Inhaltsverzeichnis zur Vorlesung: Positive Polynome

Prof. Dr. Salma Kuhlmann, Dr. Annalisa Conversano

These notes were typed by Charu Goel

SS 2010 - Korrekturen WS 2018/2019

POSITIVE POLYNOMIALS LECTURE NOTES (01: 13/04/10)

SALMA KUHLMANN

Contents

1. THE POLYNOMIAL RING $\mathbb{R}[\underline{X}]$

Notation 1.1. $\mathbb{R}[\underline{X}] := \mathbb{R}[X_1, \ldots, X_n]$ is the polynomial ring in n variables and real coefficients, where $\mathbb{R}$ is the set of real numbers.

Note that $\mathbb{R}[\underline{X}]$ is a vector space of countable dimension (a basis is $\{\underline{X}^{\underline{\alpha}} \mid \underline{\alpha} \in \mathbb{Z}_+^n\}$, where $\underline{X}^{\underline{\alpha}} := X_1^{\alpha_1} \ldots X_n^{\alpha_n}$ is a monomial).

Definition 1.2. A polynomial is said to be **homogenous** if it is a linear combination of monomials with same degree (or zero polynomial).

Convention: deg (0) := $-\infty$, where ‵‵0″ is the polynomial with 0 coefficients.

Definition 1.3. Let $f \in \mathbb{R}[\underline{x}]$, the **homogenous decomposition** of f is $f = h_0 + \ldots + h_d$, where h_i are homogenous (or 0) and $\deg(h_i) = i$ if $h_i \not\equiv 0$.

Note that if $h_d \not\equiv 0$, then $d = \deg(h_d) = \deg(f)$.

Remark 1.4. Let $f, g \in \mathbb{R}[\underline{x}]$; $f \not\equiv 0$, $g \not\equiv 0$, then:

(i) $\deg(fg) = \deg(f) + \deg(g)$

(ii) $\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$

(iii) $\deg(f + g) = \max\{\deg(f), \deg(g)\}$, if $\deg(f) \neq \deg(g)$.

2. BOREL MEASURE

Definition 2.1. Let X be a locally compact Hausdorff topological space (ie. $\forall\, x \in X\ \exists\, \mathcal{U} \ni x$ such that $\overline{\mathcal{U}}$ is compact). A **Borel measure** "μ" on X is a positive measure such that every $B \in \beta^{\delta}(X)$ is measurable, where $\beta^{\delta}(X) :=$ the smallest class of subsets of X which contain all compact sets and is closed under finite unions, complements and countable intersections.

Further we will assume that μ is **regular**, ie.
$\forall\, B \in \beta^{\delta}(X),\ \forall\, \epsilon > 0\ \ \exists\, C, \mathcal{U} \in \beta^{\delta}(X)$ with $C \subseteq B \subseteq \mathcal{U}$, where C is compact, $\mathcal{U}$ is open and $\mu(C) + \epsilon \geq \mu(B) \geq \mu(\mathcal{U}) - \epsilon$.

Definition 2.2. Let K be a closed compact subset of $\mathbb{R}^n$. K is said to be **basic closed semi-algebraic** if there exists a finite $S \subseteq \mathbb{R}[\underline{X}]$, say $S = \{g_1, \ldots, g_s\}$ (for $s \in \mathbb{N}$) such that $K = K_S = \{x \in \mathbb{R}^n \mid g_i(x) \geq 0\ \forall\, i = 1, \ldots, s\}$.

Notation 2.3. $\sum \mathbb{R}[\underline{X}]^2 := \{\sigma = \sum_{i=1}^{m} f_i^2 \mid f_i \in \mathbb{R}[\underline{X}], m \in \mathbb{N}\}$.

Theorem 2.4. (Schmüdgen's Positivstellensatz) Let $K \subseteq \mathbb{R}^n$ be a compact semi-algebraic set, $K = K_S$ (as above). Let $L : \mathbb{R}[\underline{X}] \longrightarrow \mathbb{R}$ be a linear functional. Then L can be represented by a positive Borel measure μ defined on K $\left(\text{ie. } L(f) = \int_K f d\mu \text{ for } f \in \mathbb{R}[\underline{X}]\right)$ if and only if $L(\sigma g_1^{e_1} \ldots g_s^{e_s}) \geq 0\ \forall\, \sigma \in \sum \mathbb{R}[\underline{X}]^2$ and $e_1, \ldots, e_s \in \{0, 1\}$.

See Corollary 2.6 in lecture 13.

3. PREORDERING

Definition 3.1. Let A be a commutative ring with 1,
$\Sigma A^2 := \{\Sigma a_i^2 \mid i \geq 0, a_i \in A\}$.

(1) A **quadratic module** M in A is a subset $M \subseteq A$ such that
$M + M \subseteq M$, $a^2 M \subseteq M\ \forall\, a \in A, 1 \in M$.

(2) A **preordering** T in A is a quadratic module with $TT \subseteq T$.
T is said to be **proper** if $-1 \notin T$.

Remark 3.2. If $\frac{1}{2} \in A$ then $T = A$ is the only preordering in A that is not proper.

Proof. For $a \in A$ one can write: $a = (\frac{a+1}{2})^2 + (-1)(\frac{a-1}{2})^2 \in T$ □

Examples 3.3.

(1) $\underbrace{\Sigma A^2}_{\text{(the smallest preordering)}} \subseteq T$ for a preordering T in A.

(2) Let $S = \{g_1, \dots, g_s\} \subseteq A$, then

$$T_S := \Big\{ \sum_{e_1,\dots,e_s \in \{0,1\}} \sigma_e \, g_1^{e_1} \dots g_s^{e_s} \mid \sigma_e \in \Sigma A^2, e = (e_1, \dots, e_s) \Big\}$$

is the preordering generated by $g_1, \dots, g_s$.

Definiton 3.4. A preordering $T \subseteq A$ is said to be **finitely generated** if $\exists$ a finite $S \subseteq A$ with $T = T_S$.

For example: ΣA^2 is finitely generated with $S = \phi$.

Example 3.5. Let $S \subseteq A = \mathbb{R}[\underline{X}]$ be a finite subset. We associate to S the basic closed semi-algebraic subset $K_S \subseteq \mathbb{R}^n$ and the finitely generated preordering $T_S \subseteq \mathbb{R}[\underline{X}]$. We recall that $K_S := \{\underline{x} \in \mathbb{R}^n \mid g_i(\underline{x}) \geq 0 \; \forall \; i = 1, \dots, s\}$, $S = \{g_1, \dots, g_s\}$.

For example: If $S = \phi$: $K_S = \mathbb{R}^n$, $T_S = \sum \mathbb{R}[\underline{X}]^2$.

Definiton 3.6. An element $f \in T_S$ is said to be **positive semidefinite** on K_S if $f(\underline{x}) \geq 0$ for all $\underline{x} \in K_S$.

For $K \subseteq \mathbb{R}^n$, set $\mathrm{Psd}(K) := \Big\{ f \in \mathbb{R}[\underline{X}] \mid f(\underline{x}) \geq 0 \; \forall \; \underline{x} \in K \Big\}$

Note that $T_S \subseteq \mathrm{Psd}(K_S)$.

Question. If $f \in \mathrm{Psd}(K_S)$, then does $f \in T_S$?

Answer. No.

But there is a connection of f with T_S (which will become clear through the Positivstellensatz in the next lecture).

POSITIVE POLYNOMIALS LECTURE NOTES (02: 15/04/10)

SALMA KUHLMANN

Contents

1. INTRODUCTION

Definiton 1.1. For $K \subseteq \mathbb{R}^n$,

Psd$(K) := \{f \in \mathbb{R}[\underline{X}] \mid f(\underline{x}) \geq 0 \ \forall \ \underline{x} \in K\}$.

Let $S = \{g_1, \ldots, g_s\} \subseteq \mathbb{R}[\underline{X}]$, then

$\mathbf{K_S} := \{\underline{x} \in \mathbb{R}^n \mid g_i(\underline{x}) \geq 0 \ \forall \ i = 1, \ldots, s\}$, the basic closed semi-algebraic set defined by S and

$\mathbf{T_S} := \Big\{ \sum_{e_1,\ldots,e_s \in \{0,1\}} \sigma_e \ g_1^{e_1} \ldots g_s^{e_s} \mid \sigma_e \in \Sigma\mathbb{R}[\underline{X}]^2, e = (e_1, \ldots, e_s)\Big\}$, the preordering generated by S.

We also introduce

$\mathbf{M_S} := \{\sigma_0 + \sigma_1 g_1 + \sigma_2 g_2 \ldots + \sigma_s g_s \mid \sigma_i \in \Sigma\mathbb{R}[\underline{X}]^2\}$, the quadratic module generated by S.

Remark 1.2. (i) M_S is a quadratic module in $\mathbb{R}[\underline{X}]$.

(ii) $M_S \subseteq T_S \subseteq \text{Psd}(K_S)$.
(We shall study these inclusions in more detail later. In general these inclusions may be proper.)

(iii) $\mathrm{Psd}(K_S)$ is a preordering.

Definiton 1.3. T_S (resp. M_S) is called **saturated** if $\mathrm{Psd}(K_S) = T_S$ (resp. M_S).

2. EXAMPLES

For the examples that we are about to see, we need the following 2 lemmas:

Lemma 2.1. Let $f \in \mathbb{R}[\underline{X}]$; $f \not\equiv 0$, then $\exists\ \underline{x} \in \mathbb{R}^n$ s.t. $f(\underline{x}) \neq 0$. [Here n is such that $\underline{X} = (X_1, \dots, X_n)$.]

Proof. By induction on n.
If $n = 1$, result follows since a nonzero polynomial $\in \mathbb{R}[\underline{X}]$ has only finitely many zeroes.
Let $n \geq 2$ and $0 \not\equiv f \in \mathbb{R}[X_1, \dots, X_n] = \mathbb{R}[X_1, \dots, X_{n-1}][X_n]$.
$f \not\equiv 0 \Rightarrow f = g_0 + g_1 X_n + \dots + g_k X_n^k;\ g_0, g_1, \dots, g_k \in \mathbb{R}[X_1, \dots, X_{n-1}];\ g_k \not\equiv 0$.
Since $g_k \not\equiv 0$, so by induction on n :
$\exists\ (x_1, x_2, \dots, x_{n-1})$ s.t. $g_k(x_1, x_2, \dots, x_{n-1}) \neq 0$.
$\Rightarrow$ The polynomial in one variable X_n i.e. $f(x_1, x_2, \dots, x_{n-1}, X_n) \not\equiv 0$.
Therefore by induction for $n = 1$, $\exists\ x_n \in \mathbb{R}$ s.t.
$f(x_1, x_2, \dots, x_{n-1}, x_n) \neq 0$ □

Remark 2.2. If $f \in \mathbb{R}[\underline{X}]$, $f \not\equiv 0$, then $\mathbb{R}^n \backslash Z(f) = \{x \in \mathbb{R}^n \mid f(x) \neq 0\}$ is dense in $\mathbb{R}^n$, where $Z(f) := \{x \in \mathbb{R}^n \mid f(x) = 0\}$ is the zero set of f.
Equivalently, $Z(f)$ has empty interior. In other words, a polynomial which vanishes on a nonempty open set is identically the zero polynomial.

Lemma 2.3. Let $\sigma := f_1^2 + \dots + f_k^2$; $f_1, \dots, f_k \in \mathbb{R}[\underline{X}]$ and $f_1 \not\equiv 0$, then

(i) $\sigma \not\equiv 0$

(ii) $\deg(\sigma) = 2 \max\left\{\deg f_i\ ; i = 1, \dots, k\right\}$
[In particular $\deg(\sigma)$ is even.]

Proof. (i) Since $f_1 \not\equiv 0$, so by lemma 2.1 $\exists\ \underline{x} \in \mathbb{R}^n$ s.t. $f_1(\underline{x}) \neq 0$.
$\Rightarrow \sigma(\underline{x}) = f_1(\underline{x})^2 + \dots + f_k(\underline{x})^2 > 0$
$\Rightarrow \sigma \not\equiv 0$.

(ii) $f_i = h_{i_0} + \dots + h_{i_d}$, where $d = \max\left\{\deg f_i \mid i = 1, \dots, k\right\}$; h_{i_j} homogeneous of degree j or $h_{i_j} \equiv 0$ for $i = 1, \dots, k$.

Clearly $\deg(\sigma) \leq 2d$.
To show $\deg(\sigma) = 2d$, consider the homogeneous polynomial
$h_{1_d}^2 + \ldots + h_{k_d}^2 := h_{2d}$
Note that if $h_{2d} \not\equiv 0$, then $\deg(h_{2d}) = 2d$ and h_{2d} is the homogeneous component of σ of highest degree (i.e. leading term), so $\deg(\sigma) = 2d$.
Now we know that $h_{i_d} \not\equiv 0$ for some $i \in \{1, \ldots, k\}$, so by (i) we get $h_{2d} \not\equiv 0$.
□

Now coming back to the inclusion: $T_S \subseteq \operatorname{Psd}(K_S)$

Example 2.4.(1) (i) $S = \phi$, $n = 1 \Rightarrow K_S = \mathbb{R}$ and $T_S = \sum \mathbb{R}[X]^2$
$\Rightarrow T_S = \operatorname{Psd}(\mathbb{R})$.

(ii) $S = \left\{(1 - X^2)^3\right\}$, $n = 1 \Rightarrow K_S = [-1, 1]$ (compact),
$T_S = \left\{\sigma_0 + \sigma_1(1 - X^2)^3 \mid \sigma_0, \sigma_1 \in \sum \mathbb{R}[X]^2\right\} = M_S$.
Claim. $T_S \subsetneq \operatorname{Psd}(K_S)$
For example: $(1 - X^2) \in \operatorname{Psd}[-1, 1]$ (clearly),
but $(1 - X^2) \notin T_S$, since if we assume for a contradiction that

$$(1 - X^2) = \sigma_0 + \sigma_1(1 - X^2)^3, \tag{1}$$

where $\sigma_0 = \sum f_i^2$. Then evaluating (1) at $x = \pm 1$ we get
$\sigma_0(\pm 1) = \sum f_i^2(\pm 1) = 0$
$\Rightarrow f_i(\pm 1) = 0$
$\Rightarrow f_i = (1 - X^2)g_i$, for some $g_i \in \mathbb{R}[X]$
$\Rightarrow \sigma_0 = (1 - X^2)^2 \sum g_i^2$
Substituting σ_0 back in (1) we get

$$1 = (1 - X^2) \sum g_i^2 + (1 - X^2)^2 \sigma_1 \tag{2}$$

Evaluating (2) at $x = \pm 1$ yields $1 = 0$, a contradiction.

(iii) $S = \left\{X^3\right\}$, $n = 1 \Rightarrow K_S = [0, \infty)$ (noncompact),
$T_S = \left\{\sigma_0 + \sigma_1 X^3 \mid \sigma_0, \sigma_1 \in \sum \mathbb{R}[X]^2\right\} = M_S$.
Claim. $T_S \subsetneq \operatorname{Psd}(K_S)$
For example: $X \in \operatorname{Psd}(K_S)$, but $X \notin T_S$ (we will use degree argument to show this).
We compute the possible degrees of elements $t \in T_S$; $t \not\equiv 0$
Let

$$t = \sigma_0 + \sigma_1 X^3; \sigma_0, \sigma_1 \in \sum \mathbb{R}[X]^2,$$

POSITIVE POLYNOMIALS LECTURE NOTES (03: 20/04/10)

SALMA KUHLMANN

Contents

1. GEOMETRIC VERSION OF POSITIVSTELLENSATZ

Theorem 1.1. (Recall) (Positivstellensatz: Geometric Version) Let $A = \mathbb{R}[\underline{X}]$. Let $S = \{g_1, \ldots, g_s\} \subseteq \mathbb{R}[\underline{X}]$, $f \in \mathbb{R}[\underline{X}]$. Then

(1) $f > 0$ on $K_S \Leftrightarrow \exists\, p, q \in T_S$ s.t. $pf = 1 + q$
(Striktpositivstellensatz)

(2) $f \geq 0$ on $K_S \Leftrightarrow \exists\, m \in \mathbb{Z}_+, \exists\, p, q \in T_S$ s.t. $pf = f^{2m} + q$
(Nonnegativstellensatz)

(3) $f = 0$ on $K_S \Leftrightarrow \exists\, m \in \mathbb{Z}_+$ s.t. $-f^{2m} \in T_S$
(Real Nullstellensatz (first form))

(4) $K_S = \phi \Leftrightarrow -1 \in T_S$.

Proof. It consists of two parts:
-Step I: prove that (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (4) $\Rightarrow$ (1)
-Step II: prove (4) [using Tarski Transfer]

We will start with step II:
Clearly $K_S \neq \phi \Rightarrow -1 \notin T_S$ (since $-1 \in T_S \Rightarrow K_S = \phi$), so it only remains to prove the following proposition:

Proposition 1.2. (3.2 of last lecture) If $-1 \notin T_S$ (i.e. if T_S is a proper preordering), then $K_S \neq \phi$.

For proving this we need the following results:

Lemma 1.3.1. (3.4.1 of last lecture) Let A be a commutative ring with 1. Let P be a maximal proper preordering in A. Then P is an ordering.

Proof. We have to show:

(i) $P \cup -P = A$, and

(ii) $\mathfrak{p} := P \cap -P$ is a prime ideal of A.

(i) Assume $a \in A$, but $a \notin P \cup -P$.

By maximality of P, we have: $-1 \in (P + aP)$ and $-1 \in (P - aP)$

Thus

$-1 = s_1 + at_1$ and

$-1 = s_2 - at_2$; $s_1, s_2, t_1, t_2 \in P$

So (rewritting)

$-at_1 = 1 + s_1$ and

$at_2 = 1 + s_2$

Multiplying we get:

$-a^2 t_1 t_2 = 1 + s_1 + s_2 + s_1 s_2$

$\Rightarrow -1 = s_1 + s_2 + s_1 s_2 + a^2 t_1 t_2 \in P$, a contradiction.

(ii) Now consider $\mathfrak{p} := P \cap -P$, clearly it is an ideal.

We claim that $\mathfrak{p}$ is prime.

Let $ab \in \mathfrak{p}$ and $a, b \notin \mathfrak{p}$.

Assume w.l.o.g. that $a, b \notin P$.

Then as above in (i), we get:

$-1 \in (P + aP)$ and $-1 \in (P + bP)$

So, $-1 = s_1 + at_1$ and

$-1 = s_2 + bt_2$; $s_1, s_2, t_1, t_2 \in P$

Rearranging and multiplying we get:

$(at_1)(bt_2) = (1 + s_1)(1 + s_2) = 1 + s_1 + s_2 + s_1 s_2$

$\Rightarrow -1 = \underbrace{s_1 + s_2 + s_1 s_2}_{\in P} \underbrace{-abt_1 t_2}_{\in \mathfrak{p} \subset P}$

$\Rightarrow -1 \in P$, a contradiction. □

Lemma 1.3.2. (3.4.2 of last lecture) Let A be a commutative ring with 1 and $P \subseteq A$ an ordering. Then P induces uniquely an ordering $\leq_P$ on $F := ff(A/\mathfrak{p})$ defined by:

$$\forall\, a, b \in A, b \notin \mathfrak{p} : \frac{\overline{a}}{\overline{b}} \geq_P 0 \text{ (in } F) \Leftrightarrow ab \in P, \text{ where } \overline{a} = a + \mathfrak{p}.$$ □

Recall 1.3.3. (Tarski Transfer Principle) Suppose $(\mathbb{R}, \leq) \subseteq (F, \leq)$ is an ordered field extension of $\mathbb{R}$. If $\underline{x} \in F^n$ satisfies a finite system of polynomial equations and inequalities with coefficients in $\mathbb{R}$, then $\exists\, \underline{r} \in \mathbb{R}^n$ satisfying the same system. □

Using lemma 1.3.1, lemma 1.3.2 and TTP (recall 1.3.3), we prove the proposition 1.2 as follows:

Proof of Propostion 1.2. **To show:** $-1 \notin T_S \Rightarrow K_S \neq \phi$.
Set $S = \{g_1, \ldots, g_s\} \subseteq \mathbb{R}[\underline{X}]$
$-1 \notin T_S \Rightarrow T_S$ is a proper preordering.
By Zorn, extend T_S to a maximal proper preordering P.
By lemma 1.3.1, P is an ordering on $\mathbb{R}[\underline{X}]$; $\mathfrak{p} := P \cap -P$ is prime.
By lemma 1.3.2, let $(F, \leq_P) = \left(ff\,(\mathbb{R}[\underline{X}]/\mathfrak{p})\,,\ \leq_P\right)$ is an ordered field extension of $(\mathbb{R}, \leq)$.

Now consider the system $\mathcal{S} := \begin{cases} g_1 \geq 0 \\ \vdots \\ g_s \geq 0. \end{cases}$

Claim: The system $\mathcal{S}$ has a solution in F^n, namely $\underline{X} := (\overline{X_1}, \ldots, \overline{X_n})$,
i.e. to show: $g_i(\overline{X_1}, \ldots, \overline{X_n}) \geq_P 0$; $i = 1, \ldots, s$.

Indeed $g_i(\overline{X_1}, \ldots, \overline{X_n}) = \overline{g_i(X_1, \ldots, X_n)}$, and since $g_i \in T_S \subset P$, it follows by definition of $\leq_P$ that $\overline{g_i} \geq_P 0$.

Now apply TTP (recall 1.3.3) to conclude that:
$\exists\, \underline{r} \in \mathbb{R}^n$ satisfying the system $\mathcal{S}$, i.e. $g_i(\underline{x}) \geq 0$; $i = 1, \ldots, s$.
$\Rightarrow \underline{r} \in K_S \Rightarrow K_S \neq \phi$.
This completes step II. □

Now we will do step I:
i.e. we show (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (4) $\Rightarrow$ (1)

(1) $\Rightarrow$ (2)

Let $f \geq 0$ on K_S, $f \not\equiv 0$.
Consider $S' \subseteq \mathbb{R}[\underline{X}, Y]$, $S' := S \cup \left\{Yf - 1, -Yf + 1\right\}$
So, $K_{S'} = \left\{(\underline{x}, y) \mid g_i(\underline{x}) \geq 0\ ;\ yf(\underline{x}) = 1\right\}$.

Thus $f(\underline{X}, Y) = f(\underline{X}) > 0$ on $K_{S'}$, so applying (1) $\exists\, p',\ q' \in T_{S'}$ s.t.

$$p'(\underline{X}, Y) f(\underline{X}) = 1 + q'(\underline{X}, Y)$$

Substitute $Y := \frac{1}{f(\underline{X})}$ in above equation and clear denominators by multiplying both sides by $f(\underline{X})^{2m}$ for $m \in \mathbb{Z}_+$ sufficiently large to get:

$$p(\underline{X}) f(\underline{X}) = f(\underline{X})^{2m} + q(\underline{X}),$$

with $p(\underline{X}) := f(\underline{X})^{2m} p'\left(\underline{X}, \frac{1}{f(\underline{X})}\right) \in \mathbb{R}[\underline{X}]$ and

$q(\underline{X}) := f(\underline{X})^{2m} q'\left(\underline{X}, \frac{1}{f(\underline{X})}\right) \in \mathbb{R}[\underline{X}]$.

To finish the proof we **claim** that: $p(\underline{X}),\ q(\underline{X}) \in T_S$ for sufficiently large m.

Observe that $p'(\underline{X}, Y) \in T_{S'}$, so p' is a sum of terms of the form:

$$\underbrace{\sigma(\underline{X}, Y)}_{\in\, \Sigma\mathbb{R}[\underline{X},Y]^2}\ g_1^{e_1} \dots g_s^{e_s}\ (Yf(\underline{X}) - 1)^{e_{s+1}} (-Yf(\underline{X}) + 1)^{e_{s+2}}\ ;\ e_1, \dots, e_s, e_{s+1}, e_{s+2} \in \{0, 1\}$$

say $\sigma(\underline{X}, Y) = \sum_j h_j(\underline{X}, Y)^2$.

Now when we substitute Y by $\frac{1}{f(\underline{X})}$ in $p'(\underline{X}, Y)$, all terms with e_{s+1} or e_{s+2} equal to 1 vanish.

So, the remaining terms are of the form

$$\sigma\left(\underline{X}, \frac{1}{f(\underline{X})}\right) g_1^{e_1} \dots g_s^{e_s} = \left(\sum_j \left[h_j\left(\underline{X}, \frac{1}{f(\underline{X})}\right)\right]^2 \right) g_1^{e_1} \dots g_s^{e_s}$$

So, we want to choose m large enough so that $f(\underline{X})^{2m}\ \sigma\left(\underline{X}, \frac{1}{f(\underline{X})}\right) \in\ \Sigma\mathbb{R}[\underline{X}]^2$.

Write $h_j(\underline{X}, Y) = \sum_i h_{ij}(\underline{X}) Y^i$

Let $m \geq \deg\,(h_j(\underline{X}, Y))$ in Y, for all j.

Substituting $Y = \frac{1}{f(\underline{X})}$ in $h_j(\underline{X}, Y)$ and multiplying by $f(\underline{X})^m$, we get:

$$f(\underline{X})^m\ h_j\left(\underline{X}, \frac{1}{f(\underline{X})}\right) = \sum_i h_{ij}(\underline{X})\ f(\underline{X})^{m-i},\ \text{ with } (m - i) \geq 0\ \forall\, i$$

so that $f(\underline{X})^m\ h_j\left(\underline{X}, \frac{1}{f(\underline{X})}\right) \in \mathbb{R}[\underline{X}]$, for all j.

So $f(\underline{X})^{2m}\,\sigma\Big(\underline{X}, \frac{1}{f(\underline{X})}\Big) = f(\underline{X})^{2m}\left(\sum_j \left[h_j\Big(\underline{X}, \frac{1}{f(\underline{X})}\Big)\right]^2\right)$

$$= \sum_j \left[f(\underline{X})^m\, h_j\Big(\underline{X}, \frac{1}{f(\underline{X})}\Big)\right]^2 \in \Sigma\mathbb{R}[\underline{X}]^2$$

Thus p and (similarly) $q \in T_S$, which proves our claim and hence (1) ⇒ (2). □

(2) ⇒ (3)

Assume $f = 0$ on K_S. Apply (2) to f and $-f$ to get:

$p_1 f = f^{2m_1} + q_1$ and

$-p_2 f = f^{2m_2} + q_2$; where $p_1, p_2, q_1, q_2 \in T_S$, $m_i \in \mathbb{Z}_+$

Multiplying yields:

$$-p_1p_2f^2 = f^{2(m_1+m_2)} + f^{2m_1}q_2 + f^{2m_2}q_1 + q_1q_2$$

$$\Rightarrow -f^{2(m_1+m_2)} = \underbrace{p_1p_2f^2 + f^{2m_1}q_2 + f^{2m_2}q_1 + q_1q_2}_{\in\, T_S}$$

i.e. $-f^{2m} \in T_S$, $m \in \mathbb{Z}_+$ □

(3) ⇒ (4)

Assume $K_S = \phi$

⇒ the constant polynomial $f(\underline{X}) \equiv 1$ vanishes on K_S.

Applying (3), gives $-1 \in T_S$. □

(4) ⇒ (1)

Let $S' = S \cup \{-f\}$

Since $f > 0$ on K_S we have $K_{S'} = \phi$, so $-1 \in T_{S'}$ by (4).

Moreover from $S' = S \cup \{-f\}$, we have $T'_S = T_S - fT_S$

⇒ $-1 = q - pf$; for some $p, q \in T_S$

i.e. $pf = 1 + q$ □

This completes step I and hence the proof of Positivstellensatz. □□

We will now study other forms of the Real Nullstellensatz that will relate it to Hilbert's Nullstellensatz.

2. EXKURS IN COMMUTATIVE ALGEBRA

Recall 2.1. Let K be a field, $S \subseteq K[\underline{X}]$. Define

$\mathcal{Z}(S) := \{\underline{x} \in K^n \mid g(\underline{x}) = 0 \;\; \forall\, g \in S\}$, the **zero set** of S.

Proposition 2.2. Let $V \subseteq K^n$. Then the following are equivalent:

(1) $V = \mathcal{Z}(S)$; for some finite $S \subseteq K[\underline{X}]$
(2) $V = \mathcal{Z}(S)$; for some set $S \subseteq K[\underline{X}]$
(3) $V = \mathcal{Z}(I)$; for some ideal $I \subseteq K[\underline{X}]$

Proof. (1) $\Rightarrow$ (2) Clear.

(2) $\Rightarrow$ (3) Take $I := < S >$, the ideal generated by S.

(3) $\Rightarrow$ (1) Using Hilbert Basis Theorem (i.e. for a field K, every ideal in $K[\underline{X}]$ is finitely generated):

$I = < S >$, S finite
$\Rightarrow \mathcal{Z}(I) = \mathcal{Z}(S)$. □

Definition 2.3. $V \subseteq K^n$ is an **algebraic set** if V satisfies one of the equivalent conditions of Proposition 2.2.

Definition 2.4. Given a subset $A \subseteq K^n$, we form:

$\mathcal{I}(A) := \{f \in K[\underline{X}] \mid f(\underline{a}) = 0 \;\; \forall\, \underline{a} \in A\}$.

Proposition 2.5. Let $A \subseteq K^n$. Then

(1) $\mathcal{I}(A)$ is an ideal called the **ideal of vanishing polynomials** on A.

(2) If $A = V$ is an algebraic set in K^n, then $\mathcal{Z}(\mathcal{I}(V)) = V$

(3) the map $V \longmapsto \mathcal{I}(V)$ is a 1-1 map from the set of algebraic sets in K^n into the set of ideals of $K[\underline{X}]$. □

Remark 2.6. Note that for an ideal I of $K[\underline{X}]$, the inclusion $I \subseteq \mathcal{I}(\mathcal{Z}(I))$ is always true.

[*Proof.* Say (by Hilbert Basis Theorem) $I = < g_1, \ldots, g_s >$, $g_i \in K[\underline{X}]$. Then

$\mathcal{Z}(I) = \{\underline{x} \in K^n \mid g_i(\underline{x}) = 0 \; \forall\, i = 1, \ldots, s\}$,

$$\mathcal{I}(\mathcal{Z}(I)) = \{f \in K[\underline{X}] \mid f(\underline{x}) = 0 \ \ \forall \ \underline{x} \in \mathcal{Z}(I)\}.$$

Assume $f = h_1 g_1 + \ldots + h_s g_s \in I$, then $f(\underline{x}) = 0 \ \forall \ \underline{x} \in \mathcal{Z}(I)$
[since by definition $\underline{x} \in \mathcal{Z}(I) \Rightarrow g_i(\underline{x}) = 0 \ \forall \ i = 1, \ldots, s$]
$\Rightarrow f \in \mathcal{I}(\mathcal{Z}(I))$. □]

But in general it is false that $\mathcal{I}(\mathcal{Z}(I)) = I$. Hilbert's Nullstellensatz studies necessary and sufficient conditions on K and I so that this identity holds.

then
- $\sigma_0 \not\equiv 0 \Rightarrow \deg(\sigma_0)$ is even.
- $\sigma_1 \not\equiv 0 \Rightarrow \deg(\sigma_1)$ is even.
- $\sigma_0 \equiv 0 \Rightarrow \deg(t)$ is odd and ≥ 3.
- $\sigma_1 \equiv 0 \Rightarrow \deg(t)$ is even.
- $\sigma_0 \not\equiv 0,\ \sigma_1 \not\equiv 0$, then

$$[\text{even} =]\ \deg(\sigma_0) \neq \deg(\sigma_1 x^3)\ \ [= \text{odd}]$$

So, $\deg(t) = \max\left\{\deg(\sigma_0), \deg(\sigma_1 x^3)\right\}$ is even or odd ≥ 3.

This proves that $X \notin T_S$ and hence $T_S \subsetneq \text{Psd}(K_S)$. □

Example 2.4.(2) $S = \phi, n = 2 \Rightarrow K_S = \mathbb{R}^2$ and $T_S = M_S = \sum \mathbb{R}[X,Y]^2$.
We see that $T_S \subsetneq \text{Psd}(K_S)$
For example: $m(X,Y) := X^2Y^4 + X^4Y^2 - 3X^2Y^2 + 1 \in \text{Psd}(\mathbb{R}^2)$, but $\notin T_S = \sum \mathbb{R}[X,Y]^2$.

3. POSITIVSTELLENSATZ (Geometric Version)

Theorem 3.1. (Positivstellensatz: Geometric Version) Let $A = \mathbb{R}[\underline{X}]$. Let $S = \{g_1, \ldots, g_s\} \subseteq \mathbb{R}[\underline{X}]$, K_S, T_S as defined above, $f \in \mathbb{R}[\underline{X}]$. Then

(1) $f > 0$ on $K_S \Leftrightarrow \exists\, p, q \in T_S$ s.t. $pf = 1 + q$

(2) $f \geq 0$ on $K_S \Leftrightarrow \exists\, m \in \mathbb{Z}_+, \exists\, p, q \in T_S$ s.t. $pf = f^{2m} + q$

(3) $f = 0$ on $K_S \Leftrightarrow \exists\, m \in \mathbb{Z}_+$ s.t. $-f^{2m} \in T_S$

(4) $K_S = \phi \Leftrightarrow -1 \in T_S$.

Important **corollaries** to the PSS are:

(i) The real Nullstellensatz

(ii) Hilbert's 17^{th} problem

(iii) Abstract Positivstellensatz

The proof of the PSS consists of two parts:
-Step I: prove that (1) ⇒ (2) ⇒ (3) ⇒ (4) ⇒ (1)
-Step II: prove (4) [using Tarski Transfer]

We shall start the proof with step II:

Clearly $K_S \neq \phi \Rightarrow -1 \notin T_S$ (since $-1 \in T_S \Rightarrow K_S = \phi$), so it only remains to prove the following proposition:

Proposition 3.2. If $-1 \notin T_S$ (i.e. if T_S is a proper preordering), then $K_S \neq \phi$.

For proving this we need to recall some definitions and results:

Definition 3.3.1. Let A be a commutative ring with 1, a preordering $P \subseteq A$ is said to be an **ordering** on A if $P \cup -P = A$ and $\mathfrak{p} := P \cap -P$ is a prime (hence proper) ideal of A.

Definition 3.3.2. Let P be an ordering in A, then Support$P := \mathfrak{p}$ (the prime ideal $P \cap -P$).

Lemma 3.4.1. Let A be a commutative ring with 1. Let P be a maximal proper preordering in A. Then P is an ordering.

Lemma 3.4.2. Let A be a commutative ring with 1 and $P \subseteq A$ an ordering. Then P induces uniquely an ordering on $F := ff(A/\mathfrak{p})$ defined by:

$\forall\, a, b \in A$, $\dfrac{\overline{a}}{\overline{b}} \geq_P 0$ (in F) $\Leftrightarrow ab \in P$, where $\overline{a} = a + \mathfrak{p}$.

POSITIVE POLYNOMIALS LECTURE NOTES (04: 22/04/10)

SALMA KUHLMANN

Contents

1. EXKURS IN COMMUTATIVE ALGEBRA

Recall 1.1. Let K be a field and I an ideal of $K[\underline{X}]$, then the inclusion $I \subseteq \mathcal{I}(\mathcal{Z}(I))$ is always true.

But in general it is false that

$$\mathcal{I}(\mathcal{Z}(I)) = I \tag{1}$$

Note 1.2. In other words we study the map

$$\mathcal{I} : \left\{\text{algebraic sets in } K^n\right\} \rightsquigarrow \left\{\text{Ideals of } K[\underline{X}]\right\}$$
$$V \longmapsto \mathcal{I}(V)$$

- Clearly this map is 1-1 (proposition 2.5 of last lecture).
- What is the image of $\mathcal{I}$? (2)

  Let I an ideal, $I = \mathcal{I}(V)$

  $\Rightarrow \mathcal{Z}(I) = \underbrace{\mathcal{Z}(\mathcal{I}(V)) = V}_{\text{(prop. 2.5 of last lecture)}}$

  Thus an ideal I is in the image $\Leftrightarrow I = \mathcal{I}(\mathcal{Z}(I))$

So studying the equality (1) amounts to studying (2).

2. RADICAL IDEALS AND REAL IDEALS

Remark 2.1. For an ideal $I \subseteq K[\underline{X}]$, answer to $I = \mathcal{I}(\mathcal{Z}(I))$ is known
• when K is algebraically closed (Hilbert's Nullstellensatz),
or
• when K is real closed (Real Nullstellensatz).

To formulate these two important theorems we need to introduce some terminology:

Definition 2.2. Let A be a commutative ring with 1, $I \subseteq A$, I an ideal of A. Define

(i) $\sqrt{I} := \{a \in A \mid \exists\, m \in \mathbb{N} \text{ s.t. } a^m \in I\}$, the **radical** of I.

(ii) $\sqrt[R]{I} := \{a \in A \mid \exists\, m \in \mathbb{N} \text{ and } \sigma \in \Sigma A^2 \text{ s.t. } a^{2m} + \sigma \in I\}$, the **real radical** of I.

Remark 2.3. It follows from the definition that $I \subseteq \sqrt{I} \subseteq \sqrt[R]{I}$.

Definition 2.4. Let I be an ideal of A. Then

(1) I is called **radical ideal** if $I = \sqrt{I}$, and

(2) I is called **real radical ideal** (or just **real ideal**) if $I = \sqrt[R]{I}$.

Remark 2.5. (i) Every prime ideal is radical, but the converse does not hold in general.

(ii) I real radical $\Rightarrow$ I radical (follows from Remark 2.3 and Definition 2.4).

Proposition 2.6. Let A be a commutative ring with 1, $I \subseteq A$ an ideal. Then

(1) I is radical $\Leftrightarrow \forall\, a \in A : a^2 \in I \Rightarrow a \in I$

(2) I is real radical $\Leftrightarrow$ for $k \in \mathbb{N}, \forall\, a_1, \dots, a_k \in A : \sum_{i=1}^{k} a_i^2 \in I \Rightarrow a_1 \in I$.

Proof. (1) ($\Rightarrow$) Trivially follows from definition.

($\Leftarrow$) Let $a \in \sqrt{I}$, then $\exists\, m \geq 1$ s.t. $a^m \in I$.
Let k (big enough) s.t. $2^k \geq m$, then

$$a^{2^k} = a^m a^{2^k - m} \in I$$

Now we show by induction on k that:

$$[a^2 \in I \Rightarrow a \in I] \Rightarrow [a^{2^k} \in I \Rightarrow a \in I]$$

For $k = 1$, it is clear.

Assume it true for k and show it true for $k + 1$, i.e. let $a^{2^{k+1}} \in I$, then

$$a^{2^{k+1}} = \left(a^{2^k}\right)^2 \in I \underbrace{\Rightarrow}_{\text{(by assumption)}} a^{2^k} \in I \underbrace{\Rightarrow}_{\text{(induction hypothesis)}} a \in I.$$

(2) (⇒) Trivially follows from definition.

(⇐) Let $a \in \sqrt[R]{I}$, then $\exists\, m \geq 1,\ \sigma = \Sigma a_i^2\ (\in \Sigma A^2)$ s.t. $a^{2m} + \sigma \in I$.

$$\Rightarrow (a^m)^2 + \sigma \in I \underbrace{\Rightarrow}_{\text{(by assumption)}} a^m \in I \underbrace{\Rightarrow}_{\text{(as above in (1))}} a \in I.$$ □

Remark 2.7. (i) Since real radical ideal ⇒ radical ideal, so in particular (2) ⇒ (1) in above proposition.

(ii) A prime ideal is always radical (as in Remark 2.5), but need not be real.

Proposition 2.8. Let $\mathfrak{p} \subseteq A$ be a prime ideal. Then
$\mathfrak{p}$ is real ⇔ $ff(A/\mathfrak{p})$ is a real field.

Proof. $\mathfrak{p}$ is not real

$$\Leftrightarrow \exists\, a, a_1, \ldots, a_k \in A;\ a \notin \mathfrak{p} \text{ such that } a^2 + \sum_{i=1}^{k} a_i^2 \in \mathfrak{p}$$

$$\Leftrightarrow \overline{a}^2 + \sum_{i=1}^{k} \overline{a_i}^2 = 0 \text{ and } \overline{a} \neq 0 \text{ (in } A/\mathfrak{p})$$

⇔ $ff(A/\mathfrak{p})$ is not real. □

Theorem 2.9. Let K be a field, $A = K[\underline{X}]$, $I \subseteq A$ an ideal. Then

(1) (Hilbert's Nullstellensatz) Assume K is algebraically closed, then
$\mathcal{I}(\mathcal{Z}(I)) = \sqrt{I}$.
(Proved in B5)

(2) (Real Nullstellensatz) Assume K is real closed, then

$\mathcal{I}(\mathcal{Z}(I)) = \sqrt[R]{I}$.
(Will be deduced from Positivstellensatz)

Corollary 2.10. Consider the map:

$$\mathcal{I} : \left\{\text{algebraic sets in } K^n\right\} \longrightarrow \left\{\text{Ideals of } K[\underline{X}]\right\}$$

(1) If K is algebraically closed, then
Image $\mathcal{I} = \{I \mid I \text{ is a radical ideal}\}$

(2) If K is real closed, then
Image $\mathcal{I} = \{I \mid I \text{ is real ideal}\}$ □

Now we want to deduce the Real Nullstellensatz [Theorem 2.9 (2)] from part (3) of the Positivstellensatz (PSS) [Theorem 1.1 of last lecture].

We need the following 2 (helping) lemmas:

Lemma 2.11. Let A be a commutative ring and M be a quadratic module, then:

(1) $M \cap (-M)$ is an ideal of A.

(2) The following are equivalent for $a \in A$:

(i) $a \in \sqrt{M \cap (-M)}$

(ii) $a^{2m} \in M \cap (-M)$ for some $m \in \mathbb{N}, m \geq 1$

(iii) $-a^{2m} \in M$ for some $m \in \mathbb{N}, m \geq 1$. □

Lemma 2.12. Let A be a ring, $M(= M_S)$ a quadratic module (resp. preordering) of A generated by $S = \{g_1, \dots, g_s\}; g_1, \dots, g_s \in A$. Let I be an ideal in A generated by $h_1, \dots, h_t$, i.e. $I = (h_1, \dots, h_t); h_1, \dots, h_t \in A$. Then $M + I$ is the quadratic module (resp. the preordering) generated by $S \cup \{\pm h_i \ ; \ i = 1, \dots, t\}$. □

Recall 2.13. [(3) of PSS] Let $A = \mathbb{R}[\underline{X}], S = \{g_1, \dots, g_s\} \subseteq \mathbb{R}[\underline{X}], f \in \mathbb{R}[\underline{X}]$. Then $f = 0$ on $K_S \Leftrightarrow \exists\, m \in \mathbb{Z}_+$ s.t. $-f^{2m} \in T_S$.

Corollary 2.14. (to Recall 2.13 and Lemma 2.11) Let $K = K_S \subseteq \mathbb{R}^n,\ T = T_S \subseteq \mathbb{R}[\underline{X}]$ (as in PSS), then

$$\mathcal{I}(K_S) = \sqrt{T_S \cap (-T_S)}.$$

Proof. $f = 0$ on $K_S \underbrace{\Leftrightarrow}_{\text{(by(3) of PSS)}} -f^{2m} \in T_S$ for some $m \in \mathbb{Z}_+$

$$\underbrace{\Leftrightarrow}_{\text{(by lemma 2.11)}} f \in \sqrt{T_S \cap (-T_S)}$$ □

Corollary 2.15. (to Lemma 2.11 and 2.12) Let A be a commutative ring with 1. Let I be an ideal of A. Consider the preordering $T := \Sigma A^2 + I$, then

$$\sqrt[R]{I} = \sqrt{T \cap (-T)}.$$ □

Now Corollary 2.14 and Corollary 2.15 give the proof of the Real Nullstellensatz (RNSS) as follows:

Proof of RNSS [Theorem 2.9 (2)]. Let I be an ideal of $\mathbb{R}[\underline{X}]$

We **show that:** $\mathcal{I}(\mathcal{Z}(I)) = \sqrt[R]{I}$

$\mathbb{R}[\underline{X}]$ Noetherian $\Rightarrow I = (h_1, \ldots, h_t)$ (by Hilbert Basis Theorem) .
Consider $S := \{\pm h_i \; ; \; i = 1, \ldots, t\}$
Then $K_S = \mathcal{Z}(I)$ [clearly]

Now by Lemma 2.12, we have:

$$T = T_S = \Sigma\mathbb{R}[\underline{X}]^2 + I$$

So we get,

$$\mathcal{I}(\mathcal{Z}(I)) = \mathcal{I}(K_S) \underbrace{=}_{\text{(Cor 2.14)}} \sqrt{T \cap (-T)} \underbrace{=}_{\text{(Cor 2.15)}} \sqrt[R]{I}$$ □

3. THE REAL SPECTRUM

Definition 3.1. Let A be a commutative ring with 1. Then:

$\mathcal{S}pec(A) := \{\mathfrak{p} \mid \mathfrak{p}$ is prime ideal of A $\}$ is called the **Spectrum** of A.

$\mathcal{S}per(A) = \mathcal{S}pec_r(A) := \Big\{(\mathfrak{p}, \leq) \mid \mathfrak{p}$ is a prime ideal of A and $\leq$ is an ordering on the (formally real) field $ff(A/\mathfrak{p})\Big\}$ is called the **Real Spectrum** of A.

Remark 3.2. (i) Several orderings may be defined on $ff(A/\mathfrak{p})$,
$(\mathfrak{p}, \leq_1) \neq (\mathfrak{p}, \leq_2)$.

(ii) $(\mathfrak{p}, \leq) \in \mathcal{S}per(A) \Rightarrow \mathfrak{p}$ is real radical ideal. [see Proposition 2.8 and Remark 2.5 (i).]

Note 3.3. $\mathcal{S}per(A) := \{\alpha = (\mathfrak{p}, \leq) \mid \mathfrak{p}$ is a real prime and $\leq$ an ordering on $ff(A/\mathfrak{p})\}$.

POSITIVE POLYNOMIALS LECTURE NOTES (05: 27/04/10)

SALMA KUHLMANN

Contents

1. THE REAL SPECTRUM

Definition 1.1. Let A be a commutative ring with 1. We set:

$\mathcal{S}\boldsymbol{per}(A) := \{\alpha = (\mathfrak{p}, \leq) \mid \mathfrak{p}$ is a prime ideal of A and $\leq$ is an ordering on $ff(A/\mathfrak{p})\}$.

Note 1.2. $\mathcal{S}per(A) := \{\alpha = (\mathfrak{p}, \leq) \mid \mathfrak{p}$ is a real prime and $\leq$ an ordering on $ff(A/\mathfrak{p})\}$.

Definition 1.3. Let $\alpha = (\mathfrak{p}, \leq) \in \mathcal{S}per(A)$, then $\mathfrak{p} = \mathrm{Supp}(\alpha)$, the **Support** of α.

Recall 1.4. An **ordering** $P \subseteq A$ is a preordering with $P \cup -P = A$ and $\mathfrak{p} := P \cap -P$ prime ideal of A.

Definition 1.5. Alternatively, the **Real Spectrum** of A, $\mathcal{S}per(A)$ can be defined as:

$$\mathcal{S}\boldsymbol{per}(A) := \{P \mid P \subseteq A, P \text{ is an ordering of } A\}.$$

Remark 1.6. The two definitions of $\mathcal{S}per(A)$ are equivalent in the following sense:

The map

$$\varphi\colon \Big\{\text{Orderings in } A\Big\} \rightsquigarrow \Big\{(\mathfrak{p}, \leq), \mathfrak{p} \text{ real prime}, \leq \text{ ordering on } ff(A/\mathfrak{p})\Big\}$$

$$P \longmapsto \mathfrak{p} := P \cap -P, \leq_P \text{ on } ff(A/\mathfrak{p})$$

$$\left(\text{where } \frac{\overline{a}}{\overline{b}} \geq_P 0 \Leftrightarrow ab \in P \text{ with } \overline{a} = a + \mathfrak{p}\right)$$

is bijective $\left[\text{where } \varphi^{-1}(\mathfrak{p}, \leq) \text{ is } P := \{a \in A \mid \overline{a} \geq 0\}\right]$. □

2. TOPOLOGIES ON $\mathcal{S}per(A)$

Definition 2.1. The **Spectral Topology** on $\mathcal{S}per(A)$:
$\mathcal{S}per(A)$ as a topological space, subbasis of open sets is:

$\mathcal{U}(a) := \{P \in \mathcal{S}per(A) \mid a \notin P\}$, $a \in A$.

(So a basis of open sets consists of finite intersection, i.e. of sets

$\mathcal{U}(a_1, \ldots, a_n) := \{P \in \mathcal{S}per(A) \mid a_1, \ldots, a_n \notin P\}$)

Then close by arbitrary unions to get all open sets.
This is called Spectral Topology.

Definition 2.2. The **Constructible (or Patch) Topology** on $\mathcal{S}per(A)$ is the topology that is generated by the open sets $\mathcal{U}(a)$ and there complements $\mathcal{S}per(A)\backslash\mathcal{U}(a)$, for $a \in A$.
(Subbasis for constructible topology is $\mathcal{U}(a)$, $\mathcal{S}per(A)\backslash\mathcal{U}(a)$, for $a \in A$.)

Remark 2.3. The constructible topology is finer than the Spectral Topology (i.e. more open sets).

Special case: $A = \mathbb{R}[\underline{X}]$

Proposition 2.4. There is a natural embedding

$$\mathcal{P} : \mathbb{R}^n \longrightarrow \mathcal{S}per(\mathbb{R}[\underline{X}])$$

given by

$$\underline{x} \longmapsto P_{\underline{x}} := \left\{f \in \mathbb{R}[\underline{x}] \mid f(\underline{x}) \geq 0\right\}.$$

Proof. The map $\mathcal{P}$ is well defined.

Verify that $P_{\underline{x}}$ is indeed an ordering of A.

Clearly it is a preordering, $P_{\underline{x}} \cup -P_{\underline{x}} = \mathbb{R}[\underline{X}]$.

$\mathfrak{p} := P_{\underline{x}} \cap -P_{\underline{x}} = \left\{f \in \mathbb{R}[\underline{X}] \mid f(\underline{x}) = 0\right\}$ is actually a maximal ideal of $\mathbb{R}[\underline{X}]$, since $\mathfrak{p} = \text{Ker }(ev_{\underline{x}})$, the kernel of the evaluation map

$$ev_{\underline{x}} : \mathbb{R}[\underline{X}] \longrightarrow \mathbb{R}$$
$$f \longmapsto f(\underline{x})$$

so, $\frac{\mathbb{R}[\underline{X}]}{\mathfrak{p}} \simeq \underbrace{\mathbb{R}}_{\text{a field}}$ (by first isomorphism theorem)

$\Rightarrow$ $\mathfrak{p}$ maximal $\Rightarrow$ $\mathfrak{p}$ is prime ideal. □

Theorem 2.5. $\mathcal{P}(\mathbb{R}^n)$, the image of $\mathbb{R}^n$ in $\mathcal{S}per(\mathbb{R}[\underline{X}])$ is dense in ($\mathcal{S}per(\mathbb{R}[\underline{X}])$, Constructible Topology) and hence in ($\mathcal{S}per(\mathbb{R}[\underline{X}])$, Spectral Topology). $\Big($i.e. $\overline{\mathcal{P}(\mathbb{R}^n)}^{patch} = \mathcal{S}per(\mathbb{R}[\underline{X}])\Big)$.

Proof. By definition, a basic open set in $\mathcal{S}per(\mathbb{R}[\underline{X}])$ has the form
$\mathcal{U} = \{P \in \mathcal{S}per(\mathbb{R}[\underline{X}]) \mid f_i \notin P, g_j \in P; i = i, \ldots, s, j = 1, \ldots, t\}$, for some $f_i, g_j \in \mathbb{R}[\underline{X}]$.

Let $P \in \mathcal{U}$ $\big($open neighbourhood of $P \in \mathcal{S}per(\mathbb{R}[\underline{X}])\big)$

We want to **show that:** $\exists\, \underline{y} \in \mathbb{R}^n$ s.t. $P_{\underline{y}} \in \mathcal{U}$

Consider $F = ff(\mathbb{R}[\underline{X}]/\mathfrak{p})$; $\mathfrak{p} = \mathrm{Supp}(P) = P \cap -P$ and $\leq$ ordering on F induced by P.

Then $(F, \leq)$ is an ordered field extension of $(\mathbb{R}, \leq)$.

Consider $\underline{x} = (\overline{x_1}, \ldots, \overline{x_n}) \in F^n$, where $\overline{x_i} = X_i + \mathfrak{p}$

Then by definition of $\leq$ we have (as in the proof of PSS):
$f_i(\underline{x}) < 0$ and $g_j(\underline{x}) \geq 0$; $\forall\, i = i, \ldots, s,\ j = 1, \ldots, t$.

By Tarski Transfer, $\exists\, \underline{y} \in \mathbb{R}^n$ s.t.

$f_i(\underline{y}) < 0 \left(\Leftrightarrow f_i \notin P_{\underline{y}} \right)$ and $g_j(\underline{y}) \geq 0 \left(\Leftrightarrow g_j \in P_{\underline{y}} \right)$; $i = i, \ldots, s,\ j = 1, \ldots, t$

$\Leftrightarrow P_{\underline{y}} \in \mathcal{U}$ □

3. ABSTRACT POSITIVSTELLENSATZ

Recall 3.1. T proper preordering $\Rightarrow \exists\, P$ an ordering of A s.t. $P \supseteq T$.

Definiton 3.2. Let P be an ordering of A, fix $a \in A$. We define **Sign of** a **at** P :

$$a(P) := \begin{cases} 1 & \text{if } a \notin -P \\ 0 & \text{if } a \in P \cap -P \\ -1 & \text{if } a \notin P \end{cases}$$

(Note that this allows to consider $a \in A$ as a map on $\mathcal{S}per(A)$).

Notation 3.3. We write: $a > 0$ at P if $a(P) = 1$
$a = 0$ at P if $a(P) = 0$
$a < 0$ at P if $a(P) = -1$

Note that (in this notation) $a \geq 0$ at P iff $a \in P$.

Definition 3.4. Let $T \subseteq A$, then the **Relative Spectrum** of A with respect to T is

$$\boldsymbol{\mathcal{S}per}_T(A) = \{P \mid P \supseteq T; P \subseteq A \text{ is an ordering of } A\}.$$

Proposition 3.5. Let $T \subseteq A$ be a finitely generated preordering, say $T = T_S$; where $S = \{g_1, \ldots, g_s\} \subseteq A$. Then

$$\begin{aligned}\mathcal{S}per_T(A) = \mathcal{S}per_S(A) &= \{P \in \mathcal{S}per(A) \mid g_i \in P\,; i = i, \ldots, s\} \\ &= \{P \in \mathcal{S}per(A) \mid g_i(P) \geq 0\,; i = i, \ldots, s\}\end{aligned}$$

□

Remark 3.5. Let $T \subseteq A$

(i) $\mathcal{S}per_T(A)$ inherits the relative spectral (respectively constructible) topology.

(ii) In case $T = T_{\{g_1,\ldots,g_s\}}$ is a finitely generated preordering, then the proof of Theorem 2.5 goes through to give the following relative version for $\mathcal{S}per_T$:

Theorem 3.6. (Relative version of Theorem 2.5) Let $T = T_S$ = finitely generated preordering; $S = \{g_1, \ldots, g_s\}$. Let $K = K_S = \{\underline{x} \in \mathbb{R}^n \mid g_i(\underline{x}) \geq 0\} \subseteq \mathbb{R}^n$, a basic closed semi-algebraic set. Consider ($\mathcal{S}per_T$, Constructible Topology). Then

$$\mathcal{P} : K \rightsquigarrow \mathcal{S}per_T(\mathbb{R}[\underline{X}])$$

(defined as before)

$$\underline{x} \longmapsto P_{\underline{x}} = \left\{f \in \mathbb{R}[\underline{x}] \mid f(\underline{x}) \geq 0\right\}$$

is well defined (i.e. $P_{\underline{x}} \supseteq T \;\forall\; \underline{x} \in K$).

Moreover $\mathcal{P}(K)$ is dense in $\left(\mathcal{S}per_T(\mathbb{R}[\underline{X}]), \text{Constructible Topology}\right)$.

Proof. The proof is analogous to the proof of Theorem 2.5.
(Note the fact that T is finitely generated is crucial here to be able to apply Tarski Transfer.) □

Theorem 3.7. (Abstract Positivstellensatz) Let A be a commutative ring, $T \subseteq A$ be a preordering of A (not necessarily finitely generated). Then for $a \in A$:

(1) $a > 0$ on $\mathcal{S}per_T(A) \Leftrightarrow \exists\, p, q \in T$ s.t. $pa = 1 + q$

(2) $a \geq 0$ on $\mathcal{S}per_T(A) \Leftrightarrow \exists\, p, q \in T, m \geq 0$ s.t. $pa = a^{2m} + q$

(3) $a = 0$ on $\mathcal{S}per_T(A) \Leftrightarrow \exists\, m \geq 0$ s.t. $-a^{2m} \in T$.

Proof. (1) Let $a > 0$ on $\mathcal{S}per_T(A)$. Suppose for a contradiction that there are no elements $p, q \in T$ s.t. $pa = 1 + q$ i.e. s.t. $-1 = q - pa$
i.e. $-1 \neq q - pa\ \forall\, p, q \in T$
Thus $-1 \notin T' := T - Ta$.
$\Rightarrow T'$ is a proper preordering.
So (by recall 3.1) $\exists\, P$ an ordering of A with $T' \subseteq P$.
Now observe that $T \subseteq P$ i.e. $P \in \mathcal{S}per_T(A)$ but $-a \in P$ (i.e. $a(P) \leq 0$) i.e. $a \leq 0$ on P, a contradiction to the assumption. □

Proposition 3.8. Abstract Positivstellensatz $\Rightarrow$ Positivstellensatz.

Proof. $A = \mathbb{R}[\underline{X}], T = T_S = T_{\{g_1,\ldots,g_s\}}, K = K_S$.
It suffices **to show** (2) of PSS [Theorem 1.1 of lecture 03 on 20/04/10], i.e. $f \geq 0$ on $K_S \Leftrightarrow \exists\, m \in \mathbb{Z}_+, \exists\, p, q \in T_S$ s.t. $pf = f^{2m} + q$.
Let $f \in \mathbb{R}[\underline{X}]$ and $f \geq 0$ on K_S.
It suffices [by (2) of Theorem 3.7] to **show that** $f \geq 0$ on $\mathcal{S}per_T(\mathbb{R}[\underline{X}])$:
If not then $\exists\, P \in \mathcal{S}per_T(\mathbb{R}[\underline{X}])$ s.t. $f \notin P$
So, $P \in \mathcal{U}_T(f)$
(open neighbourhood of $P \in \mathcal{S}per_T(\mathbb{R}[\underline{X}])$)
Now by [Theorem 3.6 i.e.] relative density of $\mathcal{P}(K)$ in $\mathcal{S}per_T(\mathbb{R}[\underline{X}])$:
$\exists\, \underline{x} \in K$ s.t. $P_{\underline{x}} \in \mathcal{U}_T(f)$
$\Rightarrow f \notin P_{\underline{x}} \Rightarrow f(\underline{x}) < 0$, a contradiction to the assumption. □

POSITIVE POLYNOMIALS LECTURE NOTES (06: 29/04/10)

SALMA KUHLMANN

Contents

1. GENERALITIES ABOUT POLYNOMIALS

Definition 1.1. For a **polynomial** $p \in \mathbb{R}[X_1, \ldots, X_n]$, we write

$$p(\underline{X}) = \sum_{\underline{i} \in \mathbb{Z}_+^n} c_i \, \underline{X}^{\underline{i}} \; ; \; c_i \in \mathbb{R},$$

where $\underline{X}^{\underline{i}} = X_1^{i_1} \ldots X_n^{i_n}$ is a monomial of degree $= |\underline{i}| = \sum_{k=1}^{n} i_k$ and $c_i \, \underline{X}^{\underline{i}}$ is a term.

Definition 1.2. A polynomial $p(\underline{X}) \in \mathbb{R}[\underline{X}]$ is called **homogeneous** or **form** if all terms in p have the same degree.

Notation 1.3. $\mathcal{F}_{n,m} := \{F \in \mathbb{R}[X_1, \ldots, X_n] \mid F \text{ is a form and } \deg(F) = m\}$, the set of all forms in n variables of degree m (also called set of n-ary m-ics forms), for $n, m \in \mathbb{N}$.
Convention: $0 \in \mathcal{F}_{n,m}$.

Definition 1.4. Let $p \in \mathbb{R}[X_1, \ldots, X_n]$ of degree m. The **homogenization** of p w.r.t X_{n+1} is defined as

$$p_h(x_1, \ldots, x_n, x_{n+1}) := x_{n+1}^m \, p\left(\frac{x_1}{x_{n+1}}, \ldots, \frac{x_n}{x_{n+1}}\right)$$

Note that p_h is a homogeneous polynomial of degree m and in $n+1$ variables i.e. $p_h \in \mathcal{F}_{n+1,m}$.

Proposition 1.5. (1) Let $p(\underline{X}) \in \mathbb{R}[\underline{X}]$, $\deg(p) = m$, then

$$\text{number of monomials of } p \leq \binom{m+n}{n}$$

(2) Let $F(\underline{X}) \in \mathcal{F}_{n,m}$, then

$$\text{number of monomials of } F \leq N := \binom{m+n-1}{n-1} \qquad \square$$

Remark 1.6. $\mathcal{F}_{n,m}$ is a finite dimensional real vector space with $\mathcal{F}_{n,m} \simeq \mathbb{R}^N$.

2. PSD- AND SOS- POLYNOMIALS

Definition 2.1. (1) $p(\underline{x}) \in \mathbb{R}[\underline{X}]$ is **positive semidefinite (psd)** if

$$p(\underline{x}) \geq 0 \ \forall \ \underline{x} \in \mathbb{R}^n.$$

(2) $p(\underline{x}) \in \mathbb{R}[\underline{X}]$ is **sum of squares (SOS)** if $\exists \ p_i \in \mathbb{R}[\underline{X}]$ s.t.

$$p(\underline{x}) = \sum_i p_i(\underline{x})^2.$$

Notation 2.2. $\mathcal{P}_{n,m}$:= set of all forms $F \in \mathcal{F}_{n,m}$ which are psd, and

$\sum_{n,m}$:= set of all forms $F \in \mathcal{F}_{n,m}$ which are sos.

Lemma 2.3. If a polynomial p is psd then p has even degree. $\square$

Remark 2.4. From now on (using lemma 2.3) we will often write $\mathcal{P}_{n,2d}$ and $\sum_{n,2d}$.

Lemma 2.5. Let p be a homogeneous polynomial of degree 2d, and p sos. Then every sos representation of p consists of homogeneous polynomials only, i.e.
$p(\underline{x}) = \sum_i p_i(\underline{x})^2 \Rightarrow p_i(\underline{x})$ homogenous of degree d, i.e. $p_i \in \mathcal{F}_{n,d}$. $\square$

Remark 2.6. The properties of psd-ness and sos-ness are preserved under homogenization (see the following lemma).

Lemma 2.7. Let $p(\underline{x})$ be a polynomial of degree m. Then

(1) p is psd iff p_h is psd,

(2) p is sos iff p_h is sos. $\square$

So we can focus our investigation of psdness of polynomials versus sosness of polynomials to those of forms, i.e. study and compare $\sum_{n,m} \subseteq \mathcal{P}_{n,m}$.

Theorem 2.8. (Hilbert) $\sum_{n,m} = \mathcal{P}_{n,m}$ iff

(i) $n = 2$ [i.e. binary forms] or

(ii) $m = 2$ [i.e. quadratic forms] or

(iii) $(n, m) = (3, 4)$ [i.e. ternary quartics].

For the ternary quartics case ($\mathcal{F}_{3,4}$), we shall study the **convex cones** $\mathcal{P}_{n,m}$ and $\sum_{n,m}$.

3. CONVEX SETS, CONES AND EXTREMALITY

Definition 3.1. A subset C of $\mathbb{R}^n$ is **convex set** if $\underline{a}, \underline{b} \in C \Rightarrow \lambda\underline{a} + (1 - \lambda)\underline{b} \in C$, for all $0 < \lambda < 1$.

Proposition 3.2. The intersection of an arbitrary collection of convex sets is convex.

Notation 3.3. $\mathbb{R}_+ := \{x \in \mathbb{R} \mid x \geq 0\}$.

Definition 3.4. Let $\underline{c}_1, \ldots, \underline{c}_k \in \mathbb{R}^n$. A **convex combination** of $\underline{c}_1, \ldots, \underline{c}_k$ is any vector sum

$$\alpha_1\underline{c}_1 + \ldots + \alpha_k\underline{c}_k, \text{ with } \alpha_1, \ldots, \alpha_k \in \mathbb{R}_+ \text{ and } \sum_{i=1}^{k} \alpha_i = 1.$$

Theorem 3.5. A subset $C \subseteq \mathbb{R}^n$ is convex if and only if it contains all the convex combinations of its elements.

Proof. ($\Leftarrow$) clear
($\Rightarrow$) Let $C \subseteq \mathbb{R}^n$ be a convex set. By definition C is closed under taking convex combinations with two summands. We show that it is also closed under finitely many summands.
Let $k > 2$. By Induction on k, assuming it true for fewer than k.
Given a convex combination $\underline{c} = \alpha_1\underline{c}_1 + \ldots + \alpha_k\underline{c}_k$, with $\underline{c}_1, \ldots, \underline{c}_k \in C$
Note that we may assume $0 < \alpha_i < 1$ for $i = i, \ldots, k$; otherwise we have fewer than k summands and we are done.
Consider $\underline{d} = \dfrac{\alpha_2}{1 - \alpha_1}\underline{c}_2 + \ldots + \dfrac{\alpha_k}{1 - \alpha_1}\underline{c}_k$
we have $\dfrac{\alpha_2}{1 - \alpha_1}, \ldots, \dfrac{\alpha_k}{1 - \alpha_1} > 0$ and $\dfrac{\alpha_2}{1 - \alpha_1} + \ldots + \dfrac{\alpha_k}{1 - \alpha_1} = 1$
Thus $\underline{d}$ is a convex combination of $k - 1$ elements of C and $\underline{d} \in C$ by induction.
Since $\underline{c} = \alpha_1\underline{c}_1 + (1 - \alpha_1)\underline{d}$, it follows that $\underline{c} \in C$. □

Definition 3.6. The intersection of all convex sets containing a given subset $S \subseteq \mathbb{R}^n$ is called the **convex hull** of S and is denoted by **cvx(S)**.

Remark 3.7. The convex hull of $S \subseteq \mathbb{R}^n$ is a convex set and is the uniquely defined smallest convex set containing S.

Theorem 3.8. For any $S \subseteq \mathbb{R}^n$,
$\text{cvx}(S)$ = the set of all convex combinations of the elements of S.

Proof. ($\supseteq$) The elements of S belong to $\text{cvx}(S)$, so all their convex combinations belong to $\text{cvx}(S)$ by Theorem 3.5.

($\subseteq$) On the other hand we observe that the set of convex combinations of elements of S is itself a convex set:
let $\underline{c} = \alpha_1\underline{c}_1 + \ldots + \alpha_k\underline{c}_k$ and $\underline{d} = \beta_1\underline{d}_1 + \ldots + \beta_l\underline{d}_l$, where $\underline{c}_i, \underline{d}_i \in S$, then
$\lambda\underline{c} + (1-\lambda)\underline{d} = \lambda\alpha_1\underline{c}_1 + \ldots + \lambda\alpha_k\underline{c}_k + (1-\lambda)\beta_1\underline{d}_1 + \ldots + (1-\lambda)\beta_l\underline{d}_l$, $0 \le \lambda \le 1$ is just another convex combination of elements of S.
So by minimality property of $\text{cvx}(S)$, it follows that $\text{cvx}(S) \subseteq$ the set of all convex combinations of the elements of S. □

Corollary 3.9. The convex hull of a finite subset $\{\underline{s}_1, \ldots, \underline{s}_k\} \subseteq \mathbb{R}^n$ consists of all the vectors of the form $\alpha_1\underline{s}_1 + \ldots + \alpha_k\underline{s}_k$ with $\alpha_1, \ldots, \alpha_k \ge 0$ and $\sum_i \alpha_i = 1$. □

Definitions 3.10. (1) A set which is the convex hull of a finite subset of $\mathbb{R}^n$ is called a **convex polytope**, i.e. $C \subseteq \mathbb{R}^n$ is a convex polytope if $C = \text{cvx}(S)$ for some finite $S \subseteq \mathbb{R}^n$.

(2) A point in a polytope is called a **vertex** if it is not on the line segment joining any other two distinct points of the polytope.

Remark 3.11. (1) Convex polytope is necessarily closed and bounded, i.e. compact.

(2) A convex polytope is always the convex hull of its vertices.

More general version for compact sets is the Krein Milman theorem:

Theorem 3.12. (Krein-Milman) Let $C \subseteq \mathbb{R}^n$ be a compact and convex set. Then C is the convex hull of its extreme points. □
Definitions 3.13. $\underline{x} \in C$ is **extreme** if $C \setminus \{\underline{x}\}$ is convex.

POSITIVE POLYNOMIALS LECTURE NOTES (07: 04/05/10)

SALMA KUHLMANN

This lecture was held by Dr. Annalisa Conversano.

Contents

1. CONVEX CONES AND GENERALIZATION OF KREIN MILMAN THEOREM

We want **to prove:** $\mathcal{P}_{3,4} = \sum_{3,4}$
(i.e each positive semidefinite form in 3 variables of degree 4 is a sum of squares.)
To do it , we need several notions and intermediate results.

Definition 1.1. $C \subseteq \mathbb{R}^k$ is a **convex cone** if

$$\underline{x}, \underline{y} \in C \Rightarrow \underline{x} + \underline{y} \in C, \text{ and}$$
$$\underline{x} \in C, \lambda \in \mathbb{R}_+ \Rightarrow \lambda \underline{x} \in C$$

(i.e if it is closed under addition and under multiplication by non-negative scalars.)

Fact 1.2. $C \subseteq \mathbb{R}^k$ is a convex cone if and only if it is closed under non-negative linear combinations of its elements, i.e.
$\forall\, n \in \mathbb{N},\ \forall\, \underline{x}_1, \ldots, \underline{x}_n \in C, \forall\, \lambda_1, \ldots, \lambda_n \in \mathbb{R}_+ : \lambda_1 \underline{x}_1 + \ldots + \lambda_n \underline{x}_n \in C.$

Definition 1.3. Let $S \subseteq \mathbb{R}^k$. Then

Cone(S) := {non-negative linear combinations of elements from S}

is the convex cone generated by S.

Fact 1.4. For every $S \subseteq \mathbb{R}^k$, Cone(S) is the smallest convex cone which includes S.

Fact 1.5. If $S \subseteq \mathbb{R}^k$ is convex, then

$$\text{Cone}(S) := \{\lambda \underline{x} \mid \lambda \in \mathbb{R}_+, \underline{x} \in S\}.$$

Definition 1.6. $R \subseteq \mathbb{R}^k$ is a **ray** if $\exists\, \underline{x} \in \mathbb{R}^k$, $\underline{x} \neq 0$ s.t.

$$R = \{\lambda \underline{x} \mid \lambda \in \mathbb{R}_+\} := \underline{x}^+$$

(A ray R is a half-line.)

Definition 1.7. Let $C \subseteq \mathbb{R}^k$ be a convex set:

(1) a point $\underline{c} \in C$ is an **extreme point** if $C \setminus \{\underline{c}\}$ is convex.

(2) a ray $R \subseteq C$ is an **extreme ray** if $C \setminus R$ is convex.

Notation 1.8. Let $C \subseteq \mathbb{R}^k$ convex.

(1) ext(C) := set of all extreme points in C

(2) rext(C) := set of all extreme rays in C

Definition 1.9. (1) A **straight line** $L \subseteq \mathbb{R}^k$ is a translate of a 1-dimensional subspace, i.e. $L = \{\underline{x} + \lambda \underline{y} \mid \lambda \in \mathbb{R}\}$, for some $\underline{x}, \underline{y} \in \mathbb{R}^k$, $\underline{y} \neq 0$.

(2) $C \subseteq \mathbb{R}^k$ is **line free** if C contains no straight lines.

Theorem 1.10. (Klee) Let $C \subseteq \mathbb{R}^k$ be a closed line free convex set. Then

$$C = \text{cvx}\,(\text{ext}(C) \cup \text{rext}(C))$$

Remark 1.11. (a) Let $C \subseteq \mathbb{R}^k$ be a convex cone and $\underline{x} \in C$, $\underline{x} \neq 0$. Then $\underline{x}$ is not extreme.
Also $\underline{x}^+ \subset C$.

(b) Let $C \subseteq \mathbb{R}^k$ be a line free convex cone. Then ext(C) = {0}.

Proof. If not, then $C \setminus \{0\}$ is not convex, so
$\exists\, \underline{x}, \underline{y} \in C \setminus \{0\}, \exists\, 0 < \lambda < 1$ s.t. $\lambda \underline{x} + (1-\lambda)\underline{y} \notin C \setminus \{0\}$.
But C is convex, so

$$\lambda \underline{x} + (1-\lambda)\underline{y} = \underline{0}.$$

That means that $\underline{x}^+ \cup \underline{y}^+$ is a straight line in C, a contradiction. □

Corollary 1.12. (Generalization of Krein-Milman to closed line free convex cone) Let $C \subseteq \mathbb{R}^k$ be a closed line free convex cone. Then

$$C = \text{cvx}\,(\text{rext}(C))$$

Proof. By Remark 1.11, $\text{ext}(C) = \{0\}$.
Applying Theorem 1.10, we get $C = \text{cvx}\,(\text{rext}(C))$. □

Remark 1.13. Let C be a line free convex cone

(1) $0 \neq \underline{x} \in C$ belongs to an extreme ray (equivalently, the ray $\{\lambda\underline{x} \mid \lambda \in \mathbb{R}_+\}$ generated by $\underline{x}$ is extreme) if and only if
whenever $\underline{x} = \underline{x}_1 + \underline{x}_2$, with $\underline{x}_1, \underline{x}_2 \in C$, then $\underline{x}_i = \lambda_i\underline{x}$; $\lambda_i \in \mathbb{R}_+, \lambda_1 + \lambda_2 = 1$ (i.e. $\underline{x}_1, \underline{x}_2$ belong to the ray generated by $\underline{x}$).

(2) The set of convex linear combinations of points in extremal rays = the set of sum of points in extremal rays.

2. THE CONES $\mathcal{P}_{n,2d}$ and $\sum_{2,2d}$

Lemma 2.1. $\mathcal{P}_{n,2d}$ is a closed convex cone.

Proof. It is trivial that $\mathcal{P}_{n,2d}$ is a convex cone.
Next we prove that $\mathcal{P}_{n,2d}$ is closed:
Let $(P_k)_{k\in\mathbb{N}}$ be a sequence in $\mathcal{P}_{n,2d}$ converging to P. Then for all $x \in \mathbb{R}^n, P_k(x) \to P(x)$.
We want (to show that) $P \in \mathcal{P}_{n,2d}$,
otherwise $\exists\, x_0 \in \mathbb{R}^n$, s.t. $P(x_0) = -\epsilon, \epsilon > 0$.
And since $P_k(x_0) \to P(x_0)$ in $\mathbb{R}^n$, $\forall\, \epsilon > 0, \exists\, m \in \mathbb{N}$ s.t $\forall\, k > m : |P_k(x_0) - P(x_0)| < \epsilon$, thus (taking the same ϵ as above): $|P_k(x_0) + \epsilon| < \epsilon \Rightarrow P_k(x_0) < 0$, a contradiction (since $P_k \in \mathcal{P}_{n,2d}\ \forall\, k$). So, $P \in \mathcal{P}_{n,2d}$ and hence $\mathcal{P}_{n,2d}$ is closed. □

Lemma 2.2. The cone $\mathcal{P}_{n,2d}$ is line free.

Proof. Suppose not, then there exists a straight line L in $\mathcal{P}_{n,2d}$.
Write $L = \{F + \lambda G \mid \lambda \in \mathbb{R}\}; F, G \in \mathcal{P}_{n,2d}, G \neq 0$.
Since $-G \notin \mathcal{P}_{n,2d}$, take x_0 s.t. $-G(x_0) < 0$.
Then for (large enough λ i.e.) $\lambda \to -\infty$ we have $F(x_0) + \lambda G(x_0) < 0$

$\Rightarrow L \nsubseteq \mathcal{P}_{n,2d}$.
Hence $\mathcal{P}_{n,2d}$ is line free. □

Corollary 2.3. $\mathcal{P}_{n,2d}$ is the convex hull of its extremal rays.

Proof. By Lemma 2.1 and Lemma 2.2, $\mathcal{P}_{n,2d}$ is a line free closed convex cone. And therefore by the generalization of Krein-Milmann (Corollary 1.12) it is the convex hull of its extremal rays. □

Definition 2.4. A form $F \in \mathcal{P}_{n,2d}$ is **extremal** in $\mathcal{P}_{n,2d}$ if
$F = F_1 + F_2, F_1, F_2 \in \mathcal{P}_{n,2d} \Rightarrow F_i = \lambda_i F; i = 1, 2$ for $\lambda_i \in \mathbb{R}_+$ satisfying $\lambda_1 + \lambda_2 = 1$.

Similar definition for $\sum_{n,2d}$.

Note 2.5. By Remark 1.13 this just means that the ray generated by F is extremal.

Remark 2.6. (1) $F \in \sum_{n,2d}$ extremal $\Rightarrow F = G^2$ for some $G \in \mathcal{F}_{n,d}$.

(2) The converse of (1) is not true in general.
For example: $(x^2 + y^2)^2 = (x^2 - y^2)^2 + (2xy)^2$ is not extremal in $\sum_{2,4}$.

(3) G^2 is extremal in $\sum_{n,2d} \not\Rightarrow G^2$ is extremal in $\mathcal{P}_{n,2d}$.
For instance Choi et al showed that
$p := f^2$, where $f(x, y, z) = x^4y^2 + y^4z^2 + z^4x^2 - 3x^2y^2z^2 + (x^2y + y^2z - z^2x - xyz)^2$
is extremal in $\sum_{3,12}$ but not in $\mathcal{P}_{3,12}$.

Notation 2.7. We denote by $\mathcal{E}(\mathcal{P}_{n,2d})$ the set of all extremal forms in $\mathcal{P}_{n,2d}$.

Lemme 2.8. Let $E \in \mathcal{P}_{n,2d}$. Then
$E \in \mathcal{E}(\mathcal{P}_{n,2d})$ if and only if $\forall F \in \mathcal{P}_{n,2d}$ with $E \geq F$ $\exists \alpha \in \mathbb{R}_+$ such that $F = \alpha E$.

Proof. ($\Rightarrow$) Let $E \in \mathcal{E}(\mathcal{P}_{n,2d}), F \in \mathcal{P}_{n,2d}$ s.t $E \geq F$, then
$G := E - F \in \mathcal{P}_{n,2d}$, so $E = F + G$.
Since E is extremal $\exists\, \alpha, \beta \geq 0, \alpha + \beta = 1$ such that $F = \alpha E$ and $G = \beta E$.
($\Leftarrow$) Let $F_1, F_2 \in \mathcal{P}_{n,2d}$ so that $E = F_1 + F_2$, then $E \geq F_1$, so $\exists\, \alpha \geq 0$ such that
$F_1 = \alpha E$. Therefore $F_2 = E - F_1 = (1 - \alpha)E$ with $1 - \alpha \geq 0$ (since $E, F_2 \in \mathcal{P}_{n,2d}$).
Thus E is extremal. □

Corollary 2.9. Every $F \in \mathcal{P}_{n,2d}$ is a finite sum of forms in $\mathcal{E}(\mathcal{P}_{n,2d})$.

Proof. By Corollary 2.3 and Remark 1.13 (2). □

3. PROOF OF $\mathcal{P}_{3,4} = \sum_{3,4}$

Corollary 2.9 is the first main item in the proof of Hilbert's Theorem (Theorem 2.8 of lecture 6) for the ternary quartic case. The second main item is the following lemma (which will be proved in the next lecture):

Lemma 3.1. Let $T(x, y, z) \in \mathcal{P}_{3,4}$. Then $\exists$ a quadratic form $q(x, y, z) \neq 0$ s.t. $T \geq q^2$, i.e. $T - q^2$ is psd.

Theorem 3.2. $\mathcal{P}_{3,4} = \sum_{3,4}$

Proof. Let $F \in \mathcal{P}_{3,4}$. By Corollary 2.9,
$F = E_1 + \ldots + E_k$, where E_i is extremal in $\mathcal{P}_{3,4}$ for $i = 1, \ldots, k$.
Applying Lemma 3.1 to each E_i we get
$E_i \geq q_i^2$, for some quadratic form $q_i \neq 0$
Since E_i is extremal, by Lemma 2.8, we get
$q_i^2 = \alpha_i E_i$; for some $\alpha_i > 0$, $\forall\, i = 1, \ldots, k$
and so $E_i = \left(\frac{1}{\sqrt{\alpha_i}} q_i\right)^2$ and hence $F \in \sum_{3,4}$. □

POSITIVE POLYNOMIALS LECTURE NOTES (08: 06/05/10)

SALMA KUHLMANN

This lecture was held by Dr. Mickael Matusinski.

Contents

1. PROOF OF HILBERT'S THEOREM (Continued)

Theorem 1.1. (Recall Theorem 2.8 of lecture 6) (Hilbert) $\sum_{n,m} = \mathcal{P}_{n,m}$ iff

(i) $n = 2$ or

(ii) $m = 2$ or

(iii) $(n, m) = (3, 4)$.

In lecture 7 (Theorem 3.2) we showed the proof of (Hilbert's) Theorem 1.1 part (iii), i.e. for ternary quartic forms: $\mathcal{P}_{3,4} = \sum_{3,4}$ using generalization of Krein-Milman theorem (applied to our context), plus the following lemma:

Lemma 1.2. (3.1 of lecture 7) Let $T(x, y, z) \in \mathcal{P}_{3,4}$. Then $\exists$ a quadratic form $q(x, y, z) \neq 0$ s.t. $T \geq q^2$, i.e. $T - q^2$ is psd.

Proof. Consider three cases concerning the zero set of T.

<u>**Case 1.**</u> $T > 0$, i.e. T has no non trivial zeros.

Let

$$\phi(x, y, z) := \frac{T(x, y, z)}{(x^2 + y^2 + z^2)^2}, \forall\ (x, y, z) \neq 0.$$

Let $\mu := \inf_{\mathbb{S}^2} \phi \geq 0$, where $\mathbb{S}^2$ is the unit sphere.

Since $\mathbb{S}^2$ is compact and ϕ is continous, $\exists\ (a, b, c) \in \mathbb{S}^2$ s.t. $\mu = \phi(a, b, c) > 0$

Therefore $\forall\ (x, y, z) \in \mathbb{S}^2 :\ T(x, y, z) \geq \mu(x^2 + y^2 + z^2)^2$.

Claim: $T(x,y,z) \geq \mu(x^2+y^2+z^2)^2$ for all $(x,y,z) \in \mathbb{R}^3$.

Indeed, it is trivially true at the point $(0,0,0)$, and

for $(x,y,z) \in \mathbb{R}^3 \setminus \{0\}$ denote $N := \sqrt{x^2+y^2+z^2}$, then $\left(\frac{x}{N}, \frac{y}{N}, \frac{z}{N}\right) \in \mathbb{S}^2$, which implies that

$$T\left(\frac{x}{N}, \frac{y}{N}, \frac{z}{N}\right) \geq \mu \left(\left(\frac{x}{N}\right)^2 + \left(\frac{y}{N}\right)^2 + \left(\frac{z}{N}\right)^2\right)^2.$$

So, by homogeneity we get

$T(x,y,z) \geq \mu(x^2+y^2+z^2)^2 = \left(\sqrt{\mu}(x^2+y^2+z^2)\right)^2$, as claimed.

□(**Case1**)

<u>**Case 2.**</u> T has exactly one (nontrivial) zero.

By changing coordinates, we may assume w.l.o.g. that zero to be $(1,0,0)$, i.e. $T(1,0,0) = 0$.

Writing T as a polynomial in x one gets

$$T(x,y,z) = ax^4 + (b_1y + b_2z)x^3 + f(y,z)x^2 + 2g(y,z)x + h(y,z),$$

where f, g and h are binary quadratic, cubic and quartic forms respectively.

<u>Reducing T:</u> Since $T(1,0,0) = 0$ we get $a = 0$.

Further, suppose $(b_1,b_2) \neq (0,0)$, it $\Rightarrow \exists\, (y_0,z_0) \in \mathbb{R}^2$ s.t $b_1y_0 + b_2z_0 < 0$, then taking x big enough $\Rightarrow T(x_0,y_0,z_0) < 0$, a contradiction to $T \geq 0$. Thus $b_1 = b_2 = 0$ and therefore

$$T(x,y,z) = f(y,z)x^2 + 2g(y,z)x + h(y,z) \tag{1}$$

Next, clearly $h(y,z) \geq 0$ [since otherwise $T(0,y_0,z_0) = h(y_0,z_0) < 0$ for some $(y_0,z_0) \in \mathbb{R}^2$, a contradiction].

Also $f(y,z) \geq 0$, if not, say $f(y_0,z_0) < 0$ for some (y_0,z_0), then taking x big enough we get $T(x,y_0,z_0) < 0$, a contradiction.

Thus $f,h \geq 0$.

From (1) we can write:

$$fT(x,y,z) = (xf+g)^2 + (fh - g^2) \tag{2}$$

Claim: $fh - g^2 \geq 0$

If not, say $(fh-g^2)(y_0,z_0) < 0$ for some (y_0,z_0). Then there are two cases to be considered here:

Case (i): $f(y_0,z_0) = 0$. In this case we claim $g(y_0,z_0) = 0$ because if not then $T(x,y_0,z_0) = 2g(y_0,z_0)x + h(y_0,z_0) < 0$ and we take $|x_0|$ large enough so that $2g(y_0,z_0)x_0 + h(y_0,z_0) < 0$, a contradiction.

Case (ii): $f(y_0, z_0) > 0$, we take $|x_0|$ such that $x_0 f(y_0, z_0) + g(y_0, z_0) = 0$, then $fT(x_0, y_0, z_0) = (fh - g^2)(y_0, z_0) < 0$, a contradiction.

So our claim is established and $fh - g^2 \geq 0$.

Now the polynomial f is a psd binary form, thus by Lemma 1.3 below f is sum of two squares. Let us consider the two subcases:

Case 2.1. f is a perfect square. Then $f = f_1^2$, with $f_1 = by + cz$ for some $b, c \in \mathbb{R}$. Up to multiplication by a constant $(-c, b)$ is the unique zero of f_1 and so of f. Thus

$$(fh - g^2)(-c, b) = -(g(-c, b))^2 \leq 0$$

which is a contradiction unless $g(-c, b) = 0$ which means [1] that $f_1 \mid g$, i.e. $g(y, z) = f_1(y, z) g_1(y, z)$. Then from (2) we get

$$\begin{aligned} fT &\geq (xf + g)^2 \\ &= (xf_1{}^2 + f_1 g_1)^2 \\ &= f_1{}^2 (xf_1 + g_1)^2 \\ &= f(xf_1 + g_1)^2. \end{aligned}$$

Hence $T \geq (xf_1 + g_1)^2$ as required.

Case 2.2. $f = f_1^2 + f_2^2$, with f_1, f_2 linear in y, z.

Now $f_1 \not\equiv \lambda f_2$ [otherwise we are in **Case 2.1**]

i.e. f_1, f_2 don't have same non-trivial zeroes, otherwise they would be multiples of each other and f would be a perfect square. Hence $f > 0$.

Claim 1: $fh - g^2 > 0$

If not, i.e. if $\exists\ (y_0, z_0) \neq (0, 0)$ s.t. $(fh - g^2)(y_0, z_0) = 0$, then (y_0, z_0) could be completed to a zero $\left(-\dfrac{g(y_0, z_0)}{f(y_0, z_0)}, y_0, z_0 \right)$ of T, which contradicts our hypothesis that T has only 1 zero $(1, 0, 0)$. Thus $fh - g^2 > 0$.

Claim 2: $\dfrac{fh - g^2}{f^3}$ has a minimum $\mu > 0$ on the unit circle $\mathbb{S}^1$. (clear)

So, just as in **Case 1**,

$fh - g^2 \geq \mu f^3\ \forall\ (y, z) \in \mathbb{R}^2$.

$\Rightarrow fT \geq fh - g^2 \geq \mu f^3$, by (2)

$\Rightarrow T \geq \mu f^2 \geq (\sqrt{\mu} f)^2$, as claimed. □(**Case 2**)

---

[1] See (5) implies (2) of Theorem 4.5.1 in *Real Algebraic Geometry* by J. Bochnak, M. Coste, M.-F. Roy or (5) implies (2) of Theorem 12.7 in *Positive Polynomials and Sum of Squares* by M. Marshall.

<u>Case 3.</u> T has more than one zero.

Without loss of generality, assume $(1, 0, 0)$ and $(0, 1, 0)$ are two of the zeros of T.
As in case 2, reduction $\Rightarrow T$ is of degree at most 2 in x as well as in y and so we can write:

$$T(x, y, z) = f(y, z)x^2 + 2g(y, z)zx + z^2h(y, z),$$

where f, g, h are quadratic forms and $f, h \geq 0$.
And so

$$fT = (xf + zg)^2 + z^2(fh - g^2), \tag{3}$$

with $fh - g^2 \geq 0$ [Indeed, if $(fh - g^2)(y_0, z_0) < 0$ for some (y_0, z_0), then we must have case distinction as on bottom of page 2 i.e. $f(y_0, z_0) = 0$ or $f(y_0, z_0) > 0$].

Using Lemma 1.3 if f or h is a perfect square, then we get the desired result as in the **Case 2.1**. Hence we suppose f and h to be sum of two squares and again as before (as in **Case 2.2**) $f, h > 0$. We consider the following two possible subcases on $fh - g^2$:

<u>Case 3.1.</u> Suppose $fh - g^2$ has a zero $(y_0, z_0) \neq (0, 0)$.

Set $x_0 = -\dfrac{g(y_0, z_0)}{f(y_0, z_0)}$ and

$$T_1 := T(x + x_0z, y, z) = x^2f + 2xz(g + x_0f) + z^2(h + 2x_0g + x_0^2f) \tag{4}$$

Evaluating (3) at $(x + x_0z, y, z)$, we get

$$fT_1 = fT(x + x_0z, y, z) = \Big((x + x_0)f + zg\Big)^2 + z^2(fh - g^2), \tag{3$'$}$$

Multyplying (4) by f, we get

$$fT_1 = fT(x + x_0z, y, z) = x^2f^2 + 2xzf(g + x_0f) + z^2f(h + 2x_0g + x_0^2f) \tag{4$'$}$$

Now compare the coefficients of z^2 in $(3)'$ and $(4)'$ to get

$$(x_0f + g)^2 + (fh - g^2) = f(h + 2x_0g + x_0^2f),$$

i.e. $h + 2x_0g + x_0^2f = \dfrac{(fh - g^2) + (x_0f + g)^2}{f} \quad \forall\ (y, z) \neq (0, 0)$

In particular, $h + 2x_0g + x_0^2f$ is psd and has a zero, namely $(y_0, z_0) \neq (0, 0)$.

Thus $(h + 2x_0g + x_0^2f)$, being a psd quadratic in y, z, which has a nontrivial zero (y_0, z_0), is a perfect square [since by the arguments similar to **Case 2.2**, it cannot be a sum of two (or more) squares].

Say $(h + 2x_0g + x_0^2f) = h_1^2$, with $h_1(y, z)$ linear and $h_1(y_0, z_0) = 0$

Now $(g + x_0f)(y_0, z_0) = g(y_0, z_0) + x_0f(y_0, z_0) = 0$. So, $g + x_0f$ vanishes at every zero of the linear form h_1. Therefore, we have $g + x_0f = g_1h_1$ for some g_1.

So (from (4)), $T_1 = fx^2 + 2xzg_1h_1 + z^2h_1^2$
$= (zh_1 + xg_1)^2 + x^2(f - g_1^2)$

$\Rightarrow h_1^2T_1 = h_1^2(zh_1 + xg_1)^2 + x^2(h_1^2 f - (h_1g_1)^2)$
$= h_1^2(zh_1 + xg_1)^2 + x^2 \underbrace{(hf - g^2)}_{\geq 0}$

$\Rightarrow h_1^2T_1 \geq h_1^2(zh_1 + xg_1)^2$

$\Rightarrow T(x + x_0z, y, z) =: T_1 \geq (zh_1 + xg_1)^2$

By change of variables $(x \to x - x_0z)$, we get $T \geq$ a square of a quadratic form, as desired.

<u>Case 3.2.</u> Suppose $fh - g^2 > 0$ (i.e. $fh - g^2$ has no zero).

Then (as in **Case 2.2**), $\exists\, \mu > 0$ s.t $\dfrac{fh - g^2}{(y^2 + z^2)f} \geq \mu$ on $\mathbb{S}^1$

and so $fh - g^2 \geq \mu(y^2 + z^2)f \ \forall\, (y, z) \in \mathbb{R}^2$.

Hence, by (†)

$$fT = (xf + zg)^2 + z^2 \underbrace{(fh - g^2)}_{>0}$$
$$\geq z^2(fh - g^2)$$
$$\geq \mu z^2(y^2 + z^2)f,$$

giving as required

$$T \geq (\sqrt{\mu}zy)^2 + (\sqrt{\mu}z^2)^2$$

$\Rightarrow T \geq (\sqrt{\mu}z^2)^2$ □(**Case 3**)

This completes the proof of the Lemma 1.2. □□

Next we prove Theorem 1.1 part (i), i.e. for binary forms. This was also used as a helping lemma in the proof of above lemma:

Lemma 1.3. If f is a binary psd form of degree m, then f is a sum of squares of binary forms of degree $m/2$, that is, $\mathcal{P}_{2,m} = \sum_{2,m}$. In fact, f is sum of two squares.

Proof. If f is a binary form of degree m, we can write

$$f(x, y) = \sum_{k=0}^{m} c_k x^k y^{m-k};\ c_k \in \mathbb{R}$$

$$= y^m \sum_{k=0}^{m} c_k \left(\frac{x}{y}\right)^k,$$

where m is an even number and $c_m \neq 0$, since f is psd.

Without loss of generality let $c_m = 1$.

Put $g(t) = \sum_{k=0}^{m} c_k t^k$.

Over $\mathbb{C}$, $g(t) = \prod_{k=1}^{m/2} (t - z_k)(t - \bar{z}_k)$; $z_k = a_k + ib_k, a_k, b_k \in \mathbb{R}$

$$= \prod_{k=1}^{m/2} \left((t - a_k)^2 + b_k^2\right)$$

$$\Rightarrow f(x,y) = y^m g\left(\frac{x}{y}\right) = \prod_{k=1}^{m/2} \left((x - a_k y)^2 + b_k^2 y^2\right)$$

Then using iteratively the identity

$$(X^2 + Y^2)(Z^2 + W^2) = (XZ - YW)^2 + (YZ + XW)^2,$$

we obtain that $f(x,y)$ is a sum of two squares. □

Example 1.4. Using the ideas in the proof of above lemma, we write the binary form

$$f(x,y) = 2x^6 + y^6 - 3x^4y^2$$

as a sum of two squares:

Consider f written in the form

$$f(x,y) = y^6\left(2\left(\frac{x}{y}\right)^6 + 1 - 3\left(\frac{x}{y}\right)^4\right)$$

So, the polynomial $g(t) = 2t^6 - 3t^4 + 1$. This polynomial has double roots 1 and -1 and complex roots $\pm\frac{1}{\sqrt{2}}i$.

Thus

$$g(t) = 2(t-1)^2(t+1)^2(t^2 + \frac{1}{2}) = (t^2 - 1)^2(2t^2 + 1).$$

Therefore we have

$$f(x,y) = y^6 g\left(\frac{x}{y}\right) = (x^2 - y^2)^2(2x^2 + y^2) = 2x^2(x^2 - y^2)^2 + y^2(x^2 - y^2)^2$$

written as a sum of two squares. □

Next we prove Theorem 1.1 part (ii), i.e. for quadratic forms:

Lemma 1.5. If $f(x_1, \ldots, , x_n)$ is a psd quadratic form, then $f(x_1, \ldots, , x_n)$ is sos of linear forms, that is, $\mathcal{P}_{n,2} = \sum_{n,2}$.

Proof. If $f(x_1, \ldots, x_n)$ is a quadratic form, then we can write

$$f(x_1, \ldots, x_n) = \sum_{i,j=1}^{n} x_i a_{ij} x_j, \text{ where } A = [a_{ij}] \text{ is a symmetric matrix with } a_{ij} \in \mathbb{R}.$$

We have $f = X^T AX$, where $X^T = [x_1, \ldots x_n]$.
By the spectral theorem for Hermitian matrices, there exists a real orthogonal matrix S and a diagonal matrix $D = \operatorname{diag}(d_1, \ldots, d_n)$ such that $D = S^T AS$. Then

$$f = X^T S S^T A\, S S^T X = (S^T X)^T S^T A\ S\ (S^T X)$$

Putting $Y = [y_1, \ldots, y_n]^T = S^T X$, we get

$$f = Y^T S^T A\, S\, Y = Y^T D\ Y = \sum_{i=1}^{n} d_i {y_i}^2, d_i \in \mathbb{R}\ .$$

Since f is psd, we have $d_i \geq 0\ \forall\ i$, and so

$$f = \sum_{i=1}^{n} \left(\sqrt{d_i} y_i \right)^2,$$

Thus

$$f(x_1, \ldots, x_n) = \sum_{i=1}^{n} \left(\sqrt{d_i} (s_{1,i} x_1 + \ldots, s_{n,i} x_n) \right)^2,$$

that is, f is sos of linear forms. $\square$

POSITIVE POLYNOMIALS LECTURE NOTES (09: 10/05/10)

SALMA KUHLMANN

Contents

1. PROOF OF HILBERT'S THEOREM (Continued)

Theorem 1.1. (Recall) (Hilbert) $\sum_{n,m} = \mathcal{P}_{n,m}$ iff

(i) $n = 2$ or

(ii) $m = 2$ or

(iii) $(n, m) = (3, 4)$.

And in all other cases $\sum_{n,m} \subsetneq \mathcal{P}_{n,m}$.

Note that here m is necessarily even because a psd polynomial must have even degree (see Lemma 2.3 in lecture 6).

We have shown one direction ($\Leftarrow$) of Hilbert's Theorem (1.1 above), i.e. if $n = 2$ or $m = 2$ or $(n, m) = (3, 4)$, then $\sum_{n,m} = \mathcal{P}_{n,m}$. To prove the other direction we have to show that:

$$\textstyle\sum_{n,m} \subsetneq \mathcal{P}_{n,m} \text{ for all pairs } (n, m) \text{ s.t. } n \geq 3, m \geq 4 \ (m \text{ even}) \text{ with } (n, m) \neq (3, 4). \tag{1}$$

Hilbert showed (using algebraic geometry) that $\sum_{3,6} \subsetneq \mathcal{P}_{3,6}$ and $\sum_{4,4} \subsetneq \mathcal{P}_{4,4}$. This is a reduction of the general problem (1), indeed we have:

Lemma 1.2. If $\sum_{3,6} \subsetneq \mathcal{P}_{3,6}$ and $\sum_{4,4} \subsetneq \mathcal{P}_{4,4}$, then

$$\sum_{n,m} \subsetneq \mathcal{P}_{n,m} \text{ for all } n \geq 3, m \geq 4 \text{ and } (n,m) \neq (3,4), (m \text{ even}).$$

Proof. Clearly, given $F \in \mathcal{P}_{n,m} - \sum_{n,m}$, then $F \in \mathcal{P}_{n+j,\,m} - \sum_{n+j,\,m}$ for all $j \geq 0$.

Moreover, we **claim:** $F \in \mathcal{P}_{n,m} - \sum_{n,m} \Rightarrow x_1^{2i} F \in \mathcal{P}_{n,\,m+2i} - \sum_{n,\,m+2i}\ \forall\, i \geq 0$

Proof of claim: Assume for a contradiction that

for $i = 1$ $$x_1^2 F(x_1, \ldots, x_n) = \sum_{j=1}^{k} f_j^2(x_1, \ldots, x_n),$$

then L.H.S vanishes at $x_1 = 0$, so R.H.S also vanishes at $x_1 = 0$.

So $x_1 | f_j\ \forall\, j$, so $x_1^2 | f_j^2\ \forall\, i$. So, R.H.S is divisible by x_1^2. Dividing both sides by x_1^2 we get a sos representation of F, a contradiction since $F \notin \sum_{n,m}$. □

So we just need to show that: $\sum_{3,6} \subsetneq \mathcal{P}_{3,6}$, and $\sum_{4,4} \subsetneq \mathcal{P}_{4,4}$.

Hilbert described a method (non constructive) to produce counter examples in the 2 crucial cases, but no explicit examples appeared in literature for next 80 years. In 1967 Motzkin presented a specific example of a ternary sextic form that is positive semidefinite but not a sum of squares.

2. THE MOTZKIN FORM

Proposition 2.1. The Motzkin form

$$M(x, y, z) = z^6 + x^4y^2 + x^2y^4 - 3x^2y^2z^2 \in \mathcal{P}_{3,6} - \sum_{3,6}.$$

Proof. Using the arithmetic geometric inequality (Lemma 2.2 below) with $a_1 = z^6, a_2 = x^4y^2, a_3 = x^2y^4$ and $\alpha_1 = \alpha_2 = \alpha_3 = \frac{1}{3}$, clearly gives $M \geq 0$.

Degree arguments and exercise 3 of ÜB 6 from Real Algebraic Geometry course (WS 2009-10) gives M is not a sum of squares □

Lemma 2.2. (Arithmetic-geometric inequality I) Let $a_1, a_2, \ldots, a_n \geq 0$; $n \geq 1$. Then

$$\frac{a_1 + a_2 + \ldots + a_n}{n} \geq (a_1 a_2 \ldots a_n)^{\frac{1}{n}}.$$

Lemma 2.3. (Arithmetic-geometric inequality II) Let $\alpha_i \geq 0$, $a_i \geq 0$; $i = 1, \ldots, n$ with $\sum_{i=1}^{n} \alpha_i = 1$.Then

$$\alpha_1 a_1 + \ldots + \alpha_n a_n - a_1^{\alpha_1} \ldots a_n^{\alpha_n} \geq 0$$

(with equality iff all the x_i are equal).

Proof. Exercise 2 in ÜB 5.

3. ROBINSON'S METHOD (1970)

In 1970's R. M. Robinson gave a ternary sextic based on the method described by Hilbert, but after drastically simplifying Hilbert's original ideas. He used it to construct examples of forms in $\mathcal{P}_{4,4} - \sum_{4,4}$ as well as forms in $\mathcal{P}_{3,6} - \sum_{3,6}$.
This method is based on the following lemma:

Lemma 3.1. A polynomial $P(x, y)$ of degree at most 3 which vanishes at eight of the nine points $(x, y) \in \{-1, 0, 1\} \times \{-1, 0, 1\}$ must also vanish at the ninth point.

Proof. Assign weights to the following nine points:

$$w(x, y) = \begin{cases} 1 & , \text{ if } x, y = \pm 1 \\ -2 & , \text{ if } (x = \pm 1, y = 0) \text{ or } (x = 0, y = \pm 1) \\ 4 & , \text{ if } x, y = 0 \end{cases}$$

Define the weight of a monomial as:

$$w(x^k y^l) := \sum_{i=1}^{9} w(q_i) x^k y^l (q_i) \ , \ \text{ for } \ q_i \in \{-1, 0, 1\} \times \{-1, 0, 1\}$$

Define the weight of a polynomial $P(x, y) = \sum_{k,l} c_{k,l}\, x^k y^l$ as:

$$w(P) := \sum_{k,l} c_{k,l}\, w(x^k y^l)$$

Claim 1: $w(x^k y^l) = 0$ unless k and l are both strictly positive and even.

Proof of claim 1: Let us compute the monomial weights

- if $k = 0, l \geq 0$: then we have
$$w(x^k y^l) = 1 + (-1)^l + 1 + (-1)^l + (-2) + (-2)(-1)^l = 0$$
- if $l = 0, k \geq 0$: then similarly we have $w(x^k y^l) = 0$, and
- if $k, l > 0$: then we have
$$w(x^k y^l) = 1+(-1)^l+(-1)^k+(-1)^{k+l} = \begin{cases} 0, & \text{if either } k \text{ or } l \text{ is odd} \\ 4, & \text{otherwise} \end{cases}$$

□ (claim 1)

Claim 2: $w(P) = \sum_{i=1}^{9} w(q_i)P(q_i)$

Proof of claim 2:
$$w(P) := \sum_{k,l} c_{k,l}\, w(x^k y^l) = \sum_{k,l} c_{k,l} \sum_{i=1}^{9} w(q_i) x^k y^l (q_i)$$
$$= \sum_{i=1}^{9} w(q_i) \sum_{k,l} c_{k,l} x^k y^l (q_i) = \sum_{i=1}^{9} w(q_i)P(q_i)$$

□ (claim 2)

Now, claim 1 and definition of $w(P) \Rightarrow$ if $\deg(P(x, y)) \leq 3$ then $w(P) = 0$.

Also, from claim 2 we get:
$$P(1, 1)+P(1, -1)+P(-1, 1)+P(-1, -1)+(-2)P(1, 0)+(-2)P(-1, 0)+(-2)P(0, 1)+ (-2)P(0, -1) + 4P(0, 0) = 0$$

Now verify that if $P(x, y) = 0$ for any eight (of the nine) points, then we are left with $\alpha P(x, y) = 0$ (for some $\alpha \neq 0, \alpha = \pm 1, \pm 2$) at the ninth point. □

4. THE ROBINSON FORM

Theorem 4.1. Robinsons form $R(x, y, z) = x^6 + y^6 + z^6 - (x^4y^2 + x^4z^2 + y^4x^2 + y^4z^2 + z^4x^2 + z^4y^2) + 3x^2y^2z^2$ is psd but not a sos, i.e. $R \in \mathcal{P}_{3,6} - \sum_{3,6}$.

Proof. Consider the polynomial
$$P(x, y) = (x^2 + y^2 - 1)(x^2 - y^2)^2 + (x^2 - 1)(y^2 - 1) \quad (2)$$

Note that $R(x, y, z) = P_h(x, y, z) = z^6 P(x/z, y/z)$.

By our observation: P_h is psd iff P psd; P_h is sos iff P is sos, We shall show that $P(x, y)$ is psd but not sos.

Multiplying both sides of (2) by $(x^2 + y^2 - 1)$ and adding to (2) we get:

$$(x^2 + y^2)P(x, y) = x^2(x^2 - 1)^2 + y^2(y^2 - 1)^2 + (x^2 + y^2 - 1)^2(x^2 - y^2)^2 \tag{3}$$

From (3) we see that $P(x, y) \geq 0$, i.e. $P(x, y)$ is psd.

Assume $P(x, y) = \sum_j P_j(x, y)^2$ is sos

$\deg P(x, y) = 6$, so $\deg P_j \leq 3 \ \forall\ j$.

By (2) it is easy to see that $P(0, 0) = 1$ and $P(x, y) = 0$ for all other eight points $(x, y) \in \{-1, 0, 1\}^2 \setminus \{(0, 0)\}$, therefore every $P_j(x, y)$ must also vanish at these eight points.

Hence by Lemma 3.1 (above) it follows that: $P_j(0, 0) = 0 \ \forall\ j$.

So $P(0, 0) = 0$, which is a contradiction. □

Proposition 4.2. The quarternary quartic $Q(x, y, z, w) = w^4 + x^2y^2 + y^2z^2 + x^2z^2 - 4xyzw$ is psd, but not sos, i.e., $Q \in \mathcal{P}_{4,4} - \sum_{4,4}$.

Proof. The arithmetic-geometric inequality (Lemma 2.3) clearly implies $Q \geq 0$.

Assume now that $Q = \sum_j q_j^2$, $q_j \in \mathcal{F}_{4,2}$.

Forms in $\mathcal{F}_{4,2}$ can only have the following monomials:

$x^2, y^2, z^2, w^2, xy, xz, xw, yz, yw, zw$

If x^2 occurs in some of the q_j, then x^4 occurs in q_j^2 with positive coefficient and hence in $\sum q_j^2$ with positive coefficient too, but this is not the case.

Similarly q_j does not contain y^2 and z^2.

The only way to write x^2w^2 as a product of allowed monomials is $x^2w^2 = (xw)^2$.

Similarly for y^2w^2 and z^2w^2.

Thus each q_j involves only the monomials xy, xz, yz and w^2.

But now there is no way to get the monomial $xyzw$ from $\sum_j q_j^2$, hence a contradiction.

□

Proposition 4.3. The ternary sextic $S(x, y, z) = x^4y^2 + y^4z^2 + z^4x^2 - 3x^2y^2z^2$ is psd, but not a sos, i.e., $S \in \mathcal{P}_{3,6} - \sum_{3,6}$.

Proof. Exercise 3 of ÜB 5. □

POSITIVE POLYNOMIALS LECTURE NOTES (10: 18/05/10)

SALMA KUHLMANN

Contents

1. RING OF FORMAL POWER SERIES

Definition 1.1. (Recall) Let $S = \{g_1, \dots, g_s\} \subseteq \mathbb{R}[x_1, \dots, x_n]$, then

$\mathbf{K_S} := \{x \in \mathbb{R}^n \mid g_i(x) \geq 0 \ \forall\, i = 1, \dots, s\}$,

$\mathbf{T_S} := \Big\{ \sum_{e_1,\dots,e_s \in \{0,1\}} \sigma_e\, g_1^{e_1} \dots g_s^{e_s} \mid \sigma_e \in \Sigma\mathbb{R}[\underline{X}]^2, e = (e_1, \dots, e_s) \Big\}$ is the preordering generated by S.

Proposition 1.2. Let $n \geq 3$. Let S be a finite subset of $\mathbb{R}[\underline{x}]$ such that $K_S \subseteq \mathbb{R}^n$ has non empty interior. Then $\exists\, f \in \mathbb{R}[\underline{x}]$ such that $f \geq 0$ on $\mathbb{R}^n$ and $f \notin T_S$.

To prove proposition 1.2 we need to learn a few facts about formal power series rings:

Definition 1.3. $\mathbb{R}[\![\underline{x}]\!] := \mathbb{R}[\![x_1, \dots, x_n]\!]$ **ring of formal power series** in $\underline{x} = (x_1, \dots, x_n)$ with coefficients in $\mathbb{R}$, i.e. , $f \in \mathbb{R}[\![\underline{x}]\!]$ is expressible uniquely in the form

$f = f_0 + f_1 + \dots,$

where f_i is a homogenous polynomial of degree i in the variables $x_1, \dots, x_n$.
Here:

- Addition is defined point wise, and

- multiplication is defined using distributive law:

$$\Big(\sum_{i=0}^{\infty} f_i\Big)\Big(\sum_{i=0}^{\infty} g_i\Big) = (f_0g_0)+(f_0g_1+f_1g_0)+(f_0g_2+f_1g_1+f_2g_0)+\ldots = \sum_{k=0}^{\infty}\Big(\sum_{i+j=k}(f_ig_j)\Big)$$

So, both addition and multiplication are well defined and $\mathbb{R}[[\underline{x}]]$ is an integral domain and $\mathbb{R}[\underline{x}] \subseteq \mathbb{R}[[\underline{x}]]$.

Notation 1.4. Fraction field of $\mathbb{R}[[\underline{x}]]$ is denoted by

$$ff(\mathbb{R}[[\underline{x}]] := \mathbb{R}((\underline{x})).$$

The valuation $v : \mathbb{R}[[\underline{x}]] \to \mathbb{Z} \cup \{\infty\}$ defined by:

$$v(f) = \begin{cases} \text{least } i \text{ s.t. } f_i \neq 0 & \text{, if } f \neq 0 \\ \infty & \text{, if } f = 0 \end{cases}$$

extends to $\mathbb{R}((\underline{x}))$ via

$$v\left(\frac{f}{g}\right) := v(f) - v(g) \ .$$

Lemma 1.5. Let $f \in \mathbb{R}[[\underline{x}]]$; $f = f_k + f_{k+1} + \ldots$, where f_i homogeneous of degree i, $f_k \neq 0$. Assume that f is a sos in $\mathbb{R}[[\underline{x}]]$.
Then k is even and f_k is a sum of squares of forms of degree $\frac{k}{2}$.

Proof. $f = g_1^2 + \ldots + g_l^2$, and

$$g_i = g_{ij} + g_{i,j+1} + \ldots \text{, with } j = \min\{v(g_i)\ ;\ i = 1, \ldots, l\}$$

Then $f_0 = \ldots = f_{2j-1} = 0$ and $f_{2j} = \sum_{i=1}^{k} g_{ij}^2 \neq 0$

So, $k = 2j$. □

1.6. Units in $\mathbb{R}[[\underline{x}]]$: Let $f = f_0 + f_1 + \ldots$, with $v(f) = 0$ *i.e.* $f_0 \neq 0$. Then f factors as

$$f = a(1 + t);\ \text{ where}$$

$a \in R, a \neq 0, t \in \mathbb{R}[[\underline{x}]]$ and $v(t) \geq 1$ with $a := f_0 \in \mathbb{R} \setminus \{0\}$; $t := \frac{1}{f_0}(f_1 + f_2 + \ldots)$.

Lemma 1.7. $f \in \mathbb{R}[[\underline{x}]]$ is a unit of $\mathbb{R}[[\underline{x}]]$ if and only if $f_0 \neq 0$ (i.e. $v(f) = 0$).

Proof: $\dfrac{1}{1+t} = 1 - t + t^2 - \ldots$, for $t \in \mathbb{R}[[\underline{x}]]$; $v(t) \geq 1$

is a well defined element of $\mathbb{R}[\![\underline{x}]\!]$.

So, if $v(f) = 0$, then $f = a(1+t)$ with $a \in R, a \neq 0$ gives

$$f^{-1} = \frac{1}{a}\frac{1}{(1+t)} \in \mathbb{R}[\![\underline{x}]\!]. \qquad \square$$

Corollary 1.8. It follows that $\mathbb{R}[\![\underline{x}]\!]$ is a local ring because $I = \{f \mid v(f) \geq 1\}$ is a maximal ideal (quotient is a field $\mathbb{R}$).

Lemma 1.9. Let $f \in \mathbb{R}[\![\underline{x}]\!]$ a positive unit, i.e. $f_0 > 0$. Then f is a square in $\mathbb{R}[\![\underline{x}]\!]$.

Proof. $f = a(1+t); a > 0, v(t) \geq 1$

$$\sqrt{f} = \sqrt{a}\sqrt{1+t},$$

where $\sqrt{1+t} := (1+t)^{1/2} = 1 + \frac{1}{2}t - \frac{1}{8}t^2 + \ldots$ is a well defined element of $\mathbb{R}[\![\underline{x}]\!]$

$\square$

Lemma 1.10. Suppose $n \geq 3$. Then $\exists\, f \in \mathbb{R}[\underline{x}]$ such that $f \geq 0$ on $\mathbb{R}^n$ and f is not a sum of squares in $\mathbb{R}[\![\underline{x}]\!]$.

Proof. Let $f \in \mathbb{R}[\underline{x}]$ be any homogeneous polynomial which is ≥ 0 on $\mathbb{R}^n$ but is not a sum of squares in $\mathbb{R}[\underline{x}]$ (by Hilbert's Theorem such a polynomial exists).
Now by lemma 1.5 it follows that f is not sos in $\mathbb{R}[\![\underline{x}]\!]$. $\square$

Now we prove Proposition 1.2:

Proof of Proposition 1.2. Let $S = \{g_1, \ldots, g_s\}$

- W.l.o.g. assume $g_i \not\equiv 0$, for each $i = 1, \ldots, s$. So $g := \prod_{i=1}^{s} g_i \not\equiv 0$

$\mathrm{int}(K_S) \neq \emptyset \Rightarrow \exists\, \underline{p} := (p_1, \ldots, p_n) \in \mathrm{int}(K_S)$ with $\prod_{i=1}^{s} g_i(\underline{p}) \neq 0$.

Thus $g_i(\underline{p}) > 0\ \forall\, i = i, \ldots, s$.

- W.l.o.g. assume $p = \underline{0}$ the origin

(by making a variable change $Y_i := X_i - p_i$, and noting that
$$\mathbb{R}[Y_1, \ldots, Y_n] = \mathbb{R}[X_1, \ldots, X_n]\ )$$
So $g_i(0, \ldots, 0) > 0$ for each $i = i, \ldots, s$ (i.e. has positive constant term),
that means $g_i \in \mathbb{R}[\![\underline{X}]\!]$ is a positive unit in $\mathbb{R}[\![\underline{X}]\!]\ \forall\, i = 1, \ldots, s$.
By Lemma 1.9 (on positive units in power series): $g_i \in \mathbb{R}[\![\underline{X}]\!]^2\ \forall\, i = i, \ldots, s$.

So the preordering ${T_S}^A$ generated by $S = \{g_1, \ldots, g_s\}$ in the ring $A := \mathbb{R}[\![\underline{X}]\!]$ is just $\Sigma\mathbb{R}[\underline{X}]^2$.

Now using Lemma 1.10 : $\exists\ f \in \mathbb{R}[\underline{X}]$, $f \geq 0$ on $\mathbb{R}^n$ but f is not a sum of squares in $\mathbb{R}[\![\underline{X}]\!]$ (i.e. $f \notin \Sigma\mathbb{R}[\underline{X}]^2 = {T_S}^{\mathbb{R}[\![\underline{X}]\!]}$) .

So clearly $f \notin T_S$. □(Proposition 1.2)

Proposition 1.2 that we just proved is just a special case of the following result due to Scheiderer:

Theorem 1.11. Let S be a finite subset of $\mathbb{R}[\underline{X}]$ such that K_S has dimension ≥ 3. Then $\exists\ f \in \mathbb{R}[\underline{X}]; f \geq 0$ on $\mathbb{R}^n$ and $f \notin T_S$.

To prove this result we need:
(1) a reminder about dimension of semi algebraic sets, and
(2) more facts about non singular zeros.

2. ALGEBRAIC INDEPENDENCE

Let E/F be a field extension:

Definition 2.1. (1) $a \in E$ is **algebraic** over F if it is a root of some non zero polynomial $f(x) \in F[x]$, otherwise a is a **transcedental** over F.

(2) $A = \{a_1, \ldots, a_n\} \subseteq E$ is called **algebraically independent** over F if there is no nonzero polynomial $f(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]$ s.t. $f(a_1, \ldots, a_n) = 0$.
In general $A \subseteq E$ is algebraically independent over F if every finite subset of A is algebraic independent over F.

(3) A **transcendence base** of E/F is a maximal subset (w.r.t. inclusion) of E which is algebraically independent over F.

POSITIVE POLYNOMIALS LECTURE NOTES (11: 20/05/10)

SALMA KUHLMANN

Contents

1. ALGEBRAIC INDEPENDENCE AND TRANSCENDENCE DEGREE

Definition 1.1. (Recall) Let E/F be a field extension:

(1) $A \subseteq E$ is called **algebraically independent** over F if $\forall\ a_1, \ldots, a_n \in A$ there exists no nonzero polynomial $f \in F[x_1, \ldots, x_n]$ s.t. $f(a_1, \ldots, a_n) = 0$.

(2) $A \subseteq E$ is called a **transcendence basis** of E/F if A is a maximal subset (w.r.t. inclusion) of E which is algebraically independent over F.

Lemma 1.2. Let E/F be a field extension.

(1) (Steinitz exchange) $S \subseteq E$ is algebraically independent over F iff $\forall\ s \in S\ :\ s$ is transcendental over $F(S - \{s\})$ (the subfield of E generated by $S - \{s\}$).

(2) $S \subseteq E$ is a transcendence base for E/F iff S is algebraically independent over F and E is algebraic over $F(S)$. □

Proof. Exercise 1 of ÜB 6.

Theorem 1.3. The extension E/F has a transcendence base and any two transcendence bases of E/F have the same cardinality.

Proof. The existence follows by Zorn's lemma and the second statement uses the Steinitz exchange lemma (above). □

Definition 1.4. The cardinality of a transcendence base of E/F is called the **transcendence degree** of E/F, denoted by trdeg (E) over F.

2. KRULL DIMENSION OF A RING

Definition 2.1 Let A be a commutative ring with 1.

(1) A **chain** of prime ideals of A is of the form
$\{0\} \subseteq \wp_0 \subsetneq \wp_1 \subsetneq \ldots \subsetneq \wp_k \subsetneq \ldots \subsetneq A$, where $\wp_i$ are prime ideals of A.

(2) The **Krull dimension** of A, denoted by dim (A) is defined to be the maximum k such that there is a chain of prime ideals of length k in A, i.e. $\wp_0 \subsetneq \wp_1 \subsetneq \ldots \subsetneq \wp_k$ [dim(A) can be infinite if arbitrary long chains].

Theorem 2.2. Let F be a field and I be any prime ideal in $F[\underline{X}]$. Then

$$\dim\left(\frac{F[\underline{X}]}{I}\right) = \operatorname{trdeg}\left(ff\left(\frac{F[\underline{X}]}{I}\right)\right).$$

□

Recall 2.3. For $S \subseteq F^n$
$$\mathcal{I}(S) = \{f \in F[\underline{X}] \mid f(\underline{x}) = 0, \forall\ \underline{x} \in S\}$$
is the ideal of polynomials vanishing on S.

Definition 2.4. Dimension of semi-algebraic sets $\subseteq \mathbb{R}^n$: Let $K \subseteq \mathbb{R}^n$ be a semi-algebraic set. Then
$$\dim(K) := \dim\left(\frac{\mathbb{R}[\underline{X}]}{\mathcal{I}(K)}\right).$$

In the lecture 10 (Proposition 1.2) we have proved the following proposition:

Proposition 2.5. Suppose $n \geq 3$. Let $S = \{g_1, \ldots, g_s\}$ be a finite subset of $\mathbb{R}[\underline{X}]$ such that $K_S \subseteq \mathbb{R}^n$ and int$(K_S) \neq \emptyset$. Then there exists $f \in \mathbb{R}[\underline{X}]$ such that $f \geq 0$ on $\mathbb{R}^n$ and $f \notin T_S$.

This is just a special case of the following result due to Scheiderer:

Theorem 2.6. (Scheiderer) (Theorem 1.11 of lecture 10) Let S be a finite subset of $\mathbb{R}[\underline{X}]$ and $K_S \subseteq \mathbb{R}^n$ s.t. $\dim K_S \geq 3$. Then there exists $f \in \mathbb{R}[\underline{X}]$; $f \geq 0$ on $\mathbb{R}^n$ and $f \notin T_S$.

To deduce Proposition 2.5 using Theorem 2.6 it suffices to prove the following lemma:

Lemma 2.7. Let $K \subseteq \mathbb{R}^n$ be a semi algebraic subset. Then

$$\text{int}(K) \neq \phi \Rightarrow \dim(K) = \text{n}$$

Proof. We have $\dim(K) = \dim\left(\frac{\mathbb{R}[\underline{X}]}{\mathcal{I}(K)}\right)$, and

we **claim** that $\mathcal{I}(K) = \{0\}$:

$f \in \mathcal{I}(K) \Rightarrow f = 0$ on $K \Rightarrow f = 0$ on $\underbrace{\text{int}(K)}_{(\neq\phi)} \Rightarrow f$ vanishes on a nonempty open set $\Rightarrow f \equiv 0$ (by Remark 2.2 of lecture 2).

So, $\dim(K) = \dim(\mathbb{R}[\underline{X}]) = \text{trdeg}(\mathbb{R}(\underline{X}))$ over $\mathbb{R}$

$$= n$$

□

3. LOW DIMENSIONS

Proposition 3.1. Let $n = 2$, $K_S \subseteq \mathbb{R}^2$ and K_S contains a 2-dimensional affine cone. Then $\exists\, f \in \mathbb{R}[X, Y]$; $f \geq 0$ on $\mathbb{R}^2$; $f \notin T_S$.

Definition 3.2. (For $n = 1$) Let K be a basic closed semi algebraic subset of $\mathbb{R}$. Then K is a finite union of intervals.

The natural description S of K as basic closed semi algebraic subset is defined as

1. if $a \in \mathbb{R}$ is the smallest element of K, then take the polynomial $X - a \in S$
2. if $a \in \mathbb{R}$ is the greatest element of K, then take the polynomial $a - X \in S$
3. if $a, b \in K$, $a < b$, $(a, b) \cap K = \phi$, then take the polynomial $(X-a)(X-b) \in S$
4. no other polynomial should be in S.

Proposition 3.3. Let $K \subseteq \mathbb{R}$ be a basic closed semi algebraic subset and S is the natural description of K. Then $\forall\, f \in \mathbb{R}[X]$:

$$f \geq 0 \text{ on } K \Rightarrow f \in T_S,$$

i.e. for every basic semi algebraic subset K of $\mathbb{R}$, there exists a description S (namely the natural) so that T_S is saturated.

Proposition 3.4. Let $K \subseteq \mathbb{R}$ be a non-compact basic semi algebraic subset and S' be a description of K. Then

$$T_{S'} \text{ is saturated} \Leftrightarrow S' \supseteq S \text{ (up to a scalar multiple factor).}$$

Remark 3.5. Summarizing:

(1) $\dim(K_S) \geq 3 \Rightarrow T_S$ is not saturated.

(2) $\dim(K_S) = 2 \Rightarrow T_S$ can be or cannot be saturated (depending on the geometry of K and S).

(3) $\dim(K_S) = 1 \Rightarrow T_S$ can be or cannot be saturated [but depends on K and description S of K, if $n \geq 2$).

After all this discussion about positive polynomials, strictly positive polynomials, we now want to show **Schmüdgen's Positivstellensatz**:

Theorem 3.6. (Schmüdgen's Positivstellensatz) Let $S = \{g_1, \ldots, g_s\}$ be a finite subset of $\mathbb{R}[X_1, \ldots, X_n]$ and $K_S \subseteq \mathbb{R}^n$ be a compact basic closed semi algebraic set. And let $f \in \mathbb{R}[\underline{X}]$ s.t. $f > 0$ on K_S. Then $f \in T_S$.

Note that this holds for every finite description S of K.

To prove this we first need Representation Theorem (Stone-Krivine, Kadison-Dubois), which will be proved in the next lecture.

POSITIVE POLYNOMIALS LECTURE NOTES (12: 25/05/10)

SALMA KUHLMANN

Contents

1. SCHMÜDGEN'S POSITIVSTELLENSATZ

Theorem 1.1. (Recall 3.6 of lecture 11) Let $S = \{g_1, \ldots, g_s\}$ be a finite subset of $\mathbb{R}[X_1, \ldots, X_n]$ and $K_S \subseteq \mathbb{R}^n$ be a compact basic closed semi algebraic set. And let $f \in \mathbb{R}[\underline{X}]$ s.t. $f > 0$ on K_S. Then $f \in T_S$.

To prove this we first need Representation Theorem (Stone-Krivine, Kadison-Dubois):

2. REPRESENTATION THEOREM (STONE-KRIVINE, KADISON-DUBOIS)

Let A be a commutative ring with 1. Let

$$\chi := \mathrm{Hom}(A, \mathbb{R}) = \{\alpha \mid \alpha : A \to \mathbb{R}, \alpha \text{ ring homomorphism}\}.$$

Notation 2.1. If $M \subseteq A$ denote

$$\chi_M = \{\alpha \in \chi \mid \alpha(M) \subseteq \mathbb{R}_+\} .$$

Notation 2.2. For $a \in A$ define a map

$$\hat{a} : \chi \to \mathbb{R} \quad \text{by}$$
$$\hat{a}(\alpha) := \alpha(a)$$

Remark 2.3. (i) Let $M \subseteq A$, with notations 2.1 and 2.2 we see that

$$\begin{aligned}\chi_M &:= \{\alpha \in \chi | \, \alpha(M) \subseteq \mathbb{R}_+\} \\ &= \{\alpha \in \chi | \, \alpha(a) \geq 0, \forall \, a \in M\} \\ &= \{\alpha \in \chi | \, \hat{a}(\alpha) \geq 0, \forall \, a \in M\}\end{aligned}$$

So, χ_M is "the nonnegativity set" of M in χ.

Observation 2.4. $a \in M \Rightarrow \hat{a} \geq 0$ on χ_M, because if $\alpha \in \chi_M$, then $\hat{a}(\alpha) \geq 0$ (by definition).

Conversely, answer the question: for $a \in A$, if $\hat{a} > 0$ on $\chi_M \Rightarrow a \in M$?

Exkurs 2.5. One can view $\chi = \text{Hom}(A, \mathbb{R})$ as a topological subspace of (Sper A, spectral topology) as follows:

1. Embedding of $\text{Hom}(A, \mathbb{R})$ in Sper A :

   Consider the map defined by

$$\text{Hom}(A, \mathbb{R}) \to \text{Sper } A$$
$$\alpha \mapsto P_\alpha := \alpha^{-1}(\mathbb{R}_+),$$

   where (recall that) Sper(A):= $\{P \, ; \, P$ is an ordering of $A\}$.

   Then

   (i) this map is well defined i.e. $P_\alpha \subseteq A$ is an ordering.

   (ii) this map is injective : $\alpha \neq \beta \Rightarrow P_\alpha \neq P_\beta$.

   (iii) support(P_α) = $\ker \alpha$.

2. Topology on χ :

   Endow χ with a topology : for $a \in A$

$$\{u(\hat{a}) = \{\alpha \in \chi \mid \hat{a}(\alpha) > 0\}; a \in A\}$$

   is a sub-basis of open sets. Then

   (iv) for $a \in A$, the map $\hat{a} : \chi \to \mathbb{R}$ is continuos in this topology.

   (v) in fact this topology on χ is the weakest topology on χ for which $\hat{a}$ is continuous for all $a \in A$,
   i.e. if τ is any other topology on χ which makes all these maps $\hat{a}$ (for $a \in A$) continuous then τ has more open sets than this weakest topology (i.e. $u(\hat{a})$ lies in τ).

(vi) this topology is also the topology induced on χ via the embedding $\alpha \mapsto P_\alpha$ giving Sper A the spectral topology [just use the fact that $\hat{a}(\alpha) > 0 \Leftrightarrow a \notin -P_\alpha \Leftrightarrow a >_{P_\alpha} 0$. Spectral topology: $u(a) = \{P\ ;\ a \notin -P\} = \{P \mid a >_P 0\}$].

Now we are back to the question (in Observation 2.4): for $a \in A$, does $\hat{a} > 0$ on $\chi_M \Rightarrow a \in M$?

Yes under additional assumptions on the subset M that we shall now study:

3. PREPRIMES, MODULES AND SEMI-ORDERINGS IN RINGS

Let A be a commutative ring with 1 and $\mathbb{Q} \subseteq A$. Concept of preordering generalizes in two directions:

(i) Preprimes

(ii) Modules (special case: quadratic modules)

Definitions 3.1. (1) A **preprime** is a subset T of A such that

$$T + T \subseteq T;\ \ TT \subseteq T;\ \ \mathbb{Q}_+ \subseteq T.$$

(2) Let T be a preprime of A. $M \subseteq A$ is a T**-module** if

$$M + M \subseteq M;\ \ TM \subseteq M;\ \ 1 \in M \text{ (i.e. } T \subseteq M).$$

[Note that in particular, a preprime T is a T-module.]

(3) A preprime T of A is said to be **generating** if $T - T = A$.

[Note that if T is any preprime then $T - T$ is already a subring of A because

$(t_1 - t_2) + (t_3 - t_4) = (t_1 + t_3) - (t_2 + t_4)$

$(t_1 - t_2)(t_3 - t_4) = (t_1 t_3 + t_2 t_4) - (t_1 t_4 + t_2 t_3)$.]

Proposition 3.2. Every preordering T of A is a generating preprime.

Proof. (i) For $\frac{m}{n} \in \mathbb{Q} : \frac{m}{n} = \left(\frac{1}{n}\right)^2 mn = \underbrace{\frac{1}{n^2} + \ldots + \frac{1}{n^2}}_{\text{(mn-times)}}$

so $\mathbb{Q}_+ \subset T$.

(ii) For $a \in A$, $a = \left(\frac{1+a}{2}\right)^2 - \left(\frac{1-a}{2}\right)^2$.

So $A = T - T$. □

Definitions 3.3. (1) A **quadratic module** is a T-module over the preprime $T = \sum A^2$.

(2) A T-module M is **proper** if $(-1) \notin M$.

(3) A semi-ordering M is a **quadratic module** such that moreover

$$M \cup (-M) = A; \quad M \cap (-M) = \mathfrak{p} \text{ is a prime ideal in } A.$$

Proposition 3.4.
(a) Suppose T is a generating preprime and M is a maximal proper T-module, then $M \cup (-M) = A$.

(b) Suppose T is a preordering and M a maximal proper T-module then $\mathfrak{p} = M \cap (-M)$ is a prime ideal.

(c) Therefore: if T is a preordering and M is a maximal proper T-module then M is a semi-ordering.

Proof. Similar to proof in the preordering case
(a) Let $a \in A$, $a \notin M \cup (-M)$.
By maximality of M, we have:

$-1 \in (M + aT)$ and $-1 \in (M - aT)$.

Therefore, $-1 = s_1 + at_1$ and $-1 = s_2 - at_2$; for some $s_1, s_2 \in M$ and $t_1, t_2 \in T$.

This implies $-at_1 = 1 + s_1$ and $at_2 = 1 + s_2$.

So $-at_1t_2 = t_2 + s_1t_2$ and $at_2t_1 = t_1 + s_2t_1$.

So $0 = t_2 + t_1 + s_1t_2 + t_1s_2$.

So $-t_1 = t_2 + s_1t_2 + t_1s_2 \in M$.

Now since T is generating, so pick $t_3, t_4 \in T$ such that $a = t_3 - t_4$, then

$-1 = s_1 + at_1 = s_1 + (t_3 - t_4)t_1 = s_1 + t_1t_3 + t_4(-t_1) \in M$. This is a contradiction.

(b) $\mathfrak{p} = M \cap -M$.

Clearly $\mathfrak{p} + \mathfrak{p} \subseteq \mathfrak{p}, -\mathfrak{p} = \mathfrak{p}, 0 \in \mathfrak{p}, T\mathfrak{p} \subseteq \mathfrak{p}$.

Since $A = T - T \Rightarrow A\mathfrak{p} \subseteq \mathfrak{p}$. Thus $\mathfrak{p}$ is an ideal clearly.

So far we have only used that T is a generating preprime, to show that $\mathfrak{p}$ is a prime ideal we need that T is preordering:

Suppose $ab \in \mathfrak{p}, a \notin \mathfrak{p}$. Without loss of generality assume $a \notin M$.
Now this implies: $-1 \in M + aT$, so $-1 = s + at$; $s \in M, t \in T$
$\Rightarrow -b^2 = sb^2 + ab^2t \in M + \mathfrak{p} \subseteq M$.
Now since $b^2 \in T \subseteq M$, this implies $b^2 \in M \cap -M = \mathfrak{p}$.
So we are reduced to showing: $b^2 \in \mathfrak{p} \Rightarrow b \in \mathfrak{p}$.
Suppose $b^2 \in \mathfrak{p}, b \notin \mathfrak{p}$. Without loss of generality $b \notin M$.
Thus $-1 = s + bt$, for some $s \in M$ and $t \in T$.
So $1 + 2s + s^2 = (1 + s)^2 = (-bt)^2 = b^2t^2 \in \mathfrak{p} = M \cap -M$.
Thus $-1 = 2s + s^2 + \underbrace{(-b^2t^2)}_{(\in M)} \in M$, a contradiction since $-1 \notin M$.

(c) Clear. □

Our next aim is to show that under the additional assumption: "M is archimedian", then a maximal proper module M over a preordering is an ordering not just a semi-ordering. This is crucial in proof of Kadison-Dubois.

POSITIVE POLYNOMIALS LECTURE NOTES (13: 27/05/10)

SALMA KUHLMANN

Contents

1. ARCHIMEDEAN MODULES

Let A be a commutative ring, $\mathbb{Q} \subseteq A$, T a preprime.

Definition 1.1. Let M a T-module. M is **archimedean** if:

$$\forall\, a \in A, \exists\, N \geq 1, N \in \mathbb{Z}_+ \text{ s.t. } N + a, N - a \in M\ .$$

Proposition 1.2. Let T be a generating preprime, M a maximal proper T-module. Assume that M is archimedean. Then $\exists$ a uniquely determined $\alpha \in \mathrm{Hom}(A, \mathbb{R})$ s.t. $M = \alpha^{-1}(\mathbb{R}_+) = P_\alpha$.
(In particular, M is an ordering, not just a semi-ordering.)

Proof. Let $a \in A$, define:

cut $(a) = \{r \in \mathbb{Q} \mid r - a \in M\}$, this is an **upper cut** in $\mathbb{Q}$ (i.e. final segment of $\mathbb{Q}$) .

Claim 1: $\mathrm{cut}(a) \neq \emptyset$ and $\mathbb{Q} \backslash (\mathrm{cut}(a)) := \mathrm{L}(a) \neq \emptyset$, where $\mathrm{L}(a)$ is a **lower cut** in $\mathbb{Q}$.

Proof of claim 1. Since M is archimedean $\exists\, n \geq 1$ s.t. $n - a \in M$, so $\mathrm{cut}(a) \neq \emptyset$.

Also $\exists\, m \geq 1$ s.t. $(m + a) \in M$.

If $-(m + 1) - a \in M$, then adding we get $-1 \in M$, a contradiction (since M is proper). So we have $-(m + 1) - a \notin M$, which $\Rightarrow -(m + 1) \in Q \backslash (\mathrm{cut}(a)) = \mathrm{L}(a)$.
□(claim 1)

Now define a map $\alpha : A \longrightarrow \mathbb{R}$ by

$$\alpha(a) := \inf\,(\mathrm{cut}(a))$$

α is well-defined.

Claim 2: $\alpha(1) = 1,\ \alpha(M) \subseteq \mathbb{R}_+;\ \alpha(a \pm b) = \alpha(a) \pm \alpha(b)\ \forall\ a, b \in A$ and $\alpha(tb) = \alpha(t)\ \alpha(b)\ \forall\ t \in T, b \in A$.

This is left as an exercise.

Claim 3: $\alpha(ab) = \alpha(a)\ \alpha(b)\ \forall\ a, b \in A$

Proof of claim 3. T generating $\Rightarrow a = t_1 - t_2,\ t_1, t_2 \in T$

so, $\alpha(ab) = \alpha(t_1 b - t_2 b) = \alpha(t_1 a) - \alpha(t_2 b)$

$$= \alpha(t_1)\alpha(b) - \alpha(t_2)\alpha(b) \text{ [by claim 2]}$$
$$= (\alpha(t_1) - \alpha(t_2))\alpha(b) = \alpha(t_1 - t_2)\alpha(b) = \alpha(a)\alpha(b)\ .$$

□(claim 3)

Claim 4: $\alpha^{-1}(\mathbb{R}_+) = M$

Proof of claim 4. By Claim 2, $M \subseteq \alpha^{-1}(\mathbb{R}_+)$

so, by maximality of M and since $P_\alpha = \alpha^{-1}(\mathbb{R}_+)$ is an ordering it follows that $M = \alpha^{-1}(\mathbb{R}_+)$. □

Corollary 1.3. Let A be a commutative ring with 1, T an archimedean preprime, M a T-module, $-1 \notin M$ (i.e. M proper T-module). Then $\chi_M \neq \emptyset$.

Proof. Since T is archimedean, T is generating (because $a = (n + a) - n$, for $a \in A$) and M is a proper archimedean module (archimedean module because for an archimedean preprime T, every T-module is also archimedean). By Zorn's lemma extend M to a maximal proper archimedean module Q. Apply Proposition 1.2 to Q to get $\alpha \in \text{Hom}(A, \mathbb{R})$ such that $Q = \alpha^{-1}(\mathbb{R}_+)$. This implies $M \subseteq \alpha^{-1}(\mathbb{R}_+)$. So, $\alpha \in \chi_M$, which implies $\Rightarrow\ \chi_M \neq \emptyset$. □

2. Representation Theorem (Stone-Krivine, Kadison-Dubois)

The following corollary (to Proposition 1.2 and Corollary 1.3) answers the question raised in 2.4 of lecture 12:

Corollary 2.1. (Stone-Krivine, Kadison-Dubois) Let A be a commutative ring, T an archimedean preprime in A, M a proper T-module. Let $a \in A$ and

$$\hat{a} : \chi \to \mathbb{R} \quad \text{defined by}$$
$$\hat{a}(\alpha) := \alpha(a)$$

If $\hat{a} > 0$ on χ_M, then $a \in M$.

Proof. Assume $\hat{a} > 0$ on χ_M, i.e. $\hat{a}(\alpha) > 0 \; \forall \; \alpha \in \chi_M$.

To show: $a \in M$

- Consider $M_1 := M = aT$

  Since $\alpha(a) > 0 \; \forall \; \alpha \in \chi_M$, we have $\chi_{M_1} = \emptyset$ [because if $\alpha \in \chi_{M_1}$, then $\alpha(M_1) \subseteq \mathbb{R}_+$. So, $\alpha(-a) = -\alpha(a) \geq 0$. So, $\alpha(a) \leq 0$, but $\alpha \in \chi_M$ so $\alpha(a) > 0$, a contradiction].

  So (since M_1 is an archimedean T-module), we can apply Corollary 1.3 to M_1 to deduce that $-1 \in M_1$.

  Write $-1 = s - at \, , s \in M, t \in T$

  $\Rightarrow \; at - 1 = s \in M$ $\qquad (\star)$

- Consider $\sum := \{r \in \mathbb{Q} \mid r + a \in M\}$

  We **claim** that: $\exists \, \rho \in \sum; \; \rho < 0$

  Once the claim is established we are done (with the proof of corollary) because

  $a = \underbrace{(a+\rho)}_{\in M} + \underbrace{(-\rho)}_{\in M} \in M$.

  Proof of the claim: First observe that $\sum \neq \emptyset$ (since $\exists \, n \geq 1$ s.t $n + a \in T \subseteq M$, so $n \in \sum$).

  Now fix $r \in \sum$, $r \geq 0$ and fix an integer $k \geq 1$ s.t $(k - t) \in T$

  Write: $kr - 1 + ka = \underbrace{(k-t)}_{\in T}\underbrace{(r+a)}_{\in M} + \underbrace{(at-1)}_{\in M} + \underbrace{rt}_{\in M} \in M$

  Multiplying by $\dfrac{1}{k}$, we get

  $\left(r - \dfrac{1}{k}\right) + a \in M$, i.e. $\left(r - \dfrac{1}{k}\right) \in \sum$

  Repeating we eventually find $\rho \in \sum, \; \rho < 0$. □

Note 2.2. For a quadratic module $M \subseteq \mathbb{R}[\underline{X}]$, set

$$K_M := \{x \in \mathbb{R}^n \mid g(x) \geq 0 \; \forall \; g \in M\}.$$

Note that if $M = M_S$ with $S = \{g_1, \ldots, g_s\}$, then $K_S = K_M$.

We have the following corollaries to Corollary 2.1. (Stone-Krivine, Kadison-Dubois):

Corollary 2.3. (Putinar's Archimedean Positivstellensatz) Let $M \subseteq \mathbb{R}[\underline{X}]$ be an archimedean quadratic module. Then for each $f \in \mathbb{R}[\underline{X}]$:

$$f > 0 \text{ on } K_M \Rightarrow f \in M\,.$$

Corollary 2.4. Let $A = \mathbb{R}[\underline{X}]$ and $S = \{g_1, \ldots, g_s\}$. Assume that the finitely generated preordering T_S is archimedean. Then for all $f \in A$:

$$f > 0 \text{ on } K_S \Rightarrow f \in T_S\,.$$

Remark 2.5.

1. To apply the corollary we need a criterion to determine when a preordering (quadratic module) is archimedean.
2. T_S is archimedean $\Rightarrow$ for $f = \sum X_i^2$: $\exists\, N$ s.t. $N - f = N - \sum X_i^2 \in T_S$
   $\Rightarrow N - \sum X_i^2 \geq 0$ on K_S.
   $\Rightarrow K_S$ is bounded. Also K_S is closed.
   So T_S is archimedean implies K_S is compact.

POSITIVE POLYNOMIALS LECTURE NOTES (14: 01/06/10)

SALMA KUHLMANN

Contents

1. RINGS OF BOUNDED ELEMENTS

Let A be a commutative ring with 1, $\mathbb{Q} \subseteq A$ and M be a quadratic module $\subseteq A$.

Definition 1.1. Consider

$$B_M = \{a \in A \mid \exists\, n \in \mathbb{N} \text{ s.t. } n + a \text{ and } n - a \in M\},$$

B_M is called the **ring of bounded elements**, which are bounded by M.

Proposition 1.2.

(1) M is an archimedean module of A iff $B_M = A$.

(2) B_M is a subring of A.

(3) $\forall\, a \in A$, $a^2 \in B_M \Rightarrow a \in B_M$.

(4) More generally, $\forall\, a_1, \ldots, a_k \in A$, $\sum_{i=1}^{k} a_i^2 \in B_M \Rightarrow a_i \in B_M\ \forall\, i = 1, \ldots, k$.

Proof. (1) Clear.

(2) Clearly $\mathbb{Q} \subseteq B_M$ and B_M is an additive subgroup of A.
To show: $a, b \in B_M \Rightarrow ab \in B_M$
Using the identity

$$ab = \frac{1}{4}[(a+b)^2 - (a-b)^2],$$

we see that in order to show that B_M is closed under multiplication it is sufficient to show that: $\forall\, a \in A :\ a \in B_M \Rightarrow a^2 \in B_M$.

Let $a \in B_M$. Then $n \pm a \in M$ for some $n \in \mathbb{N}$. Now $n^2 + a^2 \in M$.

Also $2n(n^2 - a^2) = (n^2 - a^2)[(n + a) + (n - a)]$

$$\text{So, } (n^2 - a^2) = \frac{1}{2n}\Big[(n + a)(n^2 - a^2) + (n - a)(n^2 - a^2)\Big]$$
$$= \frac{1}{2n}\Big[(n + a)^2(n - a) + (n - a)^2(n + a)\Big] \in M.$$

So $(n^2 + a^2)$ and $(n^2 - a^2)$ both $\in M$. So by definition $a^2 \in B_M$. □ (2)

(3) Assume $a^2 \in B_M$. Say $n - a^2 \in M$, for $n \geq 1, n \in \mathbb{N}$, then use the identity:

$$(n \pm a) = \frac{1}{2}[(n - 1) + (n - a^2) + (a \pm 1)^2] \in M.$$

So, $a \in B_M$. □ (3)

(4) If $\sum a_i^2 \in B_M$. Say $(n - \sum a_i^2) \in M$, then

$$(n - a_i^2) = \Big(n - \sum a_i^2\Big) + \sum_{j \neq i} a_j^2 \in M.$$

So, $a_i^2 \in B_M$ and so by (3), $a_i \in B_M$. □ (4)

□

Corollary 1.3. Let M be a quadratic module of $\mathbb{R}[\underline{X}]$. Then M is archimedean iff there exists $N \in \mathbb{N}$ such that

$$N - \sum_{i=1}^{n} X_i^2 \in M$$

Proof. ($\Rightarrow$) Clear.

($\Leftarrow$) First note that $\mathbb{R}_+ \subseteq M$ so, $\mathbb{R} \subseteq B_M$ (B_M subring).

Also $N - \sum_{i=1}^{n} X_i^2$ and $N + \sum_{i=1}^{n} X_i^2 \in M$. Therefore by definition $\sum_{i=1}^{n} X_i^2 \in B_M$.

So (by Proposition 1.2) $X_1, \ldots, X_n \in B_M$. This implies $\mathbb{R}[X_1, \ldots, X_n] \subseteq B_M$ and so M is archimedean. □

2. SCHMÜDGEN'S POSITIVSTELLENSATZ

Theorem 2.1. Let $S = \{g_1, \ldots g_s\} \subseteq \mathbb{R}[\underline{X}]$. Assume that $K = K_S = \{\underline{x} \mid g_i(\underline{x}) \geq 0\}$ is compact. Then there exists $N \in \mathbb{N}$ such that

$$N - \sum_{i=1}^{n} X_i^2 \in T_S = T.$$

In particular T_S is an archimedean preordering (by Corollary 1.3) and thus $\forall f \in \mathbb{R}[\underline{X}]$: $f > 0$ on $K_S \Rightarrow f \in T_S$.

Proof. [Reference: Dissertation, Thorsten Wörmann]

- K compact $\Rightarrow$ K bounded $\Rightarrow$ $\exists\, k \in \mathbb{N}$ such that $\left(k - \sum_{i=1}^{n} X_i^2\right) > 0$ on K.
- By applying the Positivstellensatz to above we get: $\exists\, p, q \in T_S$ such that $p\left(k - \sum_{i=1}^{n} X_i^2\right) = 1 + q$. So, $p\left(k - \sum_{i=1}^{n} X_i^2\right)^2 = (1+q)(k - \sum_{i=1}^{n} X_i^2)$. So, $(1+q)\left(k - \sum_{i=1}^{n} X_i^2\right) \in T_S$.
- Set $T' = T + \left(k - \sum_{i=1}^{n} X_i^2\right)T$. By Corollary 1.3, T' is an archimedean preordering. Therefore $\exists\, m \in \mathbb{N}$ such that $(m-q) \in T'$; say: $m - q = t_1 + t_2\left(k - \sum_{i=1}^{n} X_i^2\right)$ for some $t_1, t_2 \in T$.
- So, $(m-q)(1+q) = t_1(1+q) + t_2\left(k - \sum_{i=1}^{n} X_i^2\right)(1+q) \in T_S$. So $(m-q)(1+q) \in T_S$.
- Adding

$$(m-q)(1+q) = mq - q^2 + m - q \in T_S, \tag{1}$$

$$\left(\frac{m}{2} - q\right)^2 = \frac{m^2}{4} + q^2 - mq \in T_S. \tag{2}$$

yields

$$\left(m + \frac{m^2}{4} - q\right) \in T_S. \tag{3}$$

- Multiplying L.H.S. of (3) by $k \in T_S$, and adding $\left(k - \sum_{i=1}^{n} X_i^2\right)(1+q) \in T_S$ and $q\left(\sum_{i=1}^{n} X_i^2\right) \in T_S$, yields

$$k\left(m + \frac{m^2}{4} - q\right) + \left(k - \sum_{i=1}^{n} X_i^2\right)(1+q) + q\left(\sum_{i=1}^{n} X_i^2\right) \in T_S$$

i.e. $km + k\frac{m^2}{4} + k - \sum_{i=1}^{n} X_i^2 \in T_S$

i.e. $k\left(\frac{m}{2} + 1\right)^2 - \sum_{i=1}^{n} X_i^2 \in T_S$

Set $N := k\left(\frac{m}{2} + 1\right)^2$. □

(End of Schmüdgen's Positivstellensatz)

2.2. Final Remarks on Schmüdgen's Positivstellensatz (SPSS):

1. **Corollary (Schmüdgen's Nichtnegativstellensatz):**
   $f \geq 0$ on $K_S \Rightarrow \forall\epsilon$ real, $\epsilon > 0 : f + \epsilon \in T_S$.

2. SPSS fails in general if we drop the assumption that "K is compact".

   For example:

   (i) Consider $n = 1$, $S = \{X^3\}$, then $K_S = [0, \infty)$ (noncompact). Take $f = X + 1$. Then $f > 0$ on K_S. Claim: $f \notin T_S$, indeed elements of T_S have the form $t_0 + t_1X^3$, where $t_0, t_1 \in \sum \mathbb{R}[X]^2$. We have shown before at the beginning of this course (in 2.4 of lecture 2) that non zero elements of this preordering either have even degree or odd degree ≥ 3.

   (ii) Consider $n \geq 2, S = \emptyset$, then $K_S = \mathbb{R}^n$. Take strictly positive versions of the Motzkin polynomial

   $$m(X_1, X_2) := 1 - X_1^2X_2^2 + X_1^2X_2^4 + X_1^4X_2^2,$$

   i.e. $m_\epsilon := m(X_1, X_2) + \epsilon$; $\epsilon \in \mathbb{R}_+$. Then $m_\epsilon > 0$ on $K_S = \mathbb{R}^2$, and it is easy to show that $m_\epsilon \notin T_S = \sum \mathbb{R}[\underline{X}]^2\ \forall\epsilon \in \mathbb{R}_+$.

3. SPSS fails in general for a quadratic module instead of a preordering. [Mihai Putinar's question answered by Jacobi + Prestel in Dissertation of T. Jacobi (Konstanz)]

4. SPSS fails in general if the condition "$f > 0$ on K_S" is replaced by "$f \geq 0$ on K_S".

   Example (Stengle): Consider $n = 1, S = \{(1 - X^2)^3\}$, $K_S = [-1, 1]$ compact. Take $f := 1 - X^2 \geq 0$ on K_S but $1 - X^2 \notin T_S$. (This example has already been considered at the beginning of this course in 2.4 of lecture 2).

5. PSS holds for any real closed field but not SPSS:

   Example: Let R be a non archimedean real closed field. Take $n = 1, S = \{(1 - X^2)^3\}$, then $K_S = [-1, 1]_R = \{x \in R \mid -1 \leq x \leq 1\}$. Take $f = 1 + t - X^2$, where $t \in R^{>0}$ is an infinitesimal element (i.e. $0 < t < \epsilon$, for every positive rational ϵ). Then $f > 0$ on K_S. We claim that $f \notin T_S$:

   Let v be the natural valuation on R. So $v(t) > 0$ for $t > 0$. Now suppose for a contradiction that $f \in T_S$. Then

   $$1 + t - X^2 = f = t_0 + t_1(1 - X^2)^3;\ t_0, t_1 \in \sum R[X]^2 \qquad (1)$$

   Let $t_i = \sum f_{ij}^2$; for $i = 0, 1$ and $f_{ij} \in R[X]$.

   Let $s \in R$ be the coefficient of the lowest value appearing in the f_{ij}, i.e. $v(s) = \min\{v(a) \mid a \text{ is coefficient of some } f_{ij}\}$.

   Case I. if $v(s) \geq 0$, then applying the residue map $\left(\theta_v \longrightarrow \overline{R} := \dfrac{\overline{\theta_v}}{\mathcal{I}_v};\right.$ defined by $x \longmapsto \overline{x}$, where θ_v is the valuation ring $\Big)$ to (1), we obtain

   $$1 - X^2 = \overline{t_0} + \overline{t_1}(1 - X^2)^3$$

   and since $\overline{t_i} = \sum \overline{f_{ij}}^2 \in \sum \mathbb{R}[X]^2; i = 0, 1$; we get a contradiction to Example 2.4 (ii) of Lecture 2.

   Case II. if $v(s) < 0$. Dividing f by s^2 and applying the residue map we obtain

   $$0 = \overline{\frac{t_0}{s^2}} + \overline{\frac{t_1}{s^2}}(1 - X^2)^3$$

   $\Big($Note that $v(s^2) = 2v(s)$ is $\min\{v(a)\}$; a is coefficient of some f_{ij}^2, i.e. $v(s^2) \leq v(a)$ for any coefficient a, so $\dfrac{f_{ij}^2}{s^2}$ has coefficients with value ≥ 0.$\Big)$

   So we obtain

   $$0 = t_0' + t_1'(1 - X^2)^3, \text{ with } t_0', t_1' \in \sum \mathbb{R}[X]^2 \text{ not both zero.}$$

   Since t_0', t_1' have only finitely many common roots in $\mathbb{R}$ and $1 - X^2 > 0$ on the finite set $(-1, 1)$, this is impossible. □(claim)

6. SPSS holds over archimedean real closed fields.

POSITIVE POLYNOMIALS LECTURE NOTES (15: 08/06/10)

SALMA KUHLMANN

Contents

1. SCHMÜDGEN'S NICHTNEGATIVSTELLENSATZ

1.1. Schmüdgen's Nichtnegativstellensatz (Recall 2.2.1 of lecture 14): Let K_S be a compact basic closed semi algebraic set and $f \in \mathbb{R}[\underline{X}]$. Then

$$f \geq 0 \text{ on } K_S \Rightarrow \forall \epsilon \text{ real}, \epsilon > 0 : f + \epsilon \in T_S.$$

Corollary 1.2. Let $K = K_S$ be a compact basic closed semi algebraic set and $L \neq 0$ be a linear functional $L : \mathbb{R}[\underline{X}] \longrightarrow \mathbb{R}$ with $L(r) = r \; \forall \; r \in \mathbb{R}$. Then

$$\underbrace{L(T_S) \geq 0}_{\text{(i.e. } L(f) \geq 0 \; \forall \; f \in T_S)} \quad \Rightarrow \quad \underbrace{L(\text{Psd}(K_S)) \geq 0}_{\text{(i.e. } L(f) \geq 0 \; \forall \; f \geq 0 \text{ on } K_S).}$$

Proof. W.l.o.g. $L(1) = 1, L \neq 0$. Let $f \in \text{Psd}(K_S)$ and assume $L(T_S) \geq 0$,

<u>To show:</u> $L(f) \geq 0$

By 1.1, $\forall \; \epsilon > 0 : f + \epsilon \in T_S$

So, $L(f + \epsilon) \geq 0$ i.e. $L(f) \geq -\epsilon \; \forall \; \epsilon > 0$ real

$\Rightarrow L(f) \geq 0.$ □

We shall now relate this to the problem of representation of linear functionals via integration along measures (i.e. $\int d\mu$).

2. APPLICATION OF SPSS TO THE MOMENT PROBLEM

Let $\mathcal{X}$ be a Hausdorff topological space.

Definition 2.1. $\mathcal{X}$ is **locally compact** if $\forall\ x \in \mathcal{X}\ \exists$ open $\mathcal{U}$ in $\mathcal{X}$ s.t. $x \in \mathcal{U}$ and $\overline{\mathcal{U}}$ (closure) is compact.

Notation 2.2. $\mathcal{B}^\delta(\mathcal{X})$:= set of Borel measurable sets in $\mathcal{X}$
= the smallest family of subsets of $\mathcal{X}$ containing all compact subsets of $\mathcal{X}$, closed under finite $\bigcup$, set theoretic difference $A \setminus B$ and countable $\bigcap$.

Definition 2.3. A **Borel measure** μ on $\mathcal{X}$ is a positive measure on $\mathcal{X}$ s.t. every set in $\mathcal{B}^\delta(\mathcal{X})$ is measurable. We also require our measure to be **regular** i.e. $\forall B \in \mathcal{B}^\delta(\mathcal{X})$ and $\forall\ \epsilon > 0\ \exists\ K, \mathcal{U} \in \mathcal{B}^\delta(\mathcal{X}), K$ compact, $\mathcal{U}$ open s.t. $K \subseteq B \subseteq \mathcal{U}$ and $\mu(K) + \epsilon \geq \mu(B) \geq \mu(\mathcal{U}) - \epsilon$.

2.4. Moment problem is the following:
Given a closed set $K \subseteq \mathbb{R}^n$ and a linear functional $L : \mathbb{R}[\underline{X}] \longrightarrow \mathbb{R}$
Question:

$$\text{when does } \exists \text{ a Borel measure } \mu \text{ on } K \text{ s.t. } \forall\ f \in \mathbb{R}[\underline{X}] : L(f) = \int f d\mu\ ? \qquad (1)$$

Necessary condition for (1): $\forall\ f \in \mathbb{R}[\underline{X}], f \geq 0$ on $K \Rightarrow L(f) \geq 0$ (2)

in other words: $L(\text{Psd}(K)) \geq 0$ (3)

Is this necessary condition also sufficient?
The answer is YES.

Theorem 2.5. (Haviland) Given $K \subseteq \mathbb{R}^n$ closed and $L : \mathbb{R}[\underline{X}] \longrightarrow \mathbb{R}$ a linear functional with $L(1) > 0$:

$$\exists\ \mu \text{ as in (1) iff } \forall\ f \in \mathbb{R}[\underline{X}] : L(f) \geq 0 \text{ if } f \geq 0 \text{ on } K,$$

i.e. (1) $\Leftrightarrow$ (2) $\Leftrightarrow$ (3).

We shall prove Haviland's Theorem later. For now we shall deduce a corollary to SPSS.

Corollary 2.6. Let $K_S = \{\underline{x} \mid g_i(\underline{x}) \geq 0; i = 1, \ldots, s\} \subseteq \mathbb{R}^n$ be a basic closed semi-algebraic set and compact, $L : \mathbb{R}[\underline{X}] \longrightarrow \mathbb{R}$ a linear functional with $L(1) > 0$. If $L(T_S) \geq 0$, then $\exists\, \mu$ positive Borel measure on K s.t. $L(f) = \int_{K_S} f d\mu \ \ \forall\, f \in \mathbb{R}[\underline{X}]$.

Remark 2.7. Let $S = \{g_1, \ldots, g_s\}$.

1. $L(T_S) \geq 0$ can be written as

$$L(h^2 g_1^{e_1} \ldots g_s^{e_s}) \geq 0 \ \forall\, h \in \mathbb{R}[\underline{X}], e_1, \ldots, e_s \in \{0, 1\}.$$

2. Compare Haviland to Schmüdgen's moment problem, for compact K_S: we do not need to check $L(\text{Psd}(K_S)) \geq 0$ we only need to check $L(T_S) \geq 0$.

3. Reformulation of question (1) (in 2.4) in terms of moment sequences:
Let $L : \mathbb{R}[\underline{X}] \longrightarrow \mathbb{R}$, with $L(1) = 1$. Consider $\{\underline{X}^{\underline{\alpha}} = X_1^{\alpha_1} \ldots X_n^{\alpha_n};\ \underline{\alpha} \in \mathbb{N}^n\}$ a monomial basis for $\mathbb{R}[\underline{X}]$. So L is completely determined by the (multi)sequence of real numbers $\tau(\underline{\alpha}) := L(\underline{X}^{\underline{\alpha}})$; $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ (i.e. $\tau : \mathbb{N}^n \longrightarrow \mathbb{R}$ is a function) and conversely, every such sequence determines a linear functional L :

$$L\Big(\sum_{\underline{\alpha}} a_{\underline{\alpha}} \underline{X}^{\underline{\alpha}}\Big) := \sum_{\underline{\alpha}} a_{\underline{\alpha}} L(\underline{X}^{\underline{\alpha}}).$$

So, (1) (in 2.4) can be reformulated as:
Given $K \subseteq \mathbb{R}^n$ closed, and a multisequence $\tau = \tau(\underline{\alpha})_{\underline{\alpha} \in \mathbb{N}^n}$ of real numbers, $\exists\, \mu$ positive borel measure on K s.t $\int \underline{X}^{\underline{\alpha}}\, d\mu = \tau_{\underline{\alpha}}$ for all $\underline{\alpha} \in \mathbb{N}^n$?

Definition 2.8. A function $\tau : \mathbb{N}^n \longrightarrow \mathbb{R}$ is a $K-$**moment sequence** if $\exists\, \mu$ positive borel measure on K s.t $\tau(\underline{\alpha}) = \int_K \underline{X}^{\underline{\alpha}}\, d\mu$ for all $\underline{\alpha} \in \mathbb{N}^n$

So (1) can be reformulated as: given K and a function $\tau : \mathbb{N}^n \longrightarrow \mathbb{R}$, when is τ a $K-$moment sequence?

Definition 2.9. A function $\tau : (\mathbb{Z}_+)^n \longrightarrow \mathbb{R}$ is called **psd** if

$$\sum_{i,j=1}^{m} \tau\, (\underline{k}_i + \underline{k}_j)\, c_i\, c_j \geq 0,$$

for $m \geq 1$, arbitrary distinct $\underline{k}_1, \ldots, \underline{k}_m \in (\mathbb{Z}_+)^n; c_1, \ldots, c_m \in \mathbb{R}$.

Definition 2.10. Given $\tau : (\mathbb{Z}_+)^n \longrightarrow \mathbb{R}$ a function and a fixed polynomial $g(\underline{X}) = \sum_{\underline{k} \in \mathbb{Z}_+^n} a_{\underline{k}} \underline{X}^{\underline{k}} \in \mathbb{R}[\underline{X}]$. Define a new function $g(E)_\tau : (\mathbb{Z}_+)^n \longrightarrow \mathbb{R}$ by $g(E)_\tau(\underline{l}) := \sum_{\underline{k} \in \mathbb{Z}_+^n} a_{\underline{k}} \tau(\underline{k} + \underline{l})$; for any $\underline{l} \in (\mathbb{Z}_+)^n$.

Lemma 2.11. Let $L : \mathbb{R}[\underline{X}] \to \mathbb{R}$ be a linear functional and denote by

$$\tau : (\mathbb{Z}_+)^n \to \mathbb{R}$$

the corresponding multisequence (i.e. $\tau(\underline{k}) := L(\underline{X}^{\underline{k}})\ \forall\ \underline{k} \in (\mathbb{Z}_+)^n$).
Fix $g \in \mathbb{R}[\underline{X}]$, $g(\underline{X}) = \sum_{\underline{k} \in \mathbb{Z}_+^n} a_{\underline{k}} \underline{X}^{\underline{k}} \in \mathbb{R}[\underline{X}]$. Then $L(h^2 g) \geq 0$ for all $h \in \mathbb{R}[\underline{X}]$ if and only if the multisequence $g(E)_\tau$ is psd.

POSITIVE POLYNOMIALS LECTURE NOTES (16: 10/06/10)

SALMA KUHLMANN

Contents

1. APPLICATION OF SPSS TO THE MOMENT PROBLEM (continued)

Lemma 1.1. (Lemma 2.11 of last lecture) Let $L : \mathbb{R}[\underline{X}] \to \mathbb{R}$ be a linear functional and denote by

$$\tau : (\mathbb{Z}_+)^n \to \mathbb{R}$$

the corresponding multisequence (i.e. $\tau(\underline{k}) := L(\underline{X}^{\underline{k}})\ \forall\ \underline{k} \in (\mathbb{Z}_+)^n$).
Fix $g \in \mathbb{R}[\underline{X}]$, $g(\underline{X}) = \sum_{\underline{k} \in \mathbb{Z}_+^n} a_{\underline{k}}\, \underline{X}^{\underline{k}} \in \mathbb{R}[\underline{X}]$. Then $L(h^2 g) \geq 0$ for all $h \in \mathbb{R}[\underline{X}]$ if and only if the multisequence $g(E)_\tau$ is psd.

Proof. Compute:

1. $L(\underline{X}^{\underline{l}} g) = \sum_{\underline{k} \in \mathbb{Z}_+^n} a_{\underline{k}} \tau(\underline{k} + \underline{l}) = g(E)_\tau(\underline{l})$; for all $\underline{l} \in (\mathbb{Z}_+)^n$.

Thus if $h = \sum_i c_i \underline{X}^{\underline{k}_i} \in \mathbb{R}[\underline{X}]$ then $h^2 = \sum_{i,j} c_i c_j \underline{X}^{\underline{k}_i + \underline{k}_j}$.

2. So, $L(h^2 g) = L\Big[\big(\sum_{i,j} c_i c_j \underline{X}^{\underline{k}_i+\underline{k}_j}\big) g\Big] = \sum_{i,j} c_i c_j L(\underline{X}^{\underline{k}_i+\underline{k}_j} g)$

$$\underbrace{=}_{\text{[by 1.]}} \sum_{i,j} g(E)_\tau(\underline{k}_i + \underline{k}_j) c_i c_j. \qquad \square$$

Theorem 1.2. (Schmüdgen's NNSS) (Reformulation in terms of moment sequences) Let $K = K_S$ compact, $S = \{g_1, \ldots, g_s\}$ and $\tau : (\mathbb{Z}^+)^n \to \mathbb{R}$ be a given multisequence. Then τ is a K-moment sequence if and only if the multisequences $(g_1^{e_1} \ldots g_s^{e_s})(E)_\tau : (\mathbb{Z}^+)^n \to \mathbb{R}$ are all psd for all $(e_1, \ldots, e_s) \in \{0, 1\}^s$. □

Next we reformulate question (1) in 2.4 of Lecture 15 in terms of Hankel matrices:

2. SCHMÜDGEN'S NNSS AND HANKEL MATRICES

We want to understand $L(h^2 g) \geq 0; h, g \in \mathbb{R}[\underline{X}]$ in terms of Hankel matrices.

Definition 2.1. A real symmetric $n \times n$ matrix A is **psd** if $\underline{x}^T A \underline{x} \geq 0 \; \forall \; \underline{x} \in \mathbb{R}^n$.
An $\mathbb{N} \times \mathbb{N}$ symmetric matrix (say) A is psd if $\underline{x}^T A \underline{x} \geq 0 \; \forall \; \underline{x} \in \mathbb{R}^n$ and $\forall \; n \in \mathbb{N}$.

Definition 2.2. Let $L \neq 0; L : \mathbb{R}[\underline{X}] \longrightarrow \mathbb{R}$ be a given linear functional. Fix $g \in \mathbb{R}[\underline{X}]$. Consider symmetric bilinear form:

$$\langle \; , \; \rangle_g : \mathbb{R}[\underline{X}] \times \mathbb{R}[\underline{X}] \to \mathbb{R}$$
$$\langle h, k \rangle_g := L(hkg) \; ; \; h, k \in \mathbb{R}[\underline{X}]$$

Denote by S_g the $\mathbb{N} \times \mathbb{N}$ symmetric matrix with $\alpha\beta$-entry $\langle \underline{X}^{\underline{\alpha}}, \underline{X}^{\underline{\beta}} \rangle_g \; \forall \; \underline{\alpha}, \underline{\beta} \in \mathbb{N}^n$, i.e. the $\alpha\beta$-entry of S_g is $L(\underline{X}^{\underline{\alpha}+\underline{\beta}} \, g)$.

Example. Let $g = 1$, then

$\langle \underline{X}^{\underline{\alpha}}, \underline{X}^{\underline{\beta}} \rangle_1 = L(\underline{X}^{\underline{\alpha}+\underline{\beta}}) := S_{\underline{\alpha}+\underline{\beta}}$.

More generally, if $g = \sum a_{\underline{\gamma}} \, \underline{X}^{\underline{\gamma}}$ then

$$\langle \underline{X}^{\underline{\alpha}}, \underline{X}^{\underline{\beta}} \rangle_g = L\Big(\sum_{\gamma} a_{\underline{\gamma}} \, \underline{X}^{\underline{\alpha}+\underline{\beta}+\underline{\gamma}} \Big) = \sum_{\underline{\gamma}} a_{\underline{\gamma}} \, S_{\underline{\alpha}+\underline{\beta}+\underline{\gamma}} \; .$$

Proposition 2.3. Let L, g be fixed as above. Then the following are equivalent:

1. $L(\sigma g) \geq 0 \; \forall \; \sigma \in \sum \mathbb{R}[\underline{X}]^2$.
2. $L(h^2 g) \geq 0 \; \forall \; h \in \mathbb{R}[\underline{X}]$.
3. $\langle \; , \; \rangle_g$ is psd.
4. S_g is psd.

Proof. (1) $\Leftrightarrow$ (2) is clear.
Since $\langle h, h \rangle_g = L(h^2 g)$, (2) $\Leftrightarrow$ (3) is clear.
(3) $\Leftrightarrow$ (4) is also clear. □

2.4. Example. (Hamburger) Let $n = 1$. A linear functional $L : \mathbb{R}[X] \to \mathbb{R}$ comes from a Borel measure on $\mathbb{R}$ if and only if $L(\sigma) \geq 0$ for every $\sigma \in \sum \mathbb{R}[X]^2$.

Proof. From Haviland we know L comes from a Borel measure iff $L(f) \geq 0$ for every $f(X) \in \mathbb{R}[X], f \geq 0$ on $\mathbb{R}$. But $\mathrm{Psd}(\mathbb{R}) = \sum \mathbb{R}[X]^2$ (by exercise in Real Algebraic Geometry course in WS 2009-10). So the condition is clear. □

Remark 2.5. We can express Hamburgers's Theorem via Hankel matrix S_g with $g = 1$ the constant polynomial.
$n = 1$, so (for $i, j \in \mathbb{N}$) the ij th coefficient of S_1 is $s_{i+j} = L(X^{i+j})$.

Hence, $S_1 = \begin{pmatrix} s_0 & s_1 & s_2 & \dots \\ s_1 & s_2 & \dots & \\ & & \ddots & \\ s_2 & \dots & & \\ \dots & \dots & & \end{pmatrix}$ is psd.

2.1. REFORMULATION OF SCHMÜDGEN'S SOLUTION TO THE MOMENT PROBLEM IN TERMS OF HANKEL MATRICES

2.6. Let $S = \{g_1, \dots, g_s\} \subseteq \mathbb{R}[\underline{X}]$ and $K_S \subseteq \mathbb{R}^n$ is compact. A linear functional L on $\mathbb{R}[\underline{X}]$ is represented by a Borel measure on K iff the 2^S $\mathbb{N} \times \mathbb{N}$ Hankel matrices $\{S_{g_1^{e_1} \dots g_s^{e_s}} | (e_1, \dots, e_s) \in \{0, 1\}^s\}$ are psd, where $S_g := [L(\underline{X}^{\underline{\alpha}+\underline{\beta}} g)]_{\underline{\alpha},\underline{\beta}}$; $\underline{\alpha}, \underline{\beta} \in \mathbb{N}^n$.

3. FINITE SOLVABILITY OF THE K- MOMENT PROBLEM

Definition 3.1. Let K be a basic closed semi-algebraic subset of $\mathbb{R}^n$.

1. The K-moment problem (**KMP**) is **finitely solvable** if there exists S finite, $S \subseteq \mathbb{R}[\underline{X}]$ such that:
   (i) $K = K_S$, and
   (ii) $\forall$ linear functional L on $\mathbb{R}[\underline{X}]$ we have: $L(T_S) \geq 0 \Rightarrow L(\mathrm{Psd}(K)) \geq 0$ (equivalently, (iii) $L(T_S) \geq 0 \Rightarrow \exists\, \mu : L = \int d\mu$).
2. We shall say S **solves the KMP** if (i) and (ii) (equivalently (i) and (iii)) hold.

3.2. Schmüdgen's solution to the KPM for K compact b.c.s.a. Let $K \subseteq \mathbb{R}^n$ be a compact basic closed semi-algebraic set. Then S solves the KMP for any finite description S of K (i.e. for all finite $S \subseteq \mathbb{R}[\underline{X}]$ with $K = K_S$).

One can restate the condition "S solves the K-Moment problem" via the equality of two preorderings. We shall adopt this approach throughout:

Definition 3.3. Let $T_S \subseteq \mathbb{R}[\underline{X}]$ be a preordering. Define the **dual cone** of T_S:

$$T_S^{\vee} := \{L \mid L : \mathbb{R}[\underline{X}] \to \mathbb{R} \text{ is a linear functional}; L(T_S) \geq 0\},$$

and the **double dual cone**:

$$T_S^{\vee\vee} := \{f \mid f \in \mathbb{R}[\underline{X}]; L(f) \geq 0 \ \forall\ L \in T_S^{\vee}\}.$$

Lemma 3.4. For $S \subseteq \mathbb{R}[\underline{X}]$, S finite:

(a) $T_S \subseteq T_S^{\vee\vee}$

(b) $T_S^{\vee\vee} \subseteq \text{Psd}\,(K_S)$.

Proof. (a) Immediate by definition.

(b) Let $f \in T_S^{\vee\vee}$. To show: $f(\underline{x}) \geq 0 \ \forall\ \underline{x} \in K_S$.

Now every $\underline{x} \in \mathbb{R}^n$ determines an $\mathbb{R}$-algebra homomorphism

$$e_{v_x} := L_{\underline{x}} \in \text{Hom}(\mathbb{R}[\underline{X}], \mathbb{R});\ L_{\underline{x}}(g) = e_{v_x}(g) := g(\underline{x}) \ \forall\ g \in \mathbb{R}[\underline{X}],$$

this $L_{\underline{x}}$ is in particular a linear functional.

Moreover we claim that $L_{\underline{x}}(T_S) \geq 0$ for $\underline{x} \in K_S$. Indeed if $g \in T_S$ then $L_{\underline{x}}(g) = g(\underline{x}) \geq 0$ for $\underline{x} \in K_S$.

So, by assumption on f we must also have $L_{\underline{x}}(f) \geq 0$ for $\underline{x} \in K_S$, i.e. $f(\underline{x}) \geq 0$ for all $\underline{x} \in K_S$ as required.

□

We summarize as follows:

Corollary 3.5. For finite $S \subseteq \mathbb{R}[\underline{X}]$:

$$T_S \subseteq T_S^{\vee\vee} \subseteq \text{Psd}(K_S).$$

Corollary 3.6. (Reformulation of finite solvability) Let $K \subseteq \mathbb{R}^n$ be a b.c.s.a. set and $S \subseteq \mathbb{R}[\underline{X}]$ be finite. Then S solves the KMP iff

(j) $K = K_S$, and

(jj) $T_S^{\vee\vee} = \text{Psd}(K)$.

Proof. Assume (ii) of definition 3.1, i.e. $\forall\, L : L(T_S) \geq 0 \Rightarrow L(\text{Psd}(K)) \geq 0$, and show (jj) i.e. $T_S^{\vee\vee} = \text{Psd}(K)$:
Let $f \in \text{Psd}(K)$. Show $f \in T_S^{\vee\vee}$ i.e. show $L(f) \geq 0\ \forall\, L \in T_S^{\vee}$.
Assume $L(T_S) \geq 0$. Then by assumption $L(\text{Psd}(K)) \geq 0$. So, $L(f) \geq 0$ as required.

Conversely, assume (jj) and show (ii):
Let $L(T_S) \geq 0$, i.e. $L \in T_S^{\vee}$. Show $L(\text{Psd}(K)) \geq 0$, i.e show $L(f) \geq 0\ \forall\, f \in \text{Psd}(K)$.
Now [by assumption (jj)] $f \in \text{Psd}(K) \Rightarrow f \in T_S^{\vee\vee} \Rightarrow L(f) \geq 0\ \forall\, L \in T_S^{\vee}$. □

We shall come back later to $T_S^{\vee\vee}$ and describe it as closure w.r.t. an appropriate topology.

4. HAVILAND'S THEOREM

For the proof of Haviland's theorem (2.5 of lecture 15), we will recall Riesz Representation Theorem.

Definition 4.1. A topological space is said to be **Hausdorff** (or **seperated**) if it satisfies
(H4): any two distinct points have disjoint neighbourhoods, or
(T_2): two distinct points always lie in disjoint open sets.

Definition 4.2. A topological space χ is said to be **locally compact** if $\forall\, x \in \chi\ \exists$ an open neighbourhood $\mathcal{U} \ni x$ such that $\overline{\mathcal{U}}$ is compact.

Theorem 4.3. (Riesz Representation Theorem) Let χ be a locally compact Hausdorff space and $L : \text{Cont}_c(\chi, \mathbb{R}) \to \mathbb{R}$ be a positive linear functional i.e. $L(f) \geq 0\ \forall\, f \geq 0$ on χ. Then there exists a unique (positive regular) Borel measure μ on χ such that $L(f) = \int_\chi f d\mu\ \ \forall\, f \in \text{Cont}_c(\chi, \mathbb{R})$, where $\text{Cont}_c(\chi, \mathbb{R}) :=$ the ring ($\mathbb{R}$-algebra) of all continuous functions $f : \chi \to \mathbb{R}$ (addition and multiplication defined pointwise) with compact support i.e. such that the set $\text{supp}(f) := \{x \in \chi : f(x) \neq 0\}$ is compact.

Definition 4.4. L **positive** means:

$$L(f) \geq 0\ \forall\, f \in \text{Cont}_C(\chi, \mathbb{R}) \text{ with } f \geq 0 \text{ on } \chi.$$

POSITIVE POLYNOMIALS LECTURE NOTES (17: 15/06/10)

SALMA KUHLMANN

Contents

1. HAVILAND'S THEOREM (continued)

Recall Theorem 4.3 of last lecture:

Theorem 1.1. Riesz Representation Theorem:
Let χ be a locally compact Hausdorff space and $L : \mathrm{Cont}_c(\chi, \mathbb{R}) \to \mathbb{R}$ be a positive linear functional i.e. $L(f) \geq 0\ \forall f \geq 0$ on χ. Then there exists a unique (positive regular) Borel measure μ on χ such that $L(f) = \int\limits_{\chi} f d\mu \quad \forall\ f \in \mathrm{Cont}_c(\chi, \mathbb{R})$, where $\mathrm{Cont}_c(\chi, \mathbb{R})$:= the ring ($\mathbb{R}$-algebra) of all continuous functions $f : \chi \to \mathbb{R}$ (addition and multiplication defined pointwise) with compact support i.e. such that the set $\mathrm{supp}(f) := \{x \in \chi : f(x) \neq 0\}$ is compact. □

We shall use theorem 1.1 to prove the following general result. Haviland's theorem (2.5 of lecture 15) will follow as a special case.

Theorem 1.2. Let A be an $\mathbb{R}$-algebra, χ a Hausdorff space and $\hat{}: A \to \mathrm{Cont}_c(\chi, \mathbb{R})$ an $\mathbb{R}$ algebra homomorphism. Assume $\exists\ p \in A$ such that $\hat{p} \geq 0$ on χ and $\forall\ k \in \mathbb{N} :\ \chi_k := \{\alpha \in \chi \mid \hat{p}(\alpha) \leq k\}$ is compact. . . . ($\star$)
Then for any linear functional $L : A \to \mathbb{R}$ satisfying $\forall\ a \in A : \hat{a} \geq 0$ on $\chi \Rightarrow L(a) \geq 0$, $\exists$ a Borel measure μ on χ such that $L(a) = \int\limits_{\chi} \hat{a}\ d\mu\ \forall\ a \in A$.

1.3. Remarks before proof.

1. ($\star$) implies in particular that χ is locally compact (i.e. $\forall\ x \in \chi :\ \exists$ an open neighbourhood $\mathcal{U} \ni x$ such that $\overline{\mathcal{U}}$ is compact).

Proof. Let $x \in \chi$, fix $k \geq 1$ s.t. $\hat{p}(x) < k$

Set $\mathcal{U}_k := \{y \in \chi \mid \hat{p}(y) < k\}$

$\subseteq \{y \in \chi \mid \hat{p}(y) \leq k\} = \chi_k$

$\mathcal{U}_k$ is open , $x \in \mathcal{U}_k$; $\overline{\mathcal{U}_k} \subseteq \chi_k$; so $\overline{\mathcal{U}_k}$ is compact.

[$\chi_k = \hat{p}^{-1}((-\infty, k])$ being inverse image of closed set under continuous map is closed but not necessarily compact, and $\mathcal{U}_k = \hat{p}^{-1}((-\infty, k))$ being inverse image of open set under continuous map is open.] □

2. Haviland's Theorem is a corollary (to Theorem 1.2) if we set $\chi = K$ closed subset of $\mathbb{R}^n, A = \mathbb{R}[\underline{X}]$, and

$$\hat{} : \mathbb{R}[\underline{X}] \to \mathrm{Cont}(K, \mathbb{R});$$

$$f \mapsto \hat{f} \text{ (restriction of the polynomial function f to } K)$$

$\hat{p}(x) = \sum x_i^2 = ||\underline{x}||^2, \chi_k$ compact.

1.4. *Proof of Theorem 1.2.* Set $C(\chi) = \mathrm{Cont}(\chi, \mathbb{R})$ and $C_c(\chi) = \mathrm{Cont}_c(\chi, \mathbb{R})$.
Let $\hat{A} := \{\hat{a} \mid a \in A\}$ (the image under the $\mathbb{R}$-algebra homomorphism $\hat{}$ is a subalgebra).
Define $\mathcal{B}(\chi) \subseteq C(\chi)$ to be the following subalgebra of $C(\chi)$:

$$\mathcal{B}(\chi) := \{f \in C(\chi) \mid \exists\, a \in A : |f| \leq |\hat{a}| \text{ on } \chi\}.$$

Observe that $\mathcal{B}(\chi)$ is a subalgebra of $C(\chi)$ and $\hat{A} \subseteq \mathcal{B}(\chi) \subseteq C(\chi)$.

Claim 1: $C_c(\chi) \subseteq \mathcal{B}(\chi)$

Proof of Claim 1. Let $f \in C_c(\chi)$, f continuous and $\overline{\{x \in \chi : f(x) \neq 0\}}$ compact subset. Then $|f| \leq k$, for some $k \in \mathbb{N}; k \in A$, i.e. $|f| \leq \hat{k}$ on χ.
So $C_c(\chi) \subseteq \mathcal{B}(\chi)$ as claimed i.e. $C_c(\chi)$ is a subalgebra of $\mathcal{B}(\chi)$. □(Claim 1)

Let now as in the hypothesis of the theorem:
$L : A \to \mathbb{R}$ with $L(a) \geq 0$ if $\hat{a} \geq 0$ on $\chi, \forall\, a \in A$.

We define $\bar{L} : \hat{A} \to \mathbb{R}$, by $\bar{L}(\hat{a}) := L(a)$.

Claim 2: $\bar{L}$ is a well defined linear function.

Proof of Claim 2. Since $\bar{L}(\hat{a} + \hat{b}) = \bar{L}(\widehat{a+b}) = L(a + b)$, so it is enough to prove that: $\hat{a} = 0 \Rightarrow L(a) = 0$

Now $\hat{a} \geq 0 \Rightarrow L(a) \geq 0$, and $-\hat{a} \geq 0 \Rightarrow -L(a) = L(-a) \geq 0$; (together) $\Rightarrow L(a) = 0$. □(Claim 2)

Claim 3: $\bar{L}$ extends to a linear map:

$$\bar{L} : \mathcal{B}(\chi) \to \mathbb{R} \text{ with } \bar{L}(f) \geq 0 \text{ for } f \geq 0 \text{ on } \chi.$$

Proof of Claim 3. We use Zorn's lemma to prove this:
Consider the collection of all pairs $(B, \bar{L})$, where B is a $\mathbb{R}-$subspace of $\mathcal{B}(\chi)$ containing $\hat{A}$ and $\bar{L}$ is an extension of $\bar{L}$ (on A) with the property:

$$\forall\ f \in B : f \geq 0 \text{ on } \chi\ \Rightarrow \bar{L}(f) \geq 0 \qquad \ldots(\dagger)$$

and consider a partial order: $(B_1, \bar{L}_1) \subseteq (B_2, \bar{L}_2) :\Leftrightarrow B_1 \subseteq B_2$ and $\bar{L}_2|_{B_1} := \bar{L}_1$.

- this collection is nonempty since $(\hat{A}, \bar{L})$ belongs to it : $\hat{a} \geq 0$ on $\chi \Rightarrow \bar{L}(\hat{a}) = L(a) \geq 0$ (by definition)
- every chain has an upper bound
- Let $(B, \bar{L})$ be a maximal element.
  Subclaim: we claim that $B = \mathcal{B}(\chi)$
  Otherwise let $g \in \mathcal{B}(\chi) \setminus B$.
  If $f_1, f_2 \in B$ s.t. $f_1 \leq g$ and $g \leq f_2$ on χ, then $f_1 \leq f_2$ on χ so $\bar{L}(f_1) \leq \bar{L}(f_2)$.
  So we consider the following sets of reals
  $\mathcal{U} := \{\bar{L}(f_1) \mid f_1 \in B, f_1 \leq g \text{ on } \chi\} \leq \{\bar{L}(f_2) \mid f_2 \in B, g \leq f_2 \text{ on } \chi\} =: \theta$
  Note that these sets $\mathcal{U}, \theta$ are nonempty, i.e. f_1, f_2 exist.
  [e.g. let $a \in A$ s.t. $|g| \leq |\hat{a}|$ on χ
  now $(\hat{a} \pm 1)^2 \geq 0$, so $|\hat{a}| \leq \dfrac{\hat{a}^2 + 1}{2} \in \hat{A}$
  so take $f_1 := -\dfrac{\hat{a}^2 + 1}{2} \in \hat{A}$; $f_2 := \dfrac{\hat{a}^2 + 1}{2} \in \hat{A}$]
  By completeness of $\mathbb{R}$, let $e \in \mathbb{R}$ s.t.
  $\sup\{\bar{L}(f_1) \mid f_1 \in B, f_1 \leq g\} \leq e \leq \inf\{\bar{L}(f_2) \mid f_2 \in B, g \leq f_2\}$.
  Extend $\bar{L}$ to $B + \mathbb{R}g \subseteq \mathcal{B}(\chi)$ by setting
  $\bar{L}(g) := e$ and $\bar{L}(f + dg) := \bar{L}(f) + de; d \in \mathbb{R}$
  To verify: $\forall\ f + dg \in B + \mathbb{R}g : f + dg \geq 0 \Rightarrow \bar{L}(f + dg) \geq 0$. (Exercise)
  This will contradict the maximal choice of B and will complete subclaim that $B = \mathcal{B}(\chi)$, and so complete the proof of claim 3. □(Claim 3)

Thus $\bar{L}$ is defined on $\mathcal{B}(\chi)$ and satisfies:

$$\forall\ f \in \mathcal{B}(\chi) : f \geq 0 \text{ on } \chi\ \Rightarrow \bar{L}(f) \geq 0. \qquad \ldots(\dagger\dagger)$$

In particular $\bar{L}$ is defined on $C_c(\chi)$ and satisfies $(\dagger\dagger)$, i.e. $\bar{L}$ is a positive linear functional on $C_c(\chi)$. So we can apply Riesz Representation Theorem (theorem 1.1) on $\bar{L}$:

$$\exists\ \mu \text{ on } \chi \text{ such that } \bar{L}(f) = \int_\chi f d\mu\ \forall\ f \in C_c(\chi) \subseteq \mathcal{B}(\chi). \qquad \ldots(\dagger\dagger\dagger)$$

Main claim: († † †) holds also $\forall\ f \in \mathcal{B}(\chi)$, i.e. $\bar{L}(f) = \int_\chi f d\mu\ \forall\ f \in \mathcal{B}(\chi)$.

In particular the proof of the theorem will be completed after proving this since $\hat{A} \subseteq \mathcal{B}(\chi)$, and so for $f = a \in \hat{A} : L(a) \underbrace{=}_{\text{(definition)}} \bar{L}(\hat{a}) = \int_\chi \hat{a} d\mu$.

Proof of main claim. Let $f \in \mathcal{B}(\chi)$

Set $f_+ := \max\{f, 0\}, f_- := -\min\{f, 0\}; f = f_+ - f_-$

So, w.l.o.g. we are reduced to the case $f \geq 0$ on χ, $f \in \mathcal{B}(\chi)$.

Set $q := f + \hat{p}$; for $q \in \mathcal{B}(\chi)$.

For each $k \geq 1$, consider $\chi_k' := \{\alpha \in \chi \mid q(\alpha) \leq k\}$

- $\forall\ k : \chi_k' \subseteq \chi_k$ and χ_k' is closed. So χ_k' is compact.
- $\chi_k' \subseteq \chi_{k+1}'$ and $\chi = \bigcup_k \chi_k'$.

Subclaim 1: For each $k \in \mathbb{N}\ \exists\ f_k \in C_c(\chi)$ such that $0 \leq f_k \leq f$; $f_k = f$ on χ_k' and $f_k = 0$ outside χ_{k+1}'.

Subclaim 2: $\bar{L}(f) = \lim_{k\to\infty} \bar{L}(f_k)$

Note that once they are proved we are done because:

$$\int f d\mu = \lim_{k\to\infty} \int f_k d\mu = \lim_{k\to\infty} \bar{L}(f_k) = \bar{L}(f).$$

We will prove subclaim 1 and 2 in next lecture.

□

POSITIVE POLYNOMIALS LECTURE NOTES (18: 17/06/10)

SALMA KUHLMANN

Contents

1. HAVILAND'S THEOREM (continued)

We will continue the proof of the following theorem from last lecture. Havilands theorem will follow as a special case.

Theorem 1.1. (Recall 1.2 of last lecture) Let A be an $\mathbb{R}$-algebra, χ a Hausdorff space and $\hat{\ } : A \to \mathrm{Cont}_c(\chi, \mathbb{R})$ an $\mathbb{R}$ algebra homomorphism. Assume $\exists\ p \in A$ such that $\hat{p} \geq 0$ on χ and $\forall\ k \in \mathbb{N} :\ \chi_k := \{\alpha \in \chi \mid \hat{p}(\alpha) \leq k\}$ is compact.
Then for any linear functional $L : A \to \mathbb{R}$ satisfying $\forall\ a \in A : \hat{a} \geq 0$ on $\chi \Rightarrow L(a) \geq 0$, $\exists$ a Borel measure μ on χ such that $L(a) = \int_\chi \hat{a}\, d\mu\ \forall\ a \in A$.

Proof. We have $C_c(\chi) \subseteq \mathcal{B}(\chi) := \{f \in C(\chi) \mid \exists\ a \in A : |f| \leq |\hat{a}| \text{ on } \chi\}$; $\hat{A} \subseteq \mathcal{B}(\chi)$;
$\bar{L} : \hat{A} \to \mathbb{R}$, defined by $\bar{L}(\hat{a}) := L(a)$.
In particular we got (as in claim 3 in 1.4 of last lecture) $\bar{L}$ is a positive linear functional on $C_c(\chi)$ s.t.

$$\bar{L}(f) = \int_\chi f d\mu\ \forall\ f \in C_c(\chi) \subseteq \mathcal{B}(\chi).$$

We **claim** that this holds also $\forall\ f \in \mathcal{B}(\chi)$, i.e. $\bar{L}(f) = \int_\chi f d\mu\ \forall\ f \in \mathcal{B}(\chi)$.

[In particular the proof of the theorem will be completed after proving this since $\hat{A} \subseteq \mathcal{B}(\chi)$, and so for $f = a \in \hat{A} : L(a) \underbrace{=}_{\text{(definition)}} \bar{L}(\hat{a}) = \int_\chi \hat{a} d\mu$.]

Let $f \in \mathcal{B}(\chi)$. Set $q := f + \hat{p}$; for $q \in \mathcal{B}(\chi)$.
For each $k \geq 1$, consider $\chi_k' := \{\alpha \in \chi \mid q(\alpha) \leq k\}$

- $\forall\, k : \chi_k' \subseteq \chi_k$ and χ_k' is closed. So χ_k' is compact.
- $\chi_k' \subseteq \chi_{k+1}'$ and $\chi = \bigcup_k \chi_k'$.

Subclaim 1: For each $k \in \mathbb{N}\ \exists\ f_k \in C_c(\chi)$ such that $0 \le f_k \le f$; $f_k = f$ on χ_k' and $f_k = 0$ outside χ_{k+1}'.

Proof of subclaim 1. For this we need Urysohn's lemma, which states that Let X be a topological space and $A, B \subseteq X$ be closed sets such that $A \cap B = \phi$. Then $\exists\, g \in C(\chi) : g : X \to [0,1]$ such that $g(a) = 0\ \forall\, a \in A$ and $g(b) = 1\ \forall\, b \in B$. Applying it with $X = \chi_{k+1}', A = Y_k' = \{\alpha \in \chi_{k+1}' \mid k + \frac{1}{2} \le q(\alpha) \le k+1\}$, and $B = \chi_k'$, we get $g_k : \chi_{k+1}' \to [0,1]$ continuous such that $g_k = 0$ on Y_k' and $g_k = 1$ on χ_k'. Extend g_k to χ by setting $g_k = 0$ on complement of χ_{k+1}'. Set $f_k := f g_k$

Then indeed $0 \le f_k \le f$ on χ , $f_k = f$ on χ_k' and $f_k = 0$ off χ_{k+1}'. In particular $\mathrm{Supp}(f) \subseteq \chi_{k+1}'$ is compact (because closed subset of a compact set is compact), so indeed $f_k \in C_c(\chi)$. □(Subclaim 1)

Subclaim 2: $\bar{L}(f) = \lim_{k\to\infty} \bar{L}(f_k)$

Note that once the subclaim 2 is proved we are done because:

$$\int f d\mu = \lim_{k\to\infty} \int f_k d\mu = \lim_{k\to\infty} \bar{L}(f_k) = \bar{L}(f).$$

Proof of subclaim 2. Observe that the inequality

$$\frac{q^2}{k} \ge f - f_k \ge 0 \text{ on } \chi, \text{ holds } \forall\, k \in \mathbb{N}.$$

To see this first of all $f = f_k$ on χ_k', so clearly $\frac{q^2}{k} \ge f - f_k \ge 0$ on χ_k'.

Now we consider the complement of χ_k', there $q(\alpha) > k$ for $\alpha \in$ complement of χ_k'. So

$$q^2(\alpha) > kq(\alpha) = k(f(\alpha) + \hat{p}(\alpha)) \ge kf(\alpha)$$
$$\ge k(f(\alpha) - f_k(\alpha)) \text{ [Since } f_k(\alpha) \ge 0\ \forall\, \alpha \in \chi]$$

Hence $\frac{q^2(\alpha)}{k} \ge (f - f_k)(\alpha)$ for all $\alpha \in (\chi_k')^{\text{compliment}}$.

So,

$$\frac{q^2}{k} \ge f - f_k \ge 0 \text{ on } \chi\ \ \forall\, k \in \mathbb{N}.$$

So,

$$\bar{L}(\frac{q^2}{k}) \ge \bar{L}(f - f_k) \ge 0.$$

Now let $k \to \infty$ to get

$$\lim_{k\to\infty} \bar{L}(\frac{q^2}{k}) = 0 \Rightarrow \lim_{k\to\infty} \bar{L}(f_k) = \bar{L}(f).$$ □(Subclaim 2)

□

2. $\mathbb{R}[\underline{X}]$ AS TOPOLOGICAL $\mathbb{R}$-VECTOR SPACE

Let $A = \mathbb{R}[\underline{X}]$ be a countable dimensional $\mathbb{R}$-algebra.
Every finite dimensional subspace has the Euclidean Topology (ET on $\mathbb{R}^N$: open balls are a basis. If W is a finite dimensional subspace, fix $B = \{w_1, \ldots, w_N\}$ basis and get an isomorphism $W \cong \mathbb{R}^N$; pullback the ET from $\mathbb{R}^N$ to W. This topology on W is uniquely determined and does not depend on the choice of the basis because a change of basis results in a linear change of coordinates and linear transformations $\underline{x} \mapsto a\underline{x}$; $\det(A) \neq 0$ are continuous).

Definition 2.1. Define a topology on $A := \mathbb{R}[\underline{X}]$ as:
$U \subseteq A$ is **open** (respectively **closed**) iff $U \cap W$ is open (respectively closed) in W, for every finite dimensional subspace W of A.
This is called **direct limit topology** on A.
Equivalently, take $A_d = \{f \in A |\deg f \leq d\}, d \in \mathbb{Z}_+$. Then $A = \cup_{d\geq 1} A_d$, ask for:
$U \subseteq A$ is open (respectively closed) iff $U \cap A_d$ is open (respectively closed) in A_d for all $d \geq 1$.

We now list the important properties of this topology. We first need to recall the following definitions:

Definition 2.2. (i) $C \subseteq A$ is called a **cone** if C is closed under addition and scalar multiplication by (nonnegetive) positive real numbers.
(ii) $C \subseteq A$ is **convex** if $\forall\, a, b \in C; \forall\, \lambda \in [0, 1] : \lambda a + (1 - \lambda)b \in C$.
Note that a cone is automatically convex.

Theorem 2.3. 1. The open convex sets of A form a basis for the topology, i.e. A is with locally convex topology, i.e. $x \in U$ and U open subset of $A \implies$ there is a convex neighbourhood U' of x such that $U' \subseteq U$.

2. This topology is the finest non-trivial locally convex topology on A.

Proof. Later (in next lecture as theorem 1.2). □

Theorem 2.4. 1. A endowed with this topology is a topological $\mathbb{R}$−algebra, i.e. the topology is (Hausdorff) comparable with addition, scalar multiplication and multiplication, i.e.

$+ : A \times A \to A$,
$\times : A \times A \to A$, and
$. : \mathbb{R} \times A \to A$
are all continuous.

2. Every linear functional is continuous in this finest locally convex topology.

Proof. Later (1.5 of Lecture 20). □

Theorem 2.5. (Separation Theorem) Let $C \subseteq A$ be a closed cone in A and let $a_0 \in A \setminus C$. Then there is a linear functional $L : A \to \mathbb{R}$ such that $L(C) \geq 0$ but $L(a_0) < 0$.
(Equivalent statement: Let $C \subseteq A$ be a cone and $U \subseteq A$ be an open convex set such that $U \cap C = \phi; U, C \neq \phi$. Then $\exists$ a linear functional $L : A \to \mathbb{R}$ such that $L(U) < 0$ and $L(C) \geq 0$).

Proof. Later (1.8 of Lecture 20). □

Corollary 2.6. For any cone $C \subseteq A$ with $C \neq \phi$, we have

$$\overline{C} = C^{\vee\vee} := \{a \in A \mid L(a) \geq 0 \text{ for any linear functional } L \text{ such that } L(C) \geq 0\}$$

$$= \{a \in A \mid L(a) \geq 0 \ \forall\ L \in C^{\vee}\}.$$

Proof. Clearly $\overline{C} \subseteq C^{\vee\vee}$: since $C \subseteq C^{\vee\vee}$ (from definition), and $C^{\vee\vee}$ is closed (because $L \in C^{\vee}$ is continuous), so $\overline{C} \subseteq C^{\vee\vee}$.
Conversely apply separation theorem (theorem 2.5): if $a_0 \notin \overline{C}$, there exists $L \in C^{\vee}$ (i.e. $L(C) \geq 0$) with $L(a_0) < 0$. So, $a_0 \notin C^{\vee\vee}$. □

Corollary 2.7. Let $A = \mathbb{R}[\underline{X}]$, $M \subseteq A$ be a quadratic module. Then $\overline{M} = M^{\vee\vee}$ and $\overline{M}$ is a quadratic module.

Proposition 2.8. (i) Every cone C is convex.

(ii) Every quadratic module M is a cone.

(iii) If C is a cone, then $\overline{C}$ is a cone.

POSITIVE POLYNOMIALS LECTURE NOTES (19: 22/06/10)

SALMA KUHLMANN

Contents

1. TOPOLOGY ON FINITE AND COUNTABLE DIMENSIONAL $\mathbb{R}-$VECTOR SPACE

1.1. Helping lemma I. Let V be a countable dimensional $\mathbb{R}$-vectorspace. Let W be a finite dimensional subspace. Fix a basis $w_1, \dots, w_n$ of W. The map

$$\Phi : \sum r_i w_i \mapsto (r_1, \dots r_n)$$

defines a vector space isomorphism $W \cong \mathbb{R}^n$.
Let τ the pullback (induced by Φ) topology on W, i.e. a set in (W, τ) is open if it is of the form $\Phi^{-1}(U)$ with $U \subseteq \mathbb{R}^n$ open in the Euclidean topology.
(For simplicity we will write ET for Euclidean topology from now on.)

1. Note that the ET is convex because the open balls form a subbasis for the topology. So τ is locally convex.
2. τ does not depend on the choice of the basis (Hint: a basis change produces a linear change of coordinates i.e. a linear map $L : \mathbb{R}^n \to \mathbb{R}^n$ which is continuous in the ET).
3. In particular if $W_1 \subseteq W_2$ are finite dimensional subspace of V, the ET on W_1 is the same as the topology induced by the topology on W_2, i.e. the same as the relative topology.
   ($U_1 \subset W_1$ is open in the ET iff $U_1 \subset W_1$ is open in the relative topology, i.e. U_1 is of the form $U_1 = W_1 \cap U_2$ with U_2 open in W_2.)
   Now define the **finite topology** on V:
   $U \subseteq V$ open iff $U \cap W$ in W is open for any finite dimensional subspace W.

4. Fix a basis $\{v_1, \dots, v_n \dots\}$, and set $V_n = \text{Span}\{v_1, \dots, v_n\}$ a sequence of finite dimensional subspaces such that $V = \cup_i V_i$. We have $V_1 \subseteq \dots \subseteq V_n \subseteq \dots$.
   Then:

   $U \subseteq V$ is open in the finite topology iff $U \cap V_i$ is open in V_i for every i.

   Proof. Clear (Hint: Use the fact that every finite dimensional subspace is contained in a V_i and use 3. in particular.) □

Theorem 1.2. (Theorem 2.3 of last lecture) The open sets in V which are convex form a basis for the topology (i.e. the finite topology is locally convex).

Proof. If V is finite dimensional ⇒ ET is convex, so nothing to prove.
So assume without loss of generality V is infinite dimensional. Let $\{v_1, \dots, v_n, \dots\}$ be an $\mathbb{R}$ basis for V.
Set $V_n = \text{Span}\{v_1, \dots, v_n\}$. Now let $U \subset V$ be open and $x_0 \in U$.
We show that there exists convex and open $U' \subset U$ such that $x_0 \in U'$.
Since

$$T_{x_0} : V \to V$$
$$v \mapsto v - x_0 \quad \text{are continuous translations,}$$

it suffices to find a convex neighbourhood U'' of 0 with $U'' \subseteq U - x_0$. Then $U' = U'' + x_0$ is the required convex neighbourhood of x_0. In other words we are reduced to the case when $x_0 = 0$.
We proceed (by induction on $n \in \mathbb{N}$) to construct an increasing sequence $C_n \subseteq U \cap V_n$ of convex subsets as follows:

- For $n = 1$: $U \cap V_1$ is open in $V_1 = \mathbb{R}v_1$ and $0 \in U \cap V_1$. So there exists $a_1 \in \mathbb{R}, a_1 > 0$ such that $C_1 := \{y_1 v_1 \mid -a_1 \le y_1 \le a_1\} := [-a_1, a_1] \subseteq U \cap V_1$.

- By induction on $n \in \mathbb{N}$: We assume we have found $a_1, \dots, a_n \in \mathbb{R}_+$ such that

  $$C_n := \{y_1v_1 + \dots + y_nv_n \mid -a_i \le y_i \le a_i\,; i \in \{1, \dots, n\}\} := \prod_{i=1}^{n}[-a_i, a_i] \subseteq U \cap V_n.$$

  Note that C_n is closed (in V_n, as well as) in V_{n+1}; $C_n \subseteq U \cap V_{n+1}$ and $V_{n+1} \setminus U$ is closed in V_{n+1} (because $V_{n+1} \cap U$ is open in V_{n+1}).

- For $n + 1$: We claim $\exists\, a_{n+1} > 0, a_{n+1} \in \mathbb{R}$ such that

  $$C_{n+1} := \{y_1v_1 + \dots + y_nv_n + y_{n+1}v_{n+1} \mid -a_i \le y_i \le a_i\,; i \in \{1, \dots, n+1\}\}$$
  $$= \prod_{i=1}^{n+1}[-a_i, a_i] \subseteq U \cap V_{n+1}.$$

  Proof of claim by contradiction: If not, then $\forall\, N\ \exists\, x^N \in V_{n+1}$ such that

$x^N = y_1v_1 + \ldots y_nv_n + y_{n+1}v_{n+1}$ with $-a_i \leq y_i \leq a_i$; $i \in \{1, \ldots, n\}$ and $-\dfrac{1}{N} \leq y_{n+1} \leq \dfrac{1}{N}$; but $x^N \notin U$.

But x^N has form $x^N = \underbrace{y_1v_1 + \ldots + y_nv_n}_{\in C_n} + y_{n+1}v_{n+1}$, $(\star)$

i.e. the sequence $\{x^N\}_{n\in\mathbb{N}} \subseteq V_{n+1} \setminus U$.

Now for each $i \in \{1, \ldots, n\}$, since x^N has form $(\star)$:

the i^{th} coordinates of $\{x^N\}$ are bounded $\forall\ N \in \mathbb{N}$, i.e. $\{x^N\}$ is a bounded sequence of reals.
So we can find a convergent sequence of i^{th} coordinate $\forall\ i \in \{1, \ldots, n\}$, i.e. there is a subsequence $\{x^{N_j}\}_{j\in\mathbb{N}} \subseteq V_{n+1} \setminus U$ such that

(1) the first $i = 1, \ldots, n$ coordinates sequences converge, and
(2) the $(n + 1)^{th}$ coordinate sequence converges to 0.

So $\{x^{N_j}\}$ converges (in V_{n+1}) as $j \to \infty$ to $x \in C_n \subseteq U$ (since C_n is closed in V_{n+1}). So the sequence $\{x^{N_j}\}_{j\in\mathbb{N}} \subseteq V_{n+1} \setminus U$ converges to $x \in U$. This contradicts the fact that $V_{n+1} \setminus U$ is closed in V_{n+1}. Hence the claim is established.

Now consider $D_n := \prod_{i=1}^{n}(-a_i, a_i) = \{y_1v_1 + \ldots + y_nv_n \mid -a_i < y_i < a_i\ ; i \in \{1, \ldots, n\}\}$, then $D_n \subset C_n \subseteq U \cap V_n$ is open convex in V_n. Set $U' := \cup_{n\in\mathbb{N}} D_n := \prod_{n=1}^{\infty}(-a_n, a_n)$. Finally (verify that) $0 \in U'$. Then U' is open, convex and $U' \subseteq U$. □

Moreover, let V be a finite dimensional $\mathbb{R}$ vector space, τ be a locally convex topology on V and Z open in this locally convex topology. Then Z is open in the finite topology.

Theorem 1.3. (Theorem 2.4 of last lecture) V is a topological vector space with finite topology τ. Moreover (V, τ) is a topological $\mathbb{R}$-algebra if V is a $\mathbb{R}$-algebra.

1.4. Helping lemma II. Let V and V' be vector spaces of countable dimension each endowed with the corresponding locally convex (finite) topology. Then the finite topology on $V \times V'$ coincides with the product topology, i.e. $\tau_{\text{fin}}(V \times V') = \tau_{\text{fin}}(V) \times \tau_{\text{fin}}(V')$.

Proof. $(\Leftarrow)$ First observe that if a set is open in the product topology on $V \times V'$, then it is open in finite topology on $V \times V'$:
Fix a basis $\{v_1, \ldots, v_n, \ldots\}$ of V and $\{v'_1, \ldots, v'_n, \ldots\}$ of V'. Set $V_n = \text{span}\{v_1, \ldots, v_n\}$ and $V'_n = \text{span}\{v'_1, \ldots, v'_n\}$. Then $V \times V' = \cup_n(V_n \times V'_n)$.

Let $U \times U' \subseteq V \times V'$ be open in the product topology, where U open in finite topology on V and U' open in finite topology on V'.
We show $U \times U'$ is open in the finite topology on $V \times V'$.
It is enough to verify that $(U \times U') \cap (V_n \times V'_n)$ is open in ET on $V_n \times V'_n$.
But $(U \times U') \cap (V_n \times V'_n) := (U \cap V_n) \times (U' \cap V'_n)$, where $U \cap V_n$ is open in ET on V_n and $U' \times V'_n$ is open in ET on V'_n. $\square(\Leftarrow)$

$(\Rightarrow)$ Conversely we show that open set in the finite topology on $V \times V'$ implies open in the product topology.
Wlog let $\mathcal{U}''$ be a convex open neighbourhood of zero in $V \times V'$.
Set $\mathcal{U} := \{x \in V \mid (2x, 0) \in \mathcal{U}''\}$ and $\mathcal{U}' := \{y \in V' \mid (0, 2y) \in \mathcal{U}''\}$. $\mathcal{U}$ and $\mathcal{U}'$ are convex open neighbourhoods of zero in V and V' respectively. So $\mathcal{U} \times \mathcal{U}'$ is open in product topology. Also $\mathcal{U} \times \mathcal{U}' \subseteq \mathcal{U}''$ because if $(x, y) \in \mathcal{U} \times \mathcal{U}'$ then $(x, y) = \frac{1}{2}(2x, 0) + \frac{1}{2}(0, 2y) \in \mathcal{U}''$, since $\mathcal{U}''$ is convex. $\square$

POSITIVE POLYNOMIALS LECTURE NOTES (20: 24/06/10)

SALMA KUHLMANN

Contents

1. TOPOLOGY ON FINITE AND COUNTABLE DIMENSIONAL $\mathbb{R}-$VECTOR SPACE (continued)

We want to prove Theorem 2.4 of Lecture 18, i.e.

Theorem 1.1. V is a topological vector space with finite topology τ. Moreover (V, τ) is a topological $\mathbb{R}$-algebra if V is endowed with $\mathbb{R}$ algebra structure.

We still need more helping lemmas (towards proof of 1.1):

Lemma 1.2. (About finite dimensional spaces with ET)

1. Finite dimensional $\mathbb{R}$-vector spaces V with ET are topological spaces.
2. Linear functionals $L : V \to \mathbb{R}$ are continuous. More generally, let V_i, V_j be finite dimensional vectorpaces with ET and $L : V_i \times V_i \to V_j$ bilinear map, then L is continuous. □

1.3. Helping lemma III. Let $V = \bigcup_i V_i$ be a countable dimensional vector space with (finite topology) $\tau_{\text{fin}}(V)$, where V_i's are finite dimensional. Let (χ, x) be a topological space and $f : V \to \chi$ be a map. Then f is continuous (with respect to $\tau_{\text{fin}}(V)$ and χ) iff $f|_{V_i}$ is continuous (with respect to ET on V_i and χ) for each $i \in \mathbb{N}$.

Proof. (⇒) Clear.
(⇐) Let $X \subseteq (\chi, x)$ be open. To show: $f^{-1}(X)$ is open in V. Using Hilfslemma I (4) it is enough to show that $f^{-1}(X) \cap V_i$ is open in V_i ∀ i. But $f^{-1}(X) \cap V_i = (f|_{V_I})^{-1}(X)$ which is open in V_i ∀ i since $f|_{V_i}$ is assumed to be continuous ∀ i. □

Corollary 1.4. Let V be countable dimensional with finite topology $\tau_{\text{fin}}(V)$ and $L : V \to \mathbb{R}$ be a linear functional. Then L is continuous. □

1.5. *Proof of the theorem 1.1.* Helping lemma $\underbrace{\text{I} + \text{II}}_{\text{(last lecture)}}$ + III implies the proof as follows:

(i) We need to verify that $+ : (V \times V, \underbrace{\tau_{\text{fin}}(V) \times \tau_{\text{fin}}(V)}_{\text{(product topology)}}) \to (V, \tau_{\text{fin}}(V))$ is continuous.

Using Helping lemma II, it is enough to verify that

$$+ : (V \times V, \tau_{\text{fin}}(V \times V)) \to (V, \tau_{\text{fin}}(V)) \text{ is continuous.}$$

Proof. Let $V = \bigcup_{i \in \mathbb{N}} V_i$, then $V \times V = \bigcup_i (V_i \times V_i)$. By Hilfslemma III, enough to verify that

$$+ : (V_i \times V_i, ET) \to (V, \tau_{\text{fin}}(V)) \text{ is continuous.}$$

Let $U \subseteq V$ open in $\tau_{\text{fin}}(V)$. We show that $(+)^{-1}(U) \subseteq V_i \times V_i$ is open in ET.
But V_i is a subspace so $(+)^{-1}(U) = (+)^{-1}(U \cap V_i)$. Now $U \cap V_i$ is open in V_i and by lemma 1.2 we know that V_i is a topological vector space so $(+)^{-1}(U \cap V_i)$ is open. □

(ii) Scalar multiplication:

$$. : \mathbb{R} \times V \to V; (r, v) \mapsto rv \text{ is continuous.}$$

Proof. Analogous. □

(iii) Multiplication: Let V be a $\mathbb{R}$-algebra. Then

$$\times : (V \times V, \underbrace{\tau_{\text{fin}}(V) \times \tau_{\text{fin}}(V)}_{\text{(product topology)}}) \to (V, \tau_{\text{fin}}(V) \text{ is continuous.}$$

Proof. Observe that restriction of multiplication to the finite dimensional subspaces V_i is not well defined i.e. V_i need not be a sub algebra, but

Claim 1: $\exists\ j$ large enough so that

$$\times : V_i \times V_i \to V_j \text{ is well defined.}$$

Proof of claim 1: Let $\{v_1, \dots, v_i\}$ be a basis of V_i. Let j be large enough so that the product vectors $v_l v_k \in V_j$ for all $1 \leq l, k \leq i$.

Claim 2: The mapping $\times : V_i \times V_i \to V_j$ is bilinear and hence continuous by lemma 1.2. □

□□(proof of theorem 1.1)

Theorem 1.6. (Separation Theorem) (Theorem 2.5 of Lecture 18) Let V be a countable dimensional vector space, $U \subseteq V$ be open and convex, $C \subseteq V$ be a cone such that $U, C \neq \phi$ and $U \cap C = \phi$. Then there exists a linear functional $L : V \to \mathbb{R}$ such that $L(U) < 0$ and $L(C) \geq 0$.

Corollary 1.7. If $C \subseteq V$ is closed cone and $x_0 \notin C$ then there exists $L : V \to \mathbb{R}$ such that $L(x_0) < 0$ and $L(C) \geq 0$.

Proof. $\exists\, U' \ni x_0 : U'$ open and $U' \cap C = \phi$. By theorem 2.3 of Lecture 18, let U be an open convex subset of V with $x_0 \in U \subseteq U'$ and $U \cap C = \phi$. □

1.8. *Proof of the theorem 1.6.*
Consider $\{D \mid D$ is a cone in $V, D \supseteq C; D \cap U = \phi\}$. This family is nonempty. By Zorn's lemma let D be the maximal element (with these properties).
Claim 1: $-U \subseteq D$.
If not let $x \in -U, x \notin D$. By maximality: $(D + x\mathbb{R}_+) \cap U \neq \phi$.
So $\exists\, y \in D; r \geq 0; u \in U$ with $y + rx = u$. So $y = r(-x) + u$.

$$\text{So } \underbrace{\frac{y}{1+r}}_{\in D \text{ since } D \text{ is a cone}} = \underbrace{\frac{r}{1+r}(-x) + \frac{1}{1+r}u}_{\in U \text{ by convexity of } U} \in D \cap U, \text{ a contradiction.}$$

□ (claim 1)

Claim 2: $D \cup -D = V$.
Let $x \in V$ and $x \notin D$. Then $(D + \mathbb{R}_+x) \cap U \neq \phi$. So $\exists\, u = d + rx$ such that $u \in U, r > 0, d \in D$. Then $-x = \frac{1}{r}(d - u) \in \frac{1}{r}(D - U) \underbrace{\subseteq}_{\text{(by claim 1)}} \frac{1}{r}(D + D) \subseteq D$.

□ (claim 2)

Claim 3: D is closed.
If not, let $d_i \in D$ such that $\lim_{i\to\infty} d_i \to x$ and $x \notin D$. Then $(D + \mathbb{R}_+x) \cap U \neq \phi$. So $\exists\, u = d + rx$; $u \in U, r > 0, d \in D$. Then $u = d + r\lim_{i\to\infty} d_i = \lim_{i\to\infty}(d + rd_i)$. So $d + rd_i \in U$ for i sufficiently large (since U is open so complement of U is closed), but also $d + rd_i \in D$ (since D is a cone). This contradicts $U \cap D = \phi$. □ (claim 3)

Now let $W := D \cap -D$. Fix $x_0 \in U$. By previous claims we see that W is a subspace. Further $x_0 \in U \Rightarrow x_0 \notin D \Rightarrow x_0 \notin W$.
Now consider the subspace $W \oplus \mathbb{R}x_0$.
Claim 4: $V = W \oplus \mathbb{R}x_0$ (i.e. W is a hyperplane in V i.e. has codimension 1 in V).
Let $y \in V$, w.l.o.g. $y \in D$ (if $y \notin D$; $-y \in D$ same argument).
Consider $\{\lambda x_0 + (1 - \lambda)y \mid 0 \leq \lambda \leq 1\}$ and the largest λ in the interval $[0, 1]$ such that $z = \lambda x_0 + (1 - \lambda)y \in D$. Then $\lambda < 1; z \in D \cap -D = W$.

So $y = \frac{1}{1-\lambda}z + \frac{-\lambda}{1-\lambda}x_0 \in W + \mathbb{R}x_0$. □ (claim 4)

Now let $L : V \to \mathbb{R}$ be the uniquely determined functional defined by $L(W) = 0$ and $L(x_0) = -1$.
Claim 5: $L \geq 0$ on D.
Let $y \in D$. If $y \in W$ then $L(y) = 0$, so done. If $y \notin W$ then for some λ :

$\lambda x_0 + (1-\lambda)y \in W;\ 0 < \lambda < 1$. Applying L :
$\lambda L(x_0) + (1-\lambda)L(y) = -\lambda + (1-\lambda)L(y) = 0$.
So $L(y) = \dfrac{\lambda}{1-\lambda} > 0$. □ (claim 4)

□□ (proof of theorem 1.6)

POSITIVE POLYNOMIALS LECTURE NOTES (21: 29/06/10)

SALMA KUHLMANN

Contents

1. K-MOMENT PROBLEM (continuation to Lecture 17)

1.1. Framework

$$A = \mathbb{R}[\underline{X}]$$
$$S = \{g_1, \ldots, g_s\}$$
$$K = K_S; \text{ b.c.s.a.set}$$
$$T_S: \text{ f.g. preordering.}$$

We have the containment (recall 3.5 of Lecture 16)

$$T_S \subseteq \overline{T}_S \subseteq \operatorname{Psd}(K_S) \tag{1}$$

Remark 1.2. We have an interesting comparison between $\operatorname{Psd}(K_S)$ and $\overline{T}_S$. One can show:

$$\operatorname{Psd}(K_S) = \bigcap_{\alpha:\mathbb{R}[\underline{X}]\to\mathbb{R} \text{ homomorphism of } \mathbb{R}-\text{algebra with } \alpha(T_S)\geq 0} \alpha^{-1}(\mathbb{R}_+)$$

$$= \bigcap_{\alpha:\mathbb{R}[\underline{X}]\to\mathbb{R},\ \alpha=ev_{\underline{x}},\ \underline{x}\in K_S} \alpha^{-1}(\mathbb{R}_+)$$

whereas

$$\overline{T}_S = T_S^{\vee\vee} = \bigcap_{L:\mathbb{R}[\underline{X}]\to\mathbb{R} \text{ linear homomorphism of } \mathbb{R}-\text{vector spaces with } L(T_S)\geq 0} L^{-1}(\mathbb{R}_+).$$

We Shall study the containment in (1).

1.3. Recall.

(a) If T_S =Psd(K_S), then T_S is saturated.

(b) If $\overline{T}_S$ = Psd(K_S), then "S solves the K_S-MP ".

Proposition 1.4. If $T_S \subseteq \mathbb{R}[\underline{X}]$ is closed then S solves the KMP if and only if T_S is saturated.

Proof. Immediate from (a) and (b) (of 1.3 above) and $T_S = \overline{T}_S$ if T_S is closed. □

We shall therefore study closed preorderings now:

2. CLOSED FINITELY GENERATED PREORDERINGS

Proposition 2.1. Let $A = \mathbb{R}[\underline{X}]$ endowed with finite topology and $A_d = \mathbb{R}[\underline{X}]_d = \{f \in A \mid \deg f \leq d\}$; $d \in \mathbb{Z}_+$. This subspace is finite dimensional generated by $\underline{X}^{\underline{\alpha}}$ of degree $|\underline{\alpha}| := \alpha_1 + \ldots + \alpha_n \leq d$.
$\text{Dim}(A_d) = \binom{n+d}{d}$; $\{A_d\}_{d\in\mathbb{N}}; A_d \subseteq A_{d+1}; A = \bigcup_d A_d$.
So $T \subseteq A$ is closed in A if and only if $T_d := T \cap A_d$ is closed in A_d for ET; for all $d \in \mathbb{Z}_+$.

Theorem 2.2. Let $\mathbb{R}[\underline{X}] = \mathbb{R}[X_1, \ldots, X_n]$. Then

(i) $\sum \mathbb{R}[\underline{X}]^2$ is closed in $(\mathbb{R}[\underline{X}], \tau_{\text{fin}})$ (Berg et al; 1970).

(ii) Let $S = \{g_1, \ldots, g_s\}$ and $K = K_S \subseteq \mathbb{R}^n$ ba a b.c.s.a. set.

(K-M) If K_S contains a cone with nonempty interior (equivalently a cone of dimension n, equivalently just a non empty generating Cone C), then T_S is closed.

The proof of (i) will follow from a series of lemma:

Lemma 2.3. It is enough to show that $\sum_d := (\sum \mathbb{R}[\underline{X}]^2) \cap A_d$ is closed in A_d $\forall\, d \in 2\mathbb{Z}_+$. □

Lemma 2.4. Let $f \in \sum_d$, d even.

1. if $f = \sum_{i=1}^{m} h_i^2$ then $\deg(f) = \max_{i=1,\ldots,m} \{\deg h_i^2\}$

2. therefore for any representation $\sum_{i=1}^{m} h_i^2$ of f we must have $\deg(h_i) \leq \frac{d}{2}$ for all $i = 1, \dots, m$.

3. w.l.o.g. we may assume that $m \leq N := \dim A_{d/2} = \binom{n + \frac{d}{2}}{\frac{d}{2}}$.

4. Therefore (for d even) $f \in \sum_d$ can be written as: $f = \sum_{i=1}^{N} h_i^2$ with $\deg(h_i) \leq \frac{d}{2}$ $\forall\ i = 1, \dots, n$.

Proof. (1) and (2): clear.

Proof of (3): Let $f \in \mathbb{R}[\underline{X}]$, $d = \deg f = 2q$. Set $N = \binom{n+q}{q}$.

Claim: $f \in \mathbb{R}[\underline{X}^2]$ iff there exists an $N \times N$ psd symmetric matrix $M \in S_{N \times N}(\mathbb{R})$ such that $f(\underline{x}) = Y^T M Y$, where $Y = \begin{pmatrix} Y_1 \\ \vdots \\ y_N \end{pmatrix}$ where $\{Y_1, \dots, Y_N\}$ is an enumeration of all possible monomials $\underline{x}^{\underline{\alpha}} = x_1^{\alpha_1} \dots x_n^{\alpha_n}$ with $\underline{\alpha} = (\alpha_1, \dots, \alpha_n) \in \mathbb{Z}_+^n$ and $|\underline{\alpha}| := \alpha_1 + \dots + \alpha_n \leq q$.

In particular: $f \in \sum \mathbb{R}[\underline{X}]^2$ iff $f = \sum_{i=1}^{N} h_i^2$

<u>Proof of the claim:</u>

($\Rightarrow$) Assume $f \in \mathbb{R}[\underline{X}^2]$ and $f = \sum h_i^2$ where $h_i \in A_q$. Write $h_i = \begin{pmatrix} a_{i1} \\ \vdots \\ a_{iN} \end{pmatrix} \in \mathbb{R}^N$ and define $M_{\alpha\beta} := \sum_i a_{i\alpha} a_{i\beta}$ the $\alpha\beta^{th}$ coefficient of the matrix M for $\alpha, \beta \in \{1, \dots, N\}$.
Obviously it is symmetric. Check that M is PSD and that $f = Y^T M Y$.
($\Leftarrow$) Conversely if $f = Y^T M Y$ with M symmetric and psd; i.e. $M \in S_{N \times N}(\mathbb{R})$. By spectral theorem write

$$M = B^T B, \text{ where } B \in M_{N \times N}$$

So $f = (Y^T B^T)(BY) = (BY)^T (BY) = \sum_{\alpha=1}^{N} (BY)_\alpha^2$. □

Lemma 2.5. Fix a set D of $d+1$ distinct real numbers and set $\Delta := D^n \subseteq \mathbb{R}^n$. Consider the map

$$\Psi : A_d \to \mathbb{R}^\Delta$$
$$g(\underline{X}) \mapsto (g^{(\underline{a})})_{\underline{a} \in \Delta}$$

Then Ψ is linear and $\Psi(g) = \underline{0}$ iff $g \equiv 0$ (i.e. $Ker(\Psi) = \{0\}$). So Ψ is homomorphism onto a closed subspace of $\mathbb{R}^{\Delta}$.

Proof. The only thing to verify is $Ker(\Psi) = \{0\}$.
By induction on n.
If $n = 1$ and g is a polynomial of degree $\leq d$ that has $d + 1$ roots is identically the zero polynomial i.e. $g \equiv 0$. So on it follows for all n. □

Corollary 2.6. Let $\{f_j\}_j \subseteq A_d$; $f \in A_d$. Then

1. $f_j \to f$ in A_d if and only if $f_j(\underline{a}) \to f(\underline{a})$ in $\mathbb{R}$ for each $\underline{a} \in \Delta$ (i.e. point wise convergence on Δ).
2. More generally $\{f_j\}_j \subseteq A_d$ is a convergent in A_d iff $\{f_j(\underline{a})\}_j$ is convergent sequence in $\mathbb{R}$ for each $\underline{a} \in \Delta$.

Proof. Proof of 2:
($\Leftarrow$) From assumption $\Psi(f_j)$ converges to a point $\gamma \in \mathbb{R}^{\Delta}$. But since Im Ψ is a subspace of $\mathbb{R}^{\Delta}$ it is closed so $\gamma \in \mathrm{Im}\Psi$. So $\lim\limits_{j\to\infty} f_j = \Psi^{-1}(\gamma) \in A_d$. □

2.7. *Proof of Theorem 2.2 (i).*
We want to show that $\sum_d$ is closed in A_d in the Euclidean topology (i.e. convergence of coefficients).
Let $f \in A_d$; $f_j \in \sum_d$ so that $f_j \to f$ coefficientwise in A_d $(\star)$

To show: $f \in \sum_d$

Write without loss of generality: $f_j = \sum\limits_{i=1}^{N} h_{ij}^2$, $\deg h_{ij} \leq \dfrac{d}{2}$ $\forall j$; $N = \binom{n+d/2}{d/2}$.

$(\star) \Rightarrow f_j(\underline{a}) \to f(\underline{a})\ \forall\ \underline{a} \in \Delta$ as $j \to \infty$

i.e. $\sum\limits_{i}^{N} (h_{ij}(\underline{a}))^2 \to f(\underline{a})$ in $\mathbb{R}\ \forall\ \underline{a} \in \Delta$.

So $\exists\, \delta > 0$ s.t.

$$h_{ij}^2(\underline{a}) \leq f_j(\underline{a}) \leq \delta\ \forall\ \underline{a} \in \Delta, \forall j \in \mathbb{N}, \forall\ i = 1, \ldots, N$$

So for each fixed $\underline{a} \in \Delta$ and each fixed $i \in \{1, \ldots, N\}$, $\{h_{ij}(\underline{a})\}_{j\in\mathbb{N}}$ is a bounded sequence of reals so has a convergent subsequence.
Also since Δ is finite there is therefore a subsequence $\{h_{ij_k}\}_{k\in\mathbb{N}}$ of $\{h_{ij}\}$ for each fixed $i \in \{1, \ldots, N\}$ such that $\{h_{ij_k}(\underline{a})\}_{k\in\mathbb{N}}$ is convergent for each $\underline{a} \in \Delta$. So by Corollary 2.6 above:
for each $i \in \{1, \ldots, N\}$: $\{h_{ij_k}\}_{k\in\mathbb{N}}$ is convergent in $A_{d/2}$ say to h_i.

So $\sum\limits_{i=1}^{N} h_i^2 = \lim\limits_{k\to\infty} \sum\limits_{i=1}^{N} {h_{ij_k}}^2 = \lim\limits_{k\to\infty} f_{j_k} = f$.

So $f \in \sum_d$ as required. □(proof of theorem 2.2 (i))

POSITIVE POLYNOMIALS LECTURE NOTES (22: 01/07/10)

SALMA KUHLMANN

Contents

1. CLOSED FINITELY GENERATED PREORDERINGS(continue)

Theorem 1.1. (Theorem 2.2 (ii) of last lecture) Let K be a basic closed semialgebraic set. Assume $C \subseteq K$ is a non empty open cone. Let $S = \{g_1, \ldots, g_s\}$ such that $K = K_S$. Then T_S is closed.

Proof. It is enough to prove the following lemma, which is a generalization of lemma 2.4 of last lecture. □

Lemma 1.2. Let $S = \{g_1, \ldots, g_s\}$ such that K_S contains a non-empty open cone. Let $f \in A_d \cap M_S := M_d$; $f = b_0 + b_1 g_1 + \ldots + b_s g_s$ where $b_i \in \sum \mathbb{R}[\underline{X}]^2$, then

1. $\deg f = \max\{\deg b_0, \deg(b_1 g_1), \ldots \deg(b_s g_s)\}$
2. If $f = \sum_{j=1}^{m_0} (h_{0j})^2 + \sum_{j=1}^{m_1} (h_{1j})^2 g_1 + \ldots + \sum_{j=1}^{m_s} (h_{sj})^2 g_s$ then $\deg h_{0j} \leq \frac{d}{2}$ and $\deg(h_{ij}) \leq \frac{d - \deg g_i}{2}$; $i = 1, \ldots, s$.

   So w.l.o.g. $f \in M_d$ has the form
   $$f = \sum_{j=1}^{m_0} (h_{0j})^2 + \sum_{j=1}^{m_1} (h_{1j})^2 g_1 + \ldots + \sum_{j=1}^{m_s} (h_{sj})^2 g_s \text{ with } \deg(h_{ij}) \leq \frac{d}{2}.$$

To prove 1.) of this lemma we need the following two propositions:

Proposition 1.3. Let $C \in \mathbb{R}^n$ be a cone, $h \in \mathbb{R}[\underline{X}]$ and $h = h_0 + \ldots + h_\nu$ be the decomposition of h into homogeneous components, i.e. $\deg h_i = i$ and $\deg h = \deg h_\nu = \nu$. Write $LT(h) = h_\nu$.

If $h \geq 0$ in C then $LT(h) \geq 0$ on C.

Proof. Let $c \in C$. We show that $h + \nu(c) \geq 0$. Wlog $h_\nu(c) \neq 0$. Consider the following variable in one real variable λ: $P_c(\lambda) := h(\lambda c) = h_0 + h_1(c)\lambda + h_2(c)\lambda^2 + \ldots + h_\nu(c)\lambda^\nu$. For all $\lambda > 0$, $\lambda c \in C$ so $P_c(\lambda) = h(\lambda c) \geq 0$. So $P_c(\lambda) \geq 0$ on $[0, \infty) \subseteq \mathbb{R}$. So it must have positive leading coefficient i.e. $h_\nu(c) > 0$ as required. □

Proposition 1.4. Let $p_0, \ldots, p_s \in \mathbb{R}[\underline{X}]$ and assume that there is a nonempty open cone C such that $p_i \geq 0$ on $C, \forall i = 1, \ldots s$ then $\deg(p_0 + \ldots + p_s) = \max(\deg p_0, \ldots, \deg p_s)$.

Proof. Let $m = \max(\deg p_0, \ldots, \deg p_s)$. Let us gather those leading terms of degree m say $LT(p_0), \ldots, LT(p_l)), l \leq s$. We want to show that $LT(p_0) + \ldots + LT(p_l) \not\equiv 0$ (once this is shown we are done because this sum, if nonzero, is the $LT(p_0 + \ldots + p_s)$ and is of degree m so this will establish that $\deg(p_0 + \ldots + p_s) = m$ indeed). Now $LT(p_1) \neq 0$ so there is $c \in C$ such that $LT(p_1)$ does not vanish at c (a nonzero polynomial does not vanish on a nonempty open set). By proposition 1.3 we must have $LT(p_1)$ evaluated at c is > 0. Since $LT(p_i)$ evaluated at c for $i = 1, \ldots, l$ are all ≥ 0 (again proposition 1.3), we se that there are no cancellations and $LT(p_0) + \ldots + LT(p_l)$ evaluated at c is > 0. So $LT(p_0) + \ldots + LT(p_l) \not\equiv 0$ □

2. APPLICATIONS TO THE K-MOMENT PROBLEM

Corollary 2.1. $K \subseteq \mathbb{R}^n, n \geq 3$ bcsas. K contains a non empty open cone $\Rightarrow$ KMP is not finitely solvable.

Proof.

1. $\mathrm{Dim}(K) \geq 3$; $K = K_S, S -$ finite $\Rightarrow T_S$ is not saturated.
2. But T_S is closed so S solves KMP iff T_S is saturated.
3. So S does not solve KMP.

□

Corollary 2.2. $K \subseteq \mathbb{R}^n, n \geq 2$. If K contains cone of dimension 2 then KMP is not finitely solvable. Note that we do not claim that T is closed.

Corollary 2.3. If K is non compact b.c.s.a. set $K = K_S$, S any finite description. Then T_S is closed.

Proof. K contains an open infinite half line $\Rightarrow$ K contains open cone. □

3. THE FINEST LOCALLY CONVEX TOPOLOGY ON A $\mathbb{R}$-VECTOR SPACE

Recall:

1. Hausdorff: If $x_1 \neq x_2, \exists u_1, u_2$ open such that $u_1 \cap u_2 = \phi$ and $x_i \in u_i$.
2. Topological vector space: Topology continuous with + and scalar multiplication.
3. A topology is locally convex if V is a topological vector space and has a basis of convex open sets.

Theorem 3.1. Tychonoff theorem On a finite dimensional vector space there is a unique topology making it into a Hausdorff topological vector space namely the ET. (much stronger statement then the fact that all—-topologies are equivalent!)

Theorem 3.2. If V is a (Hausdorff) topological vector space and W is a subspace then W is a (Hausdorff) topological vector space with the induced topology.

We first claim the following general fact:
Let X be a topological space and $Y \subseteq X$. Then the product topology of the induced topologies on X on $Y \times Y$ is induced topology of the product topology of $X \times X$ on $Y \times Y$.

- Fact 1: Any vector space admits the finest topology (greatest number of open sets) making it into a locally convex topological vector space.
- Fact 2: This finest locally convex topology is Haudorff.

Theorem 3.3. Let V be a countable dimensional real vector space. Then the finest locally convex topology (from Fact 1) is the finite topology.

Proof. Let $u \subset V$ be open in the finest locally convex topology then we want to show that u is open in the finite topology. Let $W \subset V$ be finite dimensional subspace. We show that $W \cap u$ is open in W in ET. Now W inherits the finite locally convex topology and $W \cap u$ is open in the inherited f.l.c. topology by definition of relative topology. But the induced f.l.c. topology on W makes it into a Hausdorff topological vectorspace by theorem 3.2 and therefore is the ET by theorem 3.1. So $W \cap u$ is open in W for the ET.

Conversely, let u be an open set in the finite topology on V. it must be open in the finest locally convex topology because finite topology on a countable dimensional vector space is a locally convex topolgy. Therefore u is open in the finest locally convex topology. □

Remark 3.4. Let V be a real vector space of arbitrary dimension and define a topology on V as follows: $u \subset V$ is open iff $u \cap W$ is open for every finite dimensional subspace W of V. Then V need not to be a topological vector space as addition as a binary map is not necessarily continuous. Furthermore the topology need not be locally convex.

POSITIVE POLYNOMIALS LECTURE NOTES (23: 06/07/10)

SALMA KUHLMANN

Contents

1. THE FINEST LOCALLY CONVEX TOPOLOGY ON A VECTOR SPACE (continued)

Let E be a vectorspace. There is a finest topology making E into a locally convex topological vector space. This topology is Hausdorff. It is called the **finest locally convex topology**.
Let E be a topological vector space.

Remark 1.1. Since translation for $u \in E$, $T_u : X \mapsto X + u$ is a homomorphism of E. If B is a base for neighbourhoods of zero then $u + B$ is a base for all neighbourhoods of u. Therefore the whle topological structure of E determined by all neighbourhoods of the origin.

Definition 1.2. A function $p : E \to [0, \infty)$ is called a seminorm if it has the following properties:

1. Homogeneity: $p(\lambda X) = |\lambda| p(X), \lambda \in \mathbb{R}; X \in E$
2. Subadditivity: $p(X + Y) \leq p(X) + p(Y) \forall X, Y \in E$.

If $p^{-1}(\{0\}) = \{0\}$, then p norm.

Strategy for proof of the theorem

- **Fact 2.** A family of seminorms induces a local convex topology on E making it into a topological vector space.
- **Fact 1.** Conversely (1.4+1.6) the topology of an arbitrary local convex topological vector space is always induced by a family of seminorms.

- **Fact 3.** Take all seminorms. It induces a local convex topology making into a topological vector space by Fact 2. It is the finest by Fact 1.

Definition 1.3. Let $A \subset E$. Then A

1. is **absorbing** if $\forall X \in E$ there exists $M > 0$ such that $X \in \lambda A \forall \lambda \in \mathbb{R}; |\lambda| \geq M$.
2. is **balanced** if $\lambda A \subseteq A$ for all $\lambda \in \mathbb{R}$ with $|\lambda| \leq 1$.
3. is **absolutely convex** if it is convex and balanced.

Filter of neighbourhoods of zero just means the collection of all neighbourhoods of zero.

Proposition 1.4. Let E be a topological vector space and $\mathcal{U} = \{$ all neighbourhoods of zero$\}$. Then

1. $u \in \mathcal{U}$ is absorbing.
2. for every $u \in \mathcal{U}$ there exists $u' \in \mathcal{U}$ with $u + u' \subseteq \mathcal{U}$.
3. for every $u \in \mathcal{U}$;

$$b(u) := \cap_{|\mu| \geq 1} \mu u \text{ is a balanced neighbourbood of zero contained in } u.$$

It follows that every topological vector space has a base of balanced neighbourhoods of zero.

Proof. For every $X \in E$, the map:

$$\begin{aligned} \mathbb{R} &\to E \\ \lambda &\mapsto \lambda X \end{aligned}$$

is continuous at $\lambda = 0$. This implies (1).
Similarly the continuity at $(0, 0)$ of the map

$$\begin{aligned} E \times E &\to E \\ (X, Y) &\mapsto X + Y \end{aligned}$$

implies (2).
By continuity of

$$\begin{aligned} \mathbb{R} \times E &\to E \\ (\lambda, X) &\mapsto \lambda X \end{aligned}$$

So given $u \in \mathcal{U}$ there exists $\epsilon > 0$ and $v \in \mathcal{U}$ suc that $\lambda v \subseteq u$ for $|\lambda| \leq \epsilon$. Therefore $\epsilon v \subseteq b(u) \subseteq u$. So u contains a balanced set $b(u)$ which is a neighbourhood of zero because ϵv is a neighbourhood of zero; $X \mapsto \epsilon X$ being a homomorphism of E. □

Proposition 1.5. Let E be a locally convex topological vector space then the filter collection of neighbourhoods of zero has a base $\mathcal{B}$ with the following properties:

1. Every $u \in \mathcal{B}$ is absorbing and absolutely convex.
2. If $u \in \mathcal{B}$ and $0 \neq \lambda \in \mathbb{R}$ then $\lambda u \in \mathcal{B}$.

Proof. If u is a neighbourhood of zero then $b(u)$ is absolutely convex (by proposition 1.2). So if $\mathcal{B}_0$ is a base of convex neighbourhoods of zero then the family $\mathcal{B} := \{\lambda b(u) | u \in \mathcal{B}_0; \lambda \neq 0\}$ is a base satisfying (1) and (2). □

Converse of the above proposition: Let E have a base for a filter on E with properties (1) and (2) there is a uniqe topology on E such that E is a locally convex topological vector space with $\mathcal{B}$ as a base of neighbourhoods of zero.

1.1. CONNECTION TO SEMINORMS

Remark 1.6. If p is a seminorm and $\alpha > 0$ then the set $\{X \in E | p(X < \alpha)\}$ is convex and absorbing.

Proof. Exercise □

Let E be a vector space. Associating a seminorm candidate to a subset of E: For $A \neq \phi, A \subseteq E$ sefine a mapping:

$$p_A : E \to [0\infty]$$
$$p_A(X) := \inf\{\lambda > 0 | X \in \lambda A\}$$

(where $p_A(X) = \infty$ if the set $p_A(X)$ is empty).
When p_A is seminorm?

Lemma 1.7. If $A \neq \phi, A \subseteq E$ is

1. absorbing; then $p_A(X) < \infty$ for all $X \in E$.
2. convex, then p_A is subadditive.
3. balanced then p_A is homogeneous and $\{X \in E | p_A(X) < 1\} \subseteq A \subseteq \{A \in E | p_A(X) \leq 1\}$.

If A satisfies (1)-(3) then p_A is called the seminorm determined by A.

Proposition 1.8. Let E be a vector space and $(P_i)_{i\in I}$ a family of seminorms. There exists a coarsest topology on E with the properties that E is a topological vector space and each P_i is continuous under this topology E is locally convex and the familie of sets $\{X \in E | p_{i_1} < \epsilon, \dots, p_{i_n} < \epsilon\}$ for all $\{i_1, \dots, i_n\} \in I$ and $n \in \mathbb{N}, \epsilon > 0, \epsilon \in \mathbb{R}$ is a base for the (filter of) neighbourhoods of zero.

Proof. Later □

Proposition 1.9. The topology of an arbitrary locally convex tpological vector space E is always induced by a family of seminorms.

Proof. By proposition 1.4 let $\mathcal{B}$ be the base for neighbourhoods of zero with properties ((i) absorbing and absolutely convex and (ii) $u \in \mathcal{B}, \lambda \neq 0 \Rightarrow \lambda u \in \mathcal{B}$).

Now consider the family $\{p_u | u \in \mathcal{B}\}$. By lemma 1.6 this is a family of seminorms (Moreover since u is open we actually have $u = \{X \in E | p_u(X) < 1\}$). Verify that the topology induced by this family of seminorms (as described in Fact 1) Coincides with the given topology E. □

POSITIVE POLYNOMIALS LECTURE NOTES (24: 08/07/10)

SALMA KUHLMANN

Contents

1. TOPOLOGICAL $\mathbb{R}-$VECTOR SPACE

1.1. Fix E $\mathbb{R}$ -vector space (no assumptions in the dimension)
Notation: $\bar{0} \in E$, $0 \in \mathbb{R}$ (to distinguish them).
Let τ be a topology on E making it a topological $\mathbb{R}$-vector space, i.e. the maps

$$\begin{aligned} E \times E &\to E \\ (x, y) &\mapsto x + y, \text{ and} \end{aligned}$$

$$\begin{aligned} \mathbb{R} \times E &\to E \\ (\lambda, x) &\mapsto \lambda x \quad \text{are continuous,} \end{aligned}$$

where $\mathbb{R}$ has Euclidean topology τ_E,
$E \times E$ has the product topology $\tau \times \tau$, and
$\mathbb{R} \times E$ has the product topology $\tau_E \times \tau$.
Recall that $\{A_1 \times A_2 \mid A_1 \in \tau_1, A_2 \in \tau_2\}$ is a base for the product topology $\tau_1 \times \tau_2$.
Let $\mathcal{U}_\tau = \{U \in \tau \mid \bar{0} \in U\} = \{\tau -$ neighbourhood of $\bar{0}\}$.
Since $\forall x \in E$ the map

$$E \to E, a \mapsto a + x$$

is a τ-homeomorphism,
$\forall a \in E$, $a + \mathcal{U}_\tau = \{a + U \mid U \in \mathcal{U}_\tau\} = \{\tau -$ neighbourhood of $a \in E\}$.
Namely $\mathcal{U}_\tau$ determines all the topology τ.

We want to prove the following theorem:

Theorem 1.2. There is a finest locally convex topology τ_{max} on E. Moreover τ_{max} is Hausdorff.

Definition 1.3. Let $(p, \leq)$ be a partial order.

1. $F \subseteq P$ is a **filter** if
   - $\forall\ x, y \in F, \exists\ z \in F$ such that $z \leq x$ and $z \leq y$;
   - $\forall\ x, \in F, \forall\ y \in P$: $x \leq y \Rightarrow y \in F$
2. Let $F \subseteq P$ is a filter. Then $B \subseteq F$ is a **base** for the filter if $\forall\ x \in F\ \exists\ y \in B$ such that $y \leq x$.

Example 1.4. Let (X, τ) be a topological space and $x \in X$. Then

$$F_x = \{A \in \tau \mid x \in A\} = \{\tau - \text{ neighbourhoods of } x \in X\}$$

is a filter of the partial order $(\tau, \subseteq)$:

- $A_1, A_2 \in F_x \Rightarrow A_1 \cap A_2 \in F_x$ and $A_1 \cap A_2 \subseteq A_1, A_1 \cap A_2 \subseteq A_2$.
- For $A \in F_x, U \in \tau$: $A \subseteq U \Rightarrow U \in F_x$.

In particular $\mathcal{U}_\tau = \{\tau - \text{ neighbourhoods of } \bar{0}\}$ is a filter of $(\tau, \subseteq)$

Let $\mathcal{B} \subseteq \mathcal{U}_\tau$ be a base of the filter $\mathcal{U}_\tau$ (in sense of the above definition).

Definition 1.5. A topological space (X, τ) is said to be **locally convex** if $\forall x \in X$ and $\forall\ U_x \in \tau$ containing x, $\exists\ V \in \tau$ convex such that $x \in V \subset U_x$.

Remark 1.6. Let (E, τ) be a topological $\mathbb{R}$-vector space. In order to prove that (E, τ) is locally convex, it is enough to prove that the filter $\mathcal{U}_\tau$ of τ-neighbourhoods of $\bar{0}$ has a base B (in the sense of base of a filter) made of convex set:

Let $\mathcal{B}$ be a base for the filter $\mathcal{U}_\tau$ such that each $U \in \mathcal{B}$ is convex. Let $x \in X$, $U_x \in \tau$ containing x. Then (see page 1) $U_x = x + U$ for some $U \in \mathcal{U}_\tau$. Let $C \in \mathcal{B}$ such that $C \subseteq U$ ($\exists$ such C because $\mathcal{B}$ is a base), then $x + C \subset U_x$ is convex and contains x.

1.7. Fact 1: $U \in \mathcal{U}_\tau \Rightarrow U$ is absorbing (i.e. $\forall x \in E, \exists\ \mu > 0$ such that $|\lambda| \geq \mu \Rightarrow x \in \lambda U$).

Proof. Fix $U \in \mathcal{U}_\tau$ and $x \in E$. The map

$$f_x : \mathbb{R} \to E; \lambda \mapsto \lambda x$$

is continuous everywhere, in particular in $0 \in \mathbb{R}$.
So $f_x^{-1}(U) \subseteq \mathbb{R}$ is open and contains $0 \in \mathbb{R}$.
So $\exists\ \epsilon > 0$ such that $f_x(-\epsilon, \epsilon) \subseteq U$, (we can assume $\epsilon < 1$). In other words, $c < \epsilon \Rightarrow cx \in U \Leftrightarrow x \in c^{-1}U$. So we can take for instance $\mu = \epsilon^{-1} + 1$ □

1.8. Fact 2: $U \in \mathcal{U}_\tau \Rightarrow \exists\, V \in \mathcal{U}_\tau$ such that $V + V \subseteq U$.

Proof. The map
$$+ : E \times E \to E; (x, y) \mapsto x + y$$
is continuous in $(\bar{0}, \bar{0})$. So $+^{-1}(U)$ is open in $E \times E$. So there are $V_1, V_2 \in \mathcal{U}_\tau$ such that $V_1 + V_2 \subseteq U$ and we can take $V = V_1 \cap V_2$. □

1.9. Fact 3: Let $U \in \mathcal{U}_\tau$. Set $b(U) := \bigcap_{|\mu| \geq 1} \mu U$. Then $b(U) \subseteq U, b(U) \in \mathcal{U}_\tau$, and $b(U)$ is **balanced** (i.e. $\lambda b(U) \subseteq b(U)\ \forall\ \lambda \in \mathbb{R}, |\lambda| \leq 1$).

Proof. The map
$$\mathbb{R} \times E \to E, (\lambda, x) \mapsto \lambda x$$
is continuous at $(0, \bar{0})$. So $\exists\, \epsilon > 0, \exists\, V \in \mathcal{U}_\tau$ such that $\lambda V \subseteq U\ \forall\ \lambda \in \mathbb{R}, |\lambda| \leq \epsilon$.
Claim: $\epsilon V \subseteq b(U)$.
Let $|\mu| \geq 1$, we want $\epsilon V \subseteq \mu U$. We can take $\lambda := \frac{|\epsilon|}{|\mu|} < \epsilon$ and $\lambda V \subseteq U \Rightarrow \epsilon V \subseteq \mu U$. □

Proposition 1.10. If (E, τ) is locally convex then $\exists\, \mathcal{B} \subseteq \mathcal{U}_\tau$ base for the filter $\mathcal{U}_\tau$ with the following properties:

1. Every $U \in \mathcal{B}$ is absorbing and absolutely convex (i.e. convex and balanced).
2. If $U \in \mathcal{B}$ and $\lambda \neq 0$, then $\lambda U \in \mathcal{B}$.

Conversely, given a base $\mathcal{B}$ for a filter on E with above properties (1.) and (2.) above, there is a unique topology on E such that E is a (locally convex) topological vector space with $\mathcal{B}$ as a base for the filter of neighbourhoods of $\bar{0} \in E$.

Proof. U convex neighborhood of $\bar{0} \in E \Rightarrow b(U)$ is absolutely convex. If $\mathcal{B}_0$ is a base of convex neighbourhoods, then
$$\mathcal{B} := \{\lambda b(U) \mid U \in \mathcal{B}_0, \lambda \neq 0\}$$
has properties (1.) and (2.) above.

Conversely, Let $\mathcal{B}$ be a base for a filter F on E satisfying properties (1.) and (2.). Then $U \in F \Rightarrow \bar{0} \in U$.
The only topology which makes E a topological $\mathbb{R}$-vector space and such that $F = \mathcal{U}_\tau$, has $a + F$ as a filter of $a \in E$ (see again page 1).
Setting $G \subseteq E$ open if $\forall\, a \in G\ \exists\, U \in \mathcal{B}$ such that $a + U \in G$, we define a topology such that $a + F$ is the filter of neighbourhoods of a and E is a topological $\mathbb{R}$-vector space. □

Definition 1.11. $p : E \to [0, \infty[$ is a **seminorm** if

1. $p(\lambda x) = |\lambda| p(x), \forall x \in E, \forall \lambda \in \mathbb{R}$;
2. $p(x + y) \leq p(x) + p(y), \forall x, y \in E$

If $p^{-1}(\{0\}) = \{0\}$ then p is a **norm**.

Proposition 1.12. Let $(p_i)_{i \in I}$ be a family of seminorms on E. Then $\exists$ a coarsest topology τ_C on E such that

(a) E is a topological $\mathbb{R}$-vector space.

(b) p_i is τ_C-continuous $\forall\ i \in I$.

(E, τ_C) is locally convex and the family of sets of the form

$$\{x \in E \mid p_{i_1}(x) < \epsilon, \dots, p_{i_n}(x) < \epsilon\}; i_1, \dots, i_n \in I, n \in \mathbb{N}, \epsilon > 0$$

is a base for $\mathcal{U}_{\tau_C}$ (the τ_C-neighbourhood of $\bar{0}$).

Proof. Let $\mathcal{B}$ be the above family of sets. Then $\mathcal{B}$ is a base for a filter on E having properties (1.) and (2.) of Proposition 1.10 and the unique topology asserted in Proposition 1.10 is the coarsest topology on E making E a topological vector space in which each p_i is continuous. □

The topology given by Proposition 1.12 is said to be the topology induced by the family $(p_i)_{i \in I}$ of seminorms.

Lemma 1.13. Let τ_C be the topology induced by the family of seminorms $(p_i)_{i \in I}$ on E. Suppose that $\forall x \in E \setminus \{\bar{0}\}, \exists\ i \in I$ such that $p_i(x) \neq 0$. Then τ_C is Hausdorff.

Proof. Let $x, y \in E, x \neq y$. Then $\exists\ i \in I, \exists\ \epsilon > 0$ such that $p_i(x - y) = 2\epsilon$. So $U_x := \{u \in E \mid p_i(x - u) < \epsilon\}$ and $U_y := \{u \in E \mid p_i(y - u) < \epsilon\}$ are open disjoint neighbourhoods of x and y respectively. □

1.14. Proof of Theorem 1.2:

If we take the topology induced by the family of all seminorms on E, then we obtain the finest locally convex topology on E such that E is a topological $\mathbb{R}$-vector space. We denote it by τ_{max}. We want to see that τ_{max} is Hausdorff.

We need to verify the hypothesis of above lemma, for the family of all seminorms on E. Let $x \in E \setminus \{\bar{0}\}$. Complete $\{x\}$ to a base $\mathcal{B}$ of E as a $\mathbb{R}$-vector space. Define a linear functional

$$\begin{aligned} \chi : E &\to \mathbb{R} \\ x &\mapsto 1 \\ y &\mapsto 0, \forall\ y \in B \setminus \{x\}. \end{aligned}$$

Then $p := |\chi|$ is a semi norm on E and $p(x) \neq 0$. □

POSITIVE POLYNOMIALS LECTURE NOTES (25: 13/07/10)

SALMA KUHLMANN

Contents

1. TOPOLOGICAL $\mathbb{R}-$VECTOR SPACE (continued)

Theorem 1.1. There is unique Hausdorff topology τ on a finite dimensional $\mathbb{R}$-vector space making it a topological $\mathbb{R}$-vector space.

Remark 1.2. Lets see why the discrete topology τ_D is not good. Let V be an $\mathbb{R}$-vector space. When we ask that the map
$\cdot : \mathbb{R} \times V \to V$,
$(\lambda, v) \longmapsto \lambda v$ is continuous,
we assume that $\mathbb{R}$ is endowed with euclidean topology τ_E and $\mathbb{R} \times V$ with the product topology.
So, for instance, $\{\bar{0}\} \in \tau_D = \mathcal{P}(V)$,
and $\cdot^{-1}(\{\bar{0}\}) = (\mathbb{R} \times \{\bar{0}\}) \cup (\{0\} \times V$, which is not open in the product topology $\tau_E \times \tau_D$.

Remark 1.3. If we do not assume Hausdorffness, there are other topologies as $\tau_I = \{\phi, V\}$ (the indiscrete topology).

1.4. Let V be an $\mathbb{R}$-vector space, $\dim(V) = n \in \mathbb{N}$.
Claim: We may assume $V = \mathbb{R}^n$
Proof of claim: Let $\mathcal{B} = \{v_1, \ldots, v_n\}$ be a base of V (as a $\mathbb{R}$-vector space).
Let $\Phi_{\mathcal{B}} : V \to \mathbb{R}^n$

$$\sum_{i=1}^{n} a_i v_i \mapsto (a_1, \ldots, a_n)$$

$\Phi_{\mathcal{B}}$ is an isomorphism of $\mathbb{R}$-vector space.
We define:

$A \subset V$ open $\Leftrightarrow \Phi_{\mathcal{B}}(A) \in \tau_E$ (the Euclidean topology on $\mathbb{R}^n$).
This defines a topology τ on V that does not depend on $\mathcal{B}$ and such that (v, τ) is homeomorphic to $(\mathbb{R}^n, \tau_E)$.
Since $(\mathbb{R}^n, \tau_E)$ is a topological $\mathbb{R}$-vector space, also (V, τ) is a topological $\mathbb{R}$-vector space, and so Theorem 1.1 is equivalent to:

Theorem 1.5. The Euclidean topology τ_E on $\mathbb{R}^n$ is the unique Hausdorff topology on $\mathbb{R}^n$ such that the following maps are continuous:
$\mathbb{R} \times \mathbb{R}^n \to \mathbb{R}^n$; $(\lambda, x) \mapsto \lambda x$, and

$\mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^n$; $(x, y) \mapsto x + y$.

Proposition 1.6. Let $(P, \leq)$ be a partial order. Let F_1, F_2 be a filter of P , and $B_1 \subseteq F_1$, $B_2 \subseteq F_2$ base. Suppose that

(i) $\forall\ x \in B_1\ \exists\ y \in B_2$ s.t. $y \leq x$.

(ii) $\forall\ x \in B_2\ \exists\ y \in B_1$ s.t. $y \leq x$.

Then we conclude that $F_1 = F_2$.

Proof. "$F_1 \subseteq F_2$": Let $z \in F_2$. B_2 base for $F_2 \Rightarrow\ \exists\ x \in B_2$ s.t. $x \leq z$.
(ii) $\Rightarrow\ \exists\ y \in B_1$ s.t. $y \leq x \leq z$.
F_1 filter, $B_1 \subseteq F_1 \Rightarrow z \in F_1$.
"$F_2 \subseteq F_1$" is symmetric using (i) instead of (ii). □

1.7. Proof of Theorem 1.5:
Let τ be a topology on $\mathbb{R}^n$ s.t. τ is Hausdorff and $(\mathbb{R}^n, \tau)$ is a topological $\mathbb{R}$-vector space.
We want to show that: $\tau = \tau_E$ ...($\star$)
Since the topology is determined from what happens around $\overline{0} \in \mathbb{R}^n$, so

$$(\star) \Leftrightarrow \mathcal{U}_\tau = \mathcal{U}_{\tau_E}.$$

Consider $F_\tau = \{X \subset \mathbb{R}^n \mid \overline{0} \in U \subset X, \text{for some } U \in \tau\}$. Then F_τ is a filter.
We will show that $F_\tau = F_{\tau_E}$, by applying Proposition 1.6, where $(P, \leq) = (\mathcal{P}(\mathbb{R}^n), \subseteq\ )$, $F_1 = F_\tau, F_2 = F_{\tau_E}$, and B_1 and B_2 two bases for F_1 and F_2 with properties (i) and (ii). We will find next a good base for F_τ.

Definition 1.8. Let (E, τ) be a topological $\mathbb{R}$-vector space. $X \subset E$ is said to be **circled** if $\alpha \in \mathbb{R}, |\alpha| < 1, x \in X \Rightarrow \alpha x \in X$.

Proposition 1.9. Any topological $\mathbb{R}$-vector space (E, τ) has a base of circled neighbourhoods of $\overline{0} \in E$.

Proof. $\mathcal{B}_\tau = \{ \cup_{|\alpha|\leq 1} \alpha V \mid V \in \mathcal{U}_\tau\}$ is a base for F_τ.
(We will actually show that $\mathcal{B}_\tau$ is a base for $\mathcal{U}_\tau$, since it is equivalent)
Fix $V \in \mathcal{U}_\tau$. By continuity in $(\overline{0}, 0)$ of the product $\exists\, \epsilon > 0,\ \exists\, W \in \mathcal{U}_\tau$ s.t.
$|\lambda| \leq \epsilon$ and $x \in W \Rightarrow \lambda x \in V$.
Set $U := \epsilon W$. Then $\alpha V \subset U\ \forall\, \alpha, |\alpha| \leq 1$.
So, $\cup_{|\alpha|\leq 1}\alpha V \subseteq U$. □

1.10. Topological fact: Let (X, τ) be a topological space, $K \subseteq X$. Then
$x \in \overline{K} \Leftrightarrow\ \forall\, V_x\ \ \tau-$ open containing x, $V_x \cap K \neq \phi$.

Proof. "⇒" Suppose, for a contradiction $V_x\ \ \tau-$ open containing x, with $V_x \cap K = \phi$. Then $x \notin K$, and $A = (X \setminus \overline{K}) \cup V_x$ is open, so $A \cap K = \phi$ in contradiction with the fact that $X \setminus \overline{K}$ is the biggest open set disjoint from K (because $\overline{K}$ is the smallest closed set containing K).
"⇐" Suppose $x \notin \overline{K}$, so $x \in X \setminus \overline{K}$ which is open. Then $\exists\, V_x$ open containing x s.t. $V_x \subset V \setminus \overline{K}$, contradiction. □

Lemma 1.11. Let (X, τ) be a Hausdorff topological space. If $K \subseteq X$ is τ-compact, then K is τ-closed.

Proof. Let $x \in \overline{K}$. We want $x \in K$. Suppose on contrary $x \notin K$.
$x \in \overline{K} \Leftrightarrow \forall\, V_x\ \tau-$ open containing x, $V_x \cap K \neq \phi$.
X Hausdorff $\Rightarrow \forall\, a \in K:\ \exists\, \tau-$ open $V_a \ni a, V_a^x \ni x$ such that $V_a \cap V_a^x = \phi$.
$\{V_a \mid a \in K\}$ is an open covering of K.
K compact $\rightarrow\ \exists$ finite subcovering $\{V_{a_1}, \ldots, V_{a_n}\}$. Set $V_x := V_{a_1}^x \cap \ldots \cap V_{a_n}^x$.
Then V_x is $\tau-$open (since finite intersection of open sets is open) containing x and $V_x \cap K = \phi$, a contradiction
(otherwise if $e \in V_x \cap K$, then $\exists\, i = 1, \ldots, n$ s.t. $e \in V_x \cap V_{a_i}^x = \phi$). □

1.12. Proof of Theorem 1.5 continued:
To prove: $\tau = \tau_E$

"$\tau \subseteq \tau_E$ " : Let U be circled $\tau-$neighbourhood of $\overline{0}$, and let V be a circled $\tau-$neighbourhood of $\overline{0}$ s.t. $\underbrace{V + \ldots + V}_{n-\text{ times}} \subseteq U$.
V absorbing (see Fact 1 of last lecture) $\Rightarrow\ \exists\, k > 0$ s.t. $ke_i \in V\ \forall\, i = 1, \ldots, n$.
$\Rightarrow k \sum_{i=1}^{n} \alpha_i e_i \in U$ if $\sum_i |\alpha_i|^2 \leq 1$.
Therefore $B_k := \{x \in \mathbb{R}^n \mid \|x\|_2 < k\} \subset U$.

"$\tau_E \subseteq \tau$ " : Let $B = \{x \in \mathbb{R}^n \mid \|x\|_2 < 1\}$ and $S := \{x \in \mathbb{R}^n \mid \|x\|_2 = 1\}$.
$S\ \tau_E-$compact, $\tau \subseteq \tau_E \Rightarrow S$ is $\tau-$compact.
By Lemma 1.11, S is $\tau-$ closed.

$\overline{0} \notin S \Rightarrow \exists$ a circled $\tau-$neighbourhood V of $\overline{0}$ s.t. $V \cap S = \phi$.
We want $V \subset B$. Suppose not: $\exists\, x \in V$ s.t. $\|x\|_2 \geq 1$ ($\Leftrightarrow x \notin B$),
then $\frac{x}{\|x\|_2} \in V \cap S = \phi$, a contradiction.
Thus B is a $\tau-$ neighbourhood of $\overline{0}$. Multipying by scalars we have a $\tau-$ neighbourhood base at $\overline{0}$, so $\tau_E \subseteq \tau$.

Remark 1.13. The hypothesis that $\dim V = n \in \mathbb{N}$ cannot be avoided. Consider for instance $V = \mathbb{R}^{\mathbb{N}}$:
We saw that τ_{fin} is a topology on $\mathbb{R}^{\mathbb{N}}$ making it a topological $\mathbb{R}-$vector space. τ_{fin} is Hausdorff.
It is not the only use !
Consider for instance the product topology τ on $\mathbb{R}^{\mathbb{N}}$. τ is Hausdorff and makes $\mathbb{R}^{\mathbb{N}}$ a topological $\mathbb{R}-$ vectore space.
$\tau \subseteq \tau_{\text{fin}}$, but $\tau \neq \tau_{\text{fin}}$. For instance: $(0,1)^{\mathbb{N}} \in \tau_{\text{fin}} \setminus \tau$.