Application BASTRI
Fiches Equipes

PROVAL (SR0141OR)

Preuve de programmes
LOGICAL (SR0248RR) PROVAL PROVAL (SR0512LR)

Statut: Terminée

Responsable : Christine Paulin

Mots-clés de "A - Thèmes de recherche en Sciences du numérique - 2024" : *Aucun mot-clé.*

Mots-clés de "B - Autres sciences et domaines d'application - 2024" : *Aucun mot-clé.*

Domaine : Algorithmique, programmation, logiciels et architectures
Thème : Programmation, vérification et preuves

Période : 08/09/2005 -> 31/12/2011
Dates d'évaluation : 22/03/2011

Etablissement(s) de rattachement : U. PARIS 11 (P.-SUD), CNRS
Laboratoire(s) partenaire(s) : LRI (UMR8623)

CRI : Centre Inria de Saclay
Localisation : Centre de recherche Inria de Saclay
Code structure Inria : 111029-0

Numéro RNSR : 200518375F
N° de structure Inria: SR0141OR

Présentation

L'objectif de l'équipe-projet de recherche PROVAL est de proposer des méthodes et outils qui s'intègrent dans le cycle de développement de logiciel et qui permettent la production d'un code prouvé correct par rapport à un comportement attendu.

Ce projet, issu de l'équipe-projet LOGICAL, s'appuie sur le formalisme de la théorie des types qui donne un cadre sémantique clair pour représenter en machine les preuves et les calculs.

L'équipe-projet développe un environnement générique de preuve de programmes (Why), qui permet d'engendrer des obligations de preuves qui peuvent être ensuite déléguées à des démonstrateurs automatiques ou interactifs. Sur cet outil, sont construits des environnements dédiés pour prouver des programmes C (Frama-C) et Java (Krakatoa) annotés par des formules décrivant le comportement attendu. L'équipe-projet est également spécialisée dans la preuve de comportement des calculs en nombres flottants.

Axes de recherche

- **Modèles et méthodes de preuve de programmes**
  Nous développons des modèles des langages de programmation et des langages de spécification qui répondent aux besoins des applications critiques et se prêtent à la preuve interactive ou automatique. En particulier, nous nous intéressons à la modélisation de constructions abstraites d'ordre supérieur, de manipulation de pointeurs et de l'arithmétique des nombres flottants.
- **Architecture des environnements de preuves de programmes**
  La mise en pratique de nos méthodes dans les outils pose des problèmes de passage à l'échelle dans la génération d'obligations de preuve, de méthodologie d'écriture d'annotations, d'expressivité des langages de spécifications et d'assistance au développement de spécification.
- **Démonstration automatique**
  La preuve de programmes nécessite d'adapter et de spécialiser des démonstrateurs généraux. L'équipe-projet étudie plus particulièrement les preuves de terminaison ainsi que la combinaison de procédures de décision. Une attention particulière est portée sur la correction de ces techniques.
- **Applications**
  Les techniques développées dans l'équipe-projet trouvent leur application dans les domaines qui requièrent le développement de

Contact

- **Responsable :** Christine Paulin
- **Tél :** 01.72.92.59.05
- **Secrétariat Tél :** 01.74.85.42.80

En savoir plus

- Site de l'équipe
- Site sur inria.fr
- Site du responsable
- Derniers Rapports d'Activité :

Documents sur la structure

- Intranet
- Privés

Décisions

- 4704 (15/12/2005) : création
- 5789 (11/09/2007) : prolongation
- 6074 (19/02/2008) : changement de rattachement
- 7613 (03/01/2011) : prolongation
- 8402 (03/01/2012) : fermeture
- 8339 (19/01/2012) : prolongation

Localisation

- **Adresse postale :** Centre de recherche Inria de Saclay Campus de l'École Polytechnique - Bâtiment Alan Turing 1 rue Honoré d'Estienne d'Orves 91120 Palaiseau France
- **Coordonnées GPS :** 48.714, 2.206

logiciels critiques pour lesquels le besoin de certification est important, en particulier les secteurs bancaires, aéronautique et télécommunications. Nous visons la preuve de code embarqué en C ou en Java ainsi que la certification d'outils de génération de code.

Logiciels

- Why platform
- alt-ergo

Relations industrielles et internationales