



Recherche

Projet ANR CoqoPetri

Le projet ANR CoqoPetri, dont le porteur est Jérôme Leroux (département M2F, équipe MTV), a été accepté.

Dans ce projet on propose de développer plusieurs bibliothèques Rocq : les graphes infinis permettant de décrire la sémantique d'un système, l'arithmétique de Presburger, les ordinaux, et les hautes classes de complexité type Ackermann. La ligne directrice est la preuve en Rocq de l'algorithme d'accessibilité dans les réseaux de Petri.

C'est un projet mené en commun avec l'IRIF, sur une période de 4 ans, dont 24 mois de postdoc au LaBRI et 24 mois de postdoc à l'IRIF.

Les méthodes formelles fournissent des outils et des algorithmes pour la vérification et l'analyse de systèmes complexes qui peuvent détecter des bogues ou prouver la correction d'une propriété appelée spécification dans ce contexte. Ce domaine de recherche actif fournit de nombreuses méthodes et algorithmes qui dépendent de la classe de systèmes ainsi que de la classe de spécifications. La correction de ces résultats découle de preuves faites à la main. Elles sont généralement non triviales et sujettes aux erreurs. Et certaines d'entre elles contiennent des erreurs très subtiles qui prennent du temps à être découvertes. Fournir des garanties de correction et de terminaison des algorithmes développés dans le domaine des méthodes formelles est un problème intéressant mais difficile car les arguments découlent de preuves complexes.

Nous croyons fermement que les assistants de preuve comme Coq peuvent surmonter ce problème. Nous nous intéressons dans ce projet à l'algorithme d'accessibilité pour les réseaux de Petri. Les réseaux de Petri constituent un modèle bien étudié pour vérifier et étudier les systèmes concurrents, entre autres, et le problème de l'accessibilité est l'un des problèmes les plus fondamentaux des réseaux de Petri. L'étude de cet algorithme est un sujet d'actualité puisque, après quarante ans de tentatives infructueuses, Jérôme Leroux et Sylvain Schmitz ont récemment prouvé que la complexité du problème était Ackermann-complète. De plus, il a été prouvé que l'algorithme KLM était optimal pour ce problème.

Fournir des preuves Coq certifiées pour ces résultats nécessite un grand nombre de preuves génériques. Afin de résoudre ce problème difficile, nous proposons de développer une bibliothèque Coq pour les réseaux de Petri. L'objectif principal du projet est la conception d'une bibliothèque Coq qui pourra être utilisée dans une large gamme d'applications concernant, mais sans s'y limiter, les réseaux de Petri, une meilleure compréhension de l'algorithme.

Contacts : [David Ilcinkas](#), [Jérôme Leroux](#), [Vincent Penelle](#) et [Grégoire Sutre](#)