# ANALYSES STATIQUES : CERTIFIER ET QUANTIFIER

le 30 août 2010 14h00

ENS Rennes Salle du Conseil
Plan d'accès

**Soutenance d'HDR de David Cachera (ENS Cachan - IRISA).**
**Spécialité Informatique**

Ce travail présente quelques contributions dans le domaine des méthodes formelles de vérification des systèmes matériels et logiciels. Pendant longtemps, la seule technique utilisable à grande échelle pour vérifier un système informatique a été le test. S'il permet de trouver des erreurs, il ne garantit pas en revanche leur absence. Les méthodes formelles en revanche poursuivent cet objectif, puisqu'elles assurent l'absence de certaines classes d'erreurs.

Initialement cantonnées à la vérification de systèmes de petite taille, elles s'attaquent dorénavant à des systèmes de taille réelle, tels des processeurs ou des logiciels embarqués sur des avions. Du fait de la complexité de ces systèmes, il faut faire appel à l'outil informatique lui-même pour mécaniser ce travail de raisonnement. Pour ce faire, deux chemins peuvent être empruntés. Le premier consiste à demander une aide humaine dans la conception des preuves : on parle alors de preuve assistée par ordinateur. L'autre chemin consiste à utiliser des techniques d'analyse statique : celles-ci assurent de façon automatique que certains programmes respectent certaines propriétés, en examinant le « texte » du programme sans l'exécuter, mais ne peuvent pas toujours fournir une réponse.

Depuis leur origine, les travaux de recherche de David Cachera s'inscrivent dans ce cadre de la vérification de systèmes informatiques par application de méthodes formelles, en particulier dans le domaine des systèmes embarqués. On y parle donc de sémantiques, nécessaire à la modélisation du comportement des systèmes, de logiques, pour prouver des propriétés, d'assistants de preuve et d'analyses statiques.

Depuis 1998, ces travaux de recherche ont été menés au sein de l'Institut deRecherche en Informatique et Systèmes aléatoires (IRISA), successivement dans les équipes-projets INRIA COSI, où David Cachera s'est intéressé à la vérification de systèmes mixtes matériel-logiciel décrits dans le modèle polyédrique, puis Lande et Celtique, où il s'est intéressé à la vérification par des techniques d'analyse statique.

Le mémoire d'habilitation se concentre sur ces derniers travaux, et plus précisément sur deux aspects peu explorés auparavant : la certification d'analyses statiques, et le traitement de propriétés de nature quantitative.
L'idée de base d'une analyse statique consiste à calculer, non pas ce que ferait un programme sur n'importe laquelle de ses entrées, ce qui est impossible, mais seulement une approximation de son comportement. La théorie de l'interprétation abstraite fournit un cadre général pour définir de façon systématique des abstractions, prouver qu'elles sont correctes par rapport à la sémantique initiale des programmes, et comparer entre elles différentes abstractions.

Même si la théorie de l'interprétation abstraite fournit des outils méthodologiques pour définir des analyses statiques correctes par construction, le passage de la spécification (des formules mathématiques) à l'implémentation (le code d'un analyseur) nécessite de mettre en œuvre des techniques de vérification formelle afin de garantir que l'analyseur lui-même ne comporte pas d'erreurs. De plus, les preuves « manuelles » de correction des analyses sont souvent partielles (ne donnant pas tous les détails, parfois considérés comme implicites), voire ne font pas référence exactement à l'implantation finale de l'analyseur, qui peut comporter des optimisations. Le but de leur travail a donc été de fournir des outils, tant conceptuels que pratiques, de certification des analyses statiques. Les outils de certification que nous avons développés reposent sur

l'utilisation de l'assistant de preuve Coq, qui permet de construire des preuves de correction des analyses statiques en logique constructive et d'obtenir des analyseurs certifiés par extraction du code à partir de la preuve. Une difficulté majeure vient de la non calculabilité des spécifications d'analyses statiques par interprétation abstraite, même si l'analyseur obtenu in fine calcule un résultat effectif. La difficulté théorique consiste donc à identifier une version affaiblie de l'interprétation abstraite pouvant être traitée en logique constructive. D'un point de vue plus pratique, il faut s'assurer que les solutions proposées permettent la construction d'analyses certifiées de façon modulaire, afin de pouvoir aborder des analyses sur des propriétés et des langages réalistes.

Les aspects critiques des systèmes tiennent à leur comportement fonctionnel, c'est-à-dire au résultat de leur calcul, mais également à des caractéristiques non fonctionnelles, en particulier la consommation de ressources (temps, mémoire, énergie, etc.). Les analyses statiques quantitatives vonr s'intéresser à cet aspect. Le principal défi consiste ici à passer d'un modèle qualitatif bien connu, l'interprétation abstraite fondée sur une notion d'ensemble ordonné, à un modèle quantitatif qui ne peut se contenter de manipuler des relations d'ordre. Pour exprimer et manipuler des quantités dans les sémantiques, nous avons fait appel à la théorie des dioïdes idempotents, aux structures de moduloïdes construites sur ces dioïdes, et aux opérateurs linéaires sur ces structures. Ceci leur a permis de définir un modèle quantitatif de la sémantique d'un programme, et une théorie de l'abstraction sur ce modèle.

## THÉMATIQUE(S)

Vie des personnels, Recherche - Valorisation

## CONTACT

David Cachera

Mise à jour le 4 septembre 2015

## ARCHIVES

Séminaires 2020-2021
Séminaires 2019-2020
Séminaires 2018-2019
Séminaires 2017-2018
Séminaires 2016-2017
Séminaires 2015-2016
Séminaires 2014-2015
Séminaires 2013-2014
Séminaires 2012-2013
Séminaires 2011-2012
Séminaires 2010-2011
Séminaires 2009-2010
Séminaires 2008-2009
Séminaires 2007-2008
Séminaires 2006-2007
Séminaires 2005-2006
Séminaires 2004-2005
Séminaires 2003-2004
Séminaires 2002-2003

## JURY :

**Pierre Crégut**, Orange Labs, rapporteur
**Nicolas Halbwachs**, CNRS, rapporteur
**Sanjay Rajopadhye**, U. Colorado, rapporteur

**Roberto Giacobazzi,** U. Vérone
**Claude Jard**, ENS Cachan
**Thomas Jensen**, INRIA