ONERA
THE FRENCH AEROSPACE LAB

www.onera.fr

PROPOSITION DE STAGE EN COURS D'ETUDES

Référence : **DTIS -2019-50**
(à rappeler dans toute correspondance)

Lieu : Toulouse

Département/Dir./Serv. : **DTIS/SEAS**

Tél. : 05 62 25 29 36

Responsable(s) du stage : David Chemouil, Julien Brunel

Email. : David.chemouil@onera.fr

DESCRIPTION DU STAGE

Thématique(s) : Ingénierie des Systèmes et des Logiciels

Type de stage : ☒ Fin d'études bac+5 ☒ Master 2 ☐ Bac+2 à bac+4

Intitulé : Vérification formelle de systèmes distribués sur domaine infini

Sujet :

La formalisation des systèmes distribués constitue un objet d'étude intéressant en soi mais aussi en raison du « challenge » qu'ils posent à la spécification formelle « naturelle » et à la vérification formelle à fort degré d'automatisation.

Ivy [PLDI 2016] permet de prouver des propriétés sur des systèmes de taille infinie avec un degré d'automatisation important (comparativement aux approches fondés sur des assistants de preuve). La description du système et la spécification des propriétés à vérifier doit se faire en utilisant un fragment assez restreint de la logique du premier ordre, sur lequel le problème de satisfiabilité est décidable. Ivy a été notamment appliqué à l'analyse de systèmes distribués (ex : protocoles de la famille Paxos)).

Des travaux récents [POPL 2018] proposent d'analyser des propriétés temporelles plus riches (vivacité) à l'aide d'Ivy.

Electrum [FSE 2016], un langage développé à l'ONERA depuis 2015, a choisi une approche différente : la soécification du système et des propriétés profite de toute l'expressivité de la logique temporelle du premier ordre (FO-LTL). La vérification est entièrement automatique, mais nécessite de borner la taille du domaine du premier ordre. Electrum a également été appliqué dans [FMCAD 2018] à l'analyse de systèmes distribués, via l'étude du protocole Chord, qui traite de la maintenance d'une table de hachage distribuée dans un réseau pair-à-pair.

Le présent stage se situe dans ce contexte. In fine, il s'agit de déterminer un formalisme ou des techniques permettant de spécifier « confortablement » des systèmes distribués puis de vérifier leurs propriétés (y compris la vivacité) au moyen de techniques avec un fort degré d'automatisation. Pour ce faire, on propose le présent programme de travail :

- Étudier le protocole Chord ainsi que le modèle Electrum de Chord
- Proposer une modélisation de Chord (ou d'un sous-ensemble de Chord) en Ivy (liveness incluse)
- Étudier les propositions théoriques sous-jacentes à Ivy
- En déduire des améliorations possibles pour Ivy & Electrum.

Ce stage peut se poursuivre en thèse.

[POPL 2018] O. Padon, J. Hoenicke, G. Losa, A. Podelski, M. Sagiv, S. Shoham. Reducing liveness to safety in first-order logic. In Proceedings of the ACM on Programming Languages 2(POPL), 2018

[PLDI 2016] O. Padon, K. L.. McMillan, A. Panda, M. Sagiv, Sh. Shoham. Ivy: safety verification by interactive generalization. In Proc. of 37th ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI), 2016.

[FMCAD 2018] J. Tawa, J. Brunel & D. Chemouil. Analyzing the Fundamental Liveness Property of the Chord Protocol. In Proc of International Conference on Formal Methods in Computer-Aided Design (FMCAD), 2018

[FSE 2016] N. Macedo, J. Brunel, D. Chemouil, A. Cunha, and D. Kuperberg. Lightweight Specification and Analysis of Dynamic Systems with Rich Configurations. In Proc. ACM SIGSOFT Intl Symp. on the Foundations of Software Engineering (FSE), 2016.

[ATVA 2016] D. Kuperberg, J. Brunel, and D. Chemouil. On Finite Domains in First-Order Linear Temporal Logic. In 14th Interl Symp. on Automated Technology for Verification and Analysis (ATVA), 2016.

Est-il possible d'envisager un travail en binôme ? Non

Méthodes à mettre en oeuvre :

☒ Recherche théorique	☐ Travail de synthèse
☒ Recherche appliquée	☒ Travail de documentation
☐ Recherche expérimentale	☒ Participation à une réalisation

Possibilité de prolongation en thèse : Oui

Durée du stage : Minimum : 5 mois Maximum : 6 mois

Période souhaitée : printemps-été 2019

PROFIL DU STAGIAIRE

Connaissances et niveau requis :	Ecoles ou établissements souhaités :
Bac +5 (M2R ou école d'ingénieur) avec de bonnes connaissances en informatique théorique, méthodes formelles, logique	