Propriété du domaine borné pour la logique temporelle linéaire du premier ordre et applications à la vérification de systèmes à états infinis

Soutenance de thèse – Quentin Peyras
Vendredi 14/01/2022 à 10h00
Salle des thèses de l'ISAE-Supaero à Toulouse

Devant le jury composé de :

Mme Catherine DUBOIS	ENSIIE	Rapporteure
M. Stéphane DEMRI	LSV, CNRS	Rapporteur
M. Denis KUPERBERG	LIP, CNRS	Examinateur
M. Jean-Paul BODEVEIX,	Université Paul Sabatier	Examinateur
M. David CHEMOUIL	ONERA	Directeur de thèse
M. Julien BRUNEL	ONERA	Co-directeur de thèse

Résumé

La logique temporelle linéaire du premier ordre (FOLTL) offre un cadre naturel pour la spécification de systèmes à états infinis mais n'est pas décidable (ni même semi-décidable). Dans cette thèse, nous cherchons à exploiter des fragments décidables de FOLTL pour vérifier, idéalement automatiquement, la correction de systèmes à états infinis.

Notre approche s'appuie de manière centrale sur une variante de la propriété du modèle fini. Cette propriété d'un fragment d'une logique affirme que, pour toute formule du fragment, il est possible de calculer une borne telle que, si cette formule est satisfiable, alors elle l'est dans un modèle de taille inférieure ou égale à cette borne. La variante que nous considérons, appliquée à FOLTL, ne borne que le domaine du premier ordre, et pas l'horizon temporel. Ceci permet en pratique de réduire le problème de satisfiabilité de FOLTL à celui, décidable, de LTL.

Nos travaux s'organisent en trois étapes. Dans un premier temps, nous exhibons divers fragments relativement expressifs de FOLTL possédant cette propriété. Toutefois, ces fragments seuls ne sont pas suffisant pour y spécifier des exemples réels de systèmes à états infinis.

C'est pourquoi, dans un second temps, nous définissons trois transformations permettant d'abstraire des spécifications de systèmes à états infinis vers les fragments décrits précédemment ou existant déjà dans la littérature. Une de ces transformations est totalement automatique tandis que les deux autres requièrent une entrée de la part du spécifieur.

Enfin, nous présentons dans un dernier temps l'implémentation et l'évaluation de ces méthodes. Pour ce faire, nous définissons un langage de spécification permettant la modélisation de système à états infinis et adapté à l'application de nos trois transformations. Un prototype permet, en exploitant nos résultats, de générer un problème de satisfisabilité LTL dont la résolution est déléguée à un model checker. Cette approche est ensuite évaluée sur un ensemble de spécifications de systèmes tirées de la littérature.

Mots clés

FOLTL, Vérification, Logique temporelle, Logique du premier ordre, Systèmes distribués, Model-Checking

ONERA
THE FRENCH AEROSPACE LAB