Formal proofs for robot motion planning

Yves Bertot
Yves.Bertot@inria.fr

September 2020

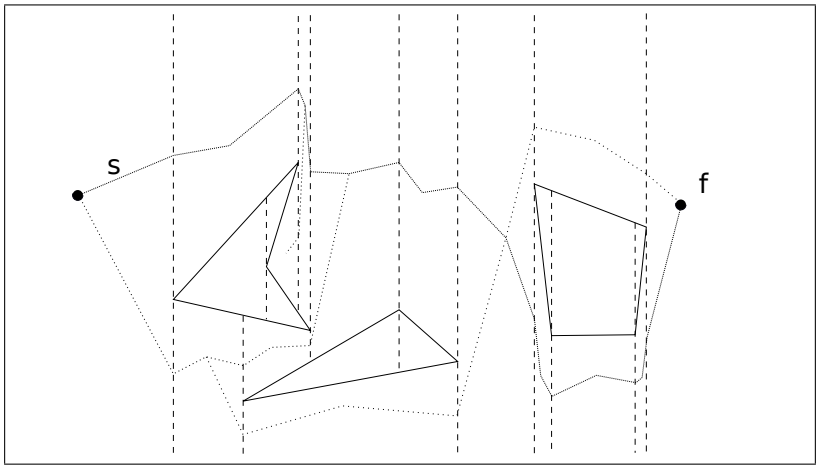
Given a collection of obstacles, one wishes to construct paths from a given start location to a given finish location. The main constraint is that the paths should not collide with the obstacles.

Algorithms for this problem have been known for while, and there are several variants, depending on whether one wishes to have maximal clearance (moving in such a way that the distance to the closest obstacle is maximized) or the shortest length. Some work is based on Voronoï diagrams, other work uses some form of vertical cell decomposition.

We contend that formal proofs can be used to verify this kind of algorithms. Moreover this should really be considered if the robots are to be used in conditions that are life-threatening. In particular, one may think of autonomous vehicles in the presence of human beings or robotic robots used for fine surgery.

The internship will choose one of the available algorithms and study how this algorithm can be modeled in an interactive proof system like Coq. References are the book by Latombe ([2] and in the book by LaValle [3].

An example for which experiments have already started can be given by the following illustration.



The work that is envisioned concentrates on writing a description of the algorithm and specifications for its correct behavior. In a long run, approaches to derive from this description programs that can be embedded in a real robot should also be studied.

All these studies should be done with the Coq system [1].

Context: Proofs will be performed using the Coq system[1] and the Mathematical Components library[2]. Some experiments may require writing example implementations in Ocaml. The supervisor and his team will provide access to computers with Coq and the relevant libraries installed and training.

[1] https://coq.inria.fr
[2] http://math-comp.github.io/math-comp/

Prerequisites: The pre-requisite for this internship is a good knowledge of functional programming.

Tasks: The intern will have to write various implementations of an algorithm, either using plain inductive data structures, or using data-types for finite sets and graphs provided in the Mathematical Components library. They will also have to write specifications expressing the required safety properties for the output. They will then have to perform proofs, mostly using the Coq system and the existing theorems of the Mathematical Components library [4].

References

[1] Bertot, Y., Castéran, P.: Interactive Theorem Proving and Program Development, Coq'Art: The Calculus of Inductive Constructions. Springer. 2004.

[2] Latombe, J.-C.: Robot Motion Planning. Kluwer Academic Publishers. 1991.

[3] LaValle, S. M.: Planning Algorithms. Cambridge University Press. 2006. `http://planning.cs.uiuc.edu/`

[4] Mahboubi A., Tassi E.: Mathematical Components. To appear. `https://math-comp.github.io/mcb/`