Preuve formelle en calcul réseau

Marc Boyer Pierre Roux (prenom.nom@onera.fr)

Laboratoire : ONERA

Ville : Toulouse

Mots clef : Coq, preuve formelle, analyse, corps des réels

De nos jours les avions ne peuvent se passer d'un important réseau embarqué pour faire communiquer les nombreux capteurs et actionneurs qui y sont disséminés. Ces réseaux ayant une fonction critique, en particulier pour les commandes de vol, il est important d'en garantir certaines propriétés telles des délais de traversé ou l'absence de débordement de buffers. Le calcul réseau est une méthode mathématique permettant de réaliser de telles preuves [2]. Elle a joué un rôle clef dans la certification du réseau AFDX, dérivé de l'ethernet, utilisé à bord des avions les plus récents (A380, A350).

Le calcul réseau se base sur des résultats mathématiques relativement simples mais déjà bien assez subtils pour qu'il soit très facile de commettre des erreurs ou des omissions lors de preuves papier. Par ailleurs, les assistants de preuve sont un bon outil pour réaliser une vérification mécanique de ce genre de preuves et obtenir un très haut niveau de confiance dans leurs résultats. Ces techniques ont même permis ces dernières années la réalisation d'un compilateur optimisant pour le langage C dont la préservation de la sémantique est prouvée. La qualification de ce compilateur pour un usage aéronautique est actuellement à l'étude.

On souhaite donc étudier la faisabilité de la preuve mécanisée de quelques propriétés fondamentales à la base de la théorie du calcul réseau. Ces résultats font intervenir des propriétés relativement basiques sur les nombres réels, telles des bornes supérieures voire des limites de fonctions linéaires par morceaux. On se propose pour cela d'utiliser l'assistant de preuve Coq ainsi que la récente librairie Coquelicot [1] étendant sa librairie de réels de base. On pourra entre autre étudier l'apport de la méthode des filtres de Bourbaki pour ce type de preuves.

Références

[1] Sylvie Boldo, Catherine Lelay, and Guillaume Melquiond. Coquelicot: A User-Friendly Library of Real Analysis for Coq. *Mathematics in Computer Science*, 9(1):41–62, March 2015.

[2] Jean-Yves Le Boudec and Patrick Thiran. *Network calculus: a theory of deterministic queuing systems for the internet*, volume 2050. Springer Science & Business Media, 2001.