David Monniaux — candidature HDR

1 Recherche passée

Avant ma thèse, suite à un stage très intéressant à SRI International, je me suis intéressé à l'analyse de protocoles cryptographiques. C'est sur ce sujet que j'ai fait mes premières publications (CSFW 99, SAS 99). Ayant suivi les cours de Christine Paulin-Mohring d'abord à Lyon puis à Paris, je me suis également intéressé aux applications des assistants de preuve. J'ai pu combiner cette curiosité avec mon attrait pour les techniques d'analyse automatique de programmes et de protocoles en faisant mon stage de DEA avec Patrick Cousot sur la réalisation d'analyseurs statiques formellement prouvés.

L'analyse statique consiste à dériver automatiquement des propriétés d'un programme par analyse de son code source (ou de son code objet), mais sans l'exécuter. Si certains incluent dans ce terme des analyses purement syntaxiques comme la détection de certains « motifs » dans le code source ou l'évaluation de la « complexité cyclomatique » du flot de contrôle, je ne me suis intéressé qu'aux analyses statiques fondées sur une relation mathématiquement définie entre le résultat de l'analyse et la sémantique du programme analysé. Il s'agit donc ici d'une « méthode formelle ».

Ma thèse (1999-2001) portait sur l'analyse statique de programmes probabilistes. Il s'est avéré que même simplement définir une sémantique concrète pour ces programmes n'est pas si aisé, notamment en présence d'une combinaison de phénomènes non-déterministes (choix totalement arbitraire entre plusieurs possibilités) et probabilistes (choix vérifiant une distribution de probabilité), qui ne doivent pas être confondus. Quant à l'analyse automatique, les techniques de model-checking ou d'abstraction qui fonctionnent bien habituellement sont assez difficiles à appliquer, en raison de la complexité des objets à abstraire (ensembles de distributions de probabilité, etc.). Mon travail était donc principalement à visée théorique.

En 2002, j'ai candidaté dans divers établissements dont le CNRS et l'INRIA (j'envisageais, par exemple, d'aller travailler dans l'équipe de Xavier Leroy). C'est à ce moment que Patrick Cousot, qui jusqu'à présent faisait plutôt un travail de théorie et d'implémentations académiques, a lancé son projet « Astrée », qui visait à fournir des analyseurs statiques adaptés à la preuve d'absence d'erreur à l'exécution sur des programmes

critiques embarqués de taille respectable — à savoir, principalement, les commandes de vol électriques des appareils Airbus. Cet objectif était très ambitieux, car une bonne partie des travaux en analyse statique de programmes s'intéressent à des codes de taille modeste, ou évitent de prendre en compte certaines particularités agaçantes comme l'usage de langages à la sémantique parfois mal définie (comme C), les calculs en virgule flottante, l'arithmétique de pointeurs, ou encore le fait que les variables entières sont prises modulo 2^n. Ici, nous combinions les difficultés, et notre seul espoir résidait dans le fait que les codes de contrôle-commande critiques sont une classe restreinte de programmes, réalisés à partir de composants élémentaires (e.g. filtres numériques) que l'on peut espérer comprendre isolément, et pour lesquels des règles de programmation assez sévères évitent les horreurs que l'on peut trouver dans les programmes C en général. Ce projet a été un grand succès, puisqu'il a permis de fournir un outil, actuellement en cours d'industrialisation par la société AbsInt, qui répondait à une demande que les outils commerciaux (par exemple l'outil PolySpace) ne satisfaisaient pas.

Bien que je sois chercheur, j'ai tenu à maintenir au cours des années une petite activité d'enseignement. Je suis depuis 2003 enseignant à temps partiel à l'École polytechnique (Palaiseau), et j'envisage d'y solliciter une promotion comme professeur chargé de cours à temps partiel (équivalent d'un professeur des universités de deuxième classe, l'École polytechnique, dépendant du Ministère de la Défense, ayant ses propres grades). J'ai également fait divers cours relatifs aux sémantiques et à l'analyse statique aux niveaux M1/M2.

2 Perspectives de recherche

Ayant quitté en 2007 l'équipe de Patrick Cousot pour le laboratoire VERIMAG de Grenoble pour des raisons familiales, j'ai décidé de m'atteler à des recherches tendant à remédier à certaines faiblesses de l'état de l'art en analyse statique que j'avais constatées notamment lors du projet Astrée :

- Les techniques d'obtention d'invariants par élargissement sont délicates (de petites perturbations apparemment anodines peuvent amener à des résultats bien plus mauvais), coûteuses (itérations nombreuses) et n'offrent pas de garantie de précision. Il est donc intéressant de pouvoir, dans certains cas, calculer des invariants par des méthodes plus directes, par exemple d'optimisation sous contraintes.
- Les analyses monolithiques, à relancer sur l'intégralité du programme en cas de modification, passent difficilement à l'échelle. Malheureusement, l'état de l'art en ce qui concerne les analyses modulaires est assez insuffisant.

En liaison avec des collègues de l'INRIA, du CEA et de l'École polytechnique, nous avons donc lancé le projet ANR « ASOPT », qui vise à appliquer des techniques de résolution géométrique, numérique ou logique sous contraintes à l'analyse de programmes. Je viens de publier des résultats s'intégrant dans ce projet (sur la réduction de la recherche de certains invariants à l'élimination de quantificateurs, et sur les moyens de faire efficacement cette élimination), mais il reste à faire un travail considérable dans ce domaine : recherche d'algorithmes de résolution plus efficaces, abstractions plus efficaces pour les variables numériques, abstractions couplées valeurs discrètes / booléens / quantités numériques... Je compte travailler sur ces sujets au cours des prochaines années.

Ces sujets me permettent également de renouer avec mon sujet de DEA. En effet, si l'on obtient l'analyseur statique non par une programmation manuelle de fonctions de transfert abstraites, mais par une dérivation automatisée à partir d'algorithmes généraux (par exemple, l'élimination de quantificateurs), il est plus facile de fabriquer, en sus de l'implémentation de l'analyse, une preuve de correction de celle-ci.

En ce qui concerne l'encadrement doctoral, la situation à Paris n'était pas très favorable. Le nombre d'étudiants au MPRI (*master parisien de recherche en informatique*), qui offre une formation en analyse de programmes et autres méthodes formelles, est en effet assez faible au regard du nombre d'équipes d'accueil possibles et il semble que les étudiants considèrent que sujets d'analyse statique sont trop ardus. J'ai cependant pu encadrer le stage d'un normalien, ainsi que ceux de deux doctorants (David Pichardie et Shivali Agarwal) que leurs directeurs de thèse voulaient voir familiariser avec l'interprétation abstraite et les techniques développées dans notre équipe.

Depuis mon arrivée à Grenoble, la situation s'est considérablement améliorée. L'an dernier, j'ai eu deux normaliens en stage, ainsi qu'un étudiant de l'ENSIMAG. J'ai pu recruter un étudiant en thèse CIFRE (coencadrée avec Nicolas Halbwachs) sur l'application de l'analyse statique à l'optimisation sur des représentations SSA dans les générateurs de codes de compilateurs. Je suis également sollicité par un polytechnicien qui voudrait venir en thèse sur l'analyse modulaire des nœuds du langage Lustre et par une étudiante de Paris 6 qui voudrait venir en stage de M2 recherche sur l'analyse statique.

Je désire obtenir l'habilitation à diriger les recherches d'une part pour pouvoir encadrer des étudiants en mon propre nom, d'autre part pour pouvoir solliciter la promotion comme professeur chargé de cours que j'évoquais plus haut.