Forum méthodes formelles

"Preuve de modèle, preuve de programme"

Février 2014

Table ronde

- *De l'utilité de l'abstraction dans la preuve, passage à l'échelle ?*
- Participants :
  - Yamine Ait Ameur (IRIT, ENSEEIHT)
  - Mathieu Clabaut (Systerel)
  - Stéphane Duprat (ATOS)
  - Florent Kirchner (CEA)
  - Emmanuel Ledinot (Dassault aviation)
  - Xavier Leroy (INRIA)
  - Benjamin Monate (TrustInSoft)
  - Christine Paulin (LRI, Univ. Paris Sud)
  - Laurence Pierre (TIMA, Univ. Grenoble)

Passage à l'échelle

- 1. Solutions pratiques pour le passage à l'échelle sur des systèmes de taille industrielle
  - Améliorations techniques pour considérer la taille/ complexité croissante des systèmes à prouver
- 2. Niveaux de complexité des spécifications industrielles et méthodes de preuve appropriées
  - Quel outil (logique, expressivité, mécanismes de preuve,...) pour quelle complexité des spécifications ?
- 3. Gestion de projet de vérification
  - Contraintes dans un contexte industriel

1. Solutions techniques pour le traitement de systèmes de taille industrielle

1. Solutions techniques

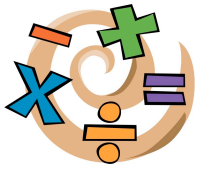
- Techniques d'abstraction
  - Pour des modèles de grande taille, ou infinis, réduction de la taille du problème à traiter P_c en le considérant de manière plus abstraite P_a
  - Sur-approximations : une propriété prouvée dans P_a sera aussi vraie dans P_c, mais *un échec sur une propriété dans P_a ne donne pas nécessairement d'information pertinente sur la validité de la propriété dans P_c*
  - Construction de P_a ?
  - Généralement utilisées dans des environnements d'analyse statique

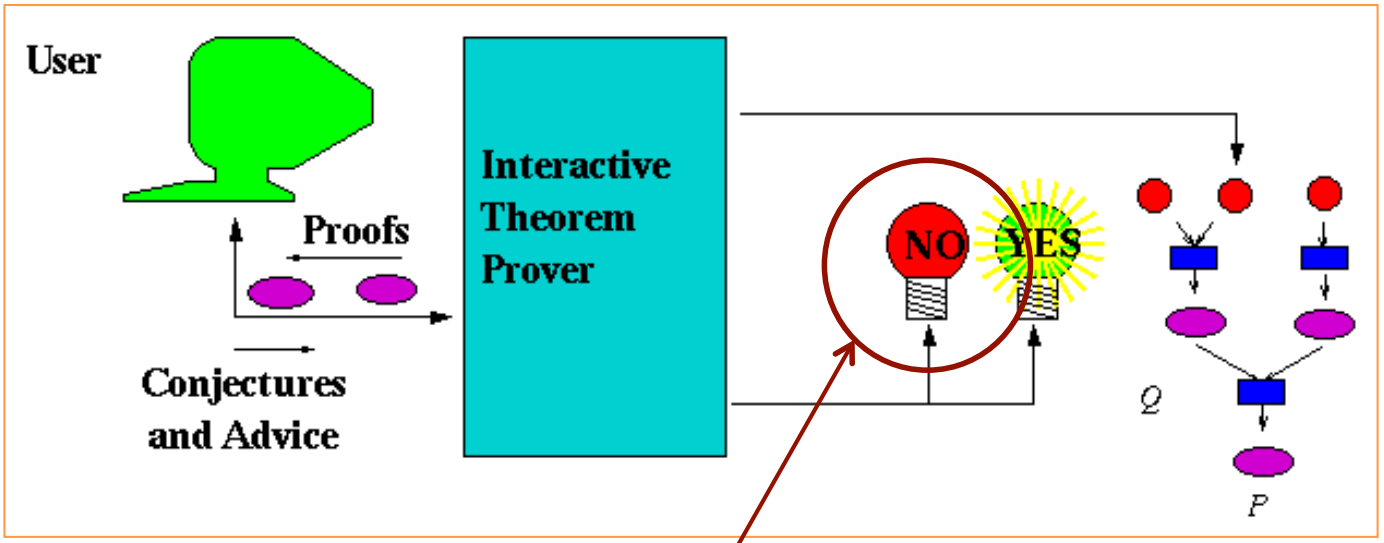
1. Solutions techniques

- Utilisation du "program slicing"
  - "Program slicing", M.Weiser, Proc. International Conference on Software engineering, 1981
  - "Program Slicing of Hardware Description Languages", E.Clarke et al, Proc. CHARME'99
  - Réduire le système considéré à un sous-ensemble, qui ne concerne que certains aspects, par exemple que les instructions dont la valeur d'une variable donnée dépend
  - Utilisation de graphes de dépendance
  - Technique exploitée dans divers contextes, dont la vérification

1. Solutions techniques

- Outils de démonstration automatique → "abstraction" inhérente à la présence de l'arithmétique, du paramétrage,... mais





Comment interpréter ce résultat ?
(décidabilité/indécidabilité !)

1. Solutions techniques

- Morale...

Vérification sans utilisation de méthodes formelles

Utilisation de méthodes formelles

1. Solutions techniques

- Parallélisation des outils de démonstration automatique
  - "A Parallelized Theorem Prover for a Logic with Parallel Execution", D.Rager, W.Hunt, M.Kaufmann, Proc. Interactive Theorem Proving 2013 : ACL2(p), version parallélisée de ACL2
  - "Shared-Memory Multiprocessing for Interactive Theorem Proving", M. Wenzel, Proc. Interactive Theorem Proving 2013 : stratégies pour la parallélisation des preuves, et version parallèle d'Isabelle