CONTROVERT : Vérification de systèmes de contrôle

Objectifs

De nombreuses erreurs, fameuses et coûteuses (comme l'échec d'Ariane 5.01, l'erreur tragique des missiles « Patriot » ou la perte de « Mars orbiter »), sont autant de rappels qu'il est nécessaire de vérifier formellement le logiciel embarqué dans les systèmes contrôlés par ordinateur, que ce soit dans le domaine aérospatial, de l'automobile, de l'appareillage médical ou tout autre système critique.

État de l'art

Cette dernière décennie, des progrès, utilisant des idées similaires d'approximation, ont été réalisés indépendamment dans deux domaines fondamentaux :

- En ce qui concerne la conception des systèmes de contrôle/commande, les méthodes empiriques traditionnelles sont de plus en plus remplacées par des méthodes non-linéaires de la programmation semi-définie basée sur la sur-approximation des trajectoires possibles du système continu par relaxation Lagrangienne.

  Ces progrès restent conceptuels, puisqu'une conception correcte des systèmes de contrôle/commande est loin de couvrir tous les désastres potentiels dans le logiciel (comme un simple débordement dans le cas d'Ariane 5.01) ;
- En analyse statique par interprétation abstraite, le projet ASTRÉE (`http://www.astree.ens.fr/`) a permis de montrer que les méthodes de sur-approximation discrète des comportements possibles de programmes synchrones de contrôle/commande passent à l'échelle pour démontrer l'absence d'erreurs à l'exécution dans des logiciels industriels embarqués critiques (comme les logiciels de contrôle de vol électrique des Airbus 340 et A380).

  Cette vérification effectuée automatiquement reste partielle et ne concerne pas la contrôlabilité du système (comme une erreur d'inversion de signe).

Dans les deux cas, les idées de sur-approximation des comportements d'un modèle du système et de son contrôleur ou de la sémantique du programme sont très similaires.

Vérification par approximation

L'idée du projet CONTROVERT est basée sur une opportunité évidente de fertilisation croisée entre les deux domaines, jusqu'ici indépendants ou, pour le moins, sur l'espoir que les méthodes de vérification utilisées en théorie du contrôle peuvent se prolonger au cours de la conception jusqu'à la vérification du programme de contrôle embarqué.

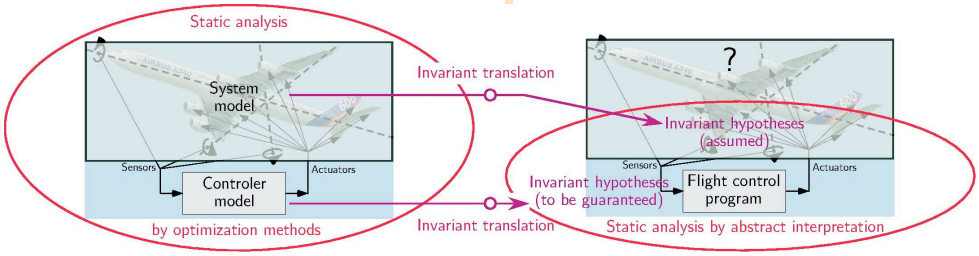
Innovation et points forts

La vérification d'un programme consiste à prouver que la sémantique du programme (définissant les comportements discrets possibles des calculs) satisfait des spécifications données. Les spécifications actuellement utilisées dans le projet ASTRÉE sont simplement liées aux limitations du matériel (comme le domaine de valeurs possibles des capteurs), mais à part ces restrictions, ignorent complètement le comportement et les propriétés du système contrôlé. Le projet CONTROVERT va permettre de faire progresser l'état de l'art actuel :

- en dérivant la spécification (hypothèse et propriétés à vérifier) par discrétisation du modèle du système et de son contrôleur ;
- en dérivant des invariants discrets du programmes à partir des propriétés continues du système contrôlé obtenues en théorie du contrôle/commande ;
- en vérifiant formellement la spécification du programme par interprétation abstraite en utilisant les invariants discrets du programme pour guider l'analyse (et tenter de démontrer leur validité sur le programme).

Partenariat

Le projet a été élaboré en regroupant des compétences complémentaires en théorie du contrôle (P. Apkarian, ONERA/DCSD & Université Paul Sabatier de Toulouse) et D. Noll (Université Paul Sabatier de Toulouse) et en interprétation abstraite (P. Cousot, ENS et R. Cousot, CNRS & École Polytechnique).



Pierre Apkarian, UPS, Toulouse, apkarian@cert.fr
Patrick Cousot, ENS, Paris, cousot@ens.fr
Radhia Cousot, CNRS, Paris, Radhia.Cousot@polytechnique.fr
Dominikus Noll, UPS, Toulouse, noll@mip.ups-tlse.fr