Magistère de Mathématiques Fondamentales et Appliquées à l'Informatique
École Normale Supérieure

Mémoire de Magistère

Élodie-Jane Sims.

Soutenu le 9 octobre 2002.

Chapitre 1

Résumé du cursus

Première année : 1999-2000

Cours de licence d'informatique

- Algorithmique et programmation *J. Stern*
- Langages de programmation et compilation *P. Cousot*
- Théorie de l'information *J. Vuillemin*
- Langages formels, calculabilité, complexité et analyse d'algorithmes *P. Gastin*

Cours de mathématique

- Logique *A. Louveau*

Cours de maîtrise d'informatique

- Bases de données *N. Spyratos*
- Sémantique des langages de programmation *P. Cousot*

Stage de maîtrise

- Planification de mouvements sans collision pour robots non holonomes, *sous la direction de Florent Lamiraux et Jean-Paul Laumond, au* L.A.A.S. *(Toulouse).*

Seconde année : 2000-2001

Cours de maîtrise d'informatique

- Réalisation de systèmes matériels *M. Shand, J. Vuillemin*
- Planification de mouvement en robotique et en animation graphique *J.-P.Laumond, F.Lamiraux*

Stage à l'étranger

- Alloy language and temporal logic – Shape analysis, *sous la direction de David Schmidt, à* Kansas State University *(U.S.A.).*

Troisième année : 2001-2002

D.E.A. Programmation : Sémantique, Preuves et Langages

Cours de D.E.A : tronc commun

- Termes en logique de premier ordre *J.-P. Jouannaud*
- λ-calcul *J.-J. Lévy*
- Preuves constructives *B. Werner*
- Sémantiques des programmes séquentiels*M. Fernandez*
- Typage et programmation *X. Leroy*

Cours de D.E.A : options

- Langages synchrones *M. Pouzet*
- Fondements de l'interprétation abstraite *P. Cousot*
- Analyse statique par interprétation abstraite *B. Blanchet, L. Mauborgne*
- Sémantique géométrique et probabiliste *É. Goubault, D. Monniaux*
- Vérification de systèmes infinis *A. Bouajjani*
- Logiques temporelles et automates *H. Comon*

Stage de D.E.A.

- Analyse statique de pointeurs et logique BI, *sous la direction de Radhia Cousot*, *à l'* École polytechnique.

Chapitre 2

Documents attachés

Mémoire de D.E.A. *(page 7)*

Titre : Analyse statique de pointeurs et logique BI

Directeur : Radhia Cousot

Lieu : École polytechnique, *équipe de Sémantique, preuve et interprétation abstraite*

Dates : Avril-Août 2002

Résumé : Mon stage s'est placé dans le cadre de l'analyse statique de logiciels comportant des objets alloués dynamiquement sur un tas et repérés par des pointeurs. La *logique BI*, récemment développée, est une logique de Hoare avec un langage d'assertions/de prédicats permettant de démontrer qu'un programme manipulant des pointeurs sur un tas est correct. Nous souhaiterions utiliser la logique BI comme interface pour exprimer les résultats d'analyses modulaires de pointeurs.

La sémantique des triplets de la logique BI est définie par des transformateurs de prédicats de style plus faible pré-condition adaptée seulement à l'analyse arrière. Pendant mon stage, j'ai prouvé la correction des plus faible pré-conditions (wlp). J'ai exprimé les plus fortes post-conditions (sp), et conditions d'absence d'erreurs et prouvé la correction de l'analyse avant. J'ai ensuite démontré la correction d'une analyse avant de partition de pointeurs en exprimant une traduction des partitions (invariants de l'analyse) dans le langage BI.

Rapport de stage à l'étranger *(page 58)*

Titre : Alloy language and temporal logic – Shape analysis

Directeur : David Schmidt

Lieu : Kansas State University (U.S.A.)

Dates : Février-Août 2001

Résumé : Mon stage, dans le cadre de la vérification statique de programmes, a consisté en deux projets, l'un lié aux logiques temporelles et l'autre lié à l'analyse de pointeurs.

Martin Rinard fait de l'analyse de pointeurs qui transforme un programme d'un langage objet en un graphe à deux types d'arêtes. Avec ce type de graphes, il veut vérifier des propriétés de correction.

Daniel Jackson travaille sur un langage appelé Alloy avec lequel nous pouvons définir un modèle et vérifier des propriétés du modèle.

Le but de ce stage était de coder les graphes de Rinard en Alloy, de donner des traductions de logiques temporelles en Alloy puis de vérifier des propriétés des graphes.

Nous avons d'abord travaillé avec Alloy et traduit CTL en Alloy mais nous avons vu que Alloy ne permettait pas de traduire LTL ou le μ-calcul. (Dans le rapport, la présentation de ce premier travail n'est pas très rédigée). Nous avons ensuite étudié l'analyse de pointeur de Martin Rinard.

Rapport de stage de maîtrise *(page 107)*

Titre : Planification de mouvements sans collision pour robots non holonomes

Directeurs : Florent Lamiraux et Jean-Paul Laumond

Lieu : L.A.A.S. (Toulouse), *groupe Robotique et Intelligence Artificielle*

Dates : Juillet-Septembre 2000

Résumé : Mon travail s'est inscrit dans le domaine de la planification de mouvements dont le but est de calculer des déplacements pour des robots.

L'équipe développait une plate-forme logicielle générique (appelée Move3D) dédiée à la planification de mouvements sans collision dans des environnements tridimensionnels encombrés. Cette plate-forme, basée sur un algorithme aléatoire, permet, si on lui fournit un planificateur local adapté au robot, de trouver un chemin s'il en existe un.

Une voiture (ou un robot à deux roues avec une remorque) est un système soumis à des contraintes de non glissement et d'angle de braquage maximal. Un chemin "faisable" par un tel robot doit respecter ces contraintes. De tels chemins existaient et le but de mon stage était l'intégration de ces chemins sous forme d'un planificateur local pour Move3D.

Chapitre 3

Projet de thèse

Analyse statique de pointeurs et logique BI

Thèse sous la direction de Radhia Cousot (École Polytechnique, France) et de David Schmidt (Kansas State University, U.S.A.), financée par une bourse BDI-C.N.R.S.

Analyse statique Le cadre de ma thèse est l'analyse statique de logiciels comportant des objets alloués dynamiquement sur un tas et repérés pas des pointeurs. Le but final étant de trouver des erreurs dans un programme (problèmes de déréférencements, d'alias...) ou de prouver qu'un programme est correct (relativement à ces problèmes) de façon automatique.

Logique BI Isthiaq, Pym, O'Hearn et Reynolds ont développé récemment la *logique BI* qui est une logique de Hoare avec un langage d'assertions/de prédicats permettant de démontrer qu'un programme manipulant des pointeurs sur un tas est correct. La sémantique des triplets de la logique BI ($\{P\}C\{P'\}$) est définie par des transformateurs de prédicats de style plus faible pré-condition.

Le langage d'assertion inclut des connecteurs spatiaux de conjonction et d'implication combinés avec les connecteurs de la logique classique. La conjonction $P * Q$ est vrai exactement quand le tas courant peut être coupé en deux composantes disjointes, une qui rend P vraie et l'autre qui rend Q vraie. L'implication $P \mathrel{-\!\!*} Q$ dit que à chaque fois que P est vraie pour un "nouveau" morceaux de tas, Q est vraie pour la combinaison du vieux et du nouveau tas. De plus, il y a une formule atomique, $E \mapsto F, G$, qui dit que E pointe sur une cellule `cons` contenant F et G. Un des intérêts de cette logique est qu'elle permet de raisonner localement.

Projet L'objectif de ma thèse est de :

1 développer des analyses statiques de pointeurs en avant et en arrière ainsi que leur combinaisons;

2 démontrer la correction des analyses 1. par interprétation abstraite des sémantiques de transformateurs de prédicats;

3 étudier la traduction des invariants abstraits produits automatiquement par les analyses 1. sous forme du langage d'assertions de la logique BI (ce qui permet d'afficher en clair les résultats des analyses de pointeurs);

4 inversement, étudier la traduction du langage d'assertions de la logique BI en termes de prédicats abstraits utilisés dans les analyses 1. (ce qui implique en général des approximations formalisées par la fonction d'abstraction spécifiant l'analyse 1.);

5 utiliser ces traductions 3. et 4. pour produire des analyses modulaires de pointeurs basées sur l'usage d'interface engendrées automatiquement ou écrites par les utilisateurs dans le langage d'assertions de la logique BI.