Final Report for Deliverable Nr. 1.6

Cylindrical Algebraic Decomposition

Responsible: Assia Mahboubi, Assia.Mahboubi@inria.fr
Site: INRIA, France

Deliverable Date: July 2013

1 Content of the deliverable

This deliverable reports on the current state of our work around the certification of a cylindrical algebraic decomposition (CAD) algorithm implemented in the Coq proof assistant. The motivation for this task was both to obtain an automated decision procedure for first order statements expressed in the language of real closed fields and to develop reusable formal libraries proving results in real algebraic geometry. The objective of this task is not achieved as such: we do not dispose as of the end of the Formath project of an implementation of a CAD algorithm which is both efficient and formally proved correct. However we have obtained several significant successes in the formalization of properties of objects that play a role in this algorithm, and we have developed libraries that study algebraic numbers, root isolation and the quantifier elimination property of the theory of real close fields. In this report, we describe these contributions.

2 Algebraic numbers

The main contribution we have obtained on this topic is the library developed by Cyril Cohen, which was an ingredient of the first distribution of the complete formal proof of the Odd Order Theorem [5]. Cyril Cohen has proposed a construction of real algebraic numbers and constructed complex algebraic numbers as their algebraic closure, following a concise and elegant proof by Derksen. Complex algebraic numbers are used to provide a concrete instance of algebraically closed field needed for the representation theory and character theory the proof of the Odd Order Theorem relies on. The code corresponding to this work is available in the public release of the proof [7]. This work is described in a publication by Cyril Cohen at the ITP'2012 conference [1] and in his PhD thesis [2].

The second line of work has been carried at the Sophia site. Yves Bertot and Maxime Dénès have supervised the internship of Konstantinos Lentzos, who has worked on the implementation and certification of efficient algorithms for algebraic numbers. However this internship proved too short for a newcomer to formal proofs to be able to obtain significant contributions on this ambitious topic.

3 Root isolation

Given a polynomial with coefficient in a discrete real closed field, it is possible to construct a list of small disjoint intervals that each approximate a root of the polynomial, and such that every root of the polynomial has an approximation in the list. This elementary property, called real roots isolation, plays a crucial role in real algebraic geometry. Efficient algorithms of real roots isolation are based on variants of Descartes law and on a dichotomy process involving at each step the decomposition of the polynomial on parametric Bernstein bases. We have obtained two contributions on this topic.

Yves Bertot (Inria), Frédérique Guilhot (Inria) and Assia Mahboubi (Inria) have worked on the properties of Bernstein polynomials. In particular, they have proved a version of Descartes' law of signs. They also have formally proved the de Casteljau algorithm for Bernstein polynomials which ensures the efficiency of a dichotomy process based on the representation of polynomial on parametric Bernstein bases. This work is described in a paper published in a special issue of the Mathematical Structures for Computer Sciences journal [8].

A second contribution is obtained by Julianna Szido during her postdoctoral stay at the Inria Sophia site. She has worked on an other aspect of Bernstein based real root isolation: the non trivial argument ensuring the termination of the dichotomy process. This termination is based on a result known as the theorem of three circles, and requires to consider the roots of the polynomial in an algebraic closure of the real closure. The proof of this theorem is completely formalized and this work is described in a journal paper submitted for publication and available as a preprint [9].

4 Quantifier Elimination for Real Closed Fields

Cyril Cohen and Assia Mahboubi have formally proved the property of quantifier elimination the structures of (discrete) algebraic closed fields [3] and (discrete) real closed fields (see [4] and deliverable 1.3). They are currently collaborating with Marie-Françoise Roy (University of Rennes, France) and Henri Lombardi (University of Besançon, France) in order to improve the formal description they have provided for the case of real closed fields toward the formal description of a cylindrical algebraic decomposition algorithm. Several working session between theses collaborators have been organized in the context of the Formath project.

In order to become a cylindrical algebraic decomposition algorithm, the procedure described in our previous publication [4] has to be modified along two directions. First the complexity of the projection operator that is used to eliminate a single variable should be improved by replacing the naive computations of pseudo-remainder sequences by the use of subresultant coefficients. We expect this part to be completed soon thanks to the results that Cyril Cohen has recently successfully formalized, as described in deliverable 1.5. The second improvement is more demanding : a key point in the efficiency of the cylindrical algebraic algorithm is the use of sample points. The proof that this method is correct requires first a formal definition of the concept of cylindrical algebraic decomposition of R^n for R a (discrete) real closed field and second a formal study of semi-algebraic functions. Both these

ingredients were not needed in our previous work on a more naive algorithm and represent challenging and interesting extensions of our libraries. Interestingly, Marie-Françoise Roy and Henri Lombardi pointed us to the fact that a proof of the correctness of a cylindrical algebraic decomposition algorithm relies on a preliminary proof of the decidability of the first order theory of real closed fields. We hence expect to rely on our previous formal proof of a naive quantifier elimination algorithm which actually provides the decidability result needed here.

Cyril Cohen and Assia Mahboubi are presently working on a formal description of semi-algebraic functions. Our current plan is to define this property by the existence of a first order description of the graph of the function, based on the available infrastructure on reified syntax for first order statements. The challenge is to ease the bureaucracy between the meta-level of reified formulas and the mathematical level. Once this concept is formalized, we can use it to define partitions of decomposition of R^n for R a (discrete) real closed field that are a cylindrical algebraic decomposition. Here the difficulty is to describe the recursive structure of the partition and its construction by stratified cells bounded by semi-algebraic functions.

The objective of obtaining a certified implementation of a cylindrical algebraic decomposition algorithm inside the Coq system seems a more distant objective. Moreover, we think that from the perspective of improving the automation available in the system, this complete but extremely expensive algorithm could be less useful than a toolbox of incomplete but more efficient procedures. Components of this toolbox could be obtained from the results of Victor Magron (see deliverable 4.4) or from an approach similar to the work carried in the PVS proof assistant [6].

References

[1] Cyril Cohen. Construction of real algebraic numbers in coq. In Lennart Beringer and Amy Felty, editors, *Interactive Theorem Proving*, volume 7406 of *Lecture Notes in Computer Science*, pages 67–82. Springer Berlin Heidelberg, 2012. http://dx.doi.org/10.1007/978-3-642-32347-8_6.

[2] Cyril Cohen. *Formalized algebraic numbers: construction and first-order theory.* PhD thesis, École polytechnique, 2012.

[3] Cyril Cohen and Assia Mahboubi. A formal quantifier elimination for algebraically closed fields. In Serge Autexier, Jacques Calmet, David Delahaye, PatrickD.F. Ion, Laurence Rideau, Renaud Rioboo, and AlanP. Sexton, editors, *Intelligent Computer Mathematics*, volume 6167 of *Lecture Notes in Computer Science*, pages 189–203. Springer Berlin Heidelberg, 2010.

[4] Cyril Cohen and Assia Mahboubi. Formal proofs in real algebraic geometry: from ordered fields to quantifier elimination. *Logical Methods in Computer Science*, 8(1), 2012.

[5] Gonthier, Georges and Asperti, Andrea and Avigad, Jeremy and Bertot, Yves and Cohen, Cyril and Garillot, Franois and Roux, Stéphane and Mahboubi, Assia and O'Connor, Russell and Ould Biha, Sidi and Pasca, Ioana and Rideau, Laurence and Solovyev, Alexey

and Tassi, Enrico and Théry, Laurent. A machine-checked proof of the odd order theorem. In Sandrine Blazy, Christine Paulin-Mohring, and David Pichardie, editors, *Interactive Theorem Proving*, volume 7998 of *Lecture Notes in Computer Science*, pages 163–179. Springer Berlin Heidelberg, 2013.

[6] César Muñoz and Anthony Narkawicz. Formalization of a representation of Bernstein polynomials and applications to global optimization. *Journal of Automated Reasoning*, 51(2):151–196, 2013.

[7] The Mathematical Component Team. A Formal Proof of the Odd Order Theorem. https://gforge.inria.fr/frs/download.php/31572/feit_thompson.tar.gz.

[8] Frédérique Guilhot Yves Bertot and Assia Mahboubi. A formal study of bernstein coefficients and polynomials. *Mathematical Structures in Computer Science*, 21:731–761, 8 2011.

[9] Julianna Zsido. Theorem of three circles in coq. *CoRR*, abs/1306.0783, 2013. http://arxiv.org/abs/1306.0783.