RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ONERA
THE FRENCH AEROSPACE LAB

www.onera.fr

PROPOSITION DE SUJET DE THESE

Intitulé : Vérification automatique de systèmes non bornés

Référence : **TIS-DTIS-2025-34**
(à rappeler dans toute correspondance)

Début de la thèse : rentrée 2025	**Date limite de candidature :**

Mots clés

spécification formelle ; preuve formelle ; vérification semi-automatique ; systèmes à états infinis

Profil et compétences recherchées

Master / ingénieur informatique ou logique

Présentation du projet doctoral, contexte et objectif

La présence de grande quantité de logiciels embarqués au sein de systèmes critiques rend essentielle la tâche de vérification de leur bon fonctionnement. Ce besoin est notamment présent dans les systèmes aérospatiaux et robotiques qui sont étudiés au sein du département DTIS à l'ONERA. Des études en cours portent par exemple sur l'analyse de systèmes embarqués dans des drones, ou l'analyse de protocoles utilisés par une constellation de satellites d'observation terrestre. L'idée est d'utiliser une approche permettant de modéliser un tel système afin de prouver qu'il satisfait bien ses exigences. Proposer une telle approche, applicable à une grande classe de systèmes, est un défi scientifique en raison du langage très riche nécessaire pour exprimer à la fois la structure et la dynamique du système, et des techniques de vérifications qui doivent pouvoir explorer un très grand nombre de configurations différentes du système.

De nombreuses approches, basées sur des langages munis de techniques de vérification formelle comme TLA+ [Lamport] ou Alloy [Jackson], ont été proposées pour analyser une vaste classe de systèmes. Ces travaux renoncent en général à l'un des deux aspects suivants :

- une vérification *automatique* : en y renonçant, l'utilisateur doit guider la preuve « manuellement » ce qui s'avère fastidieux et complexe,
- une vérification *complète* : en effet, une solution pour rendre la vérification automatique est de borner la taille du système étudié. Une erreur qui se produirait pour un système de taille supérieure à cette borne ne peut pas être détectée par la vérification, qu'on appelle alors *incomplète*.

Des travaux réalisés à l'ONERA ont par exemple étudié le système distribué pair-à-pair Chord, soit en renonçant à l'aspect automatique [FM2019] soit en renonçant à la complétude [FMCAD2018]. Plus récemment, une technique basée sur un fragment de la logique temporelle du premier ordre FO-LTL a été proposée [ATVA2016, InfComp2021,CAV2021]. Elle permet d'aller vers plus d'automatisation sans renoncer à la complétude. Toutefois, son applicabilité reste limitée à des systèmes distribués relativement simples.

Le présent doctorat se situe dans ce contexte : il s'agit de déterminer un formalisme ou des techniques permettant de spécifier «naturellement » des systèmes réalistes dont le domaine est bon borné, puis de vérifier leurs propriétés (y compris la vivacité), au moyen de techniques à fort degré d'automatisation. Ce travail s'appuiera sur des résultats précédents mais aura aussi vocation à élaborer ses propres solutions.

Le travail consistera dans un premier temps à se familiariser avec l'approche proposée dans [InfComp21] et [CAV21]. Il s'agira de bien maîtriser le fragment de FOLTL utilisé et d'identifier son manque d'expressivité, qui nécessite dans la plupart des cas de modéliser une abstraction du système étudié plutôt que le système lui-même. Cela pourrait permettre d'appliquer l'approche à des systèmes qui n'ont pas encorde été validés formellement.

Dans un second temps, l'approche proposée dans [CAV21] pourrait être généralisée. Une piste consistant à proposer une extension des automates de Büchi semble prometteuse. Ceux-ci constituent en effet un cadre très utile pour la résolution du problème de satisfiabilité en logique temporelle, et pourraient être étendus de manière à prendre en compte de la logique du premier-ordre. Cela pourrait constituer un cadre, qui en plus de généraliser l'approche [CAV21], pourrait avoir un impact important sur la vérification de systèmes non bornés.

Références

[CAV2021] Quentin Peyras, Jean-Paul Bodeveix, Julien Brunel, David Chemouil. Sound Verification Procedures for Temporal Properties of Infinite-State Systems.. In *33rd International Conference on Computer-Aided Verification (CAV 2021)*.

[InfComp2021] Quentin Peyras, Julien Brunel, David Chemouil. A Decidable and Expressive Fragment of Many-Sorted First-Order Linear Temporal Logic. In Information and Computation, Vol. 280, Elsevier, 2021.

[FM2019] Jean-Paul Bodeveix, Julien Brunel, David Chemouil, Mamoun Filali. Mechanically Verifying the Fundamental Liveness Property of the Chord Protocol. In 3rd World Congress on Formal Methods (FM 2019), Lecture Notes in Computer Science.

[FMCAD2018] Julien Brunel, David Chemouil, Jeanne Tawa. Analyzing the Fundamental Liveness Property of the Chord Protocol. In 18th Conference on Formal Methods in Computer-Aided Design (FMCAD 2018), IEEE Press

[ATVA2016] Denis Kuperberg, Julien Brunel, David Chemouil. On Finite Domains in First-Order Linear Temporal Logic. In 14th International Symposium on Automated Technology for Verification and Analysis (ATVA 2016), Lecture Notes in Computer Science.

[Lamport] Leslie Lamport. Specifying Systems: The TLA+ Language and Tools for Hardware and Software Engineers, Addison-Wesley, 2002.

[Jackson] Daniel Jackson. Software Abstractions (revised edition) Logic, Language, and Analysis, MIT Press, 2016.

Collaborations envisagées

Xavier Thirioux, ISAE

Laboratoire d'accueil à l'ONERA	**Directeur de thèse**
Département : Traitement de l'information et Systèmes	Nom : Julien Brunel
Lieu (centre ONERA) : Toulouse	Laboratoire :
Contact : David Chemouil, Julien brunel	Tél. : 05 62 25 26 81
Tél. : 05 6225 2936 Email : Julien.brunel@onera.fr	Email : Julien.brunel@onera.fr

Pour plus d'informations : https://www.onera.fr/rejoindre-onera/la-formation-par-la-recherche