Titre: Domaines abstraits numériques sous-approximants

Mots-clés: Méthodes formelles, analyse d'atteignabilité

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@lix.polytechnique.fr

Présentation générale: La plupart des domaines numériques abstraits (notamment les classiques intervalles, octogones, polyèdres, zonotopes, etc) concus pour la verification de programmes par analyse statique construisent des sur-appproximations des ensembles atteignables par les variables des programmes analysés. Lorsque l'analyse ne sait pas garantir la sûreté du programme analysé, alors l'utilisateur ne peut pas conclure s'il s'agit réellement d'un défaut de son programme, ou d'un manque de precision de son analyse. C'est ainsi que ces dernières années ont vu se multiplier les nouveaux domaines abstraits, tentant de trouver le meilleur compromis entre efficacité et precision, ou de raffiner les résultats d'une analyse existante.

Une démarche alternative consiste à construire des domaines abstraits sous-approximants, c'est-à-dire calculant des sous-ensembles des ensembles des valeurs atteignables, dont on est capable de prouver que chaque état est effectivement atteignable. Combinés à des sur-approximations, ils donnnent une estimation de la précision d'une analyse. De plus, ils permettent de prouver l'existence de comportements erronnés, ce qu'une analyse sur-approximée ne peut pas prouver.

Mais calculer des sous-approximations est notoirement plus difficile que des sur-approximations. Nous avons proposé dans le passé une approche pour calculer des sous-approximations, que nous avons pour le moment essentiellement appliquée à l'analyse d'atteignabilité de systèmes dynamiques sans gardes / expressions conditionnelles [HSCC14, HSCC17, CAV18].

Objectifs du stage: Le stage vise à étendre l'utilisation de ces sous-approximations à l'interprétation de structures conditionnelles, et plus généralement construire un domaine sous-abstrait sous-approximé. Il s'agira également de l'implémenter dans un cadre permettat d'expérimenter et diffuser largement ce travail, par exemple dans la bibliothèque CRAB (https://github.com/seahorn/crab) qui contient déjà de nombreuses analyses classiques.

Possibilité de thèse.

Bibliographie:

[HSCC14] E. Goubault, M. Kieffer, O. Mullier and S. Putot, Inner approximated reachability analysis, actes de Conference on Hybrid Systems: Computation and Control HSCC 2014
[HSCC17] E. Goubault, S. Putot, Forward Inner-Approximated Reachability of Non-Linear Continuous Systems. actes de la conférence HSCC 2017
[CAV18] E. Goubault, S. Putot et L. Sahlman, Inner and Outer Approximating Flowpipes for Delay Differential Equations, actes de Conference on Computer Aided Verification CAV 2018