page 1

Real closed fields Elimination of prime cones

September 2006

Printable version of these slides

http://hlombardi.free.fr/publis/LectureDoc4.pdf

Directly related paper

http://hlombardi.free.fr/publis/NullstellensatzDynamic.pdf

page 2

Hilbert's Nullstellensatz classical setting

Theorem 1.

Let $\mathbf{K}$ *be a discrete field and* $f_1, \ldots, f_s, g \in \mathbf{K}[X_1, \ldots, X_n] = \mathbf{K}[\underline{X}]$.
Let Σ *be the system of conditions:*

$$f_1(\underline{x}) = \cdots = f_s(\underline{x}) = 0,\ g(\underline{x}) \text{ is invertible.}$$

Let $\mathbf{A} = \mathbf{K}[\underline{x}] = \mathbf{K}[\underline{X}]/\langle f_1, \ldots, f_s\rangle$, $\mathbf{B} = \mathbf{A}[1/g(\underline{x})]$ *and* $\mathbf{L}$ *some algebraically closed field containing* $\mathbf{K}$.

T.F.A.E.

1. *The system* Σ *has no solution, in any nonzero* $\mathbf{K}$*-algebra.*
2. $\mathbf{B} = 0$, *i.e.,* $\exists m \in \mathbb{N},\ g^m \in \langle f_1, \ldots, f_s\rangle$.
3. *The system* Σ *has no solution, in any field containing* $\mathbf{K}$.
4. *The system* Σ *has no solution, in any finite algebraic extension of* $\mathbf{K}$.
5. $g = 0$ *on the variety of zeros of* $f_1, \ldots, f_s$ *in* $\mathbf{L}^n$.

page 3

Proofs of Hilbert's Nullstellensatz (classical mathematics)

1. $\iff$ 2. is clear. (direct constructive)
3. $\implies$ 2. if $\mathbf{B} \neq 0$ take a **prime ideal** $\mathfrak{p}$ in $\mathbf{B}$ and consider the corresponding field $\mathrm{Frac}(\mathbf{B}/\mathfrak{p})$.
4. $\implies$ 2. if $\mathbf{B} \neq 0$ take a **maximal ideal** $\mathfrak{m}$ in $\mathbf{B}$, consider the corresponding field $\mathbf{B}/\mathfrak{m}$ and apply Lemma 2.
4. $\iff$ 5. is clear. (direct and constructive, once you have an algebraically closed field containing $\mathbf{K}$)

Lemma 2. (very weak Nullstellensatz) *(constructive)*
If a finitely generated $\mathbf{K}$*-algebra is a field, it is an algebraic extension of* $\mathbf{K}$.

page 4

Classical proof via model theory

Consider the following first order theories:

$\mathcal{T}_0$. Rings containing $\mathbf{K}$, plus axioms corresponding to Σ,
i.e., $\exists x_1, \ldots, x_n,\ f_1(\underline{x}) = \cdots = f_s(\underline{x}) = 0,\ g(\underline{x})$ is invertible.

$\mathcal{T}_1$. Fields containing $\mathbf{K}$, plus axioms corresponding to Σ.

$\mathcal{T}_2$. $\mathcal{T}_1$ plus axioms of algebraically closed fields.

$\mathcal{T}_3$. Algebraically closed fields containing $\mathbf{K}$.

Since a nontrivial ring contains a prime, theories $\mathcal{T}_0$ and $\mathcal{T}_1$ are simultaneously consistant.
Since every field is contained in an algebraically closed field, theories $\mathcal{T}_1$ and $\mathcal{T}_2$ are simultaneously consistant.
Since there is a decision procedure in $\mathcal{T}_3$, if $\mathcal{T}_2$ is consistant then every algebraically closed field containing $\mathbf{K}$ is a model of $\mathcal{T}_2$.

Constructive deciphering of the proof via model theory

a) The argument saying that a non trivial ring contains a prime has to be replaced by a direct proof that the two theories $\mathcal{T}_0$ and $\mathcal{T}_1$ are simultaneously inconsistant. This is done using the algebraic heart of the classical proof that a non trivial ring contains a prime.
b) The argument saying "Since every field is contained in an algebraically closed field the two theories $\mathcal{T}_1$ and $\mathcal{T}_2$ are simultaneously consistant." has to be replaced by a direct proof that the two theories $\mathcal{T}_1$ and $\mathcal{T}_2$ are simultaneously inconsistant. This is done using the algebraic heart of the classical proof that a field can be embedded in an algebraically closed field: *i.e.*, an euclidean division.

Constructive reformulation

Theorem 3. *T.F.A.E.*

1. *The system Σ has no solution, in any nonzero $\mathbf{K}$-algebra.*
2. $\mathbf{B} = 0$*, i.e.,* $\exists m \in \mathbb{N}$, $g^m \in \langle f_1, \dots, f_s \rangle$.
3. *Theory $\mathcal{T}_i$ is inconsistant, i.e., it proves* $0 = 1$ *(*$i = 0, 1$ *or* 2*).*
4. *The system Σ has no solution, in any $\mathbf{K}$-algebra which is finite as $\mathbf{K}$-vector space.*
5. $g = 0$ *on the variety of zeros of* $f_1, \dots, f_s$ *in* $\mathbf{L}^n$ *(here you need an algebraically closed field containing* $\mathbf{K}$*).*

More precisely, either you find an identity 2., or you find a point satisfying Σ with coordinates in a $\mathbf{K}$-algebra which is finite as $\mathbf{K}$-vector space.

Dynamical algebraic structures

We reformulate the preceding arguments "without using logic".
We replace logic by a purely computational machinery related to uncompletely specified algebraic structures.
Axioms have to be "dynamic axioms" (axioms of a simple form, as in usual algebraic structures, we will see on examples).
A dynamical structure (for a given dynamical theory) is given by generators and relations. Naturally, this works usually for purely equational theories. But we need also dynamical fields, for example. Since a system of generators and relations fail in general to define a field, we see the dynamical structure as a way of exploring all properties that can be deduced from axioms, generators and relations. It is the constructive counterpart of the magic "consider first an arbitrary prime ideal in the ring and then the fraction field of the quotient ring".

Dynamical algebraic structures. Examples. 1.

First example, (commutative) *nontrivial rings.*
The *unary language of rings* $\mathcal{L}_r$ has constants 0, 1, -1 and binary functions $+$ and $\times$ and only one unary relational symbol $= 0$.

$$\begin{array}{rlr}
 & \vdash\ 0 = 0 & D(1)_r \\
x = 0,\ y = 0 & \vdash\ x + y = 0 & D(2)_r \\
x = 0 & \vdash\ xy = 0 & D(3)_r \\
1 = 0 & \vdash\ \bot & C_r
\end{array}$$

Remark 1: Axioms of commutative rings are replaced by computations inside $\mathbb{Z}[G]$ where G is the set of elements of the structure occurring in the proofs.
Remark 2: The structure given by a set of generators G and a subset R of $\mathbb{Z}[G]$ ($a \in R$ means $a = 0$) collapses exactly if $1 \in \langle R \rangle$.

Dynamical algebraic structures. Examples. 2.

Second example, *rings with a proper multiplicative monoid.*
We consider the *unary language of fields* $\mathcal{L}_f$, which is the unary language of rings with a new unary relation $\neq 0$. The new axioms are:

$$\begin{array}{rll} x = 0,\ y \neq 0 & \vdash\ x + y \neq 0 & D(1)_f \\ x \neq 0,\ y \neq 0 & \vdash\ xy \neq 0 & D(2)_f \\ & \vdash\ 1 \neq 0 & D(3)_f \\ 0 \neq 0 & \vdash\ 1 = 0 & C_f \end{array}$$

Remark 3: The structure given by a set of generators G and two subsets R, S of $\mathbb{Z}[G]$ ($a \in R$ means $a = 0$ and $u \in S$ means $u \neq 0$) collapses exactly if $0 = s + r$ for some $r \in \langle R \rangle$ and s in the multiplicative monoid generated by S. This is basically the same thing as the equivalence 1. $\iff$ 2. in the Hilbert's Nullstellensatz.

Dynamical algebraic structures. Examples. 3.

Third example, (nontrivial) *discrete domains.*
Add the disjunctive axiom

$$\vdash\ x = 0\ \vee\ x \neq 0 \qquad\qquad Dy(1)_f$$

It is now possible to deduce simplification rules.

$$\begin{array}{rll} xy = 0, x \neq 0 & \vdash\ y = 0 & S(1)_f \\ xy \neq 0 & \vdash\ x \neq 0 & S(2)_f \end{array}$$

Remark 4: The "discrete domain structure" given by a set of generators G and two subsets R, S of $\mathbb{Z}[G]$ collapses simultaneously with the similar structure of "ring with proper monoid".
This is basically the simulatneous inconsistency of theories $\mathcal{T}_0$ and $\mathcal{T}_1$. The proof is given by the algebraic heart of the classical proof of existence of prime ideals.
See the following slide.

Dynamical algebraic structures. Examples. 4.

Proof of the simultaneaous collapsus, for rings with proper monoid and discrete domains.
Consider a dynamical ring with proper monoid given by generators G and relations R, $S \subset \mathbb{Z}[G]$.
Let I the ideal generated by R and M the monoid generated by S.
The structure collapses iff there are $r \in I$, $s \in M$ s.t. $r + s = 0$.
Assume the structure collapses as a dynamic discrete domain. E.g., you have open two branches. The one with $t = 0$, the second one with $t \neq 0$ (for a certain term t). In the first branch the collapsus means $s_1 + r_1 - at = 0$, in the second one it means $t^n s_2 + r_2 = 0$. Eliminating t you get $s_2(s_1 + r_1)^n = -a^n r_2$, and this can be rewritten as $s_3 + r_3 = 0$.

Dynamical algebraic structures. Examples. 5.

Proof of Krull's Theorem for prime ideals.
Consider a ring $\mathbf{A}$ with an ideal I and a monoid M. Krull's Theorem says that if $0 \notin I + M$ there exists a prime ideal $\mathfrak{p}$ such that $I \subseteq \mathfrak{p} \subseteq \mathbf{A} \setminus M$.
By Zorn's lemma we have a maximal pair (J, N) extending (I, M) under the constraint $0 \notin J + N$.
We have to show that $J \cup N = \mathbf{A}$. If not let t in the complement. Since (J, N) is maximal, adding

t to J produces a collapsus, i.e., there is $r_1 \in J$, $a \in \mathbf{A}$ and $s_1 \in N$ such that $s_1 + r_1 - at = 0$. Similarly, adding t to M produces a collapsus, i.e., there is $r_2 \in J$, $n \in \mathbb{N}$ and $s_2 \in N$ such that $t^n s_2 + r_2 = 0$. Eliminating t you get $s_2(s_1 + r_1)^n = -a^n r_2$, and this can be rewritten as $s_3 + r_3 = 0$. But this implies $0 \in J + N$, a contradiction.

Dynamical algebraic structures. Examples. 6.

Fourth example, (nontrivial) *discrete fields.*
Add the axiom

$$x \neq 0 \quad \vdash \exists y \; xy - 1 = 0 \qquad\qquad Dy(2)_f$$

Remark 5: The "discrete field structure" given by a set of generators G and two subsets R, S of $\mathbb{Z}[G]$ collapses simultaneously with the similar structure of "discrete domain".
This is basically the same thing as the construction of the fraction field of a discrete domain, or the Rabinovitch trick.

Dynamical algebraic structures. Examples. 7.

Fifth example, the theory of *discrete algebraically closed fields* is obtained by adding a scheme of axioms.
For every degree n we have the axiom:

$$\vdash \exists y \; y^n + x_{n-1}y^{n-1} + \cdots + x_1 y + x_0 = 0 \quad Dy_n(3)_f$$

Remark 6: The "discrete algebraically closed field structure" given by a set of generators G and two subsets R, S of $\mathbb{Z}[G]$ collapses simultaneously with the similar structure of "discrete field".
This is basically the same thing as an euclidean division, which is the constructive content of the construction of the algebraic closure of a field in classical mathematics.

End of the constructive rereading of Hibert's Nullstellensatz proof via model theory

All this was very simple. It was only an explanation of the computations that are hidden in the classical proof of equiconsistency of the theories $\mathcal{T}_i$ $(i = 0, 1, 2)$.
It remains to examine carefully the decision algorithm in the theory of discrete algebraically closed fields containing a given discrete field $\mathbf{K}$.
So we have "deciphered" the classical proof made using model theory. One may wonder if a decision algorithm is hidden in the first classical proof which used a generic maximal ideal. Maybe such an algorithm could be found in the constructive proofs of Lemma 2.

Ordered fields

A *discrete ordered field* is a (nontrivial) discrete field $\mathbf{K}$ with a set P of "nonnegative elements" satisfying:

$$P + P \subseteq P,\; PP \subseteq P,\; P \cap -P = \{0\}\,,\; P \cup -P = \mathbf{K}.$$

$\mathbf{K}$ contains $\mathbb{Q}$, P contains the sums of squares (denoted as $\sum \mathbf{K}^2$).
An *o-ring* is a commutative ring $\mathbf{A}$ with two subsets P and S satisfying:

$$\sum \mathbf{A}^2 \subseteq P,\; P + P \subseteq P,\; PP \subseteq P,\; S \subseteq P,\; P + S \subseteq S,\; SS \subseteq S,\; 1 \in S,\; 0 \notin_{\mathbf{A}} S.$$

P is called a cone (sometimes a preorder). An ordered field is an o-ring if one takes $S_{\mathbf{K}} = P_{\mathbf{K}} \backslash \{0\}$.
A $\mathbf{K}$-*o-algebra* is an o-ring $(\mathbf{A}, P, S)$ with a morphism of o-rings $\alpha : \mathbf{K} \to \mathbf{A}$.

Positivstellensatz

Theorem 4. (here: classical ≡ constructive)
Let $\mathbf{K}$ be a discrete ordered field and $(r_i)_{i\in I}, (p_j)_{j\in J}, (s_k)_{k\in K} \in \mathbf{K}[\underline{X}]$.
Let Σ be the system of conditions:

$$\bigwedge_i f_i(\underline{x}) = 0,\ \bigwedge_j p_j(\underline{x}) \geq 0,\ \bigwedge_k s_k(\underline{x}) > 0.$$

Let $\mathbf{A} = \mathbf{K}[\underline{x}] = \mathbf{K}[\underline{X}]/\langle f_1, \dots, f_s\rangle$, S the subset of $\mathbf{A}$ of elements forced to be > 0 by Σ, $\mathbf{B} = S^{-1}\mathbf{A}$ and $\mathbf{L}$ some real closed field containing $\mathbf{K}$.
T.F.A.E.

1. *The system Σ has no solution, in any nonzero $\mathbf{K}$-o-algebra.*
2. *$\mathbf{B} = 0$, i.e., $s + p + f = 0$ where ....*
3. *The system Σ has no solution, in any ordered field containing $\mathbf{K}$.*
4. *The system Σ has no solution, in any real closed field $\mathbf{K}' \supseteq \mathbf{K}$.*
5. *The system Σ has no solution in $\mathbf{L}$.*

NB: the real closure of a discrete ordered field can be constructed in an effective way.

Positivstellensatz, 2.

This works as for the Nullstellensatz by introducing convenient dynamical theories.
The central theory we consider is the theory of ordered fields. The *unary language of ordered fields $\mathcal{L}_{of}$* is the unary language of rings $\mathcal{L}_r$ with two more unary predicates ≥ 0 and > 0.
A presentation of a structure using this language is given by a set generators G and three subsets S, P, R of $\mathbb{Z}[G]$ where $s \in S$ means $s > 0$, $p \in P$ means $p \geq 0$ and $r \in R$ means $r = 0$.
The unary predicate $x \neq 0$ is not introduced. It is considered as an abbreviation for $x^2 > 0$.

Positivstellensatz, 3.

Axioms of *proto-ordered rings* (or o-rings) are axioms of rings and the following axioms.

$$\begin{array}{rll}
 & \vdash\ x^2 \geq 0 & D(1)_{of} \\
x = 0,\ y \geq 0 & \vdash\ x + y \geq 0 & D(2)_{of} \\
x \geq 0,\ y \geq 0 & \vdash\ x + y \geq 0 & D(3)_{of} \\
x \geq 0,\ y \geq 0 & \vdash\ xy \geq 0 & D(4)_{of} \\
 & \vdash\ 1 > 0 & D(5)_{of} \\
x = 0,\ y > 0 & \vdash\ x + y > 0 & D(6)_{of} \\
x > 0,\ y \geq 0 & \vdash\ x + y > 0 & D(7)_{of} \\
x > 0,\ y > 0 & \vdash\ xy > 0 & D(8)_{of} \\
x > 0 & \vdash\ x \geq 0 & D(9)_{of} \\
0 > 0 & \vdash\ 1 = 0 & C_{of}
\end{array}$$

The collaspus of a corresponding algebraic structure is obtained by constructing an element which is $= 0$ and > 0. This is the meaning of the (easy) equivalence between 1 and 2 in Theorem 4.

Positivstellensatz, 4.

Discrete ordered domains are o-rings satisfying the following axioms:

$$\begin{array}{rll}
x \geq 0,\ -x \geq 0 & \vdash\ x = 0 & S(1)_{of} \\
 & \vdash\ x \geq 0\ \vee\ -x > 0 & Dy(1)_{of}
\end{array}$$

The simultaneous collapsus of a given dynamical algebraic structure viewed either as an o-ring and or as a discrete ordered domain gives the algebraic constructive content of the classical "construction" of a prime cone containing a given cone.

The following simplification rules can be deduced.

$$\begin{array}{rcll}
xy > 0 & \vdash & x^2 > 0 & \qquad S(2)_{of} \\
x^2 \leq 0 & \vdash & x = 0 & \qquad S(3)_{of} \\
x > 0,\ xy \geq 0 & \vdash & y \geq 0 & \qquad S(4)_{of} \\
x \geq 0,\ xy > 0 & \vdash & y > 0 & \qquad S(5)_{of} \\
c \geq 0,\ x(x^2+c)\ \geq 0 & \vdash & x \geq 0 & \qquad S(6)_{of}
\end{array}$$

Positivstellensatz, 5.

The simultaneous collapsus of o-rings and ordered domains gives the constructive content of the classical: " *In a non trivial ring every cone can be embedded in a prime cone* ".
Discrete ordered fields are discrete ordered domains satisfying the following axiom:

$$x > 0 \quad \vdash \exists y\ xy - 1 = 0 \qquad\qquad Dy(2)_{of}$$

The simultaneous collapsus with the theory of discrete ordered domains is as usually a Rabinovitch trick.
The simultaneous collapsus of o-rings and ordered fields gives the constructive content of the equivalence between points 2 and 3 in Theorem 4.

Positivstellensatz, 6.

Real closed discrete fields are discrete ordered fields satisfying the following axioms:

$$-p(a)p(b) \geq 0 \ \vdash \exists y \ \ p(y) = 0 \qquad Dy_n(3)_{of}$$

(a, b, y and coefficients of the monic degree n polynomial p are distinct variables, and there is an axiom for each degree).
The simultaneous collapsus of discrete ordered fields and real closed fields is the difficult part of the constructive proof of the Positivstellensatz.
It uses a tricky inductive argument or Artin-Schreier for proving that if f is an odd degree irreducible polynomial in $\mathbf{K}[X]$ and $\mathbf{K}$ is real then $\mathbf{K}[X]/\langle f(X)\rangle$ is also a real field.
This simultaneous collapsus gives the constructive content of the equivalence between points 3 and 4 in Theorem 4.

Positivstellensatz, 6.

The proof of the Positivstellensatz ends with a close examination of a decision algorithm for the theory of real closed fields containing a given discrete ordered field $\mathbf{K}$.
It happens that the very simple decision algorithm of Cohen-Hörmander gives a dynamic proof of the result (as in the Nullstellensatz's case). So we don't need to use a cut elimination procedure for passing from a first order proof to a dynamic proof.
This gives the equivalence between points 4 and 5 in Theorem 4.
Here model theory simplifies Artin's work, who used subtle specialization lemmas for obtaining (the geometric translation of) this equivalence.

THE END