Science fiction, photography, music, movie, mountain hiking.

Aachen, Germany, September 9th, 2009

¹<http://nemerle.org/~malekith/gont/>

²<http://nemerle.org/>

³This was the first grant awarded by Microsoft for research activity in Poland.

⁴<http://nemerle.org/fx7/>

⁵<http://vcc.codeplex.com/>