Formal proofs of the basic linear programs in the Kepler conjecture proof

Assia Mahboubi, Assia.Mahboubi@inria.fr
INRIA Saclay – Île de France, LIX, École Polytechnique
91128 Palaiseau Cedex France

Keywords

Linear programming, decision procedures, formal proofs, Coq proof assistant, Kepler conjecture.

Context

The Kepler Conjecture asserts that no packing of congruent balls in Euclidean space has density greater than the density of the face-centered cubic packing. Otherwise said, the usual way greengrocers pile the oranges on their stall is the densest. This conjecture was proved by Thomas Hales and Samuel Ferguson in 1998. Yet the two authors had to wait until 2005 to see their proof published [Hal05], with a disclaimer. In fact, this proof involves a fair amount of computations performed by computer code developed on purpose by the authors. The referees' claim was that though they were confident in the pen-and-paper part of the proof, they could not faithfully check such a complex piece of software.

Since then, Thomas Hales has started a collaborative effort [The09] to develop a formal proof for this theorem. The use of proof assistants is precisely what could give the highest possible guarantee on such a composite proof. Significant steps toward this direction have already been achieved [HHM$^+$09].

Objectives

A part of the programs involved in the Kepler conjecture proof deals with solving linear programming problems. Each of these linear programs describes a candidate configuration to be of highest density. Hence these problems should all be unsatisfiable, except the two ones describing the optimal packing. In the original proof, these problems were solved using a state-of-the-art commercial linear programming tool. The formal treatment of these problems has recently been investigated [ON09] in the context of the Isabelle proof assistant, leading to important extensions of the proof assistant, and using GLPK (Gnu Linear

Programming Kit). The aim of this work is to investigate how such a verification could be carried on in the Coq system [BC04]. The Coq system is indeed well skilled for trusted computations. Moreover linear problems are suited for certificate based approaches [Bes06]. This means one can delegate expensive computations to untrusted external efficient oracles, and only verify formally the correctness of some certificates provided by the oracle. The Isabelle formalization has left 10 % of the Kepler conjecture linear problems unverified. The objective of this work is to verify them all. A good understanding of this problem would moreover lead to enhanced proof automation for linear arithmetic inside the Coq system.

Practical aspects

This internship will take place at the LIX Laboratory, École Polytechnique, headed by Philippe Baptiste. It will be supervised by Assia Mahboubi, in the INRIA TypiCal team. The work will also be a collaboration with Pierre-Yves Strub (INRIA Rocquencourt - Beijing University), and possibly with the other members of the ANR project DECERT (`http://decert.gforge.inria.fr/index.html`).

References

[BC04] Yves Bertot and Pierre Castéran. *Interactive Theorem Proving and Program Development, Coq'Art: the Calculus of Inductive Constructions*. Springer-Verlag, 2004.

[Bes06] F. Besson. Fast reflexive arithmetic tactics: the linear case and beyond. In *Types for Proofs and Programs (TYPES'06)*, volume 4502 of *LNCS*, pages 48–62. Springer, 2006.

[Hal05] Thomas Hales. A proof of the kepler conjecture. *Annals of Mathematics*, 162:1065–1185, 2005.

[HHM+09] Thomas C. Hales, John Harrison, Sean McLaughlin, Tobias Nipkow, Steven Obua, and Roland Zumkeller. A revision of the proof of the Kepler conjecture. *Discrete and Computational Geometry*, 2009. Published online Mar. 2009.

[ON09] Steven Obua and Tobias Nipkow. Flyspeck II: The basic linear programs. *Annals of Mathematics and Artificial Intelligence*, 2009. Published online Nov. 2009.

[The09] The Flyspeck project. Flyspeck project page, 2009. `http://code.google.com/p/flyspeck/`.