ONERA
THE FRENCH AEROSPACE LAB

www.onera.fr

PROPOSITION DE STAGE EN COURS D'ETUDES

Référence : **DTIS -2019-44** *(à rappeler dans toute correspondance)*	Lieu : Toulouse
Département/Dir./Serv. : DTIS/SEAS	Tél. : 05 62 25 26 81
Responsable(s) du stage : Julien Brunel, David Chemouil	Email. : Julien.brunel@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 performante pour la logique temporelle du premier ordre

Sujet : Alloy (D. Jackson et al, MIT) est un langage de spécification formelle qui connaît un certain succès en raison du compromis pertinent qu'il propose entre simplicité de modélisation pour l'utilisateur et efficacité des analyses formelles. En pratique, la spécification se fait en logique relationnelle bornée (une logique du premier ordre avec termes relationnels et dont les domaines d'interprétation sont bornés par l'utilisateur) et la vérification automatisée de propriétés est effectuée par traduction en problème de satisfiabilité pour la logique propositionnelle (on tire parti des récents progrès importants effectués dans le domaine des moteurs SAT). Alloy se prête très bien à l'analyse de modèles où les propriétés vérifées sont essentiellement structurelles. Or, de nombreux problèmes comportent aussi une dimension comportementale, abordables en Alloy mais avec un certain nombre de lacunes.

Le DTIS, en collaboration avec le HasLab de l'université du Minho (Portugal) a récemment élaboré un langage formel, nommé Electrum [FSE 2016], qui peut être vu comme une extension comportementale d'Alloy. En pratique, le langage s'appuie sur la logique relationnelle bornée étendue par la logique temporelle linéaire avec opérateurs du passé (PLTL). Deux techniques de vérification ont été mises au point : dans les deux cas, le domaine des termes du premier ordre est borné ; en revanche, un outil repose sur une analyse avec horizon temporel borné (bounded model checking) tandis que le second, conçu à l'ONERA, travaille sur horizon non-borné.

L'objectif de ce stage sera d'améliorer les analyses actuelles en suivant certaines des pistes suivantes :

- Une piste intéressante consiste à tirer parti des symétries présentes dans les modèles Electrum : celles-ci permettent de réduire considérablement l'espace d'états. À l'heure actuelle, nous ne tenons compte que de certaines symétries sur les données, mais pas des symétries temporelles. De manière plus générale, l'emploi de techniques automatiques d'abstraction paraît prometteur.
- Les analyses actuelles ne tirent pas assez profit de la différence entre la description du « système » d'une part, et de la spécification des propriétés que le système doit vérifier d'autre part. Une récente extension d'Electrum [ABZ 2018] avec des actions permet justement une distinction plus claire entre ces deux éléments au sein du langage. De nouvelles analyses peuvent donc être imaginées, en particulier en s'inspirant des algorithmes récents basés sur une représentation SMT (Satisfiability Modulo Theory) du système et des propriétés.
- Nous avons débuté dans [ATVA 2016] une étude de la propriété du modèle fini (PMF) pour la logique sous-jacente à Electrum (FO-LTL). L'identification de certains fragments de la logique qui ont la PMF ouvrent à la voie à une vérification complète (sans borne sur les termes du permier ordre).

Références :

[ABZ 2018] Julien Brunel, D . Chemoui, A. Cunha, Th. Hujsa, N. Macedo, J. Tawa. Proposition of an Action Layer for Electrum. In Proc. of *6th Int. Conf. on ASM, Alloy, B, TLA, VDM, Z (ABZ), 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	