

Assistance à la Certification d'Applications Distribuées et Embarquées ACADIE

■ Problématique et résultats

Le développement de logiciels certifiés constitue une demande croissante de l'industrie du logiciel dans la mesure où les systèmes informatiques embarqués deviennent de plus en plus omniprésents dans de multiples domaines. En particulier, le secteur de l'aéronautique et de l'espace, pôle d'excellence de la région Midi-Pyrénées, présente un fort potentiel de développement dans le domaine des applications distribuées et embarquées.

L'équipe ACADIE a donc pour objectif de contribuer à l'amélioration des méthodes et outils de certification des logiciels distribués embarqués.

Pour ce faire, ces thématiques de recherche se développent selon trois axes complémentaires du plus théorique au plus applicatif : théorie des types et de la démonstration, développement et validation de méthodes, modélisation et validation d'algorithmes répartis.

THÉORIE DES TYPES ET DE LA DÉMONSTRATION

Nos travaux de recherche sont essentiellement centrés sur :

- le lambda-calcul et la théorie des types [2349],
- la théorie de la démonstration dans des systèmes logiques non-classiques ;
- les catégories munies de structure additionnelle,
- les applications des méthodes de ces trois domaines en informatique.

Le lambda-calcul et la théorie de types sont utilisés dans une grande majorité des systèmes de preuve. Nous nous intéressons actuellement au contenu calculatoire des théories de types qui contiennent les types inductifs et la récursion, et des méthodes d'incorporer les règles du calcul dans des systèmes de réduction de lambda-termes, ceci peut augmenter considérablement l'efficacité du calcul dans des systèmes de preuve assistée.

Les travaux dans le domaine de la théorie de la démonstration dans des systèmes logiques non-classiques et le domaine des catégories munies de structure additionnelle ont comme objectif l'utilisation directe des preuves dans le calcul formel, notamment, la vérification de la commutativité des diagrammes utilisant les méthodes de la théorie de la preuve [4529].

Ces travaux ont en particulier abouti à des extensions convergentes du lambda-calcul simplement typé avec des types inductifs (thèse D. Chemouil).

PERSONNEL

Directeur de recherche

Pierre Maurice

Chargés de recherche

Mamoun Filali

Ralph Matthes (09/05→), HDR

Professeurs

Jean-Paul Bodeveix

Gérard Padiou

Sergei Soloviev

Maîtres de conférence

Ousmane Koné, HDR

Philippe Mauran

Philippe Quéinnec

Martin Strecker (09/04→)

Doctorants

Freiric Barral

(cotutelle Martin Hoffman, Munich 09/02→)

Rachid Bouaziz (09/04→)

Julien Brunel (09/04→)

Christophe Cubat

dit Cros (09/01→)

David Chemouil (→9/04)

Laurent Mehats (09/01→)

Odile Nasr (09/02→)

Miloud Rached (09/02→)

Florent Peres (cotutelle avec François Vernadat, LAAS 09/04→)

Jean-François Rolland
(09/04→)
Pham Thi Xuan Loc
(→11/04)

Contractuel

Semra Sarpdag (2002)

Collaborateurs occasionnels

Jean-Louis Durieux
Prof. M. Charpentier
(Université de Durham,
New Hampshire, USA)
Prof. A. Flegontov
(SPIIRAN, S. Petersbourg)
Prof. Z. Luo
(Université de Londres)
Dr. Sara Negri
(Université de Helsinki)
Prof. T. Nipkow
(TU Munich)
Prof. V. Orevkov
(Institut de mathématiques,
St. Petersbourg)
Prof. J. von Plato
(Université de Helsinki)
Prof. P. Urzyczin
(Université de Varsovie)
Prof. N. Vasyliov
(Institut de mathématiques,
St. Petersbourg)
Prof. H. Schwichtenberg
(Université de Munich)
Prof. M. van den Brand
(CWI, Amsterdam)

DÉVELOPPEMENT ET VALIDATION DE MÉTHODES

Un des buts de l'équipe est de développer des supports pour la production de logiciels certifiés. Après nous être intéressés aux concepts fournis par des cadres logiques traditionnels tels que HOL, Coq et PVS ou des méthodes formelles telles que B, nous nous intéressons maintenant aux outils pour les systèmes réactifs et temps réel, tels que les langages d'architecture : AADL pour l'avionique et le spatial, les langages de transformation : ATL pour la transformation de modèles et plus généralement les DSL : Bossa pour les ordonnanceurs et SPL pour la téléphonie.

Dans chacune de ces études, nous cherchons à réutiliser voire améliorer les concepts de base offerts par les cadres logiques actuels basés sur la théorie des types ou la théorie des ensembles [3561]. Ainsi, il devient possible de réutiliser des environnements de preuve disponibles pour ces théories.

Il est à noter que cette réutilisation peut être considérée comme à la base de la sûreté de ces outils utilisés dans ces domaines spécifiques et donc de la certification des logiciels produits à l'aide de ces outils.

Nous nous intéressons en particulier aux transformations mises en oeuvre dans le cadre des langages d'architecture pour les systèmes embarqués [5709]. Nous étudions la validation des traductions vers les modèles sémantiques tels que les automates temporisés ou les systèmes de transitions temporels.

Toujours dans le contexte des langages d'architecture, nous nous intéressons à la production de tests à partir des modèles produits lors des différentes phases du processus de développement [5711, 5713].

MODÉLISATION ET VALIDATION D'ALGORITHMES RÉPARTIS

La modélisation et la validation des algorithmes répartis se heurtent au nombre d'états possibles de tels systèmes, nombre souvent infini. Les méthodes de vérification par exploration exhaustive du domaine d'états sont alors impossibles.

Face à ce problème, l'approche adoptée comporte deux aspects complémentaires :

- d'une part, un effort de modélisation : il s'agit de définir des abstractions de haut niveau exprimant la répartition d'un calcul et/ou des données pour en simplifier la description et l'analyse ;
- d'autre part, une démarche de preuve par raffinement : il s'agit, partant d'une solution centralisée du problème, solution plus simple à valider, d'introduire la répartition par raffinements successifs. Chaque raffinement doit bien sûr être validé.

Cette approche a été appliquée à de nombreux algorithmes classiques (exclusion mutuelle, réplique de données, terminaison de calcul diffusant, etc.) ou originaux (observations, vecteurs de chemins) [4494].

■ Prospective

Du point de vue théorique, nous chercherons à rendre plus efficaces les liens entre la preuve et le calcul formel : il s'agira notamment d'étudier des représentations du calcul adaptées aux assistants de preuve.

D'un point de vue méthode, le passage à l'échelle de leur application apparaît comme un problème crucial. La théorie des catégories nous semble une piste intéressante pour aborder ce problème.

Les activités concernant la validation d'algorithmes répartis s'orientent vers un contexte de communication dynamique : validation de construction de groupes dans les réseaux ad hoc par exemple et vers la modélisation et la validation de calculs répartis à base d'agents mobiles [6069].

■ Thèses et habilitations

- **David Chemouil.** Types inductifs, isomorphismes et réécriture extensionnelle. Thèse UPS, 09/2004
- **Pham Thi Xuan Loc.** Adaptation des composants centrée sur l'utilisation, Thèse INPT, 11/2004
- **Ralph Matthes.** Types inductifs au-delà de la stricte positivité. HDR 5/2005

■ Collaborations, contrats et transfert

- Projet RNTL Cotre : Composants temps réel (2002-2004)
- Projets ACI Sécurité Informatique
 - CORSS : Composition et raffinement de systèmes sûrs(2003-2006)
 - DISPO : Formalisation et modélisation du concept de disponibilité (2003-2006)
 - FIACRE : Fiabilité de composants réutilisables (2004-2007)
- Projets STIC CNRS
 - Isomorphisme de types (ISOT 2002)
 - Invertibilité de lambda-termes et ses applications (2004-2005)
 - ARTS - Test de Systèmes Embarqués (2005)
- Projet du pôle de compétitivité Midi-Pyrénées Aquitaine : TOPCASED (Toolkit in Open-source for Critical Application SystEms Development)
- Théorie de types et calcul formel (INRIA - Institut Liapounov)
- Projet européen « Types » (sous-site) (2004-2006)
- Projet Docomo Euro Lab (2005)
- Projet Centre de Coopération Franco-Bavarois (2005)
- Avant-projets FÉRIA
 - DISPO : Logiques pour l'expression et la vérification de politiques de disponibilité (2004)
 - FLUX : Flux multimédias coordonnés (2004)
 - COTRE-AADL : Annexe comportementale pour le standard AADL (2005)
- Action Spécifique n°195 du RTP SECC et du GdR ARP : CAT - Composants et Architectures Temps réel (2004)
- Collaboration avec le CWI (Pays-Bas) : vérification statique de spécifications TLA+ dans l'environnement de réécriture ASF+SDF
- Distribution de FMONA : interface d'ordre supérieur permettant d'exprimer des méthodes de vérification (abstraction, accélération, ...) dans la logique WS1S

■ Animation, gestion et vulgarisation de la recherche

- Comités de programme
 - AFADL Approches Formelles dans l'Assistance au Développement de Logiciels
 - FMPPTA Formal Methods for Parallel Programming : Theory and Applications
 - ICFEM International Conference on Formal Engineering Methods
 - ZB Formal Specification and Development in Z and B
 - WADL'04 Workshop on Architecture Description Languages
 - ETR'05 (école temps réel session langages de description d'architecture)
- Organisation de manifestations
 - DISC'2002 International Symposium on DIStributed Computing
 - WIT2002 Workshop sur l'isomorphisme de Types
 - WADL'04 Workshop on Architecture Description Languages
 - WIT2005 Workshop sur l'invertibilité de lambda-termes et ses applications
 - Journées FAC FÉRIA (annuelles)

RÉFÉRENCES

[2349]

*Sergei Soloviev,
Zhaohui Luo.*

Coercion Completion and Conservativity in Coercive Subtyping. Dans : Annals of Pure and Applied Logic, Elsevier, V. 113 N. 1-3, p. 297-322, 2002.

[3561]

*Jean-Paul Bodeveix,
Mamoun Filali.*

Reduction and quantifier elimination techniques for program validation. Dans : Formal Methods in System Design, V. 20 N. 1, p. 69 - 89, 2002.

[4494]

*Mamoun Filali, Philippe Mauran,
Gérard Padiou, Philippe Quéinnec.*

Set based trees for the validation of a diffusing computation reconstruction algorithm. Dans : 2nd Int'l Workshop on Refinement of Critical Systems: Methods, Tools and Developments, Turku, Finland, 3 juin - 6 juin 2003.

[4529]

Sergei Soloviev, Vladimir Orevkov.

On categorical equivalence of Gentzen-style derivations in IMML. Dans : Theoretical Computer Science, Elsevier, V. 303, p. 245-260, 2003.

[5709]

Jean-Paul Bodeveix, David
Chemouil, Mamoun Filali,
Martin Strecker.

*Towards formalizing AADL
in proof assistants.*

Dans : *Formal Foundations
of Embedded software
and component-based softare
architectures (ETAPS), Edinburgh,
avril 2005. Juliana Kuster-Filipe,
Iman Poernomo, Ralf Reussner,
Sandeep Shukla (Eds.),
LFCS (University of Edinburgh),
p. 137 - 153.*

[5711]

Ousmane Koné, P. Félix.

*An interoperability testing
approach to wireless application
protocols. Journal of Universal
Computer Science,
J.UCS Springer Co.Pub,
V. 9, p. 1220-1243, 2003.*

[5713]

Ousmane Koné.

*Conformance testing to real-time
communications systems.
Computer Communications,
Elsevier Science,
V. 25, p. 32-45, 2002*

[6029]

Gérard Padiou, Michel
Charpentier, Philippe Quéinnec.

*Collaborative Mobile Agents
to gather Global Information.*

Dans : *The 4th IEEE International
Symposium on Network
Computing and Applications
(IEEE NCA05), Cambridge, MA,
USA., 27 juillet 29 juillet 2005.
IEEE Computer Society,
p. 120-123*

- Autres
 - gestion (implantation, administration, ...) d'applications et de sites Web pour l'IRIT (P. Maurice)
- Plusieurs présentations et démonstrations à la Fête de la Science.