Formalisation des polyèdres dans l'assistant de preuve Coq

Xavier Allamigeon
xavier.allamigeon@inria.fr

28 janvier 2019

Mots-clés. Preuve formelle, formalisation des mathématiques, géométrie discrète et combinatoire, optimisation mathématique.

Localisation du stage. Centre de Mathématiques Appliquées (CMAP), Ecole polytechnique, Palaiseau

Equipe d'accueil. Equipe "Tropical", commune à INRIA Saclay – Ile-de-France et au CMAP, Ecole polytechnique

Encadrant référent. Xavier Allamigeon (xavier.allamigeon@inria.fr)

1 Contexte

Les polyèdres convexes sont les ensembles de $\mathbb{R}^n$ définis par des systèmes d'inégalités linéaires (affines). Ils jouent un rôle majeur en mathématiques pures (géométrie algébrique, mathématiques discrètes, combinatoire), en mathématiques appliquées (optimisation, recherche opérationnelle, contrôle), et en informatique (géométrie algorithmique, vérification formelle de programmes, compilation et optimisation de programmes, résolution de contraintes). L'importance croissante des logiciels mathématiques dans l'étude de problèmes ouverts en mathématiques, et la nature critique des applications mentionnées précédemment fournissent une motivation forte pour la formalisation des polyèdres convexes dans un assistant de preuve. Une première contribution dans cette direction a été réalisée dans [AK18], où les propriétés de base des polyèdres, telles que la vacuité, le caractère borné, le lemme de Farkas, ont été formalisées en Coq, au moyen du mécanisme de réflection booléenne fourni par la bibliothèque Mathematical Components [GMT16]. Cela a conduit au développement de la bibliothèque Coq-Polyhedra [1].

2 Objectifs du stage

Le travail de stage s'inscrit directement dans le projet de formalisation de la théorie des polyèdres dans Coq et son application à des problèmes mathématiques. Nous proposons ci-dessous deux exemples d'axes de travail qui peuvent être adaptés en fonction des goûts du/de la stagiaire.

1. https://github.com/nhojem/Coq-Polyhedra

Le premier axe porte sur l'implémentation de l'élimination de Fourier–Motzkin dans la bibliothèque. Cet algorithme est une brique de base permettant de prouver facilement plusieurs propriétés clés sur les polyèdres, par exemple le caractère polyédral de l'enveloppe convexe d'un nombre fini de points, ou bien l'invariance de la classe des polyèdres par les transformations affines. Son extraction vers du code exécutable présenterait un intérêt indépendant puisque l'algorithme est utilisé dans de nombreux solveurs SAT/SMT.

Le second axe porte sur la formalisation de techniques de preuve à base de perturbations dans Coq-Polyhedra. Il est en effet très fréquent dans les démonstrations sur les polyèdres de perturber certains objets par une petite quantité (typiquement notée ε), de manière à exclure certaines configurations spéciales *sans perte de généralité*. Ce type d'arguments est particulièrement délicat à capturer dans un assistant de preuve, puisqu'il est nécessaire de quantifier explicitement l'ordre de grandeur de la perturbation à effectuer. On propose de manière alternative d'implémenter ces raisonnements en ayant recourt à des perturbations symboliques. Dans ce cas, la quantité ε est une variable formelle, et on en est réduit à faire des calculs symboliques sur des polynômes en ε et d'utiliser l'ordre lexicographique pour la comparaison de quantités perturbées.

Références

[AK18] Xavier Allamigeon et Ricardo D. Katz : A formalization of convex polyhedra based on the simplex method. *Journal of Automated Reasoning*, Aug 2018.

[GMT16] Georges Gonthier, Assia Mahboubi et Enrico Tassi : A Small Scale Reflection Extension for the Coq system. Research Report RR-6455, Inria Saclay Ile de France, 2016.