Soutenance de thèse

Quentin PEYRAS soutiendra sa thèse de doctorat, préparée au sein de l'équipe d'accueil doctoral ISAE-ONERA MOIS et intitulée «*Propriété du domaine borné pour la logique temporelle linéaire du premier ordre et applications à la vérification de systèmes à états infinis*»

Le 14 janvier 2022 à 10h00, salle des thèses à l'ISAE-SUPAERO

devant le jury composé de

M. David CHEMOUIL	Ingénieur de recherche ONERA	Directeur de thèse
Mme Catherine DUBOIS	Professeure ENSIIE	Rapporteure
M. Stéphane DEMRI	Directeur de recherche LMF	Rapporteur
M. Julien BRUNEL	Ingénieur de recherche ONERA	CoDirecteur de thèse
M. Denis KUPERBERG	Chargé de recherche ENS de Lyon	
M. Jean-Paul BODEVEIX	Professeur Université Toulouse 3	

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 : FO, LTL, Propriété du modèle fini, Model checking

Summary: First-Order Linear-Temporal Logic (FOLTL) provides a natural framework for the specification of infinite-state systems but is not even semi-decidable. In this thesis, we seek to use decidable fragments of FOLTL to verify, in the best case automatically, the correctness of infinite-state systems. Our approach mainly relies on a variant of the finite model property. This property of a fragment of a logic asserts that, for any formula of the fragment, it is possible to compute a bound such that if this formula is satisfiable, then it is satisfiable by a model of size less or equal than this

bound. In practice, this makes it possible to reduce the satisfiability problem of FOLTL to the (decidable) one of LTL. Our work is organized in three steps.
First, we exhibit various relatively expressive fragments of FOLTL enjoying this property. However, these fragments alone are not sufficient to specify real examples of infinite-state systems. This is why, in a second step, we define three transformations allowing to abstract specifications from infinite-state systems to the fragments described previously or already existing in the literature. One of these transformations is fully automatic while the other two require input from the specifier.
Finally, we present the implementation and evaluation of these methods. To do this, we define a specification language allowing the modeling of infinite-state system and adapted to the application of our three transformations. A prototype allows, by exploiting our results, to generate an LTL satisfisability problem whose resolution is delegated to a model checker. This approach is then evaluated on a set of system specifications drawn from the literature.
Keywords: FO, LTL, Finite Model Property, Model checking