

BENJAMIN WERNER

Born on june the 10th 1966 in Munich (Germany)

LIX , Ecole Polytechnique,
91128 PALAISEAU cedex
tel: 01 69 33 41 41
Fax: 01 69 33 46 03

42 bis rue Antoine Thomas
94200 IVRY-SUR-SEINE
tel: 06 63 53 43 44

E-mail: benjamin.werner@inria.fr
URL: <http://benjamin.werner.name>

Current responsibilities

- Researcher at INRIA, scientific leader of the INRIA project-team Typical. This team is central to the development of Coq, and is hosted by the *Laboratoire d'Informatique de l'École Polytechnique (LIX)*.
- I am member of the team Mathematical Components from the INRIA and Microsoft Research joint research centre.
- I am part-time *Professeur Chargé de Cours* at École Polytechnique.

Diplomas

- PhD (*Thèse de Doctorat*), Université Denis-Diderot. Defended may 2nd 1994. The jury was Serge Grigorieff (president), Jean-Pierre Jouan-
naud and Jean Gallier (referees), Christine Paulin-Mohring (advisor),
Gérard Huet and Jean-Louis Krivine. *Magna cum laude*.
- D.E.A. (MSc) *Informatique Mathématique et Applications* Ecole Poly-
technique and D.E.A. *Logique et Fondements des Mathématiques*,
Université Denis-Diderot, Paris, 1990.
- Graduation from Ecole Polytechnique (promotion X86), 1989.
- French-German Baccalaureate, 1984.

Employements

- 1994–present, Chargé de Recherches INRIA. In Rocquencourt from 1994 to 2002; in Polytechnique since.
- 1994, Post-doc (employed by INRIA) in Cornell (Pr. Constable) and Ryukoku University (Pr. Hayashi, Kyoto, Japan).
- 1989-1993, Graduate scholarship.
- 1986-1989, student Ecole Polytechnique.

Studies

- 1984–1986, Classes Préparatoires, Lycée Hoche, Versailles.
- 1986–1989, École Polytechnique.
- 1989–1990, Student at Université Denis-Diderot (DEA *Logique et Fondements de l'Informatique* et de l'École Polytechnique (DEA *Informatique Mathématique et Applications*)).
- 1990–1994, PhD student at Université Denis-Diderot (Paris 7) in computer science, advised by Christine Paulin-Mohring.

Teaching

Since september 2007, I am *Professeur Chargé de Cours* at École Polytechnique.

I have been responsible for a Master's course at DEA SPP and then the MPRI Master since their creations in 1997.

I have given courses at several European TYPES summer schools and several French graduate schools. I have been invited to teach type theory and Coq at the universities of Bologna, La Coruña and Kobe.

I have taught Coq and formal methods for undergraduate at french *grandes école* ENSTA between 1997 and 2005. 2005.

I have taught programming at Ecole Polytechnique and CNAM.

Administrative responsibilities

- Since 2008, I am scientific leader of the INRIA project-team TypiCal. Since 2006, I had been practically leading the INRIA LogiCal project.
- I coordinate the *proofs and numbers* activity in the *Mathematical Components* of the INRIA-MSR joint research centre.
- I am elected member of INRIA's scientific counsel (mandate until 2010).
- I was elected member of INRIA's Evaluation Commission from 2002 to 2005.
- I have been member of the recruiting committee of *École Normale Supérieure* for computer science since 2000.
- I was member of the recruiting committee of *Université de Paris-12 Créteil* for computer science from 2001 to 2006.
- I coordinated INRIA sites and subsites for the European coordination action TYPES.
- I was coordinating my team's involvement in french research actions CFC (*Calcul Formel Certifié*) and MAO (*Mathématiques sur Ordinateur*).

Visibility

In relation to my involvement in the formal proof of the four-color theorem and to the INRIA-MSR joint centre, I was quoted or mentioned in several mainstream or scientific medias; among others: Le Monde, New Scientist, The Register, Le Figaro, Science et Vie, La Recherche, Le Télégramme de Brest, ...

I was interviewed on Radio-France International en 2007.

Conferences

- I co-organized the TYPES 2004 conference and co-edited the Springer LNCS proceedings with Christine Paulin-Mohring and Jean-Christophe Filliâtre.

- I was invited to give hold the seminar of the Physics Department of the *Ecole Normale Supérieure* in february 2008.
- I gave an invited talk at the conference in honor of André Hirschowitz in 2005 in Nice (four-color theorem).
- I gave an invited talk at the Calculemus Conference in 1998 (on the formalization of Buchberger's algorithm in Coq).
- I was PC member FLOPS 2008 and JFLA 2001 and 2007.
- With Benjamin Grégoire and Laurent Théry I organized the Workshop on Numbers and Proofs in june 2006.

PhD committes

Apart from the PhD's I advised (Bruno Barras, David Delahaye et Benjamin Grégoire), I was a referee for the PhD's of Sylvain Boulmé (Paris 6, advisor Thérèse Hardin), of Laurent Chikli (Nice, advisor André Hirschowitz), Gilberto Perez-Vega (University of la Coruña) and Vincent Bernat (advisor Hubert Comon-Lundh). I was also member of the PhD committees of Fabrice Barbier (Evry, advisor Marc Aiguier) and Assia Mahboubi (Nice, advisor Loïc Pottier).

PhD advisor

Bruno Barras. Defended 1999. Bruno is now INRIA researcher.

Sujet: Self-Valisation of a proof system with inductive families, *Auto-validation d'un systeme de preuves avec familles inductives*.

This PhD was about validating Coq's proof-checking kernel using Coq itself. This is the critical part of the proof system, which is thus essential for the trust one can have in the formal proofs themselves. Bruno formalized most of the metatheory of Inductive Constructions in Coq. This work remains today the most impressive in the field.

David Delahaye. Defended in 2001. David is now assistant professor at *Conservatoire National des Arts et Métiers*.

Sujet: An extensible proof-language for Coq, *Conception de langages pour décrire les preuves et les automatisations dans les outils d'aide à la preuve: une étude dans le cadre du système Coq.*

This PhD proposed a new proof-language for Coq which allows the user to dynamically create new proof tactics. This work is part of Coq today.

Benjamin Grégoire. Co-advised (50-50) with Xavier Leroy. Benjamin is now INRIA researcher at Sophia-Antipolis.

Sujet: Compilation of proof-terms: a (new) marriage between Coq and Caml, *Compilation des termes de preuves: un (nouveau) mariage entre Coq et Ocaml.*

This work remains particularly important for coq. Benjamin used compilation techniques used for Caml (thus the co-advising with Xavier Leroy) to accelerate the execution of programs inside Coq. This feature today gives Coq an, often decisive, advantage over comparable systems. In his work, Benjamin showed how to extend ML's execution mechanism to open terms. He also constructed a formal verification of these new mechanisms.

Roland Zumkeller. Defence expected 2008.

Sujet: Verification in Coq of inequalities used in the proof of the Kepler conjecture.

In 1998, Thomas Hales proposed a proof of the Kepler conjecture, which had been withstanding the efforts of mathematicians for 400 years. This proof involves several complex computations which can only be performed by machines. As a consequence, this proof was reluctantly accepted by the mathematical community; in turn Hales decided to launch an effort to formally check it. Roland contributes to this effort by focusing on the most computational part: a set of about 2000 inequalities involving six real variables, which can be checked using techniques of numerical optimization.

This work is emblematic for the use of computations on (formal) proofs.

Arnaud Spiwack. Started in 2006 jointly at Polytechnique and Chalmers University (Göteborg, Sweden); co-advised with Thierry Coquand.

Other Advising

Post-doc

Gyesik Lee, in 2006-2007 on the set-theoretical semantics of Coq.

Guillamue Melquiond since 2007, on the construction of an efficient floating point number library for Coq.

Master's theses

Samuel Boutin (with Gérard Huet), Bruno Barras, David Delahaye, Benjamin Grégoire, Clément Renard, Roland Zumkeller, Arnaud Spiwack.

Publications

Editor for conference proceedings

- Jean-Christophe Filliâtre, Christine Paulin-Mohring et Benjamin Werner. *Types for Proofs and Programs, International Workshop, TYPES 2004, Jouy-en-Josas, France, December 15-18, 2004, Revised Selected Papers*. Lecture Notes in Computer Science 3839, Springer-Verlag, 2005.

International Journals

- Gilles Dowek et Benjamin Werner. Proof Normalization Modulo. *Journal of Symbolic Logic*, volume 68(4), pages 1289-1316, 2003.
- Christine Paulin-Mohring et Benjamin Werner. Synthesis of ML Programs in the System Coq. *Journal of Symbolic Computation*. Volume 15 (5/6), pages 607-640, 1993.
- Benjamin Werner. On the strength of proof-irrelevant type theories. A paraître dans *Logical Methods in Computer Science*. 19 pages, 2008.

International refereed conference with published proceedings

1. François Garillot et Benjamin Werner. Simple types in Type Theory: deep and shallow encodings. *Theorem Proving in higher-Order Logics, 2007*, Kaiserslautern, Allemagne, septembre 2007. Pages 368-382, Lecture Notes in Computer Science 4732, Springer-Verlag, 2007.
2. Benjamin Werner. On the strength of proof-irrelevant type theories. *Proceedings of the Third International Joint Conference, IJCAR 2006, 2006*, Seattle, WA, USA, August 17-20, pages 604-618, Lecture Notes in Artificial Intelligence 4130, Springer-Verlag, 2006. *Acceptation rate 30%*.
3. Benjamin Grégoire, Laurent Théry et Benjamin Werner. A Computational Approach to Pocklington Certificates in Type Theory. *Functional and Logic Programming, 8th International Symposium, FLOPS 2006, Fuji-Susono, Japan, April 24-26, 2006, Proceedings*, pages 97-113, Lecture Notes in Computer Science 3945, Springer-Verlag, 2006. *Acceptation rate 33%*.
4. Alexandre Miquel and Benjamin Werner. The Not So Simple Proof-Irrelevant Model of CC. *Proceedings of TYPES 2002*, pages 240-258, Lecture Notes in Computer Science 2646, Springer-Verlag, 2002.
5. Benjamin Werner. Sets in Types, Types in Sets. *Theoretical Aspects of Computer Software, Third International Symposium, TACS '97*, Sendai, Japan, September 23-26, 1997. Lecture Notes in Computer Science 1281, Springer-Verlag, 1997. *Acceptation rate 43%*
6. Paul-André Melliès et Benjamin Werner. A Generic Normalisation Proof for Pure Type Systems. *Proceedings of TYPES 1996*. Lecture Notes in Computer Science 1512, Springer-Verlag, 1998. *Acceptation rate about 50%*
7. Gilles Dowek et Benjamin Werner. Arithmetic as a theory modulo. *Term Rewriting and Applications, 16th International Conference, RTA 2005*, Nara, Japan, April 19-21, 2005. Lecture Notes in Computer Science 3467, Springer-Verlag, 2005. *Acceptation rate 39%*.
8. Martin Abadi, Georges Gonthier et Benjamin Werner. Choice in dynamic linking. *Foundations of Software Science and Computation*

Structures, 7th International Conference, FOSSACS 2004, Barcelona, Spain, March 29 - April 2, 2004. Lecture Notes in Computer Science 2987, Springer-Verlag, 2004. *Acceptation rate 24%*.

9. Herman Geuvers et Benjamin Werner. On the Church-Rosser Property for Expressive Type Systems and its Consequences for their Metatheoretic Study. *Proceedings, Ninth Annual IEEE Symposium on Logic in Computer Science*, 4-7 July 1994, Paris, France. IEEE, 1994. *Acceptation rate about 25%*
10. Gilles Dowek et Benjamin Werner. Proof Normalization Modulo. *Proceedings of TYPES'98*, Kloster Irsee, Germany, March 27-31, 1998, Selected Papers. Lecture Notes in Computer Science 1657, pages 62-77, Springer Verlag, 1999.

French book chapters

- Benjamin Werner. La Vérité et la Machine. Dans *Images des Mathématiques 2006*, édité par Jacques Istas et Étienne Ghys, pages 161-168, CNRS.

Unpublished or submitted

- Gilles Dowek et Benjamin Werner. A constructive proof of Skolem theorem for constructive logic. Submitted.
- Gilles Dowek, Gérard Huet et Benjamin Werner. On the eta-long form in type systems of the cube. Not published but often cited.
- Samuel Lacas et Benjamin Werner. Which Choices imply the Excluded Middle. Not published but often cited.
- Bruno Barras et Benjamin Werner. Coq in Coq. Revision.
- Gilles Dowek et Benjamin Werner. A constructive proof of Skolem theorem for constructive logic (manuscript).
- Gilles Dowek et Benjamin Werner. An inconsistent theory modulo defined by a confluent and terminating rewrite system, manuscript, 2000.

Formal Proofs in Coq

- Strong Normalization of the Calculus of Constructions (with B. Baras).
- Correction of Buchberger's Algorithm (with G. Perez Vega).
- Formalisation of Zermelo-Fränkel set theory in Coq.
- Four Color Theorem (main author: G. Gonthier).
- Correction of normalization by Evaluation.

Others

Bilingual French and German. Fluent English. Reasonably good spoken Japanese.