Soutenance de thèse

Paul ROUSSE soutiendra sa thèse de doctorat préparée au sein de l'ISAE-ONERA MOIS et intitulée «*Cosimulation ensembliste d'une interconnexion de systèmes*»

Le 5 novembre 2020 à 10h00, Amphi 2 - ISAE-SUPAERO

devant le jury composé de

M. Pierre-Loïc GAROCHE	Ingénieur de recherche ONERA	Directeur de thèse
M. Anders RANTZER	Professeur Lund University	Rapporteur
Mme Thao DANG	Directrice de recherche VERIMAG	Rapporteur
M. Didier HENRION	Directeur de Recherche LAAS	Co-directeur de thèse
Mme Sylvie PUTOT	Professeure Ecole Polytechnique	
M. Eric FERON	Professeur Georgia Tech	
Mme Sonia CAFIERI	Professeure ENAC	
M. Alexandre CHAPOUTOT	Professeur ENSTA Paritech	

Résumé : L'ensemble d'atteignabilité d'un système embarqué est central dans la vérification de propriété de sureté. Cet ensemble géométrique est en général complexe à décrire (il peut être non convexe et/ou non connecté même dans des cas simples) et complexe à calculer. Cette thèse propose trois méthodes pour surapproximer cet ensemble. La première méthode, la ``méthode ellipsoïdale'', surapproxime avec des coniques l'ensemble d'atteignabilité d'un système linéaire sujet à des perturbations bornées par des inégalités en norme 2 ou en norme inf. La seconde méthode, la ``méthode des intervalles'', surapproxime avec des intervals l'ensemble d'atteignabilité d'un système non linéaire sujet à des perturbations bornées par une inégalité de norme 2. La dernière méthode, la ``méthode de cosimulation'', formalise par une approche interpretation abstraite la surapproximation de l'ensemble d'atteignabilité d'une interconnexion de systèmes. La ``méthode ellipsoidale'' s'intéresse à des systèmes linéaires variant dans le temps sujet à des perturbations bornées par des inégalités norme 2 (Contrainte Intgrale Quadratique -IQC-) ou norme inf (Contrainte Quadratique -QC-). Ces modèles permettent de modéliser des systèmes à délais, des systèmes soumis à des perturbations de croissance bornée (rate-limiters systems), the contraintes énergétiques, ou des inégalités sectorielles. L'ensemble d'atteignabilité est surapproximé avec des coniques variant dans le temps. Le coefficient de ces coniques est solution d'une Équation Différentielle de Riccati (DRE). Contrairement aux travaux existants, cette DRE est dépendante d'un paramètre (libre) variant dans le temps. Chaque choix de paramètres génère une surapproximation différente. Ce paramètre peut-être choisit pour satisfaire différents critères: par exemple, pour obtenir la surapproximation de volume minimal, ou bien pour obtenir une surapproximation qui ``touche'' l'ensemble d'atteignabilité. La ``méthode des intervalles'' applique une méthode d'intégration guaranties basée sur l'arithmetique des intervalles à la surapproximation de l'ensemble d'atteignabilité d'un système IQC non-linéaire. La contrainte intégrale est utilisée pour définir un contracteur. Le contracteur et l'opérateur de propagation (qui propage un ensemble d'états le long du flux du système) sont successivement appliqué sur une surapproximation (a priori) du reachable tube jusqu'à ce qu'un point fixe soit atteint. L'algorithme a été intégré dans le framework DynIbex pour simuler des systèmes de dimension infinie (système à délais). Enfin, la ``méthode de cosimulation'' associe les deux méthodes précédentes dans une approche générique permettant ainsi l'analyse d'une classe plus large de systèmes: une interconnexion de systèmes. Chaque système dans l'interconnexion est considéré comme un opérateur sur un espace de signals (en temps continu ou discret) et l'interconnexion de systèmes est exprimée à l'aide de compositions et des point-fixes de ces opérateurs. Le formalisme de l'interprétation abstraite est ensuite utilisé pour représenter des abstractions correctes de ces signaux. Nous détaillons plusieurs domaines abstraits permettant de représenter des ensembles de trajectoires et les appliquons à des exemples-jouets

Mots-clés : vérification, systèmes automatique, validation

Summary: Embedded systems and in particular those of control-command are already very widespread in our environment. For example, for the most critical transport systems: airplane, train, car, but also in nuclear power plants, civil or military

drones, etc. All these systems rely on essentially numerical algorithms: a linear or non-linear controller to control the aircraft, algorithms for the calculation of trajectories, avoidance of other aircraft, etc. The problem of certifying the correct behavior of these systems and software is already a major issue. In the case of controllers, the synthesis of these controllers is carried out in conjunction with their analysis. In a more general way these algorithms must be certified before being 'embarquable'. This certification phase relies mainly on intensive use of the test and simulation. However, recent developments in these certification standards, such as the DO178C and its DO-333 supplement for avionics software, open the door to the use of comprehensive mathematical methods for certification in the sense of proof. We are therefore concerned here with the development of automatic methods for analyzing such controllers or algorithms, either at the model level or at the level of the embedded code. We propose to use the tools of semi-defined programming and more generally numerical optimization to perform such analyzes.

Keywords: control system, validation, verification