

## BENJAMIN WERNER

Né le 10 juin 1966 à Munich (Allemagne)

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](mailto:benjamin.werner@inria.fr)  
URL: <http://benjamin.werner.name>

### Responsabilités actuelles

- Chargé de Recherches INRIA, co-responsable de l'équipe-projet INRIA *LogiCal* au Laboratoire d'Informatique de l'École Polytechnique (LIX).
- Membre du centre de recherche joint entre l'INRIA et Microsoft Research.
- Professeur Chargé de Cours à l'École Polytechnique.

### Titres et diplômes

- Thèse de Doctorat, Université Denis-Diderot. Soutenue le 2 mai 1994 devant Serge Grigorieff (président), Jean-Pierre Jouannaud et Jean Gallier (rapporteurs), Christine Paulin-Mohring (directrice), Gérard Huet et Jean-Louis Krivine. Mention Très Honorable avec Félicitations du Jury.
- D.E.A. *Informatique Mathématique et Applications* Ecole Polytechnique et D.E.A. *Logique et Fondements des Mathématiques*, Université Denis-Diderot, Paris, 1990.
- Diplôme d'Ingénieur de l'Ecole Polytechnique (promotion X86), 1989.
- Baccalauréat Franco-Allemand, 1984.

## Parcours

- 1994–présent, Chargé de Recherches INRIA. Promotion à la première classe en 1997. A Rocquencourt de 1994 à 2002; sur le plateau de Saclay depuis.
- 1994, Post-doc (employé par l'INRIA) à Cornell (Pr. Constable) et Ryukoku University (Pr. Hayashi, Kyoto, Japon).
- 1989-1993, Bourse DEA puis thèse (DRET).
- 1986-1989, Elève de l'École Polytechnique.

## Études

- 1984–1986, Classes Préparatoires au Lycée Hoche à Versailles.
- 1986–1989, Élève de l'École Polytechnique.
- 1989–1990, Étudiant de l'Université Denis-Diderot (DEA *Logique et Fondements de l'Informatique* et de l'École Polytechnique (DEA *Informatique Mathématique et Applications*)).
- 1990–1994, Inscrit en Thèse à l'Université Denis-Diderot (Paris 7) en thèse d'Informatique sous la direction de Christine Paulin-Mohring.

## Enseignement

Je suis depuis septembre Professeur Chargé de Cours à l'École Polytechnique.

J'ai été responsable de cours dans le DEA SPP puis le Master MPRI tout au long de leur existence (depuis 1997).

J'ai donné des cours à plusieurs École d'été européennes TYPES et plusieurs Écoles des Jeunes Chercheurs. J'ai été invité à donner un cours de Théorie des Types et de Coq à l'Université de Bologne, l'Université de La Corogne et l'Université de Kobe.

J'ai assuré des cours de méthodes formelles à l'ENSTA entre 1997 et 2005.

J'ai effectué des TD à l'École Polytechnique et au CNAM.

## Responsabilités administratives

- Depuis janvier 2008, je suis responsable scientifique de l'équipe-projet TypiCal. Depuis 2006, je dirigeais dans les faits le projet LogiCal de l'INRIA.
- Je coordonne l'activité "Preuves et Nombres" au sein de l'action *Mathematical Components* du Centre de Recherche Commun INRIA-Microsoft Research.
- Je suis membre du Conseil Scientifique de l'INRIA (mandat jusqu'en 2010).
- J'ai été membre de la Commission d'Evaluation de l'INRIA (l'équivalent du Comité National) de 2002 à 2005.
- Je suis membre de la Commission de Spécialistes (Informatique) de l'École Normale Supérieure (rue d'Ulm) depuis 2000.
- J'ai été membre de la Commission de Spécialistes (Informatique) de l'Université de Paris-12 Créteil, de 2001 à 2006.
- Je coordonne la participation à l'action européenne TYPES des équipes de l'INRIA-Futurs, l'INRIA-Sophia Antipolis, de Minho (Portugal), Bologne (Italie) et Dassault-Aviation.
- J'ai été correspondant dans mon projet de l'ACI MAO (Mathématiques sur Ordinateur) et je l'ai été pour l'ERC CFC (Calcul Formel certifié).

## Visibilité

En rapport avec ma participation à la preuve formelle du théorème des quatre couleurs en Coq, ainsi que de ma participation au Centre de Recherche Commun INRIA-Microsoft Research, j'ai été cité ou mentionné dans divers titres de la presse généraliste ou scientifique grand public; entre autres dans Le Monde, Le Figaro, Science et Vie, La Recherche, Le Télégramme de Brest, New Scientist, The Register. . .

Je suis intervenu sur Radio-France International en 2007.

## Conférences

- J'ai co-organisé la conférence TYPES 2004 à Jouy-en-Josas. J'ai co-édité les actes dans la collection Lecture Notes in Computer Science avec Christine Paulin-Mohring et Jean-Christophe Filliâtre.
- Invité au séminaire du Département de Physique de l'École normale Supérieure, février 2008.
- Exposé invité à la conférence pour les 61 ans d'André Hirschowitz en 2005 à Nice (sur la formalisation de la preuve du théorème des quatre couleurs en Coq).
- Exposé invité à la conférence Calculemus (Calcul Formel et Logique), à Eindhoven en 1998 (sur la formalisation en Coq de l'algorithme de Buchberger et de sa preuve de correction).
- Je suis membre du comité de programme de FLOPS 2008 (Japon, actes publiés par Springer).
- J'ai été membre du Comité de Programme des Journées Francophones des Langages Applicatifs en 2001 et 2007.
- J'ai organisé avec Benjamin Grégoire et Laurent Théry le *Workshop on Numbers and Proofs* les 12 et 13 juin 2006 à Orsay, avec le support de Working Group Européen TYPES et du Centre de Recherche Commun entre l'INRIA et Microsoft Research.

## Jurys de Thèses

En dehors des thèses que j'ai (co-)encadrées (Bruno Barras, David Delahaye et Benjamin Grégoire), j'ai été rapporteur des thèses de Sylvain Boulmé (Paris 6, directrice Thérèse Hardin), de Laurent Chicli (Nice, directeur André Hirschowitz), de Vincent Bernat (Cachan, directeur Hubert Comon-Lundh) et de Gilberto Perez-Vega (Université de la Corogne). J'ai également fait partie des jurys de thèse de Fabrice Barbier (Evry, directeur Marc Aiguier) et Assia Mahboubi (Nice, directeur Loïc Pottier).

## Thèses encadrées

**Bruno Barras.** Thèse soutenue en 1999. Bruno est maintenant Chargé de Recherche à l'INRIA.

Sujet: *Auto-validation d'un système de preuves avec familles inductives.*

Cette thèse portait sur la validation en Coq du noyau de Coq lui-même. Le noyau du système de preuves est la partie du logiciel qui vérifie que la preuve formelle construite se conforme bien aux règles du formalisme logique. C'est donc la *partie critique* pour la confiance que l'on peut accorder au système. Dans cette thèse Bruno a donc formalisé l'essentiel de la méta-théorie des Théories des Types telles que celle implémentée dans Coq. Cette thèse reste, après plusieurs années, un sommet du genre.

**David Delahaye.** Thèse soutenue en 2001. David est maintenant Maître de Conférences au Conservatoire National des Arts et Métiers.

Sujet: *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.*

Cette thèse proposait un nouveau langage de description de preuves formelles pour Coq. Ce langage permet à l'utilisateur de créer dynamiquement de nouvelles "tactiques" de preuves. Par ailleurs, la sémantique du langage était formellement décrite. Le contenu de la thèse fait toujours partie du langage de preuves implémenté dans Coq. C'était une des premières thèses du genre.

Cette thèse a été co-encadrée nominalement par Christine Paulin-Mohring.

**Benjamin Grégoire.** Thèse co-encadrée (50-50) avec Xavier Leroy. Benjamin est maintenant Chargé de Recherches à l'INRIA Sophia-Antipolis.

Sujet: *Compilation des termes de preuves: un (nouveau) mariage entre Coq et Ocaml.*

Cette thèse reste particulièrement importante pour Coq. Benjamin a utilisé les techniques de compilation utilisées pour Caml (d'où le co-encadrement avec Xavier Leroy) pour accélérer l'exécution de programmes à l'intérieur de Coq. C'est cette caractéristique qui donne aujourd'hui à Coq un avantage souvent décisif sur ses concurrents. Dans cette thèse, Benjamin montre

comment étendre le mécanisme d'exécution de Caml à des termes ouverts. Il propose également des certification formelles (en Coq) de ces nouveaux mécanismes d'exécution.

**Roland Zumkeller.** Thèse débutée en 2003.

Sujet: *Vérification en Coq des inégalités réelles intervenant dans la preuve de la conjecture de Kepler.*

En 1998, Thomas Hales a proposé une preuve de la conjecture de Kepler, qui résistait aux efforts des mathématiciens depuis près de 400 ans. Cette preuve repose sur un certain nombre de calculs complexes qui ne peuvent être effectués que par un ordinateur. En conséquence, cette preuve a été difficilement acceptée par la communauté mathématique ce qui a conduit Hales à démarrer un effort de formalisation de sa preuve, sur le modèle de ce qui a été fait pour le théorème des quatre couleurs. Roland participe à cet effort en se concentrant sur la partie la plus calculatoire de cette preuve: un ensemble d'environ 2000 inéquations réelles à 6 inconnues, qui peuvent être vérifiés par des techniques d'optimisation numérique. Il s'agit donc de coder les algorithmes correspondants en Coq de manière exécutable et de faire la preuve de leur correction. Ce travail est en bonne voie et a déjà fait l'objet d'une publication.

Cette thèse est actuellement nominalement co-encadrée par Gilles Dowek.

**Arnaud Spiwack.** Thèse démarrée en 2006 en co-tutelle avec l'Université Chalmers de Göteborg en Suède; co-encadré (50-50) avec Thierry Coquand.

## **Autres Encadrements**

### **Post-doc**

**Gyesik Lee**, en 2006-2007 sur la sémantique ensembliste de Coq.

**Guillamue Melquiond** depuis 2007, sur la construction d'une bibliothèque de nombres flottants efficaces en Coq.

## DEA et Master

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

## Publications

### Édition d' Actes de Conférences

- 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.

### Articles de Revues Internationales

- 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.

### Articles de Conférences Internationales avec Comité de Programme

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. *Taux d'acceptation* 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. *Taux d'acceptation* 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. *Taux d'acceptation* 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. *Taux d'acceptation estimé* 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. *Taux d'acceptation: 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. *Taux d'acceptation* 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. *Taux d'acceptation estimé: env. 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.

### **Chapitre d'ouvrage en Français**

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

### **Manuscrits et articles soumis**

- Gilles Dowek et Benjamin Werner. A constructive proof of Skolem theorem for constructive logic. Soumis.
- Gilles Dowek, Gérard Huet et Benjamin Werner. On the eta-long form in type systems of the cube. Non publié mais plusieurs fois cité.
- Samuel Lacas et Benjamin Werner. Which Choices imply the Excluded Middle. Non publié mais plusieurs fois cité.
- Bruno Barras et Benjamin Werner. Coq in Coq. En révision.
- Gilles Dowek et Benjamin Werner. A constructive proof of Skolem theorem for constructive logic (manuscrit).
- Gilles Dowek et Benjamin Werner. An inconsistent theory modulo defined by a confluent and terminating rewrite system, manuscrit, 2000.

### **Preuves formelles en Coq**

- Normalisation forte du calcul des constructions (avec B. Barras).
- Correction de l'algorithme de Buchberger (avec G. Perez Vega).
- Formalisation de la théorie des ensembles de Zermelo-Fränkel en Coq.
- Théorème des quatre couleurs (auteur principal G. Gonthier).
- Correction de la normalisation par évaluation en Coq.

## Présentation du Domaine de Recherches

Le principe fondateur de la *preuve formelle* est qu'un raisonnement mathématique, s'il est totalement détaillé, est lui-même un objet formel dont la correction est définie de manière non-ambiguë par les règles syntaxiques de la logique. Il est donc décidable de vérifier si une preuve formelle est correcte; aussi est-il naturel d'attribuer cette tâche à un ordinateur.

De fait, depuis les premiers *systèmes de preuves* apparus dans les années 1960, il est possible de construire *en pratique* des preuves formelles non triviales. Longtemps néanmoins, la construction de telles preuves était vue comme une activité relativement marginale aussi bien de la part de la communauté mathématique qu'informatique.

Ceci a changé, et continue de changer, avec les progrès des outils et des techniques de formalisation. Parmi les facteurs de progrès, on peut bien sûr citer les progrès de ce que l'on appelle la démonstration automatique. Mais celle-ci est souvent assez peu décisive dans les preuves de grandes tailles. Un facteur important est en revanche l'évolution des formalismes logiques.

Un formalisme est une manière de décrire les "règles du jeu mathématique". Un système de preuves implémente donc un formalisme particulier un peu comme un compilateur implémente un langage de programmation. A partir du moment où l'on construit *effectivement* des preuves dans un formalisme (et non plus seulement *en principe* comme c'est le cas dans les mathématiques informelles) on va demander au formalisme d'être non seulement d'être expressif, mais également pratique: permettre de coller à l'intuition du mathématicien, permettre de construire des preuves aussi concises que possible, être un bon support à l'automatisation des preuves. . .

Le système de preuves Coq implémente un formalisme qui est une variante de ce que l'on appelle la *Théorie des Types*. J'ai travaillé particulièrement sur la justification logique de ces formalismes (preuves de cohérence et de normalisation) et sur des nouvelles techniques de preuve par le calcul, propres à la théorie des types.

J'ai ainsi participé à l'un des succès les plus visibles de la formalisation, avec la preuve formelle du théorème des quatre couleurs (avec Georges Gonthier).

## **Divers**

Bilingue Français et Allemand. Anglais courant. Bon niveau de Japonais à l'oral.