

Titre: Approximations intérieures et vérification de propriétés temporelles de systèmes hybrides
Mots-clés: Méthodes formelles, analyse d'atteignabilité, systèmes hybrides, logique temporelle

Lieu et équipe: LIX, Bâtiment Turing, campus de l'Ecole Polytechnique.

Au sein du laboratoire d'informatique de l'Ecole Polytechnique (LIX), le stagiaire intégrera l'équipe Cosynus, dont les recherches portent sur la sémantique et l'analyse statique des systèmes logiciels, distribués, hybrides et cyber-physiques.

Encadrement: Sylvie Putot & Eric Goubault – email: {putot,goubault}@lix.polytechnique.fr

Présentation générale: La vérification de systèmes de contrôle critiques, classiquement modélisés sous forme de systèmes hybrides, suppose de vérifier que leurs exécutions possibles satisfont des spécifications, données sous forme de propriétés temporelles sur les valeurs prises par certaines variables de ce système. Ces systèmes comportent des incertitudes sur leurs paramètres, ce qui demande des abstractions permettant de vérifier ou infirmer ces propriétés non seulement sur des trajectoires, mais de façon globale sur des ensembles de trajectoires.

Le but du projet est de développer les outils théoriques et pratiques permettant à terme de construire un model-checker abstrait de propriétés numériques temporelles des systèmes hybrides, propriétés exprimées dans des logiques du type MTL (Metric Temporal Logic) ou STL (Signal Temporal Logic).

Objectifs du stage: Le stage vise à combiner des approximations intérieures et extérieures de l'ensemble des états atteignables de systèmes hybrides incertains, de façon à pouvoir prouver ou réfuter des propriétés temporelles de ces systèmes.

Le calcul de sur-approximations (ou approximations extérieures) des états ou trajectoires atteignables pour des systèmes hybrides linéaires, et plus récemment, non linéaires, devient un sujet relativement classique. Mais calculer des sous-approximations (ou approximations intérieures), est notoirement plus difficile. Les objectifs du stage seront de:

- étendre et expérimenter pour des systèmes hybrides, les sous-approximations proposées dans [HSCC14, HSCC17], en les combinant avec des méthodes de Taylor pour l'évaluation des transistions continues. La partie implementation pourra par exemple reposer partiellement sur l'outil Ibex (<http://www.ibex-lib.org>).
- définir une interpretation, basée sur les sur et sous-approximations précédemment définies, de propriétés temporelles possiblement quantifiées sur les valeurs des paramètres.
- expérimenter ces méthodes sur des modèles de drones réels (avec incertitudes), comme ceux dont nous disposons dans l'équipe (TurtleBot3, crazyflie2.0 etc.), avec comparaison des résultats avec la pratique. Un axe pourrait être également de tenter d'embarquer certaines versions de ces algorithmes d'atteignabilité en horizon (très) borne, sur ces plateformes peu puissantes, pour faire du monitoring de fonctions de plus haut niveau (planification de trajectoires, évitement d'obstacles etc.)

L'accent pourra porter plus fortement sur l'un ou l'autre de ces axes, avec un aspect développement et expérimentation plus ou moins fort.

Possibilité de poursuivre en thèse.

Bibliographie:

[HSCC 2014] E. Goubault, M. Kieffer, O. Mullier and S. Putot, Inner approximated reachability analysis, Proceedings of Hybrid Systems: Computation and Control HSCC 2014

[HSCC 2017] E. Goubault, S. Putot, Forward Inner-Approximated Reachability of Non-Linear Continuous Systems. HSCC2017