Formalisation des polyèdres dans l'assistant de preuve Coq

Xavier Allamigeon
xavier.allamigeon@inria.fr

12 octobre 2018

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 Context

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 [AK17], 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 recherche dans ce projet qui peuvent être adaptés en fonction des goûts du/de la stagiaire, et qui mènent naturellement à une poursuite en thèse sur le sujet.

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

Le premier axe porte sur la mise en œuvre effective de la bibliothèque Coq-Polyhedra sur des instances de polyèdres de taille très importante, et qui demande déjà un temps de calcul conséquent pour les bibliothèques de calcul informel. Par exemple, un but à moyen terme du projet est la falsification formelle de la célèbre conjecture de Hirsch, avec la vérification du contre-exemple de [MSW15], un polyèdre en dimension 20 ayant 40 facettes, et 36 425 sommets.[2] A notre connaissance, les assistants de preuve n'ont pas été utilisés jusqu'à maintenant pour des volumes de données ou de calculs de cet ordre de grandeur. Le défi est de dépasser les limitations de calcul inhérentes aux types très abstraits qui sont utilisés pour représenter les objets mathématiques dans Coq et la libraire Mathematical Components. Pour cela, il faut utiliser des types « bas niveau » adaptés au calcul et sur lesquels peuvent être développés des algorithmes beaucoup plus efficaces, puis transposer les résultats valides sur les structures « haut niveau » vers celles « bas niveau ». Dans un but de maintenabilité, il sera nécessaire d'automatiser autant que possible ces étapes de transposition. On pourra pour cela s'inspirer des techniques explorées dans [CDM13]. L'objectif est d'obtenir un facteur de ralentissement modéré (de l'ordre de 10) par rapport à l'utilisation d'une bibliothèque informelle de calculs polyédraux, de manière à pouvoir envisager d'interfacer Coq-Polyhedra avec des logiciels mathématiques tels que Polymake [GJ00] et Sage [The18].

Le second axe porte sur la représentation des polyèdres dans l'assistant de preuve. Les polyèdres admettent en effet plusieurs représentations différentes par inégalités, et il est aussi possible de les représenter à l'aide de leurs sommets. Ces différentes représentations équivalentes doivent être rassemblées dans une seule et même structure (notamment une structure quotient pour celles par inégalités). Mais de plus, ces structures doivent se combiner élégamment avec l'ensemble des autres propriétés des polyèdres. Par exemple, les faces des polyèdres, qui sont au cœur de la combinatoire des polyèdres, sont aussi des polyèdres admettant de multiples représentations possibles. Si l'on raisonne simultanément sur un polyèdre et ses faces, on doit veiller à pouvoir manipuler des représentations compatibles entre elles. Le choix de la représentation d'un polyèdre n'est donc pas forcément donné par une procédure de normalisation, mais il dépend du contexte dans lequel on la manipule. Le but est donc de trouver une formalisation qui permette de manipuler dans l'assistant de preuve les différentes représentations possibles d'un polyèdre aussi aisément que dans une preuve sur papier. Pour cela, on s'appuiera sur les importants travaux de formalisation de hiérarchies de structures mathématiques qui ont été menés dans la bibliothèque Mathematical Components [GMT16], cf. [GGMR09] et plus spécialement [Coh13] pour une contribution récente sur les structures quotients.

Références

[AK17] Xavier Allamigeon et Ricardo D. Katz : *A Formalization of Convex Polyhedra Based on the Simplex Method*, pages 28–45. Springer International Publishing, Cham, 2017.

[CDM13] Cyril Cohen, Maxime Dénès et Anders Mörtberg : Refinements for free ! *In* Georges Gonthier et Michael Norrish, éditeurs : *Certified Programs and Proofs*, volume 8307 de *Lecture Notes in Computer Science*, pages 147–162. Springer International Publishing, 2013.

2. Nous renvoyons à la description de la vérification informelle du contre-exemple à la conjecture de Hirsch à l'aide du logiciel lrs, `https://sites.google.com/site/christopheweibel/research/hirsch-conjecture`.

[Coh13] Cyril Cohen : Pragmatic quotient types in coq. *In* Sandrine Blazy, Christine Paulin-Mohring et David Pichardie, éditeurs : *Interactive Theorem Proving*, pages 213–228, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg.

[GGMR09] François Garillot, Georges Gonthier, Assia Mahboubi et Laurence Rideau : Packaging mathematical structures. *In* Stefan Berghofer, Tobias Nipkow, Christian Urban et Makarius Wenzel, éditeurs : *Theorem Proving in Higher Order Logics*, pages 327–342, Berlin, Heidelberg, 2009. Springer Berlin Heidelberg.

[GJ00] Ewgenij Gawrilow et Michael Joswig : `polymake` : a framework for analyzing convex polytopes. *In Polytopes—combinatorics and computation (Oberwolfach, 1997)*, volume 29 de *DMV Sem.*, pages 43–73. Birkhäuser, Basel, 2000.

[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.

[MSW15] Benjamin Matschke, Francisco Santos et Christophe Weibel : The width of five-dimensional prismatoids. *Proceedings of the London Mathematical Society*, 110(3) :647–672, 2015.

[The18] The Sage Developers : *SageMath, the Sage Mathematics Software System (Version 8.3)*, 2018. `http://www.sagemath.org`.