Enumération efficace des sommets d'un polyèdre en Coq

Xavier Allamigeon Pierre-Yves Strub

9 septembre 2019

Mots-clés. Preuve formelle, formalisation des mathématiques, algorithmes en géométrie discrète et combinatoire.

Localisation du stage. Ecole Polytechnique, Palaiseau

Laboratoire d'accueil. Centre de Mathématiques Appliquées & LIX, Ecole Polytechnique

Encadrants. Xavier Allamigeon (`xavier.allamigeon@inria.fr`)
Pierre-Yves Strub (`strub@lix.polytechnique.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 informatique (géométrie algorithmique, vérification formelle de programmes, compilation et optimisation de programmes, résolution de contraintes), en mathématiques pures (géométrie algébrique, mathématiques discrètes, combinatoire), comme en mathématiques appliquées (optimisation, recherche opérationnelle, contrôle). Ces nombreuses applications, pour certaines de nature critique, fournissent une motivation très forte pour la formalisation des polyèdres convexes dans un assistant de preuve. Une première contribution dans cette direction a été réalisée dans [AK17], dans laquelle on a fourni une preuve formelle de l'algorithme du simplexe, ainsi que formalisé les propriétés de base des polyèdres. Cela a conduit au développement de la bibliothèque Coq-Polyhedra [1].

2 Objectifs du stage

Le but visé à terme par la librairie Coq-Polyhedra est de fournir à la communauté des informaticiens et mathématiciens un ensemble d'algorithmes prouvés formellement pour le calcul sur les polyèdres. Le stage proposé s'inscrit dans ce projet, et propose de formaliser un algorithme d'énumération des sommets d'un polyèdre, qui est une primitive cruciale dans de nombreuses opérations sur les polyèdres.

Deux pistes sont envisagées : (i) une approche de certification formelle a posteriori d'une liste de sommets fournie par un logiciel non prouvé ; (ii) ou bien la formalisation de l'algorithme *reverse search* [AF96], qui présente l'avantage d'être très efficace sur les instances de polyèdres non-dégénérées. Dans les deux cas, on cherche à obtenir une implémentation capable de passer à

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

l'échelle sur de instances à la combinatoire élevée. En effet, le nombre de sommets d'un polyèdre peut être exponentiel en le nombre d'inégalités. Ainsi, le contre-exemple de [MSW15] à la célèbre conjecture de Hirsch est 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 habituellement utilisés pour manipuler les objets mathématiques dans Coq. 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 mathématiques prouvés formellement sur les structures « haut niveau » vers celles « bas niveau ». Dans un souci 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 stage débouche naturellement à une poursuite en thèse, par exemple sur la formalisation de la théorie des polyèdres en Coq.

Références

[AF96] David Avis et Komei Fukuda : Reverse search for enumeration. *Discrete Applied Mathematics*, 65(1):21 – 46, 1996. First International Colloquium on Graphs and Optimization.

[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.

[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.

[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`.

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`.