

Analyse statique par interprétation abstraite de systèmes hybrides

Olivier Bouissou

Laboratoire Modélisation et Analyse de Systèmes en Interaction,
CEA - Centre de Saclay, F-91191 Gif-sur-Yvette Cedex

Résumé Si l'intérêt et l'efficacité des méthodes d'analyse statique par interprétation abstraite pour la vérification des programmes critiques embarqués ne sont plus à démontrer, il est maintenant nécessaire d'obtenir des méthodes les plus précises possibles. Si l'utilisation de domaines abstraits relationnels de plus en plus élaborés permet de diminuer la surapproximation dont souffrent les domaines les plus simples, les analyses actuelles souffrent toujours d'une mauvaise prise en compte des entrées du programme. Ces entrées sont fournies par un capteur qui mesure une grandeur physique, et sont généralement surapproximées par un intervalle. Une piste d'étude récente pour mieux gérer ces entrées continues consiste à étudier, outre le programme lui-même, l'environnement physique dans lequel il est exécuté. On obtient ainsi un système plus complexe comprenant une dynamique discrète (le programme) et une dynamique continue (l'environnement). L'étude de tels systèmes hybrides repose actuellement essentiellement sur des extensions des automates à états finis et des algèbres de processus introduisant une dynamique continue. L'analyse de ces systèmes par des techniques de *model-checking* souffre encore d'une explosion combinatoire excluant leur utilisation pour les logiciels embarqués critiques les plus gros.

La première contribution de cette thèse est une extension des langages de programmation impératifs permettant de décrire à la fois le programme, l'environnement extérieur et les interactions entre le programme et l'environnement. L'environnement physique est décrit par un ensemble d'équations différentielles représentant chacune un mode continu, et les interactions entre le programme et l'extérieur sont modélisés par deux mots clés représentant les capteurs et actionneurs. Nous donnons à l'ensemble (programme plus environnement physique) une sémantique dénotationnelle qui reste très proche de celle définie pour les langages impératifs classiques. La difficulté majeure dans la construction de cette sémantique a été de définir une sémantique pour la partie continue : les solutions des équations différentielles sont exprimées comme le plus petit point fixe d'un opérateur monotone dans un CPO, et nous montrons que les itérées de Kleene convergent vers ce point fixe.

La seconde contribution est une méthode d'analyse statique par interprétation abstraite de ces systèmes hybrides. Cette méthode fonctionne en deux temps. Tout d'abord, sous certaines restrictions portant sur le programme à analyser, on construit un recouvrement de l'espace des variables d'entrée via une analyse par intervalle couplée à une analyse d'atteignabilité en avant. On obtient ainsi une abstraction de l'impact qu'a le programme sur l'évolution continue : l'espace d'entrée du programme est découpé en zones dans lesquelles on est sûr qu'un actionneur sera activé. Dans un deuxième temps, nous utilisons ce recouvrement et une méthode d'intégration garantie des équations différentielles pour obtenir une surapproximation de l'évolution continue. Un analyseur prototype implémentant ces techniques a été développé et les tests sur les exemples classiques de systèmes hybrides montrent de bons résultats.

Enfin, la troisième contribution de cette thèse est une nouvelle méthode d'intégration garantie nommée GRKLib. Contrairement aux méthodes existantes, GRKLib se fonde sur un schéma d'intégration numérique non garantie (nous avons choisi un schéma de Runge-Kutta d'ordre 4, mais n'importe quelle autre convient) et nous calculons, en utilisant l'arithmétique d'intervalles, l'erreur globale commise lors de l'intégration numérique. Cette erreur s'exprime comme la somme de trois termes : l'erreur sur un pas, la propagation de l'erreur et l'erreur due aux nombres flottants. Chaque terme est calculé séparément et des techniques avancées permettent de les réduire et de contrôler au mieux le pas d'intégration pour limiter l'accroissement de l'erreur globale. Une librairie C++ implémentant ces concepts a été développée, et les résultats présentés dans cette thèse sont prometteurs.

Mots clés : *interprétation abstraite ; systèmes hybrides ; sémantique dénotationnelle ; équations différentielles ; intégration garantie ; analyse par intervalles.*