Forum Méthodes Formelles

http://projects.laas.fr/IFSE/FMF/

04/02/2014 "Preuve de modèle, preuve de programme"

Table ronde « De l'utilité de l'abstraction dans la preuve, passage à l'échelle ? »

Notes prises par Laurence Pierre (TIMA)

• Les participants à la table ronde ont proposé trois objets de réflexion relativement à cette notion de "passage à l'échelle" dans un contexte industriel :

1. Solutions pratiques pour le passage à l'échelle sur des systèmes de taille industrielle.
Il s'agit ici des diverses améliorations techniques des outils de preuve, réalisées récemment ou encore nécessaires, permettant de prendre en compte la *taille/complexité croissante des systèmes à prouver*.
Autrement dit, on considère ici la capacité à dérouler industriellement un processus de vérification par preuve, de façon *efficace* et la plus automatique possible, sur des programmes pour lesquels la spécification formelle à vérifier ne pose pas nécessairement de problème.
Parmi les évolutions techniques est notamment mentionnée la parallélisation de certains outils[1].

2. Niveaux de complexité des spécifications industrielles et méthodes de preuve appropriées.
La question ici est "quel outil (logique, expressivité, mécanismes de preuve,...) pour quelle *complexité des spécifications* ?". Autrement dit, l'accent est mis sur la capacité à traiter par preuve (en incluant la spécification) des programmes pouvant poser des difficultés nouvelles dans la spécification même.
Certains outils sont d'utilisation relativement facile/automatisée mais ne permettent pas de traiter tout type d'exigence de vérification. Des environnements de vérification plus puissants, mais moins intuitifs, peuvent être nécessaires selon les spécifications à considérer[2].

3. Problème de la gestion de projet de vérification.
Il s'agit ici des *contraintes associées à un projet de vérification* dans un contexte industriel (travail en équipe, gestion des évolutions et résistance de la preuve au

---

[1] Pour information à ce sujet, références relatives à des versions parallèles des assistants de preuve ACL2 et Isabelle :
"A Parallelized Theorem Prover for a Logic with Parallel Execution", D.Rager, W.Hunt, M.Kaufmann, Proc. Interactive Theorem Proving 2013.
"Shared-Memory Multiprocessing for Interactive Theorem Proving", M.Wenzel, Proc. Interactive Theorem Proving 2013.

[2] On rappelle notamment les capacités de paramétrisation des preuves et de prise en compte de l'arithmétique offertes par les systèmes de démonstration automatique présentés dans la journée.

changement, mesure du reste à faire, adéquation aux normes, contraintes sur les outils, alternatives de vérification lorsque la preuve n'est pas réalisable, ...)

• Pendant la discussion avec la salle, divers points ont été évoqués :

- quelles que soient les méthodes de preuve formelle retenues suivant le contexte, et malgré les progrès réalisés par les outils en termes d'utilisabilité, une certaine *expertise* est nécessaire pour mener au mieux le processus de preuve[3]. Il est nécessaire que les équipes industrielles en aient conscience et forment, ou recrutent, des spécialistes. Il peut être envisagé de former des ingénieurs en interne. Selon les méthodes à maîtriser, le temps nécessaire pour acquérir un vrai niveau d'expertise peut représenter de plusieurs jours à quelques mois. Diverses expériences ont prouvé que cela pouvait être fait avec succès. En particulier, lorsque des procédures ont été définies pour être déployées dans l'entreprise/le service, il est facile de former d'autres ingénieurs à ces procédures.

- on note qu'avec la diversité des spécifications à prouver, *un seul outil de preuve ne peut généralement être suffisant* pour un programme/système complexe. Il faut tirer profit de la richesse et de la complémentarité des outils de preuve. Cela nécessite de savoir comment exploiter cette complémentarité. En ce qui concerne le point précédent, on note donc que les ingénieurs devront en fait être formés à divers principes et divers outils. Le bénéfice obtenu en contrepartie quant à la qualité du système produit peut pleinement justifier cet effort.

- la prise en compte de *l'arithmétique* a été évoquée à plusieurs reprises dans la journée comme un point fort des assistants de preuve. Des questions restent encore ouvertes cependant quant à l'importance, pour l'acceptation de la preuve, de la perte de précision qui peut être induite par l'utilisation de l'arithmétique flottante.

- un point important qui peut se présenter également est lié à la nécessité de *qualification* des outils, induite par la nécessité de qualification des systèmes développés. Un effort supplémentaire peut donc être requis pour réaliser cette qualification, mais il faut ici aussi considérer la valeur ajoutée obtenue en retour, pour un effort consenti une fois pour toutes.

[3] Par exemple : dans le cas où le recours à l'abstraction est nécessaire, il faut savoir comment guider l'abstraction et interpréter ses résultats (ex. sur-approximations) ; dans le cas où une approche déductive (assistant de preuve) est utilisée, il faut savoir appréhender des résultats négatifs pouvant être imputables à l'indécidabilité de la logique utilisée.