REAL ALGEBRAIC GEOMETRY LECTURE NOTES (12 Continued: 26/11/2009 - BEARBEITET 3/12/18)

SALMA KUHLMANN

THE TARSKI-SEIDENBERG PRINCIPLE

Recall. Let R be a real closed field, $a \in R$. Define

$$sign(a) := \begin{cases} 1 & \text{if } a > 0, \\ 0 & \text{if } a = 0, \\ -1 & \text{if } a < 0. \end{cases}$$

The Tarski-Seidenberg Principle is the following result.

Theorem 1. 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 $(\underline{T} = (T_1, \ldots, T_n), X)$ with coefficients in $\mathbb{Z}$. Let ϵ be a function from $\{1, \ldots, s\}$ to $\{-1, 0, 1\}$. Then there exists a finite boolean combination $B(\underline{T}) := S_1(\underline{T}) \vee \ldots \vee S_p(\underline{T})$ of polynomial equations and inequalities in the variables $T_1, \ldots, T_n$ with coefficients in $\mathbb{Z}$ such that for every real closed field R and for every $\underline{t} \in R^n$, the system

$$\begin{cases} sign(f_1(\underline{t}, X)) = \epsilon(1) \\ \qquad\vdots \\ sign(f_s(\underline{t}, X)) = \epsilon(s) \end{cases}$$

has a solution $x \in R$ if and only if $B(\underline{t})$ holds true in R.

Notation I. Let $f_1(X), \ldots, f_s(X)$ be a sequence of polynomials in $R[X]$. Let $x_1 < \ldots < x_N$ be the roots in R of all f_i that are not identically zero.

Set $x_0 := -\infty$, $x_{N+1} := +\infty$

Remark 1. Let $m := max(deg f_i, i = 1, \ldots, s)$. Then $N \leq sm$.

Set $I_k :=]x_k, x_{k+1}[$, $k = 0, \ldots, N$

Remark 2. $sign(f_i(x))$ is constant on I_k, for each $i \in 1, \ldots, s$, for each $k \in 0, \ldots, N$.

Set $sign(f_i(I_k)) := sign(f_i(x)),\ x \in I_k$

Notation II. Let $SIGN_R(f_1, \dots, f_s)$ be the matrix with s rows and $2N + 1$ columns whose i^{th} row (for $i = \{1, \dots, s\}$) is

$$sign\big(f_i(I_0)\big), sign\big(f_i(x_1)\big), sign\big(f_i(I_1)\big), \dots, sign\big(f_i(x_N)\big), sign\big(f_i(I_N)\big).$$

i.e. $SIGN_R(f_1, \dots, f_s)$ is an $s\times(2N+1)$ matrix with coefficients in $\{-1, 0, 1\}$ and

$$SIGN_R(f_1, ..., f_s) := \begin{pmatrix} signf_1(I_0) & signf_1(x_1) & \dots & signf_1(x_N) & signf_1(I_N) \\ signf_2(I_0) & signf_2(x_1) & \dots & signf_2(x_N) & signf_2(I_N) \\ \vdots & \vdots & & \vdots & \vdots \\ signf_s(I_0) & signf_s(x_1) & \dots & signf_s(x_N) & signf_s(I_N) \end{pmatrix}$$

Remark 3. Let $f_1, \dots, f_s \in R[X]$ and $\epsilon : \{1, \dots, s\} \to \{-1, 0, +1\}$. The system

$$\begin{cases} sign(f_1(X)) = \epsilon(1) \\ \qquad\vdots \\ sign(f_s(X)) = \epsilon(s) \end{cases}$$

has a solution $x \in R$ if and only if one column of $SIGN_R(f_1, \dots, f_s)$ is precisely the matrix $\begin{bmatrix} \epsilon(1) \\ \vdots \\ \epsilon(s) \end{bmatrix}$.

Notation III. Let $M_{P\times Q}$:= the set of $P\times Q$ matrices with coefficients in $\{-1, 0, +1\}$.

Set $W_{s,m}$:= the disjoint union of $M_{s\times(2l+1)}$, for $l = 0, \dots, sm$.

Notation IV. Let $\epsilon : \{1, \dots, s\} \to \{-1, 0, 1\}$. Set

$$W(\epsilon) = \{M \in W_{s,m} : one\ column\ of\ M\ is\ \begin{bmatrix} \epsilon(1) \\ \vdots \\ \epsilon(s) \end{bmatrix}\} \subseteq W_{s,m}$$

Lemma 2. (Reformulation of remark 3 using notation IV) Let $\epsilon : \{1, \dots, s\} \to \{-1, 0, +1\}$, R real closed field and $f_1(X), \dots, f_s(X) \in R[X]$ of degree $\leq m$. Then the system

$$\begin{cases} sign(f_1(X)) = \epsilon(1) \\ \vdots \\ sign(f_s(X)) = \epsilon(s) \end{cases}$$

has a solution $x \in R$ if and only if $SIGN_R(f_1, \dots, f_s) \in W(\epsilon)$.

By Lemma 2 (setting $W' = W(\epsilon)$), we see that the proof of Theorem 1 reduces to showing the following proposition:

Main Proposition 3. Let $f_i(\underline{T}, X) := h_{i,m_i}(\underline{T})X^{m_i} + \dots + h_{i,0}(\underline{T})$ for $i = 1, \dots, s$ be a sequence of polynomials in $n+1$ variables with coefficients in $\mathbb{Z}$, and let $m := max\{m_i | i = 1, \dots, s\}$. Let W' be a subset of $W_{s,m}$. Then there exists a boolean combination $B(\underline{T}) = S_1(\underline{T}) \vee \dots \vee S_p(\underline{T})$ of polynomial equations and inequalities in the variables $\underline{T}$ with coefficients in $\mathbb{Z}$, such that, for every real closed field R and every $\underline{t} \in R^n$, we have

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

The proof of the main Proposition will follow by induction from the next main lemma, where we will show that $SIGN_R(f_1, \dots, f_s)$ is completely determined by the "$SIGN_R$"of a (possibly) longer but simpler sequence of polynomials, i.e. $SIGN_R(f_1, \dots, f_{s-1}, f_s', g_1, \dots, g_s)$, where f_s' = the derivative of f_s, and $g_1, \dots, g_s$ are the remainders of the euclidean division of f_s by $f_1, \dots, f_{s-1}, f_s'$, respectively.

First we will state and prove the lemma and then prove the proposition.