ASTRÉE : Analyse Statique de logiciels Temps-RÉel Embarqués

2002
Exploratoire

Objectifs

1) Le problème considéré est de ***démontrer*** statiquement (à la compilation) et automatiquement l'*absence d'erreur à l'exécution* dans des ***logiciels critiques temps-réel embarqués*** ;
2) Le problème étant indécidable la technique retenue est celle de l'*analyse statique* basée sur *la théorie de interprétation abstraite* en procédant par approximation de la sémantique des programmes et de l'environnement d'exécution ;
3) Pour de grands programmes complexes, les analyseurs statiques généraux produiraient trop de fausses alarmes ;
4) L'objectif ultime est d'***éliminer toute fausse alarme***.

Innovation & Points forts

L'objectif du projet ASTRÉE est de concevoir un ***analyseur statique automatique adaptatif par paramétrisation*** :

- dédié à :
  - une classe de logiciels critiques, temps réel embarqués, et
  - une classe de propriétés relatives à la sûreté de fonctionnement et au temps réel ; et
- spécialisable à un programme quelconque de la famille grâce à un choix interactif assisté :
  - des parties du programme nécessitant des raffinements des propriétés abstraites utilisées par l'analyseur, et
  - des spécifications de l'environnement d'exécution,

et ce pour tendre vers zéro fausse alarme. Cette nouvelle approche est une ***première dans le domaine de l'analyse statique***, les analyseurs généraux actuellement disponibles n'étant pas paramétrables pour s'adapter aux besoins des utilisateurs.

Retombées

Montrer que l'analyse statique par interprétation abstraite (actuellement principalement utilisée pour la vérification de programmes lors de leur mise au point) peut également être utilisée comme technique de ***preuve de correction de propriétés de sûreté et fiabilité*** de logiciels complexes ;

Analyser des logiciels en cours de développement pour les nouveaux programmes d'Airbus France ;

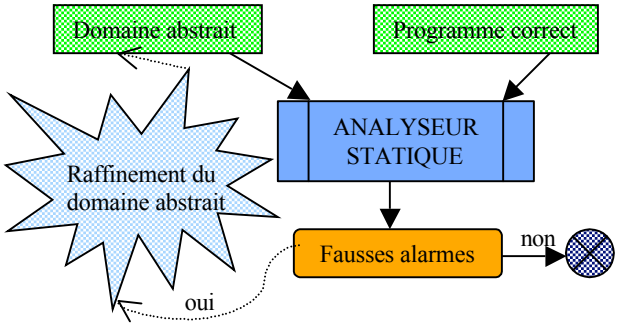
Mettre la ***technologie au service de la communauté***.

Partenariat

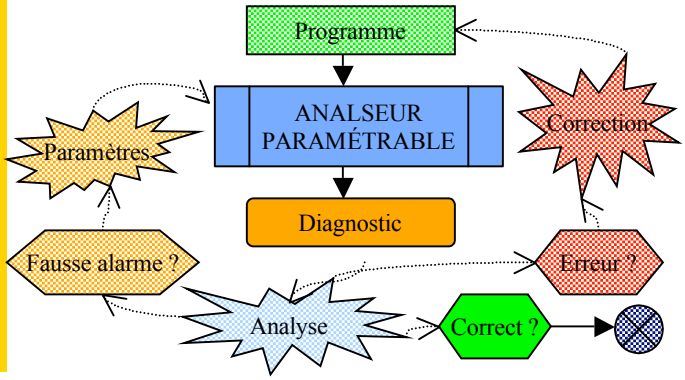
1) Les partenaires académiques (***CNRS — École normale supérieure*** et ***CNRS — École polytechnique***), spécialistes de l'interprétation abstraite, sont chargés de la conception et de la réalisation de l'analyseur statique et de son adaptation à la famille de logiciels considérée ;
2) Le partenaire industriel (***Airbus France***) conduit l'expérimentation et l'évaluation de l'analyseur statique sur ses logiciels.

Principe de base

Première phase : ***conception expérimentale d'un analyseur adaptatif*** pour une famille de logiciels réputés corrects par des spécialistes de l'analyse statique ;



Deuxième phase : l'utilisateur final prouve l'absence d'erreurs à l'exécution de nouveaux logiciels de la famille par ***paramétrisation de l'analyseur statique adaptatif*** :



Réalisations et résultats

Le projet ASTRÉE est en cours d'installation.

À défaut de pouvoir faire état de réalisations et résultats pour un projet qui n'a pas encore commencé, nous faisons état de la problématique du projet ASTRÉE.

Parmi les garanties de conformité à des spécifications comportementales, temporelles et de sûreté de fonctionnement figurent en première place la ***preuve d'absence d'erreurs à l'exécution***.

Le ***verrou technologique*** est de concilier ***correction*** (ce qui exclut les méthodes non exhaustives comme la simulation ou le test), ***automatisation*** (ce qui exclut le model-checking (où il faut fournir un modèle du programme) et les méthodes déductives (où il faut fournir une aide manuelle à la preuve)), ***précision*** (ce qui exclut les analyseurs statiques généraux qui ne prendraient pas en compte les spécificités des logiciels qu'ils analysent), ***passage à l'échelle*** (pour des logiciels de quelques centaines de milliers de lignes) et ***efficacité*** (pour intégration dans un processus de production industrielle de logiciel).

Contacts projet : Patrick COUSOT, École normale supérieure, cousot@ens.fr, Radhia COUSOT, École polytechnique, Radhia.Cousot@polytechnique.fr, Famantanantsoa RADIMBIVOLOLONA, Airbus France, famanta.randim@airbus.com, http://www.di.ens.fr/~cousot/projets/ASTREE

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'ÉCONOMIE DES FINANCES ET DE L'INDUSTRIE
MINISTERE DE LA RECHERCHE