Programme des journées nationales du GDR GPL 2009

mercredi 28 janvier 14h-16h30	Ouverture des journées	Yves Ledru

Conférencier invité :	Alessandro Cimatti,	Center for Information Technology,	Fondazione Bruno Kessler,	Trento

Titre : Software Model Checking via SMT solving

Président de session : Christel Seguin

Pause café et	posters
mercredi 28 janvier 16h-17h30	Session Action AFSEC

Président de session : Franck Barbier

Titre : Modéliser et vérifier les systèmes embarqués : pourquoi et comment ?

Auteur :

Jean-Pierre Elloy, Ecole Centrale / IRCCyN, Nantes

Titre : Dépliages de réseaux d'automates et application à la supervision

Auteur :

Claude Jard, ENS Cachan, IRISA, Université Européenne de Bretagne

Titre : Expressivité comparée de modèles temporisés.

Auteur :

Olivier H. Roux, IRCCyN, Université de Nantes

Session GT	Transformation

Président de session : Jean-Michel Couvreur

Titre : Génération de canevas de programmation dédiés pour les applications de téléphonie avancées

Auteurs :

Wilfried Jouve INRIA/LaBRI,	Nicolas Palix, DIKU, Université de Copenhague,	Christophe Consel, INRIA/LaBRI,	Jacques Kadionik, IMS,	Université

Session GT FORWAL

Président de session : Jean-Michel Couvreur

Titre : Approximations régulières pour l'analyse d'accessibilité

Auteurs :

Y. Boichut, LIFO, Université d'Orléans

R. Courbis, LIFC, INRIA-CASSIS, Université de Franche-Comté
P.-C. Héam, LSV, CNRS-INRIA, Ecole Normale Supérieure de Cachan
O. Kouchnarenko3, LIFC, INRIA-CASSIS, Université de Franche-Comté

Titre : Vérification et systèmes de réécriture : de plus en plus efficace Auteurs : Emilie Ba

mercredi 28 janvier 17h45-19h30 Réunion Bureau GDR + Responsables des Groupes de Travail + Comité s
Bilan première année GDR GPL et projets pour la 2e année.
jeudi 29 janvier 9h-10h30 Conférencier invité : Paul Klint (Centrum Wiskunde & Informatica (CWI)
Titre : Grammarware is everywhere and what to do about that?

Président de session : Laurence Duchien
Pause café et posters
jeudi 29 janvier 11h-12h30 Session GT MFDL
Président de session : Yamine Ait-Ameur

Titre : Un cadre formel pour le contrôle d'accès Auteur : Mathieu Jaume - SPI - LIP6 - Université Paris 6

Titre : Une approche incrémentale combinant test et extraction de modèles
Auteurs :
Roland Groz, LIG, Grenoble Universités
Muzammil Shahbaz, France Telecom R&D
Keqin Li, LIG, Grenoble Universités

Titre : Développement formel par composants : assemblage et vérification à l'aide de B
Auteurs :
Arnaud Lanoix, COLOSS/LINA,
Samuel Colin et Jeanine Souquières (DEDALE/LORIA)
Session GT COSMAL
Président de session : Philippe Lahire

Titre : Construction dynamique d'annuaires de composants par classification de services utilisant l'analyse formelle de concepts
Auteurs:
Gabriela Arévalo, LIFIA - Facultad de Informática (UNLP), La Plata, Argentina
Nicolas Desnos, LGI2P - Ecole des Mines d'Alès, Nîmes
Marianne Huchard - LIRMM - UMR 5506 - CNRS and Univ. Montpellier 2
Christelle Urtado - LGI2P - Ecole des Mines d'Alès, Nîmes
Sylvain Vauttier - LGI2P - Ecole des Mines d'Alès, Nîmes

Titre : Vers la génération de modèles de sûreté de fonctionnement
Auteurs :
Xavier Dumas, Claire Pagetti, Laurent Sagaspe, Pierre Bieber, ONERA-CERT
Philippe Dhaussy, ENSIETA - LiSyC - DTN

Titre : Composition et expression qualitative de politiques d'adaptation pour les composants Fractal

Auteurs :
Franck Chauvel, Peking University, Chine
Olivier Barais, Noel Plouzeau, IRISA (INRIA & Université de Rennes 1)
Isabelle Borne, VALORIA (Université de Bretagne Sud)
Jean-Marc Jézéquel, (INRIA & Université de Rennes 1)

Repas	
jeudi 29 janvier 14h-15h30	Session Action IDM

Président de session : Mireille Blay-Fornarino

Titre : Retours sur Models 2008

Auteur :
Xavier Blanc, INRIA Lille-Nord Europe, LIFL CNRS UMR 8022, Université des Sciences et Technologies

Titre : Des plate-formes pour l'IDM: "OPEES, OpenEmbeDD, Papyrus, TOPCASED..."

Auteur :
Sébastien Gérard, CEA LIST

Titre : Alignement de métamodèles pour la génération automatique de transformation de modèles

Auteurs :
Jean-Rémy Falleri, Marianne Huchard, Mathieu Lafourcade et Clémentine Nebut, LIRMM, CNRS et Univ

Session LGT, LMH

Président de session : Jean-Louis Giavitto

Titre : Sémantiques formelles d'un mini-langage impératif BSP - Application à la preuve de programmes et à l'optimisation

Auteurs:
Jean Fortin et Frédéric Gava , LACL, Université Paris Est

Titre : Functional meta-programming for parallel skeletons

Auteurs :
Jocelyn Serot, LASMEA, CNRS/U. Blaise Pascal
Joel Falcou, LRI, Université Paris-Sud

Titre : Placement d'applications distribuées hétérogènes sur des architectures de type grappe

Auteurs :
Sylvain Jubertie, Emmanuel Melin, Jérémie Vautard, Arnaud Lallouet, Laboratoire d'Informatique Fonda

Pause café et	posters
jeudi 29 janvier 16h-17h30	Session Posters et démos
jeudi 29 janvier 17h30-18h30	Table ronde (V. Donzeau-Gouge, Luis Farinas, Jean-Louis Giavitto) animé

Thème : Quel rôle pour les conférences francophones?

Dîner

vendredi 30 janvier 9h-10h30 Conférencier invité : Xavier Leroy , INRIA Paris-Rocquencourt

Titre : Vérification formelle d'un compilateur C réaliste

Président de session : Yves Ledru

Pause café et posters

vendredi 30 janvier 11h-12h30 Session GT LTP

Président de session : Pierre Castéran

Titre : Classes de types de première classe

Auteurs :

Matthieu Sozeau, LRI, INRIA/Université Paris Sud

Nicolas Oury, Université de Nottingham

Titre: Code porteur de preuve pour la vérification de bytecode Java

Auteurs :

Gilles Barthe, IMDEA Software, Madrid, Spain

Pierre Crégut, France Télécom, France

Benjamin Grégoire, INRIA Sophia-Antipolis Méditerranée, France

Thomas Jensen, IRISA/CNRS, France

David Pichardie, IRISA/INRIA Rennes Bretagne Atlantique, France

Titre : Vérification formelle d'un algorithme d'allocation de registres par coloration de graphe

Auteurs :

S. Blazy, B. Robillard et E. Sexton, Laboratoire CEDRIC

Session GT MTV2

Président de session : Fatiha Zaïdi

Titre : Constraint-Based Software Testing

Auteurs :

Sebastian Bardin, Bernard Botella, CEA LSL

Frédéric Dadeau, University of Franche-Comté, LIFC / INRIA projet CASSIS

Florence Charreteur, Arnaud Gotlieb, INRIA Rennes-Bretagne Atlantique, projet LANDE

Bruno Marre, CEA LSL

Claude Michel, Michel Rueher, University of Nice-Sophia Antipolis, projet CeP

Nicky Williams, CEA LSL

Titre : Simulated annealing applied to test generation: landscape characterization and stopping criteria

Auteurs :

Hélène Waeselynck, Pascale Thévenod-Fosse, Olfa Abdellatif-Kaddour, LAAS-CNRS.

Titre : Coverage-biased Random Exploration of Models

Auteurs :

Alain Denise, Marie-Claude Gaudel, Sandrine-Dominique Gouraud, Université de Paris-Sud 11 & CNRS

Richard Lassaigne, Université Paris Diderot 7 & CNRS

Johan Oudinet, Sylvain Peyronnet, Université de Paris-Sud 11 & CNRS

Repas	
vendredi 30 janvier 14h-15h30	Session GT RIMEL
Président de session : Salah Sadou	

Titre : On the Use of Formal Techniques to Support Model Evolution

Auteurs :
Mens Tom, Service de Génie Logiciel, Université de Mons-Hainaut, Belgique
Van Der Straeten Ragnhild, Systems and Software Engineering Lab, Vrije Universiteit Brussel, Belgique

Titre : Conciliating Property Stability and System Evolution through Software Model Analysis

Auteur : Ilham ALLOUI, LISTIC - Polytech'Savoie

Titre : Le contrat d'évolution d'architectures : un outil pour le maintien de propriétés non fonctionnelles

Auteurs:
Régis Fleurquin, VALORIA, Université Bretagne-Sud et IRISA, INRIA Rennes,
Chouki Tibermacine, LIRMM, Université Montpellier II
Salah Sadou, VALORIA, Université Bretagne-Sud

vendredi 30 janvier 15h30-16h	Clôture : proclamation du meilleur poster et du nouveau logo du GDR

Journées Nationales du GDR GPL : résumés des présentations

Conférenciers Invités

Titre : Software Model Checking via SMT solving

Conférencier:
Alessandro Cimatti, Center for Information Technology, Fondazione Bruno Kessler
Résumé :
Software model checking is a fully automated approach to the verification of software, that has received substantial interest in the last decade. In this talk, I will first review the field, focussing on different forms of software model checking based on predicate abstraction. Then, I will present some recent improvements, showing how the use of modern Satisfiability Modulo

Theories (SMT) procedures can increase the accuracy and the efficiency of the analysis.

Titre : Grammarware is everywhere and what to do about that?

Conférencier :
Paul Klint (Centrum Wiskunde & Informatica (CWI) , Amsterdam)
Résumé:
Many aspects of software engineering are based on grammars albeit that they occur in disguise. From the grammars for mainstream programming languages that are hidden in compilers to the grammars for Domain-specific Languages that are part of dedicated DSL implementations. From XML schemas or MDA models to Application Programming Interfaces for large systems. In all these cases large amounts of software may depend on such grammars and will be affected when the grammar is erroneous or is subject to evolution.
While software engineers use rigorous engineering principles for developing source code, this is much less the case when developing grammars in their various forms. What is the quality of a grammar? What is the effect of grammar modifications on the software that depends on it? What is the effect of API changes? How to refactor DSL programs?
In the first part of the talk I will sketch these problems and identify *grammarware engineering* a s a promising research area that contains many interesting problems [1].
In the second part of the talk I will present some of our results in this area. After a brief overview of the Meta-Environment [2] I zoom in on current work on the design and implementation of the *Rascal* language, a special purpose scripting language for source code analysis and transformation [3]. Rascal provides many fundamental concepts like parsing, regular/list/set matching, term rewriting, backtracking and relational calculus in an integrated form that is as unintimidating as possible for the average programmer without a formal background. Design goals, the language itself and the current state of its implementation will be briefly discussed. We believe that this approach will enable the development of new tools not only for grammarware engineering but also for other problems in refactoring, software analysis and software transformation.
[1] Paul Klint, Ralf Lämmel and Chris Verhoef, Toward an engineering discipline for grammarware, ACM Transactions on Software Engineering Methodology, 2005(14), 331--380.
[2] Meta-Environment Home Page, http://www.meta-environment.org .
[3] Joint current research with Jurgen Vinju and Tijs van der Storm.

Titre : Vérification formelle d'un compilateur C réaliste

Conférencier :
Xavier Leroy, INRIA Paris-Rocquencourt

Travail en commun avec
Yves Bertot (INRIA Sophia-Antipolis),
Sandrine Blazy (ENSIIE),
Pierre Letouzey (Université Paris 7), et
Laurence Rideau (INRIA Sophia-Antipolis).

Les compilateurs sont des logiciels fort complexes qui parfois contiennent des erreurs entraînant la production de code exécutable faux à partir d'un programme source correct. L'existence de tels bugs introduits par le compilateur affaiblissent les garanties que l'on peut obtenir par l'application de méthodes formelles au niveau du programme source.

Cet exposé présente le projet CompCert: une expérience en cours consistant à développer et à prouver correct un compilateur réaliste, modérément optimisant, produisant de l'assembleur PowerPC à partir d'un large sous-ensemble du langage C. La preuve de correction, menée sur machine avec l'assistant de preuve Coq, établit que le code PowerPC engendré se comporte exactement comme prescrit par la sémantique du source C, éradiquant ainsi toute possibilité de bugs introduits par le compilateur et établissant un niveau de confiance sans précédent envers ce compilateur.

Session Action AFSEC

Titre : Modéliser et vérifier les systèmes embarqués : pourquoi et comment ?

Auteur :
Jean-Pierre Elloy, Ecole Centrale / IRCCyN, Nantes

Résumé :
Le particularisme des systèmes embarqués, en particulier la finitude du nombre de leurs objets constitutifs a permis l'émergence de démarches spécifiques pour leur conception ainsi que pour vérifier la conformité du produit obtenu aux exigences initiales de l'application. Dans ces démarches, la modélisation est l'abstraction charnière qui : décrit le comportement du système à développer, sert de support à son développement, et doit reconnaître les propriétés du système développé. Mais pour atteindre ces objectifs, la modélisation d'un système embarqué doit être soigneusement élaborée. Il faut identifier avec précision le périmètre du modèle à établir, puis l'immerger dans un environnement le saturant de toutes les circonstances qui peuvent l'affecter. Il faut recenser les actions pertinentes du modèle au regard des propriétés qu'il doit vérifier, pour ensuite en démontrer leur satisfaction. Il faut s'assurer que les opérateurs de manipulation des modèles respectent la sémantique des mêmes opérations effectuées sur les systèmes modélisés, pour autoriser une conception incrémentale du système à construire. Il faut enfin inscrire avec soin les phases d'exploitation d'un modèle dans le processus général de conception du système.

On examinera ces différents aspects dans le cas où le système à concevoir est le dispositif de pilotage d'un équipement embarqué. On indiquera quelles sont les types de fautes qui peuvent en "distordre" le fonctionnement, puis on se focalisera sur la modélisation comportementale (causale) de ce système de pilotage. On montrera ainsi qu'il est nécessaire de porter une attention soutenue à cette modélisation pour aboutir à un système embarqué aux prestations réellement sûres de fonctionnement.

Titre : Dépliages de réseaux d'automates et application à la supervision

Auteur :
Claude Jard, ENS Cachan, IRISA, Université Européenne de Bretagne

Résumé :
Cet article présente des techniques de dépliages de réseaux d'automates. Elles permettent de mettre en évidence les relations causales d'ordre partiel existant entre les événements d'un modèle des comportements des systèmes répartis. Elles sont donc particulièrement adaptées pour traiter la question de la supervision. Etant donné une séquence d'actions observées durant l'exécution d'une application répartie, il s'agit, à l'aide d'un modèle du système, de déterminer les transitions du modèle ayant produit ces actions et d'inférer les relations de causalité ou d'indépendance qui les relient. Nous explorons notamment le contexte original de la supervision de systèmes modélisés par des réseaux d'automates temporisés et montrons comment on peut aussi inférer les dates possibles d'occurrence des actions à l'aide de contraintes symboliques.

Titre : Expressivité comparée de modèles temporisés.

Auteur :
Olivier H. Roux, IRCCyN, Université de Nantes
Résumé :
Il y a en général une opposition entre l'expressivité d'un modèle, c'est-à-dire sa capacité à représenter un nombre important de caractéristiques d'un système, et sa simplicité en termes de vérification ou de contrôle (décidabilité et complexité algorithmique). Dans cet article, nous nous intéressons à des modèles dits temporisés pour lesquels le temps est manipulé de manière explicite et, plus particulièrement, aux automates temporisés et à différentes classes de réseaux de Petri temporels. Nous donnons les principaux résultats de décidabilité sur ces modèles et nous comparons leur expressivité en termes de bisimulation temporelle.

Session Action IDM

Titre : Retours sur Models 2008

Auteur :
Xavier Blanc, INRIA Lille-Nord Europe, LIFL CNRS UMR 8022, Université des Sciences et Technologies de Lille
Résumé :
La conférence Models est la conférence phare de l'IDM (Ingénierie Dirigée par les Modèles). Sa onzième édition a eu lieu en France, à Toulouse, au mois d'Octobre 2008. Cet article présente les articles Français publiés lors de cet événement et montre la richesse et la forte implication de la communauté française dans ce domaine.

Titre : Des plate-formes pour l'IDM: "OPEES, OpenEmbeDD, Papyrus, TOPCASED..."

Auteur :
Sébastien Gérard, CEA LIST
Résumé :
L'objectif de cet article court est, d'une part, de rapidement introduire trois initiatives françaises liées à des développements d'outils ou suites d'outils visant à fournir un support à l'ingénierie des modèles, et, d'autre part, de présenter deux initiatives de fédération de ces outils et de leur développement dans un cadre européen et international, au travers de travaux menés avec la fondation Eclipse.

Titre : Alignement de métamodèles pour la génération automatique de transformation de modèles

Auteurs :
Jean-Rémy Falleri, Marianne Huchard, Mathieu Lafourcade et Clémentine Nebut, LIRMM, CNRS et Université de Montpellier 2
Le résumé :
L'application d'une approche dirigée par les modèles entraîne la création de nombreux métamodèles, dans la mesure où l'IDM prône l'usage intensif de modèles définis par des métamodèles. Des métamodèles avec des objectifs similaires sont donc inévitablement créés. Un problème récurrent est alors de rendre compatibles des modèles dont les métamodèles sont similaires, par exemple en vue de les utiliser au sein d'un même outil. Classiquement, ce

problème est résolu par le développement de transformations de modèles ad hoc.
Dans ce papier, nous proposons une approche détectant automatiquement les correspondances entre deux métamodèles, qui sont ensuite utilisées pour générer un alignement entre les métamodèles. Cet alignement doit ensuite être vérifié manuellement et peut ensuite être utilisé pour générer une transformation de modèle. Notre approche est basée sur l'algorithme Similarity Flooding, utilisé dans les domaines de la mise en correspondance de schémas et de l'alignement d'ontologies. Ce papier fournit également des résultats expérimentaux comparant l'efficacité de plusieurs implémentations de notre approche sur plusieurs métamodèles du monde réel.

Session GT COSMAL

Titre : Construction dynamique d'annuaires de composants par classification de services utilisant l'analyse formelle de concepts

Auteurs:
Gabriela Arévalo, LIFIA - Facultad de Informática (UNLP), La Plata, Argentina
Nicolas Desnos, LGI2P - Ecole des Mines d'Alès, Nîmes
Marianne Huchard - LIRMM - UMR 5506 - CNRS and Univ. Montpellier 2
Christelle Urtado - LGI2P - Ecole des Mines d'Alès, Nîmes
Sylvain Vauttier - LGI2P - Ecole des Mines d'Alès, Nîmes

Résumé :
Les annuaires de composants permettent d'indexer et de localiser rapidement les composants selon les services qu'ils offrent. Ils donnent ainsi aux assemblages en cours d'exécution la possibilité d'évoluer dynamiquement par remplacement de composants, en cas de défaillance, ou par intégration de nouvelles fonctionnalités, en réponse à de nouveaux besoins. Dans ce travail, nous visons des méthodes semi-automatiques d'évolution. Nous posons les bases théoriques d'une utilisation de l'Analyse Formelle de Concepts pour une construction incrémentale des annuaires de composants basée sur les définitions syntaxiques des services requis et fournis. Dans ces annuaires, les composants sont organisés de manière plus intelligible et les descriptions externes de composants plus abstraits et plus réutilisables sont suggérées. Mais surtout, cette organisation rend plus efficaces les tâches automatisées d'assemblage et de remplacement.

Titre : Vers la génération de modèles de sûreté de fonctionnement

Auteurs :
Xavier Dumas, Claire Pagetti, Laurent Sagaspe, Pierre Bieber, ONERA-CERT
Philippe Dhaussy, ENSIETA - LiSyC - DTN

Titre : Composition et expression qualitative de politiques d'adaptation pour les composants Fractal

Auteurs :
Franck Chauvel, Peking University, Chine
Olivier Barais, Noel Plouzeau, IRISA (INRIA & Université de Rennes 1)
Isabelle Borne, VALORIA (Université de Bretagne Sud)
Jean-Marc Jézéquel, (INRIA & Université de Rennes 1)

Session GT FORWAL

Titre : Approximations régulières pour l'analyse d'accessibilité

Auteurs :
Y. Boichut, LIFO, Université d'Orléans
R. Courbis, LIFC, INRIA-CASSIS, Université de Franche-Comté
P.-C. Héam, LSV, CNRS-INRIA, Ecole Normale Supérieure de Cachan
O. Kouchnarenko, LIFC, INRIA-CASSIS, Université de Franche-Comté

Titre : Vérification et systèmes de réécriture : de plus en plus efficace

Auteurs : Emilie Balland, équipe PAREO, INRIA Lorraine, Nancy Yohan Boichut, équipe PRV, LIFO, Orléans Pierre-Etienne Moreau, équipe PAREO, INRIA Lorraine, Nancy

Thomas Genet, équipe LANDE, INRIA Rennes

Résumé :

Les systèmes de réécriture (TRSs) sont de plus en plus utilisés pour la modélisation d'applications ou de systèmes. Pour ces modèles, l'analyse d'atteignabilité, i.e. prouver qu'un terme est atteignable par réécriture à partir d'un ensemble de termes donné et pour un système de réécriture donné, n'est rien d'autre qu'une forme de technique de vérification.

Par l'utilisation d'une technique de complétion sur des automates d'arbres, il a été démontré que la non-atteignabilité d'un terme t peut être vérifiée par le calcul d'une sur-approximation de l'ensemble des termes réellement atteignables et par la non-appartenance de t à cette sur-approximation. Puisque la vérification de programmes ou de systèmes concrets donne lieu à des modèles de réécriture de tailles significatives, des implantations efficaces de la complétion dans notre cadre sont essentielles.

L'objectif principal de cet article est de présenter une transformation de systèmes de réécriture qui, dans un premier

temps préserve l'analyse d'atteignabilité, puis dans un second temps donne naissance à des systèmes de réécriture beaucoup plus simples à appliquer que les originaux. Cette approche a été implantée en Tom, un langage ajoutant des primitives de réécriture au langage Java. Les premières expérimentations sont très prometteuses en comparaison avec l'outil de référence pour cette technique : Timbuk.

Session GT LaMHa

Titre : Sémantiques formelles d'un mini-langage impératif BSP - Application à la preuve de programmes et à l'optimisation

Auteurs:
Jean Fortin et Frédéric Gava , LACL, Université Paris Est

Résumé :
Dans cet exposé, nous décrivons plusieurs sémantiques d'un mini-langage impératif muni d'opérations pour leparallélisme BSP (dans un style SPMD). Un intérêt de ce travail est que tout le développement des sémantiques ainsi que les preuves des propriétés (et des programmes) ont été réalisés dans l'assistant de preuve Coq, ce qui augmente fortement la confiance que l'on peut apporter à notre propos.

Titre : Functional meta-programming for parallel skeletons

Auteurs :
Jocelyn Serot, LASMEA, CNRS/U. Blaise Pascal
Joel Falcou, LRI, Université Paris-Sud

Résumé :
We describe the implementation in MetaOcaml of a small domain specific language for skeleton-based parallel programming. We show how the meta-programming facilities offered by this language make it possible to virtually eliminate the run-time overhead for the resulting

programs, compared to a hand-crafted, low-level implementation written in C+MPI.

Titre : Placement d'applications distribuées hétérogènes sur des architectures de type grappe

Auteurs :
Sylvain Jubertie, Emmanuel Melin, Jérémie Vautard, Arnaud Lallouet, Laboratoire d'Informatique Fondamentale d'Orléans

Session GT LTP

Titre : Classes de types de première classe

Auteurs:
Matthieu Sozeau, LRI, INRIA/Université Paris Sud
Nicolas Oury, Université de Nottingham

Résumé:
Les classes de types ont démontré leur utilité pour la programmation polymorphique de haut-niveau en Haskell et la construction de hiérarchies de structures mathématiques dans l'assistant de preuve Isabelle. Ce mécanisme de surcharge très versatile peut se généraliser aux types dépendants et offre alors de nouvelles formes de généricité. Il permet aussi d'intégrer une forme de programmation logique au moment du typage. On présente une implémentation légère d'un système de classes de types de première classe ainsi que des exemples mettant en oeuvre les classes pour programmer, prouver et organiser les développements en Coq.

Titre: Code porteur de preuve pour la vérification de bytecode Java

Auteurs :
Gilles Barthe, IMDEA Software, Madrid, Spain
Pierre Crégut, France Télécom, France
Benjamin Grégoire, INRIA Sophia-Antipolis Méditerranée, France
Thomas Jensen, IRISA/CNRS, France
David Pichardie, IRISA/INRIA Rennes Bretagne Atlantique, France

Résumé: Le code porteur de preuve est une technique permettant de transmettre un

programme en l'accompagnant d'une preuve qui atteste de sa validité vis-à-vis d'une certaine politique de sécurité. Nous présenterons un panorama des activités du projet européen Mobius pour développer les techniques de code porteur de preuve pour la vérification de programme bytecode Java mobile. Cette présentation insistera plus particulièrement sur l'utilisation de techniques de vérification statiques certifiée, i.e. dont la validité sémantique a été formellement établie avec l'assistant de preuve Coq.

Titre : Vérification formelle d'un algorithme d'allocation de registres par coloration de graphe

Auteurs :
S. Blazy, B. Robillard et E. Soutif, Laboratoire CEDRIC
Résumé :
Le travail présenté dans cet article est à l'interface entre la recherche opérationnelle et les méthodes formelles. Il s'inscrit dans le cadre du projet CompCert ayant pour but le développement et la vérification formelle, utilisant l'assistant de preuve Coq, d'un compilateur du langage C potentiellement utilisable pour la production de logiciels embarqués critiques. Nous nous intéressons dans cet article à l'allocation de registres, qui consiste à optimiser l'utilisation des registres du processeur. Nous proposons d'aborder cette optimisation en la modélisant par un problème dit de coloration avec préférences dont nous vérifions formellement la résolution. Cette vérification prend deux formes : preuve de correction de la spécification Coq pour la première partie de l'algorithme et validation a posteriori pour la seconde.

Session GT MFDL : Méthodes Formelles dans le Développement Logiciel

Titre : Un cadre formel pour le contrôle d'accès

Auteur : Mathieu Jaume - SPI - LIP6 - Université Paris 6 Résumé : Un des aspects de la sécurité en informatique concerne le contrôle des accès aux données d'un système pour lequel différentes politiques de sécurité peuvent être mises en application. Toutefois, rien ne sert de mettre en place une politique de sécurité pour gérer un système si les programmes chargés de garantir le bon fonctionnement de cette politique ne sont pas fiables. Cet article rend compte de manière informelle de différentes expériences permettant d'obtenir des développements formels de politiques de contrôle d'accès. Ces développements nous conduisent à introduire un ``cadre sémantique'' dans lequel il est possible de spécifier et d'implanter des modèles de contrôle d'accès. Ce cadre permet de définir des mécanismes de comparaisons de modèles et d'analyser ces modèles en termes de flots d'informations qu'ils autorisent.

Titre : Une approche incrémentale combinant test et extraction de modèles

Auteurs :
Roland Groz, LIG, Grenoble Universités
Muzammil Shahbaz, France Telecom R&D
Keqin Li, LIG, Grenoble Universités

Résumé :
Un des principaux obstacles à l'utilisation d'approches formelles est l'absence de modèles. Nous nous intéressons ici au problème de l'intégration et du test de composants logiciels. Dans la pratique industrielle actuelle, il est de plus en plus fréquent de travailler en intégrant des composants logiciels externes dont aucun modèle n'est disponible. La documentation fournit en général une spécification insuffisante. Afin de guider l'intégration, nous proposons d'utiliser des algorithmes d'inférence de machines pour extraire des modèles des composants. L'interaction entre ces modèles dans une composition permet de déduire d'autres tests qui peuvent être confrontés au système. L'ingénieur chargé de l'intégration dispose ainsi d'outils lui permettant de découvrir les interactions effectives entre les composants et de guider son processus d'intégration et de test pour valider les combinaisons de comportements. Nous travaillons sur des modèles d'automates étendus avec des paramètres et des prédicats, mais sans variables internes.

Titre : Développement formel par composants : assemblage et vérification à l'aide de B

Auteurs :
Arnaud Lanoix, COLOSS/LINA,
Samuel Colin et Jeanine Souquières (DEDALE/LORIA)

Résumé :
Dans une approche composants pour le développement de logiciels, les composants sont considérés comme des boîtes noires. Une application consiste en un assemblage de composants qui communiquent via leurs interfaces. Une description formelle de ces interfaces est nécessaire pour s'assurer de leur compatibilité. En général, les interfaces ne sont pas directement compatibles et un adaptateur doit être introduit. Nous proposons des schémas pour assembler des composants de manière systématique et vérifier leur interopérabilité; ces schémas sont définis à l'aide de concepts issus de la méthode B. L'assemblage est un raffinement des interfaces requises qui inclut les interfaces fournies; la correction du processus est validée par les obligations de preuves usuelles.

Session GT MTV2

Titre : Constraint-Based Software Testing

Auteurs :
Sebastian Bardin, Bernard Botella, CEA LSL
Frédéric Dadeau, University of Franche-Comté, LIFC / INRIA projet CASSIS
Florence Charreteur, Arnaud Gotlieb, INRIA Rennes-Bretagne Atlantique, projet LANDE
Bruno Marre, CEA LSL

Claude Michel, Michel Rueher, University of Nice-Sophia Antipolis, projet CeP
Nicky Williams, CEA LSL

Résumé :
Constraint-Based Testing (CBT) is the process of generating test cases from programs or models by using the Constraint Programming technology. Recently, this method received much attention due to several Research projects launched in France and abroad. This paper aims at presenting the main CBT tools developped by four Research labs: CEA Laboratoire de Sûreté des Logiciels, INRIA Lande research team, Laboratoire d'Informatique de Franche-Comté, and CeP team of University of Nice–Sophia Antipolis. The paper concludes by drawing some perspectives on open problems in CBT.

Titre : Simulated annealing applied to test generation: landscape characterization and stopping criteria

Auteurs :
Hélène Waeselynck, Pascale Thévenod-Fosse, Olfa Abdellatif-Kaddour, LAAS-CNRS.

Résumé :
This paper investigates a measurement approach to support the implementation of Simulated Annealing (SA) applied to test generation. SA, like other metaheuristics, is a generic technique that must be tuned to the testing problem under consideration. Finding an adequate setting of SA parameters, that will offer good performance for the target problem, is known to be difficult. Our measurement approach is intended to guide the implementation choices to be made. It builds upon advanced research on how to characterize search problems and the dynamics of metaheuristic techniques applied to them. Central to this research is the concept of landscape. Existing measures of landscape have mainly been applied to combinatorial problems considered in complexity theory. We show that some of these measures can be useful for testing problems as well. The diameter and autocorrelation are retained to study the adequacy of alternative settings of SA parameters. A new measure, the Generation Rate of Better Solutions (GRBS), is introduced to monitor convergence of the search process and implement stopping criteria. The measurement approach is experimented on various case studies, and allows us to successfully revisit a problem issued from our previous work on testing control systems.

Titre : Coverage-biased Random Exploration of Models

Auteurs :
Alain Denise, Marie-Claude Gaudel, Sandrine-Dominique Gouraud, Université de Paris-Sud 11 & CNRS
Richard Lassaigne, Université Paris Diderot 7 & CNRS
Johan Oudinet, Sylvain Peyronnet, Université de Paris-Sud 11 & CNRS

Résumé :
This paper describes a set of methods for randomly drawing traces in large models either uniformly among all traces, or with a coverage criterion as target. Classical random walk methods have some drawbacks. In case of irregular topology of the underlying graph, uniform choice of the next state is far from being optimal from a coverage point of view. Moreover, for the same reason, it is generally not practicable to get an estimation of the coverage obtained after one or several random walks: it would require some complex global analysis of the model topology. We present here some methods that give up the uniform choice of the next state. These methods bias this choice according to the number of traces, or states, or transitions, reachable via each successor.

Session GT RIMEL

Titre : On the Use of Formal Techniques to Support Model Evolution

Auteurs :
Mens Tom, Service de Génie Logiciel, Université de Mons-Hainaut, Belgique
Van Der Straeten Ragnhild, Systems and Software Engineering Lab, Vrije Universiteit Brussel, Belgique

Résumé :
Model-driven engineering (MDE) is an emerging software engineering discipline that relies on model transformation. Model transformations can be very diverse, and encompass, among others, the following techniques: code generation, reverse engineering, model refinement and model refactoring. Due to the inherently volatile nature of all kinds of software artefacts, and models in particular, all existing and future MDE approaches should explicitly take into account the inevitable process of model evolution. In this paper, we explain why formal support for model evolution is needed. We motivate this by using the formalism of description logics to support the activity of model inconsistency management, and by using the formalism of graph transformation to support the activity of model refactoring.

Titre : Conciliating Property Stability and System Evolution through Software Model Analysis

Auteur : Ilham ALLOUI, LISTIC - Polytech'Savoie

Résumé :
Model-driven software engineering is founded on the idea of transforming abstract models into more concrete ones. Within this context, software model evolution is a kind of transformation that aims at obtaining a new model of software through the application of change operations on the starting software model. One main issue how to ensure stability of desired properties in the new model? Among such properties, are structural ones (e.g. cardinality of model elements, connectivity, etc.) and behavioral ones (e.g. safety, fairness, etc.). Stability of

software system properties refers to the system capability to accommodate changes from its environment while avoiding unexpected effects. A subsequent issue is how to scope model analysis so that only those parts of the model that could be affected will be analyzed.
To conciliate property stability and system evolution, the paper proposes a model evolution process founded on both property verification and techniques of change impact analysis.

Titre : Le contrat d'évolution d'architectures : un outil pour le maintien de propriétés non fonctionnelles

Auteurs:
Régis Fleurquin, VALORIA, Université Bretagne-Sud et IRISA, INRIA Rennes,
Chouki Tibermacine, LIRMM, Université Montpellier II
Salah Sadou, VALORIA, Université Bretagne-Sud

Résumé :
Tout logiciel doit évoluer pour répondre aux exigences changeantes de ses utilisateurs et aux modifications de son environnement. Ces changements, souvent imprévisibles, réalisés par un tiers et dans l'urgence, mènent parfois le logiciel vers un état que ses créateurs n'auraient pas souhaité. Nous présentons dans cet article un cadre pour une évolution contrôlée d'applications à base de composants. Ce contrôle garantit la préservation de propriétés architecturales et par là de certaines propriétés non fonctionnelles.

Session GT Transformations

Titre : Génération de canevas de programmation dédiés pour les applications de téléphonie avancées

Auteurs :
Wilfried Jouve INRIA/LaBRI,

Nicolas Palix, INRIA/LaBRI, Charles Consel, INRIA/LaBRI, Patrice Kadionik, IMS, Université de Bordeaux

Résumé :

Nous proposons l'approche DiaSpec fondée sur le protocole SIP pour faciliter la programmation et permettre l'exécution des applications de téléphonie avancées. Un canevas de programmation dédié est généré pour chaque application cible et fournit des opérations haut niveau faisant abstraction des technologies sous-jacentes.

Table Ronde : Quel rôle pour les conférences francophones?

Participants : V. Donzeau-Gouge, L. Farinas, J-L Giavitto
Animateur : Yves Ledru

Nous avons connu en 2008 une diminution des soumissions aux conférences francophones proches du GDR GPL. D'aucuns y voient la conséquence d'une dépréciation des publications francophones. En effet, les critères retenus
pour déclarer un chercheur comme "publiant" font la part belle aux revues et conférences internationales. D'autres y voient un signe de l'internationalisation de nos laboratoires où beaucoup de nos doctorants ne sont pas francophones.

Dans ce contexte quelle est aujourd'hui le rôle des conférences et des revues francophones? Sont-elles vouées à disparaître? Ont-elles vocation à devenir le petit village gaulois où se trouvent les irréductibles défenseurs de la langue française? Doivent-elles se regrouper en un unique événement annuel pour atteindre une masse critique? Faut-il adopter l'anglais pour ainsi attirer des contributeurs venus de toute la planète à l'instar de ce qui se fait chez nos voisins allemands? Faut-il privilégier l'événement social où germent les projets nationaux et où les jeunes chercheurs préparent leur mobilité?

Cette table ronde donnera la parole à des représentants du CNRS et de l'AERES pour qu'ils précisent le rôle qu'ils voient jouer à ces conférences et revues, ainsi qu'au GDR GPL, dans une organisation de la recherche en profond renouvellement.

Posters et Démos

Titre : Infrastructure logicielle pour l'auto-management d'unités mobiles. Application à l'autotest pour téléphones portables. (POSTER)
Auteurs :
Youssef Ridene, LIUPPA
Franck Barbier, LIUPPA

Titre : LETO - Un oracle de test pour les systèmes critiques avioniques (POSTER et DEMO)

Auteurs :
Guy Durrieu ONERA
Hélène Waeselynck LAAS-CNRS
Virginie Wiels ONERA

Titre : MOCAS : un modèle de composant basé états pour l'adaptation dynamique (POSTER et DEMO)
Auteurs :
Cyril Ballagny LIUPPA
Nabil Hameurlain LIUPPA Laboratory
Franck Barbier LIUPPA

Titre : Garantie des conformités par rejeu de patterns (POSTER)
Auteurs :
Clémentine Nemo i3S / UNSA
Mireille Blay-Fornarino i3S / UNSA

Titre : MAY : Make Agents Yourself, Un générateur d'API agent à base de composants logiciels (POSTER et DEMO)
Auteurs :
Victor Noël IRIT-UPS
Sylvain Rougemaille UPETEC
Jean-Paul Arcangeli IRIT-UPS
Jean-Pierre Georgé IRIT-UPS
Frédéric Migeon IRIT-UPS
Stéphane Dudouit IRIT-UPS

Titre : COLOSS Team : Dependable Components and Systems (POSTER)
Auteurs :
Arnaud Lanoix Equipe COLOSS - LINA - Université de Nantes
Pascal Andre Equipe COLOSS - LINA - Université de Nantes
Gilles Ardourel Equipe COLOSS - LINA - Université de Nantes
Christian Attiogbe Equipe COLOSS - LINA - Université de Nantes
Mohamed Messabihi Equipe COLOSS - LINA - Université de Nantes

Titre : AMPLE Traceability Framework: Un outil pour la traçabilité dans les lignes de produits

logiciels (POSTER et DEMO)
Auteurs :
Nicolas Anquetil École des Mines de Nantes
Jean-Claude Royer École des Mines de Nantes

Titre : SafeCode : Développement de Composants sûrs de fonctionnement (POSTER)
Auteurs :
Daniel Deveaux Université de Bretagne Sud
Gersan Moguérou Université de Bretagne Sud
Georges Mariano INRETS - ESTAS
Walter Schön UTC - Eudiasyc

Titre : Réécriture pour la vérification d'applications Java (POSTER)
Auteurs :
Thomas Genet Université Rennes I, INRIA/Lande
Emilie Balland INRIA/Paréo
Yohan Boichut LIFO
Benoît Boyer INRIA/Lande
Pierre-Cyrille Héam LIFC, University of Franche-Compte, INRIA/CASSIS
Thomas Jensen INRIA/Lande
Olga Kouchnarenko LIFC, University of Franche-Comté, INRIA/CASSIS
Pierre-Etienne Moreau INRIA/Paréo
Vlad Rusu INRIA/Lande
Roméo Courbis LIFC, INRIA/CASSIS

Titre : Conception de systèmes par applications de modèles paramétrés (POSTER et DEMO)

Auteurs :
Olivier caron LIFL
Bernard Carré LIFL
Areski Flissi LIFL
Alexis Muller LIFL
Gilles Vanwormhoudt LIFL, Telecom Lille I

Titre : SoCKET (POSTER)
Auteur :
Jean-Michel Bruel IRIT

Titre : Traçabilité d'exigences temporelles dans l'outil UML/SysML TTool (POSTER et DEMO)

Auteurs :
Pierre de Saqui-Sannes ISAE et LAAS-CNRS, Université de Toulouse
Ludovic Apvrille Institut TELECOM, TELECOM ParisTech

Titre : Vérification formelle et optimisation de l'allocation de registres (POSTER)
Auteurs :
Benoît Robillard CEDRIC-CNAM
Sandrine Blazy CEDRIC-ENSIIE
Soutif Eric CEDRIC-CNAM

Titre : Une première formalisation du modèle des exigences (POSTER)
Auteurs :
Abderrahman matoussi LACL - University Paris Est
Frédéric Gervais LACL - University Paris Est
Régine Laleau LACL - University Paris Est

Titre : From Rules to Constraint Programs with the Rules2CP Modelling Language (POSTER et DEMO)
Auteurs :
François Fages INRIA Rocquencourt
Julien Martin INRIA

Titre : Moose: an Agile Reengineering Environment (POSTER et DEMO)
Auteurs :
Alexandre Bergel INRIA Lille
Stephane Ducasse INRIA Lille

Titre : MotOrBAC: a tool to specify, administrate and deploy security policies (POSTER et DEMO)
Auteurs :
Autrel Fabien ENST Bretagne
Frederic Cuppens ENST Bretagne
Nora Cuppens-Boulahia Département RSM Telecom Bretagne
Celine Coma ENST Bretagne

Titre : Modélisation des langages de programmation et Processus de développement de logiciels (POSTER)
Auteurs :
Thanh Thanh LE THI IRIT - UPS

Thierry Millan IRIT - UPS
Erwann Poupart CNES
Laurent Sabatier SOFT- MAINT/SODIFRANCE
Jean-charles Dalbin Airbus

Titre : CALICO : a Component Assembly Interaction Control Framework (POSTER)
Auteurs :
Guillaume Waignier INRIA/LIFL/Université de Lille 1
Anne-Francoise Le Meur INRIA/LIFL/Université de Lille 1
Laurence Duchien INRIA/LIFL/Université de Lille 1

Titre : FoCalTest : Un outil de test automatique pour FoCal (POSTER)
Auteurs :
Matthieu Carlier ENSIIE-CÉDRIC
Catherine Dubois ENSIIE-CÉDRIC

Titre : FraSCAti: An Open SCA Platform (POSTER)
Auteurs :
Nicolas Dolet INRIA
Laurence Duchien USTL - INRIA
Damien Fournier INRIA
Philippe Merle INRIA
Lionel Seinturier USTL - INRIA

Titre : Programmer des Fonctions Biologiques Synthétiques (POSTER)
Auteurs :
DELAPLACE Franck IBISC (UNIV.EVRY)
GIAVITTO Jean Louis IBISC (UNIV. EVRY)
MICHEL Olivier LACL - PXII
SPICHER Antoine LACL - PXII

Titre : Bad smell de conception et leçons apprises en conception objets (POSTER)
Auteurs :
Cédric BOUHOURS IRIT - équipe MACAO
Hervé LEBLANC IRIT - équipe MACAO
Christian PERCEBOIS IRIT - équipe MACAO

Titre : Extraction d’architecture guidée par les modèles (POSTER)
Auteurs :

Sorana Cimpan LISTIC Lab., Polytech'Savoie, Université de Savoie (France)
Hervé Verjus LISTIC Lab., Polytech'Savoie, Université de Savoie (France)
Azadeh Razavizadeh LISTIC Lab., Polytech'Savoie, Université de Savoie (France)

Titre : Concretising Software Architectures based on the Pi-Architecture Description Language (POSTER et DEMO)
Auteurs :
Zawar QAYYUM Université Européenne de Bretagne - UBS/VALORIA
Flavio OQUENDO Université Européenne de Bretagne - UBS/VALORIA

Titre : SmPL: SimPLe SamPLes to Update Device Drivers (POSTER)
Auteurs :
Gilles Muller Ecole des Mines de Nantes
Yoann Padioleau University of Illinois-Champaign
Julia Lawall DIKU

Titre : A Component Framework for Java-based Real-Time Distributed Embedded Systems (POSTER)
Auteurs :
Ales Plsek INRIA Futurs, team ADAM
Frederic Loiret INRIA Lille - Nord Europe
Michal Malohlava Charles University
Philippe Merle INRIA Lille - Nord Europe
Lionel Seinturier INRIA Lille - Nord Europe

Titre : Composition de modèles par points de vue dans le profil VUML (POSTER)
Auteurs :
Younes Lakhrissi IRIT
Adil Anwar IRIT
Bernard Coulette IRIT