

Analyse initialisation et retard non initialisé dans Vélus

Timothy Bourke et Marc Pouzet

18 décembre 2017

L'opérateur « pre » de Lustre a une valeur indéfinie au premier instant. Il est indispensable de montrer que la sémantique d'un programme ne dépend pas de cette valeur. Une analyse d'initialisation par typage est définie dans l'article [2]¹ et elle est implémentée dans le compilateur industriel KCG de SCADE 6. L'objectif de ce stage est de la formaliser, de la mettre en œuvre dans le compilateur formellement vérifié Vélus [1] et d'en prouver la correction complète, c'est-à-dire jusqu'au code exécutable produit par CompCert. Ce travail, qui permet d'ajouter l'opérateur « pre » à Vélus (celui-ci n'a que « fby » pour l'instant), présente plusieurs difficultés nouvelles : la preuve de correction dans un assistant de preuve d'une analyse statique utilisée industriellement ; la génération de code ; le lien avec le modèle mémoire de CompCert.

Si le temps le permet, le stage pourra aborder un langage étendu avec des automates hiérarchique à la SCADE 6.

Ce stage s'adresse à un étudiant ayant un fort goût pour la programmation et la formalisation de sémantiques de langages de programmation en Coq, la compilation et le typage.

Références

- [1] T. Bourke, L. Brun, P.-É. Dagand, X. Leroy, M. Pouzet, and L. Rieg. A formally verified compiler for Lustre. In *Proceedings of the 2017 ACM SIGPLAN Conference on Programming Language Design and Implementation*, pages 586–601, Barcelona, Spain, June 2017. ACM Press.
- [2] J.-L. Colaço and M. Pouzet. Type-based initialization analysis of a synchronous dataflow language. *International Journal of Software Tools for Technology Transfer*, 6(3) :245–255, Aug. 2004.

1. <http://www.di.ens.fr/~pouzet/bib/sttt04.pdf>