RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ONERA
THE FRENCH AEROSPACE LAB

www.onera.fr

PROPOSITION DE SUJET DE THESE

Intitulé :
Fiabilisation du model checking par preuves formelles et génération de certificats vérifiables

Référence : **TIS-DTIS-2026-29**
(à rappeler dans toute correspondance)

Début de la thèse : 01/10/2026	**Date limite de candidature :**

Mots clés

Méthodes formelles – Model checking – Logique – Preuve

Profil et compétences recherchées

Étudiant en informatique avec des notions en informatique théorique (logique, vérification, preuve).

Présentation du projet doctoral, contexte et objectif

Contexte et objectifs

Le **model-checking** est une méthode de vérification automatique visant à garantir qu'un système satisfait une propriété formelle, telle que le fait qu'un état redouté n'est jamais atteint. Dans ce domaine, l'algorithme **IC3**, également connu sous le nom **PDR** (Property Directed Reachability), constitue aujourd'hui une approche **state-of-the-art** pour la vérification d'invariants dans les systèmes de transitions finis, notamment dans les circuits matériels et les logiciels critiques. PDR a par la suite été étendu à certaines classes de systèmes de transitions infinis.

Un atout majeur d'IC3/PDR réside dans sa capacité à **produire un invariant inductif** (c'est-à-dire une preuve formelle de correction), par de la génération de clauses inductives et du **raisonnement symbolique**, sans exploration explicite de l'espace d'états. Cet invariant inductif peut être ensuite utilisé comme **certificat vérifiable** par un solveur SMT externe (p. ex. z3). IC3/PDR est au cœur de nombreux outils (Spacer, nuXmv, ABC) où il a prouvé son efficacité. Cependant, **la complexité conceptuelle de l'algorithme IC3** rend difficile sa compréhension, sa mise en œuvre correcte, et son adaptation à des variantes spécialisées.

Objectifs de la thèse

L'objectif global de cette thèse est de **renforcer la confiance dans le model checking** en développant des garanties formelles de bout en bout. Le travail s'articule autour de deux axes complémentaires.

Axe 1 – Spécification formelle d'IC3/PDR

Le premier axe de recherche consiste à **spécifier formellement IC3/PDR** à divers niveaux d'abstraction pour en clarifier les principes fondamentaux, séparer les aspects algorithmiques des optimisations pratiques, et pouvoir dériver des variantes certifiées. Cet axe de travail porte donc moins sur la preuve d'une implémentation particulière, que sur la construction progressive d'une spécification formelle **modulaire** et **abstraite** de l'algorithme IC3/PDR, dans le langage WhyML du système **Why3**. L'objectif est de poser les fondations permettant : (1) une modélisation rigoureuse des concepts clés (états, frames, clauses, induction), (2) une séparation nette entre les composants logiques et les stratégies de gestion de l'espace d'états, et (3) la possibilité de

dériver ou certifier plusieurs implémentations, optimisées ou spécialisées (par ex. pour certaines classes de systèmes).

Axe 2 – Génération de certificats vérifiables

Le second axe de recherche vise, une fois les concepts clés d'IC3/PDR intégrés, à étudier la **génération de certificats** vérifiables pour **d'autres extensions d'IC3/PDR ou méthodes** de model checking. L'idée est de produire, en plus du verdict de l'outil (c'est-à-dire la propriété est vraie ou fausse), un objet formel tel qu'un invariant inductif ou un contre-exemple, qui puisse être vérifié indépendamment par un solveur externe ou un assistant de preuve. Ainsi, chaque résultat de vérification serait accompagné de sa justification formelle.

Dans cette perspective, l'étude portera également sur des extensions vers des **logiques temporelles** plus expressives comme LTL et sur des **systèmes infinis**, où la question des certificats reste largement ouverte (p. ex. en travaillant dans un premier temps sur des extensions d'IC3/PDR). Alors que la certification est aujourd'hui un sujet central dans la communauté des solveurs SMT, elle demeure émergente dans celle du model checking, ce qui confère à ce projet un intérêt scientifique et applicatif fort.

Pourquoi Why3 ?

Why3 est une plateforme de vérification déductive reposant sur le langage **WhyML**. Elle permet d'écrire des programmes annotés de spécifications formelles, de générer des **obligations de preuve** logiques, et de les vérifier automatiquement (SMT) ou manuellement (Coq).

Why3 offre un cadre structuré pour construire des **spécifications stratifiées**, en isolant les modules, les types abstraits, et les propriétés logiques associées. Cela en fait un outil idéal pour spécifier **des algorithmes complexes comme PDR** de manière claire, structurée, et vérifiable.

Références indicatives

- A. R. Bradley, "SAT-Based Model Checking Without Unrolling," *VMCAI*, 2011.
- Gurfinkel et al., "Efficiently Solving Logic-Based Model Checking Problems with PDR," *FMCAD*, 2015.
- Giulia Sindoni, Alberto Griggio, Stefano Tonetta, "Certifying rlive: A New Proof Strategy for Liveness Model Checking". FroCoS, 2025.
- C. Marché et al., "The Why3 platform," *Journal of Automated Reasoning*, 2013.
- Why3 : https://why3.lri.fr/

Collaborations envisagées

Nicolas Amat (DTIS, ONERA) et Pierre-Loïc Garoche (ENAC)

Laboratoire d'accueil à l'ONERA	**Directeur de thèse**
Département : Traitement de l'information et Systèmes	Nom : David Chemouil
Lieu (centre ONERA) : Toulouse	Laboratoire : DTIS, ONERA
Contact : N. Amat	Tél. : 05 62 25 29 36
Tél. : 05 62 25 29 36 Email : nicolas.amat@onera.fr	Email : david.chemouil@onera.fr

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