Effective Positivstellensatz

Real Algebraic Geometry 2011

Rennes, June 2011
H. Lombardi, Besançon
Henri.Lombardi@univ-fcomte.fr, http://hlombardi.free.fr
Joint work with Daniel Perrucci and M.-F. Roy
http ://hlombardi.free.fr/publis/Raag2011Slides.pdf
To print these slides in an economic way :
http ://hlombardi.free.fr/publis/Raag2011Doc.pdf

The Positivstellensatz
Historical and general background

17th Hilbert's Problem

For $P \in \mathbb{R}[X_1, \ldots, X_n]$ everywhere nonnegative on $\mathbb{R}^n$, write P as a sum of squares in $\mathbb{R}(X_1, \ldots, X_n)$.
Algebraic certificate of nonnegativity.
More rational : for $P \in \mathbb{Q}[X_1, \ldots, X_n]$ everywhere nonnegative on $\mathbb{Q}^n$, write P as a sum of squares in $\mathbb{Q}(X_1, \ldots, X_n)$.
More generally (Artin), let $\mathbf{K}$ be an ordered field where > 0 elements are sums of squares. For $P \in \mathbf{K}[X_1, \ldots, X_n]$ everywhere nonnegative on $\mathbf{R}^n$, write P as a sum of squares in $\mathbf{K}(X_1, \ldots, X_n)$. Here $\mathbf{R}$ is a real closure of $\mathbf{K}$.

The Positivstellensatz. General background

Real Nullstellensatz

If $g \in \mathbb{R}[X_1, \ldots, X_n]$ is zero at the zeroes of $f_1, \ldots, f_s \in \mathbb{R}[\underline{X}]$ in $\mathbb{R}^n$, there is an algebraic certificate for this.

$$g^{2m} + \text{ a S.O.S. } + f = 0, \quad \text{where } f \in \langle f_1, \ldots, f_s \rangle$$

Weak form

If $f \in \mathbb{R}[\underline{X}]$ has no zero in $\mathbb{R}^n$, there is an algebraic certificate for this.

$$1 + \text{ a S.O.S. } + fh = 0.$$

The Positivstellensatz. General background

Krivine-Stengle Positivstellensatz. Rational form.

Let $\mathbf{K}$ be an ordered field, contained in a real closed field $\mathbf{R}$.
If $\mathcal{H}$ is a system of sign conditions (> 0, ≥ 0, $= 0$) on a finite family

$$((s_1, \ldots, s_k), (p_1, \ldots, p_\ell), (g_1, \ldots, g_m)) = (\mathcal{H}_>, \mathcal{H}_\geq, \mathcal{H}_=)$$

in $\mathbf{K}[X_1, \ldots, X_n]$ which is impossible in $\mathbf{R}^n$, there is a rational algebraic certificate for this :

$$S + P + N = 0,$$

– S is > 0 from $\mathcal{H}_>$,
– P is ≥ 0 from $\mathcal{H}_> \cup \mathcal{H}_\geq$,
– N is $= 0$ from $\mathcal{H}_=$.

The Positivstellensatz. General background

More precisely.

1. "S is > 0 from $\mathcal{H}_>$" means that S belongs to the multiplicative monoid generated by the s_i's and $\mathbf{K}^{>0}$.
2. "P is ≥ 0 from $\mathcal{H}_> \cup \mathcal{H}_\geq$" means that P belongs to the cone in $\mathbf{K}[\underline{X}]$ generated by the s_i's, the p_i's, and $\mathbf{K}^{>0}$.
3. "N is $= 0$ from $\mathcal{H}_=$" means that P belongs to the ideal of $\mathbf{K}[\underline{X}]$ generated by the g_i's.

The Positivstellensatz. General background

Some remarks.

1. This Positivstellensatz implies many variants.
   E.g., "an algebraic certificate for a polynomial being > 0 on a given semi-algebraic set"
2. The Positivstellensatz follows "easily" from the weak real Nullstellensatz (via variants of the Rabinovitch trick).
3. The Positivstellensatz implies improved solution for the 17th.
4. It seems impossible to deduce de Positivstellensatz from a solution for the 17th.

The Positivstellensatz. General background

Related problems to this context.

Geometric hypothesis implies Algebraic certificate.

1. Is the geometric hypothesis a concrete, decidable hypothesis ?
2. When this is the case, can we construct the algebraic certificate (a nice formula) from the hypothesis ?
3. Does the nice formula depends continuously on the hypothesis.

Answers for 1 and 2 are YES in a *discrete* setting, i.e., when we have a sign test in $\mathbf{K}$.
Answer for 1 is a priori NO for the usual real number field $\mathbb{R}$.
Answer for 2 is unclear for $\mathbb{R}$.
Answer for 3 is YES for the 17th (so we can drop the discreteness) and for other "good" cases : when the parameters vary on a locally closed semi-algebraic set.

The Positivstellensatz
Logical background

An algebraic certificate is a very simple proof of the result (emptiness of a specified semi-algebraic set).
Constructing a Positivstellensatz can be seen as a *proof transformation*.
We start from a complicated proof of the hypothesis, we transform the proof in a simpler and simpler one, until we reach the simplest possible form : an algebraic certificate.
In the discrete setting (today we shall work in this context), the hypothesis admits certainly a proof by the completeness of the first order theory of discrete real closed fields.

The Positivstellensatz. Logical background

In the nondiscrete setting, things are more mysterious, since we don't know a priori the content of the hypothesis : i.e., some proof of emptiness.
Note that this kind of problem is always present in mathematics when some conclusion has a truly concrete form. A priori, the corresponding concrete form of the hypothesis has to be a constructive proof of the hypothesis.
If this is not the case, something very strange appears : a kind of miracle to be understood.
E.g., for Heine-Borel there is no known concrete form of the hypothesis (more precisely, the only known concrete form of the hypothesis is the conclusion).

The Positivstellensatz. Logical background

Logically complicated proofs may be much shorter than simpler proof.
E.g., there exist emptiness tests of rather low complexity ($\sim$ single exponential) using infinitesimals and Morse theory.
But it seems very difficult to transform this kind of proof in a first order proof, without, at the same time, getting a much longer proof.
Even the Collins CAD (double exponential complexity) is not easy to transform in a first order proof. Indeed it is based on semi-algebraic connectedness of cells. But semi-algebraic connectedness is not a first order property in the theory of DRCF.

The Positivstellensatz. Logical background

Our general plan to attack the problem is as follows.
1) Find a first order proof which is not too long, and rather simple (no quantifiers, or a minimal use of quantifiers).

2) Transform each step of the proof in a suitable :
construction of algebraic certificates from algebraic certificates.
The best first order proof we have found is a suitable modification of the CAD. When "eliminating one variable" we need to saturate the family by derivation and to build algebraic certificates for the signs of the family in each cell.
These algebraic certificates are based on real counting à la Hermite.

First order theory of
discrete real closed fields

$$(\mathbf{K}, \bullet = 0, \bullet > 0, \bullet \geq 0, +, -, \times, 0, 1)$$

- $x = y$ means $x - y = 0$
- $x \geq y$ means $x - y \geq 0$
- $x > y$ means $x - y > 0$
- $x \neq y$ means $(x - y)^2 > 0$

Direct rules

1. $(\mathbf{K}, = 0, +, -, \times, 0, 1)$ is a commutative ring. I.e., computational machinery of commutative rings, plus three direct axioms :

$$\vdash 0 = 0, \qquad x = 0 \vdash xy = 0, \qquad x = 0,\ y = 0 \vdash x + y = 0.$$

2. $\vdash\ 1 > 0$
3. $x = 0\ \vdash\ x \geq 0$
4. $x > 0\ \vdash\ x \geq 0$
5. $\vdash\ x^2 \geq 0$
6. $(x > 0,\ y \geq 0)\ \vdash\ x + y > 0$
7. $(x > 0,\ y > 0)\ \vdash\ xy > 0$
8. $(x \geq 0,\ y \geq 0)\ \vdash\ x + y \geq 0$
9. $(x \geq 0,\ y \geq 0)\ \vdash\ xy \geq 0$

First order theory of discrete real closed fields

Simplification rules

11. $x^2 \leq 0\ \vdash\ x = 0$
12. $(c \geq 0,\ cs > 0)\ \vdash\ s > 0$
13. $(s > 0,\ cs \geq 0)\ \vdash\ c \geq 0$
14. $(c \geq 0,\ x(x^2 + c) \geq 0)\ \vdash\ x \geq 0$

Dynamic rules

15. $x + y > 0\ \vdash\ x > 0 \vee y > 0$
16. $xy > 0\ \vdash\ x > 0 \vee -y > 0$
17. $x^2 > 0\ \vdash\ \exists y\ xy = 1$
18. $x \geq 0\ \vdash\ \exists y\ x = y^2$ (Euclidean field)
19. $\vdash\ \exists y\ y^3 + ay^2 + by + c = 0$ (Real closure, degree 3) ...

Discreteness

DOF $\vdash\ x = 0 \vee x^2 > 0$

Transformation of each step of the proof

Weak inference

Assume first that $\mathcal{H}_1$ and $\mathcal{H}_2$ are systems of sign conditions and that we have a rather easy logical deduction rule $\boxed{\mathcal{H}_1 \vdash \mathcal{H}_2}$ valid in the theory of DRCF.
E.g., a direct rule or a simplification rule.
We transform logic into computation in the following way.
We note $\boxed{\downarrow \mathcal{H} \downarrow}$ as an abbreviation for :
here is an algebraic certificate for the impossibility of $\mathcal{H}$.
Now our aim is to prove the *weak inference* $\boxed{\mathcal{H}_1 \vdash_w \mathcal{H}_2}$,
which means :
if $\mathcal{H}$ is an arbitrary context, we explain how to construct $\downarrow \mathcal{H}_1, \mathcal{H} \downarrow$ from $\downarrow \mathcal{H}_2, \mathcal{H} \downarrow$.
Moreover we compute a "degree function" which is a bound on the degree of $\downarrow \mathcal{H}_1, \mathcal{H} \downarrow$ from a bound on the degree of $\downarrow \mathcal{H}_2, \mathcal{H} \downarrow$.

Transformation of each step of the proof

Weak disjunction

Assume that $\mathcal{H}_i$ $(i = 1, 2, 3)$ are systems of sign conditions and that we have a rather easy deduction rule $\boxed{\mathcal{H}_1 \vdash \mathcal{H}_2 \vee \mathcal{H}_3}$ valid in the theory of DRCF.

Our aim is to prove the *weak inference* (or weak disjunction) $\boxed{\mathcal{H}_1 \vdash_w \mathcal{H}_2 \vee \mathcal{H}_3}$ which means :

If $\mathcal{H}$ is an arbitrary context, we explain the construction of $\downarrow \mathcal{H}_1, \mathcal{H} \downarrow$ from $\downarrow \mathcal{H}_2, \mathcal{H} \downarrow$ and $\downarrow \mathcal{H}_3, \mathcal{H} \downarrow$.

Moreover we compute a "degree function" which is a bound on the degree of $\downarrow \mathcal{H}_1, \mathcal{H} \downarrow$ from bounds on the degrees of $\downarrow \mathcal{H}_2, \mathcal{H} \downarrow$ and $\downarrow \mathcal{H}_3, \mathcal{H} \downarrow$.

Transformation of each step of the proof

Weak existence

Assume that $\mathcal{H}_1$ and $\mathcal{H}_2$ are systems of sign conditions, T, U are variables present in $\mathcal{H}_2$ but not in $\mathcal{H}_1$ and that we have a rather easy deduction rule $\boxed{\mathcal{H}_1 \vdash \exists T, U\ \mathcal{H}_2}$ valid in the theory of DRCF.

Our aim is to prove *weak inference* (or weak existence)

$$\boxed{\mathcal{H}_1 \vdash_w \exists T, U\ \mathcal{H}_2}$$

which means :

if $\mathcal{H}$ is an arbitrary context without the variables T, U, we explain the construction of $\downarrow \mathcal{H}_1, \mathcal{H} \downarrow$ from $\downarrow \mathcal{H}_2, \mathcal{H} \downarrow$.

Moreover we compute a "degree function" which is a bound on the degree of $\downarrow \mathcal{H}_1, \mathcal{H} \downarrow$ from a bound on the degree of $\downarrow \mathcal{H}_2, \mathcal{H} \downarrow$.

A simple and short first order proof

What do we want to prove ?

Given an arbitrary polynomial system $f_1, \ldots, f_s \in \mathbf{K}[X_1, \ldots, X_n]$ we want to find a "simple" first order proof of the disjunction giving all possible combinations of signs for the family :

$$\vdash\ \mathcal{H}_1 \vee \mathcal{H}_2 \vee \cdots \vee \mathcal{H}_\ell$$

If the proof involves only simple deduction rules, we are able to transform this proof in the corresponding weak disjunction

$$\vdash_w\ \ \mathcal{H}_1 \vee \mathcal{H}_2 \vee \cdots \vee \mathcal{H}_\ell$$

Now, if $\mathcal{H}$ is a system of sign conditions not appearing in the list, we have $\downarrow \mathcal{H}, \mathcal{H}_i \downarrow$ for each i, and the weak disjunction computes $\downarrow \mathcal{H} \downarrow$ from these $\downarrow \mathcal{H}, \mathcal{H}_i \downarrow$. If the simple "dynamical proof" is not too long, we get a degree bound not too high for $\downarrow \mathcal{H} \downarrow$.

A certified cylindric algebraic decomposition

A CAD for the given family gives all possible sign combinations.

The problem comes from the difficulty to have a simple proof that the CAD gives actually all possible sign combinations.

By simple proof, we mean a proof using only few "simple" dynamical rules, which is a kind of quantifier free proof.

Note that the final algebraic identity gives a proof inside the theory of ordered rings using only very simple direct rules. In particular it does not use existential rules, nor discreteness.

page 19

A certified cylindric algebraic decomposition

Surprinsingly difficult simple results

In fact, even if real roots do not appear in the conclusion, it seems impossible to get some rather elementary results without using real roots in the proof.
E.g., the fact that the Sturm count gives always a nonnegative number of roots on an interval remains a crucial challenge :
no "reasonable" bounds are known for the corresponding algebraic certificates.

page 20

A certified cylindric algebraic decomposition

Weak existence of real roots

Weak existence of a real root on an interval where the sign changes is a crucial tool for CAD. The computation for the weak existence of a real root of polynomial of degree $p = 2q + 1$ mimics Artin's proof of the following result.
Theorem If $f = X^p + \sum_{i=0}^{p-1} a_i X^i \in \mathbf{K}[X]$ is irreducible, where $\mathbf{K}$ is a real field, then $\mathbf{K}[x] = \mathbf{K}[X]/\langle f \rangle$ is a real field.
The weak existence of a root of f when a_i are polynomials in parameters is obtained by induction on q and gives a rather bad degree-function.

page 21

A certified cylindric algebraic decomposition

Weak existence of real roots : a bad degree function

– $h(k,p) = 2^{3\cdot 2^{\frac{k+1}{2}}-3} p^{2^{\frac{k+1}{2}}-1}$,
– $h(p) = h(p,p)$. Approximately $h(p) = p^{2^p}$
– degree-function : $\Delta(\delta, \rho; p, d) = (\delta + d\rho)h(p)$.
where ρ is the T-degree of the initial incompatibility and d is the degree of f in other variables than T

page 22

A certified cylindric algebraic decomposition

Hermite theory for certifying signs at the zeroes

We have to certify that a given family $\mathcal{F}$ of polynomial in $\mathbf{K}[X_1, \ldots, X_k][Y]$ has the same behaviour over all the points of a given cell when "we eliminate Y", i.e., when we make a projection $\mathbf{R}^{k+1} \to \mathbf{R}^k$.
The family has to be saturated w.r.t. Y-derivation, and we want to know the sign of each polynomial of $\mathcal{F}$ at the zeroes of the other polynomials of $\mathcal{F}$. As a consequence, we will have the Thom's-coding of each zero.
We use Hermite's theory for real counting and an algorithm à la BKR, modified in such a way that there are not too many branches in the computation.

page 23

A certified cylindric algebraic decomposition

Hermite theory for certifying signs at the zeroes

Hermite's theory uses *signature of quadratic forms*. We need to develop a theory of signatures of symmetric real matrices in a pure "algebraic identities form".
We get *algebraic certificates related to the signature* : they show that the computed signature cannot be different when counted in two different ways.
Hermite's theory uses *all complex roots of the given real polynomial* we have to study.
So we need the *weak existence for complex roots of a real polynomial*.

Laplace proof of the FTA

Laplace proof of the FTA can be formalized in the theory of RCDF.
Starting with a polynomial of degree $p = 2^r(2s+1)$, it constructs a polynomial of odd degree $\leq p^{2^r} \leq p^p$. We use the weak existence of a real root for this polynomial in order to get the weak existence of a complex root of the initial polynomial.
This leads to a triple exponential degree-function for the weak existence corresponding to the decomposition of the polynomial in a product of complex linear factors.

From signs at the zeroes to signs on all the real line

When we have algebraic certificates for the zeroes of a family $\mathcal{F}$ above a cell, we get algebraic certificates for the signs of the polynomials of $\mathcal{F}$ on the intervals defined by the zeroes.
This is almost for free, because variants of Taylor formulas do the job.

Controlling the total number of cells

When eliminating the variable Y in $\mathbf{K}[X_1, \ldots, X_k][Y]$, we have to use *test coefficients* in $\mathbf{K}[\underline{X}]$.
In the usual CAD, they are Y-resultants of pairs of polynomials in $\mathcal{F}$.
Here, we need more coefficients, controlling the signatures of suitable Hankel matrices related to Hermite theory.
Nevertheless, we are able to control not only the degrees of the test coefficients, but also the number of these coefficients. This is related to bounds on the number of possible sign combinations for a given (rather large) family of polynomials in few ($= k$) variables.

Degree bound for this kind of proof

A bound for degrees of polynomials in a CAD is classically double exponential.
The main ingredient for the complexity comes from Laplace proof of the FTA, which leads, for weak existence, to a triple exponential bound w.r.t. the degree of polynomials occurring in the CAD.
The number of cells and of polynomials seems rather well controlled (doubly exponential).
So, if no unsuspected catastroph appears in the computation, we think to obtain a 5-exponential bound as

$$2^{2^{2^{2^{n+s+d}}}}$$