Assistants de preuve
Fondements et applications

Christine Paulin-Mohring

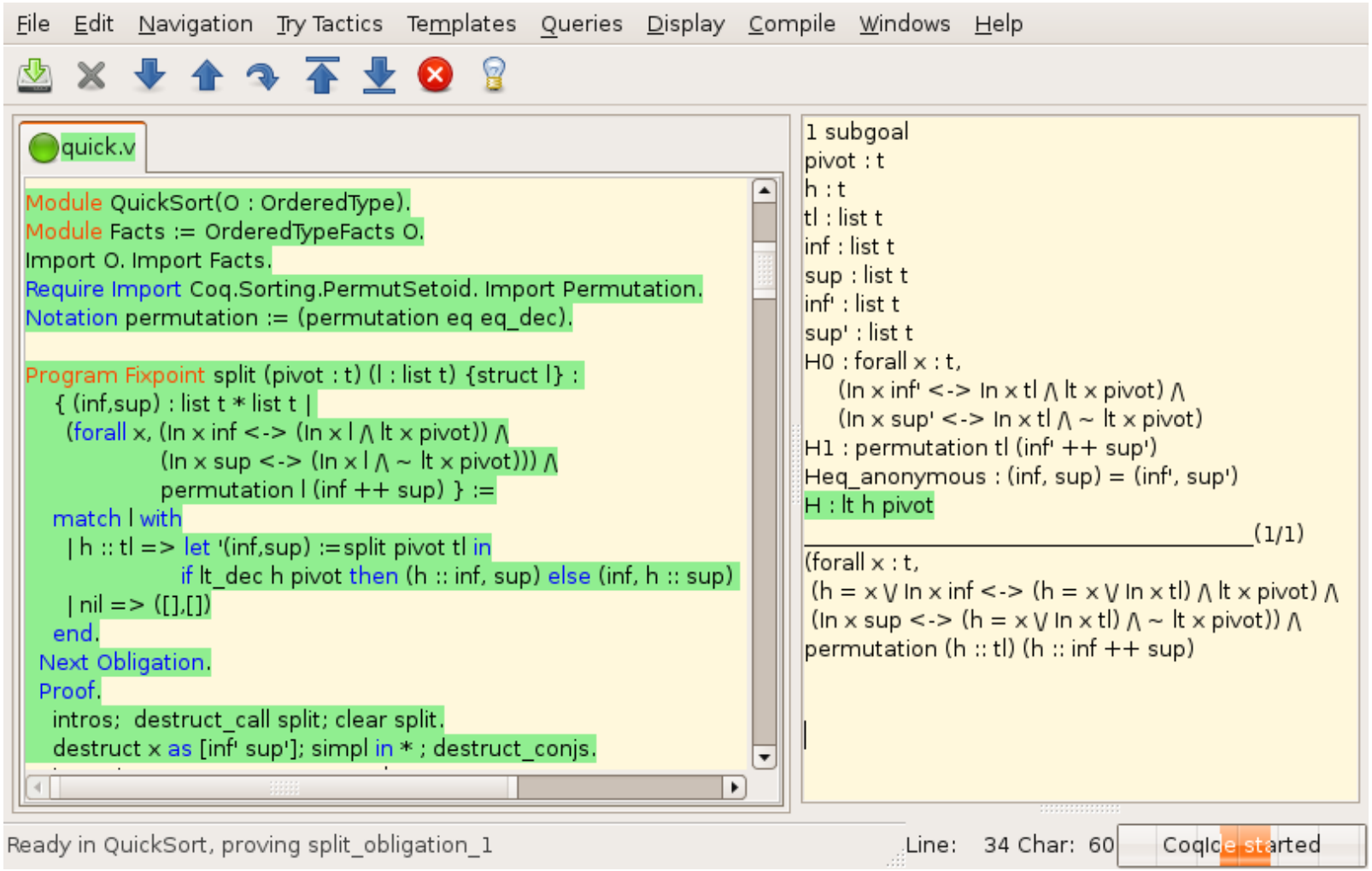
Master Parisien de recherche en Informatique
Master Informatique Université Paris-Sud

18 septembre 2009

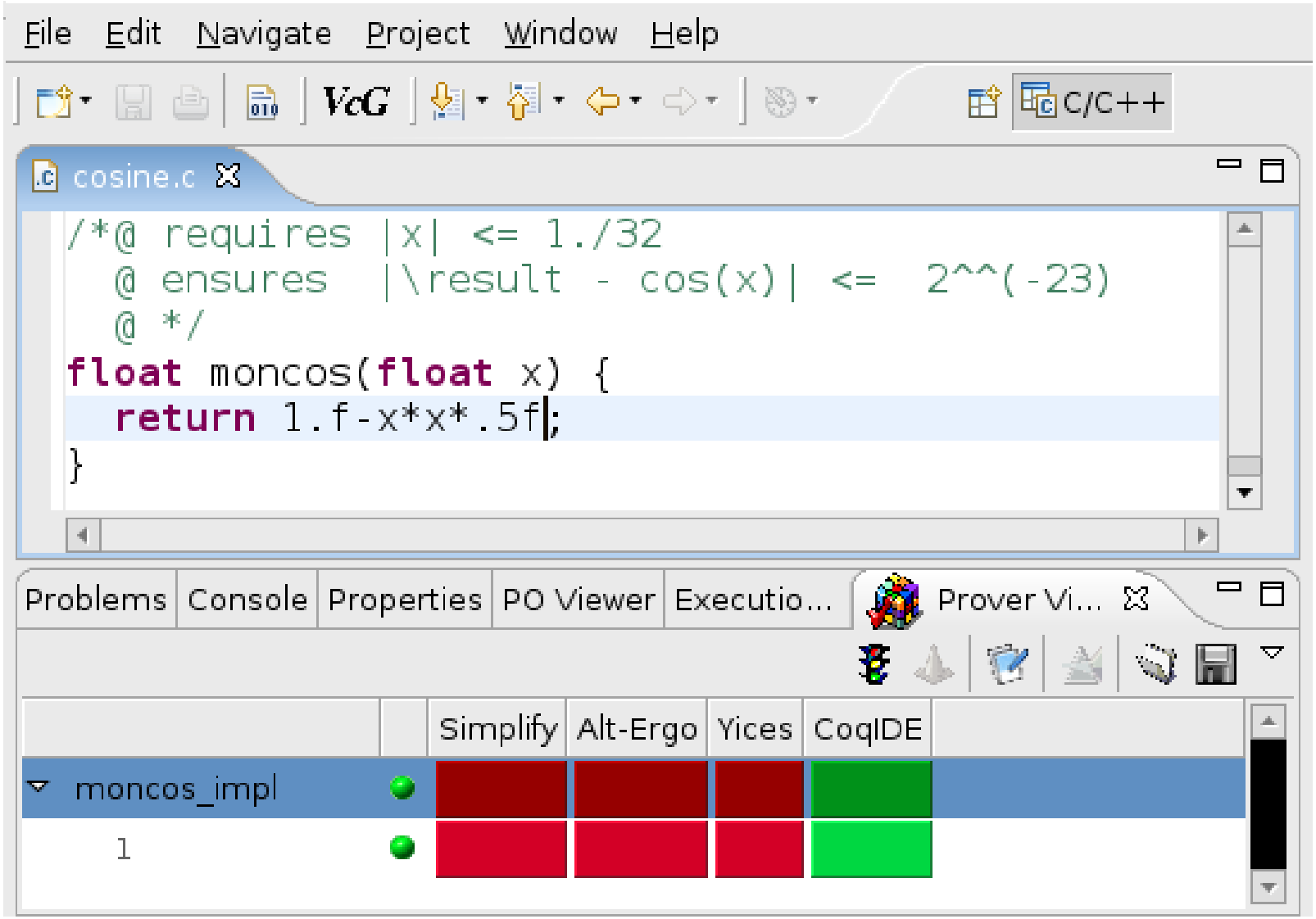
Introduction

- Construire des environnements interactifs pour le raisonnement mathématique
  - Un langage de description mathématique
  - Un moteur de vérification de preuve
  - Des procédures pour automatiser les preuves
- Applications
  - Mathématiques : théorème des 4 couleurs, théorème de Kepler . . .
  - Preuve de programmes : compilateur C optimisant certifié . . .
  - Modélisation informatique : plateforme JavaCard, cryptographie . . .
- Thématiques
  - logique, démonstration automatique, programmation, interfaces . . .

Exemple de preuve Coq



Preuve de programme



Organisation

Deux cours qui se suivent

- Fondements des systèmes de preuve
  - notion de preuve en tant qu'objet mathématique et informatique
  - théorie des types
- Assistants de preuve
  - assistants de preuves en théorie des types
  - applications à la preuve de programmes

- Initiation à l'assistant Coq (mini-projet)
- Equipes dans ce domaine en France
  (Rennes, Nice, Marseille, Bordeaux, Microsoft Research . . .)
  en Europe (Chalmers, Munich Nottingham, Nijmegen, Varsovie, Yale, Harvard . . .)
  et ailleurs

Détails pratiques

- http://www.mpri.master.univ-paris7.fr/
- cours le mardi de 08h45 à 11h45 à Chevaleret
  - Fondements des systèmes de preuve :
    15 septembre-20 novembre
    Gilles Dowek, Sylvie Boldo
  - Assistants de preuve : 24 novembre-12 février
    Christine Paulin-Mohring, Bruno Barras, Guillaume Melquiond
- se faire connaitre auprès des responsables