REAL ALGEBRAIC GEOMETRY LECTURE NOTES (13: 01/12/2009 - BEARBEITET 10/12/18)

SALMA KUHLMANN

THE TARSKI-SEIDENBERG PRINCIPLE

Main Proposition. Let $f_i(\underline{T}, X) := h_{i,m_i}(\underline{T})X^{m_i} + \ldots + h_{i,0}(\underline{T})$ for $i = 1, \ldots, s$ be a sequence of polynomials in $n+1$ variables with coefficients in $\mathbb{Z}$, and let $m := max\{m_i | i = 1, \ldots, s\}$. Let W' be a subset of $W_{s,m}$. Then there exists a boolean combination $B(\underline{T}) = S_1(\underline{T}) \vee \ldots \vee S_p(\underline{T})$ of polynomial equations and inequalities in the variables $\underline{\text{T}}$ with coefficients in $\mathbb{Z}$, such that, for every real closed field R and every $\underline{t} \in R^n$, we have

$$SIGN_R\big(f_1(\underline{t}, X), \ldots, f_s(\underline{t}, X)\big) \in W' \Leftrightarrow B(\underline{t}) \text{ holds true in } R.$$

Proof. Without loss of generality, we assume that none of $f_1, \ldots, f_s$ is identically zero and that $h_{i,m_i}(\underline{T})$ is not identically zero for $i = 1, \ldots, s$. To every sequence of polynomials $(f_1, \ldots, f_s)$ associate the s-tuple $(m_1, \ldots, m_s)$, where $deg(f_i) = m_i$. We compare these finite sequences by defining a strict order as follows:

$$\sigma := (m_1', \ldots, m_t') \prec \tau := (m_1, \ldots, m_s)$$

if there exists $p \in \mathbb{N}$ such that, for every $q > p$,
-the number of times q appears in σ = the number of times q appears in τ, and
-the number of times p appears in $\sigma <$ the number of times p appears in τ.

This order $\prec$ is a total order [1] on the set of finite sequences.

Example: let $m = \max(\{m_1, \ldots, m_s\}) = m_s$ (say), σ and τ be the sequence of degrees of the sequences $(f_1, \ldots, f_{s-1}, f_s', g_1, \ldots, g_s)$ and $(f_1, \ldots, f_{s-1}, f_s)$ respectively, i.e.
$\sigma \rightsquigarrow (f_1, \ldots, f_{s-1}, f_s', g_1, \ldots, g_s)$,
$\tau \rightsquigarrow (f_1, \ldots, f_{s-1}, f_s)$

[1] This was a mistake in the book *Real Algebraic Geometry* of J. Bochnak, M. Coste, M.-F. Roy. For corrected argument, see Appendix I following this proof.

then $\sigma \prec \tau$.

Let $m = \max\{m_1, \ldots, m_s\}$.

In particular using $p = m$ we have:

$\big(deg(f_1), \ldots, deg(f_{s-1}), deg(f_s^{'}), deg(g_1), \ldots, deg(g_s)\big) \prec \big(deg(f_1), \ldots, deg(f_s)\big)$.

If $\underline{m = 0}$, then there is nothing to show, since $SIGN_R\big(f_1(\underline{t}, X), \ldots, f_s(\underline{t}, X)\big) = SIGN_R\big(h_{1,0}(\underline{t}), \ldots, h_{s,0}(\underline{t})\big)$ $\big[$the list of signs of "constant terms"$\big]$.

Suppose that $\underline{m \geq 1}$ and $m_s = m = max\{m_1, \ldots, m_s\}$. Let $W^{''} \subset W_{2s,m}$ be the inverse image of $W^{'} \subset W_{s,m}$ under the mapping φ (as in main lemma). Set $W^{''} = \big\{SIGN_R(f_1, \ldots, f_{s-1}, f_s^{'}, g_1, \ldots, g_s) \mid SIGN_R(f_1, \ldots, f_s) \in W^{'}\big\}$.

-**Case 1.** By the main lemma, for every real closed field R and for every $\underline{t} \in R^n$ such that $h_{i,m_i}(\underline{t}) \neq 0$ for $i = 1, \ldots, s$, we have

$$SIGN_R\big(f_1(\underline{t}, X), \ldots, f_s(\underline{t}, X)\big) \in W^{'}$$

$$\Leftrightarrow$$

$$SIGN_R\big(f_1(\underline{t}, X), \ldots, f_{s-1}(\underline{t}, X), f_s^{'}(\underline{t}, X), g_1(\underline{t}, X), \ldots, g_s(\underline{t}, X)\big) \in W^{''},$$

where $f_s^{'}$ is the derivative of f_s with respect to X, and $g_1, \ldots, g_s$ are the remainders of the euclidean division (with respect to X) of f_s by $f_1, \ldots, f_{s-1}, f_s^{'}$, respectively (multiplied by appropriate even powers of $h_{1,m_1}, \ldots, h_{s,m_s}$, respectively, to clear the denominators).
Now, the sequence of degrees in X of $f_1, \ldots, f_{s-1}, f_s^{'}, g_1, \ldots, g_s$ is smaller than [the sequence of degrees in X of $f_1, \ldots, f_s$ i.e.] $(m_1, \ldots, m_s)$ w.r.t. the order $\prec$.

-**Case 2.** At least one of $h_{i,m_i}(\underline{t})$ is zero
In this case we can truncate the corresponding polynomial f_i and obtain a sequence of polynomials, whose sequence of degrees in X is smaller than $(m_1, \ldots, m_s)$ w.r.t. the order $\prec$.

This completes the proof of main propostion and also proves the Tarski-Seidenberg principle. $\square\square$

APPENDIX I: ORDER ON THE SET OF TUPLES OF INTEGERS

Set $N := \bigcup_{n\in\mathbb{N}} \mathbb{N}^n$

We define on N an equivalence relation $\sim$:

for $\sigma := (n_1, \dots, n_s)$ and $\tau := (m_1, \dots, m_t)$ in N, we write $\sigma \sim \tau$ if and only if the following holds:

$s = t$ and there exists a permutation g of $\{1, \dots, s\}$ such that $m_i = n_{g(i)}$ for all $i \in \{1, \dots, s\}$.

For any $\sigma \in N$, the equivalence class of σ will be denoted by $[\sigma]$

For any $\sigma \in N$ and $p \in \mathbb{N}$, we set $f_p(\sigma) :=$ (number of occurrences of p in σ).

For any $\sigma, \tau \in N$ and $p \in \mathbb{N}$ we define the property $\mathcal{P}(p, \sigma, \tau)$ by:

$\mathcal{P}(p, \sigma, \tau) \equiv (f_p(\sigma) < f_p(\tau)) \wedge (\forall q > p, f_q(\sigma) = f_q(\tau))$.

Set $M := N/\sim$

Note that if σ', τ' are permutations of σ and τ, then $\mathcal{P}(p, \sigma, \tau)$ is equivalent to $\mathcal{P}(p, \sigma', \tau')$ for all $p \in \mathbb{N}$. This allows us to define a binary relation $<$ on M:

$[\sigma] < [\tau]$ if and only if there exists $p \in \mathbb{N}$ such that $\mathcal{P}(p, \sigma, \tau)$ is satisfied.

Remark 1

`If` $p \in \mathbb{N}$ `satisfies` $\mathcal{P}(p, \sigma, \tau)$`, then for all` $q \geq p$, $f_q(\sigma) \leq f_q(\tau)$

Proposition 1

$<$ defines a strict order on M.

Proof. We want to prove that $<$ is antisymmetric and transitive:

antisymmetry: Let $\sigma, \tau \in N$ such that $[\sigma] < [\tau]$; we want to show $[\tau] \not< [\sigma]$

Choose $p \in \mathbb{N}$ satisfying $\mathcal{P}(p, \sigma, \tau)$ and let $q \in \mathbb{N}$.

If $q \geq p$, then by remark 1 we have $f_q(\tau) \not< f_q(\sigma)$ so the first condition of $\mathcal{P}(q, \tau, \sigma)$ fails. Moreover, we have $f_p(\sigma) < f_p(\tau)$, so if $q < p$ the second condition of $\mathcal{P}(q, \tau, \sigma)$ fails.

Thus, $\mathcal{P}(q, \tau, \sigma)$ fails for every $q \in \mathbb{N}$, which proves $[\tau] \not< [\sigma]$.

transitivity: Let $\sigma, \tau, \rho \in N$ such that $[\rho] < [\sigma]$ and $[\sigma] < [\tau]$

Choose $p_1, p_2 \in \mathbb{N}$ such that $\mathcal{P}(p_1, \rho, \sigma)$ and $\mathcal{P}(p_2, \sigma, \tau)$ hold.

Set $p := max(p_1, p_2)$.

If $q > p$, then in particular $q > p_1$ so $f_q(\rho) = f_q(\sigma)$; similarly, we have $q > p_2$ so $f_q(\sigma) = f_q(\tau)$ hence $f_q(\rho) = f_q(\tau)$.

Since $p \geq p_1, p_2$, we have by remark 1: $f_p(\rho) \leq f_p(\sigma) \leq f_p(\tau)$. If $p = p_1$, the first inequality is strict, hence $f_p(\rho) < f_p(\tau)$; if $p = p_2$ then the second inequatlity is strict, which leads to the same conclusion.

This proves that $\mathcal{P}(p, \rho, \tau)$ is satisfied, hence $[\rho] < [\tau]$.

□

Proposition 2
The order $<$ is total on M

Proof. Let $\sigma = (n_1, \ldots, n_s), \tau = (m_1, \ldots, m_t) \in N$ be non-equivalent.

Set $A := \{q \in \{n_1, \ldots, n_s, m_1, \ldots, m_t\} \mid f_q(\sigma) \neq f_q(\tau)\}$.

Note that $A = \varnothing$ if and only if $\sigma \sim \tau$, so by hypothesis we have $A \neq \varnothing$. Thus, we can define $p := maxA$.

By definition of p, we have $f_q(\tau) = f_q(\sigma)$ for all $q > p$.

Moreover, since $p \in A$, we have $f_p(\sigma) \neq f_p(\tau)$.

If $f_p(\sigma) < f_p(\tau)$, then $\mathcal{P}(p, \sigma, \tau)$ is satisfied, so $[\sigma] < [\tau]$; if $f_p(\tau) < f_p(\sigma)$, then $\mathcal{P}(p, \tau, \sigma)$ is satisfied, so $[\tau] < [\sigma]$.

□

Note that we have an algorithm which determines how to order the pair (σ, τ) and gives us an apropriate p:

$p := max\{n_1, \ldots, n_s, m_1, \ldots, m_t\}$.
while $p \geq 0$:
  if $f_p(\sigma) > f_p(\tau)$ return $(\sigma > \tau, p)$
  if $f_p(\sigma) < f_p(\tau)$ return $(\sigma < \tau, p)$
  $p := p - 1$

Proposition 3
$(M, <)$ **is well-ordered:**

Proof. For any $\sigma = (n_1, \ldots, n_s) \in N$, set $m_\sigma := max(n_1, \ldots, n_s)$. Since m_σ is left unchanged by permutation of σ, so we can define $m_{[\sigma]} := m_\sigma$ unambiguously.

Note that for any $a, b \in M$, $m_a < m_b$ implies $a < b$. Indeed, if $m_a < m_b$, then for any $p > m_b$, we have $f_p(b) = 0 = f_p(a)$; moreover, $f_{m_b}(a) = 0 < f_{m_b}(b)$, which proves that $\mathcal{P}(m_b, a, b)$ holds.

Let A be a non-empty subset of M and set $m := min\{m_a \mid a \in A\}$
We are going to prove by induction on m that A has a smallest element.

m=0: If $m = 0$, then the set $A_0 := \{[\sigma] \in A \mid \sigma$ only contains zeros $\}$ is non-empty. Let a be the element of A_0 of minimal length; then I claim that a is the smallest element of A.

Indeed: let $b \in A$, $b \neq a$.

If $b \in A_0$, then a and b both only contain zeros, so for all $p > 0$ $f_p(a) = 0 = f_p(b)$; moreover, by choice of a, we have $f_0(a) = length(a) < length(b) = f_0(b)$. This proves that $\mathcal{P}(0, a, b)$ holds, hence $a < b$.

If $b \in A \backslash A_0$, then $m_b > 0 = m_a$ so $b > a$.

$m - 1 \to m$: Assume $m \geq 1$.

Set $B := \{a \in A \mid m_a = m\}$, $n := min\{f_m(a) \mid a \in B\}$ and $C := \{a \in B \mid f_m(a) = n\}$.

I claim that for any $c \in C$ and any $a \in A \backslash C$, $c < a$.

Indeed:

- if $a \in B \backslash C$, then by definition of C we have $f_m(c) < f_m(a)$. Since $a, c \in B$, it follows from the definition of B that m is the maximal element of both a and c, so that $f_p(a) = 0 = f_p(c)$ for all $p > m$. Thus, $\mathcal{P}(m, c, a)$ holds.
- If $a \notin B$, then by definition of B we have $m_a > m = m_c$, hence $a > c$.

Thus, it suffices to prove that C has a smallest element.

For any $c \in C$, we denote by c' the element of M obtained from c by removing every occurrence of m. Set $C' := \{c' \mid c \in C\}$. Since m is the maximal element of every $c \in C$, we have $m_{c'} \leq m - 1$ for every $c' \in C'$, hence $min\{m_{c'} \mid c' \in C'\} \leq m - 1$. By induction hypothesis, C' then has a smallest element c'. c is then the smallest element of C.

□

Note that there is a recursive algorithm which takes a subset of M as an argument and returns its smallest element:

smallest_element(A):
    $m := min\{m_a \mid a \in A\}$

$B := \{a \in A \mid m_a = m\}$
$n = min\{f_m(b) \mid b \in B\}$
$C := \{b \in B \mid f_m(b) = n\}$
if C is a singleton then return its only element
$C' := \{c' \mid c \in C\}$
c':=smallest_element(C')
return the concatenation of c' with $\underbrace{(m, \ldots, m)}_{n \text{ times}}$

Proposition 4
The ordinal type of $(M, <)$ is ω^ω

Proof. For any $n \in \mathbb{N}$, set $A_n := \{a \in M \mid m_a = n\}$.

We are going to build an isomorpism from ω^ω to M by induction. More precisely, we are going to build a sequence $(\phi_n)_{n\in\mathbb{N}}$ of maps such that:

- for any $n \in \mathbb{N}$, ϕ_n is an isomorphism from ω^{n+1} to A_n.
- for any $n \in \mathbb{N}$, ϕ_{n+1} extends ϕ_n.

Taking $\phi := \bigcup_{n\in\mathbb{N}} \phi_n$, we obtain an isomorphism ϕ from $\bigcup_{n\in\mathbb{N}} \omega^{n+1} = \omega^\omega$ to $\bigcup_{n\in\mathbb{N}} A_n = M$.

$\underline{n = 0}$ Note that we have $(0) < (0, 0) < (0, 0, 0) < (0, 0, 0, 0) < \ldots$, so an isomorphism from ω to A_0 is given by $n \mapsto \underbrace{(0, 0, \ldots, 0)}_{n+1 \text{ times}}$

$\underline{n \to n + 1}$ Assume we have an isomorphism $\phi_n : \omega^{n+1} \to A_n$. Remember that ω^{n+2} is the order type of $(\omega \times \omega^{n+1}, <_{lex})$.

Define: $\phi_{n+1}(\alpha, \beta) := \phi_n(\beta) \wedge \underbrace{(n + 1, \ldots, n + 1)}_{\alpha \text{ times}}$

(here '$\wedge$' means concatenation). This is an isomorphism from $(\omega \times \omega^{n+1}, <_{lex})$ to A_{n+1}.

□