Polynomial Optimization Sums of squares and moments Part 2



Monique Laurent

POEMA 1st Workshop – Florence, January 2020

Solving polynomial equations Finite rank moment matrices

Recap on polynomial optimization

Given polynomials p, g_1, \dots, g_m , compute:

$$p_{\min} = \inf_{x \in K} p(x), \qquad K = \{x \in \mathbb{R}^n : g_1(x) \ge 0, \cdots, g_m(x) \ge 0\}.$$

Recall:

- $\overline{p} = (p_{\alpha})_{\alpha}$ is the vector of coefficients of p.
- $[x]_{\infty} = (x^{lpha})_{lpha \in \mathbb{N}^n}$ is the vector of monomials.

•
$$p(x) = \sum_{\alpha} p_{\alpha} x^{\alpha} = \overline{p}^{\mathsf{T}}[x]_{\infty}.$$

- Define the set $\mathcal{C}_{\infty}(\mathcal{K}) = \operatorname{conv}\{[x]_{\infty} : x \in \mathcal{K}\}.$
- Then, $p_{\min} = \inf_{x \in K} \overline{p}^{\mathsf{T}}[x]_{\infty} = \inf_{y = (y_{\alpha}) \in \mathbb{R}^{\mathbb{N}^n}} \{ \overline{p}^{\mathsf{T}}y : y \in \mathcal{C}_{\infty}(K) \}.$

Goal: Describe the set $\mathcal{C}_{\infty}(K)$

Plan of the lecture

- 1. For an ideal $I \subseteq \mathbb{R}[x]$, basic facts about the quotient algebra $\mathcal{A} = \mathbb{R}[x]/I$:
 - Relate dim \mathcal{A} and $|V_{\mathbb{C}}(I)|$.
 - The eigenvalue method to find $V_{\mathbb{C}}(I)$.
- 2. Moment matrices M(y):
 - The kernel of M(y) is an ideal I.
 - If $M(y) \succeq 0$ then I is a real radical ideal.
- Characterization of the sequences y ∈ C_∞(K) in terms of positivity and finite rank condition on the moment matrix M(y).

Ideals and varieties

Let $I \subseteq \mathbb{C}[x]$ be an ideal.

- $V_{\mathbb{C}}(I) = \{x \in \mathbb{C}^n : f(x) = 0 \ \forall f \in I\}$ is the complex variety of I.
- $V_{\mathbb{R}}(I) = V_{\mathbb{C}}(I) \cap \mathbb{R}^n$ is the **real variety** of *I*.
- If $I = (h_1, \dots, h_m)$ is generated by h_1, \dots, h_m , the elements $v \in V_{\mathbb{C}}(I)$ are the **common complex roots** of h_1, \dots, h_m .
- The vanishing ideal of a subset $V \subseteq \mathbb{C}^n$ is

$$\mathcal{I}(V) = \{ f \in \mathbb{C}[x] : f(v) = 0 \ \forall v \in V \}.$$

• Clearly: $I \subseteq \mathcal{I}(V_{\mathbb{C}}(I))$.

Radical ideals and Hilbert's Nullstellensatz

• The radical of *I* is the ideal:

 $\sqrt{I} = \{ f \in \mathbb{C}[x] : f^m \in I \text{ for some } m \in \mathbb{N} \}.$

- Clearly: $I \subseteq \sqrt{I} \subseteq \mathcal{I}(V_{\mathbb{C}}(I)).$
- Example: For $I = (x^2)$, $V_{\mathbb{C}}(I) = \{0\}$, $x \in \sqrt{I}$, but $x \notin I$.
- Hilbert's Nullstellensatz: $\sqrt{I} = \mathcal{I}(V_{\mathbb{C}}(I)).$

A polynomial f vanishes at all common complex roots of I if and only if some power of f belongs to I.

• **Definition:** The ideal *I* is said to be **radical** if $I = \sqrt{I}$ or, equivalently, if $I = \mathcal{I}(V_{\mathbb{C}}(I))$.

Real radical ideals & the Real Nullstellensatz

Let *I* be an ideal in $\mathbb{R}[x]$.

• The real radical of *I* is the ideal:

 $\sqrt[\mathbb{R}]{I} = \{ f \in \mathbb{R}[x] : f^{2m} + s \in I \text{ for some } m \in \mathbb{N}, s \in \Sigma \}.$

- Clearly: $I \subseteq \sqrt[\mathbb{N}]{I} \subseteq \mathcal{I}(V_{\mathbb{R}}(I)).$
- **Example:** For $I = (x^2 + y^2)$, we have $V_{\mathbb{R}}(I) = \{(0,0)\}$. Then, $x, y \in \sqrt[\infty]{I}$, but $x, y \notin I$.
- Real Nullstellensatz: $\sqrt[N]{I} = \mathcal{I}(V_{\mathbb{R}}(I)).$
- Definition: The ideal *I* is said to be real radical if *I* = ^ℝ/_I or, equivalently, if *I* = *I*(*V*_ℝ(*I*)).

Some technical lemmas

1. Lemma 1: / is real radical if and only if

$$\forall f_1, \cdots, f_m \in \mathbb{R}[x] \quad f_1^2 + \cdots + f_m^2 \in I \Longrightarrow f_1, \cdots, f_m \in I.$$

2. Lemma 2: If $I \subseteq \mathbb{R}[x]$ is a real radical ideal and $|V_{\mathbb{R}}(I)| < \infty$, then

$$V_{\mathbb{C}}(I) = V_{\mathbb{R}}(I).$$

Lemma 3: Let V ⊆ Cⁿ be a finite set. There exist interpolation polynomials p_v ∈ C[x] for v ∈ V, i.e., satisfying:

$$p_{v}(u) = \delta_{u,v} \quad \forall u, v \in V.$$

If $V = \overline{V}$, the interpolation polynomials p_v can be chosen in $\mathbb{R}[x]$.

For any polynomial $f \in \mathbb{C}[x]$, $f - \sum_{v \in V_{\mathbb{C}}(I)} f(v) p_v \in \mathcal{I}(V)$.

The quotient algebra $\mathbb{R}[x]/I$

The quotient algebra $\mathbb{C}[x]/I$

Let $I \subseteq \mathbb{C}[x]$ be an ideal.

The quotient $\mathcal{A} = \mathbb{C}[x]/I$ is an algebra:

• Elements: cosets $[f] = f + I = \{f + q : q \in I\}.$

• Addition:
$$[f] + [g] = [f + g].$$

- Scalar multiplication: $\lambda[f] = [\lambda f]$.
- Multiplication: [f][g] = [fg].

A set $\mathcal{B} = \{[b_1], [b_2], \ldots\} \subseteq \mathcal{A}$ is a **linear basis** of \mathcal{A} if any polynomial $f \in \mathbb{C}[x]$ can be written (uniquely) as

$$[f] = \sum_{i} \lambda_i [b_i]$$
 i.e., $f = \sum_{i} \lambda_i b_i + q$,

where $\lambda_i \in \mathbb{C}$ and $q \in I$.

The dimension of $\mathcal{A} = \mathbb{C}[x]/I$

Lemma 4: Let p_v ($v \in V_{\mathbb{C}}(I)$) be interpolation polynomials at $V_{\mathbb{C}}(I)$ and define

$$\mathcal{L} := \{ [p_v] : v \in V_{\mathbb{C}}(I) \}.$$

- \mathcal{L} is linearly independent in \mathcal{A} .
- \mathcal{L} is generating in $\mathbb{C}[x]/\mathcal{I}(V_{\mathbb{C}}(I))$.
- \mathcal{L} is a basis of \mathcal{A} if I is radical.

Theorem:

1. dim $\mathcal{A} < \infty \iff |V_{\mathbb{C}}(I)| < \infty$.

2. Assume $|V_{\mathbb{C}}(I) < \infty$. Then,

$$|V_{\mathbb{C}}(I)| \leq \dim \mathcal{A},$$

with equality if and only if the ideal I is radical (i.e., $I = \sqrt{I}$).

Multiplication operators and roots of equations

Given a polynomial h, define the **'multiplication by** h**' linear map:**

$$egin{array}{rcl} m_h: & \mathcal{A} & o & \mathcal{A} \ & & [f] & \mapsto & [fh] \end{array}$$

Theorem: Assume $|V_{\mathbb{C}}(I)| < \infty$.

1. Let $\mathcal{B} = \{[b_1], \dots, [b_N]\}$ be a basis of \mathcal{A} and let M_h be the matrix of m_h in the basis \mathcal{B} . For $v \in V_{\mathbb{C}}(I)$, the vector $[v]_{\mathcal{B}} = (b_i(v))_{i=1}^N$ is a left **eigenvector** of M_h :

$$[v]_{\mathcal{B}}^{\mathsf{T}}M_{h} = h(v)[v]_{\mathcal{B}}^{\mathsf{T}}.$$

2. $\{h(v) : v \in V_{\mathbb{C}}(I)\}$ is the set of all the **eigenvalues** of M_h .

→ Can compute $V_{\mathbb{C}}(I)$ via the eigenvalues/eigenvectors of M_h for random linear $h = \sum_{i=1}^n h_i x_i$ → the eigenvalues h(v) are all distinct, so one can recover $[v]_{\mathcal{B}}$ and thus v.

Univariate example

• Let
$$I = (x^3 - 6x^2 + 11x - 6)$$
 be generated by
 $x^3 - 6x^2 + 11x - 6 = (x - 1)(x - 2)(x - 3).$

- Thus: $V_{\mathbb{C}}(I) = \{1, 2, 3\}.$
- The set $\mathcal{B} = \{[1], [x], [x^2]\}$ is a basis of $\mathcal{A} = \mathbb{R}[x]/I$.
- 'Multiplication by x' matrix (*companion matrix*):

$$M_{x} = \begin{bmatrix} x \\ x \end{bmatrix} \begin{bmatrix} x^{2} \\ x^{3} \end{bmatrix}$$
$$M_{x} = \begin{bmatrix} x \\ x \end{bmatrix} \begin{bmatrix} 1 \\ x^{2} \end{bmatrix} \begin{pmatrix} 0 & 0 & 6 \\ 1 & 0 & -11 \\ 0 & 1 & 6 \end{pmatrix}$$

- M_{x}^{T} has three eigenvectors:
 - 1. (1, 1, 1) with eigenvalue $\lambda = 1$, 2. (1, 2, 4) with eigenvalue $\lambda = 2$, 3. (1, 3, 9) with eigenvalue $\lambda = 3$.

Eigenvectors are indeed of the form $[v]_{\mathcal{B}} = (1, v, v^2)$ for $v \in \{1, 2, 3\}$.

Finite rank moment matrices

Recap on moment matrices

Definition: Let $y = (y_{\alpha})_{\alpha}$ be a sequence of real numbers indexed by \mathbb{N}^{n} .

1. Define the corresponding **linear functional** L_y on $\mathbb{R}[x]$:

L

$$egin{array}{rcl} & & & & & \mathbb{R}[x] & o & & \mathbb{R} \ & & & & & & & L_y(x^lpha) = y_lpha \ & & & f = \sum_lpha f_lpha x^lpha & \mapsto & & L_y(f) = \sum_lpha f_lpha y_lpha. \end{array}$$

Define the moment matrix M(y), as the real symmetric matrix indexed by Nⁿ with

$$M(y)_{\alpha,\beta} = L_y(x^{lpha}x^{eta}) = y_{lpha+eta} \ \ orall lpha, eta \in \mathbb{N}^n.$$

Example: If $y = [v]_{\infty}$ with $v \in \mathbb{R}^n$, then L_y is the **evaluation at** v:

$$L_y(f) = f(v) \quad \forall f \in \mathbb{R}[x],$$

and

$$M(y) = (v^{\alpha+\beta})_{\alpha,\beta}.$$

Positivity conditions for M(y) and L_y

Lemma 5: Let $y = (y_{\alpha})_{\alpha}$ and L_y the associated linear functional on $\mathbb{R}[x]$.

For $f, g \in \mathbb{R}[x]$:

$$L_y(f^2) = \overline{f}^{\mathsf{T}} M(y) \overline{f}, \quad L_y(gf^2) = \overline{f}^{\mathsf{T}} M(gy) \overline{f},$$

where $\mathbf{g}\mathbf{y} \in \mathbb{R}^{\mathbb{N}^n}$ is the new sequence with lpha-th entry

$$(gy)_{\alpha} = L_y(gx^{\alpha}) = L_y\Big(\Big(\sum_{\gamma} g_{\gamma} x^{\gamma}\Big) x^{\alpha}\Big) = \sum_{\gamma} g_{\gamma} y_{\alpha+\gamma} \quad \forall \alpha \in \mathbb{N}^n.$$

Therefore,

$$L_y \ge 0 \text{ on } \Sigma \iff M(y) \succeq 0,$$

 $L_y \ge 0 \text{ on } g\Sigma \iff M(gy) \succeq 0.$

The kernel of M(y) is an ideal

Lemma 6: Let $y = (y_{\alpha})_{\alpha}$ and L_y the associated linear functional on $\mathbb{R}[x]$. Set

$$I := \{ f \in \mathbb{R}[x] : L_y(hf) = 0 \ \forall h \in \mathbb{R}[x] \}.$$

Then:

1. A polynomial f belongs to I if and only if its coefficient vector \overline{f} belongs to the kernel of M(y).

So we can write: $I = \ker M(y)$.

- 2. *I* is an **ideal** in $\mathbb{R}[x]$.
- 3. If $M(y) \succeq 0$ then *I* is a **real radical ideal**.

using the facts:

•
$$f \in I \iff L(f^2) = 0.$$

• *I* is real radical if and only if $\sum_i f_i^2 \in I \implies f_i \in I$ for all *i*

Characterization of the set $\mathcal{C}_{\infty}(K)$

Finite rank moment matrix theorem: [Curto-Fialkow 1996, 2000]

Let
$$K = \{x \in \mathbb{R}^n : g_1(x) \ge 0, \cdots, g_m(x) \ge 0\}.$$

Let $y = (y_{\alpha})_{\alpha}$ and L_y the corresponding linear functional on $\mathbb{R}[x]$.

The following assertions are equivalent:

y ∈ C_∞(K), i.e., y = ∑^r_{i=1} λ_i[v_i]_∞ for λ_i > 0, ∑_i λ_i = 1, v_i ∈ K,
 i.e., y has a representing measure which is finite atomic and supported by K.

Proof of the implication $(2) \Longrightarrow (1)$

- 1. $I := \ker M(y)$ is a real radical ideal. [since $M(y) \succeq 0$]
- 2. dim $\mathbb{R}[x]/I = \operatorname{rank} M(y) =: r$.
- 3. $V_{\mathbb{C}}(I) = \{v_1, \cdots, v_r\} \subseteq \mathbb{R}^n$. [I real radical with finite variety]
- 4. Let $p_{v_1}, \dots, p_{v_r} \in \mathbb{R}[x]$ be interpolation polynomials at v_1, \dots, v_r . Their cosets form a basis of $\mathbb{R}[x]/I$.
- 5. $L_y = \sum_{i=1}^r L_y(p_{v_i})\mathcal{L}_{v_i}$. $[\mathcal{L}_{v_i} = \text{`evaluation at } v_i\text{'} \text{ liner functional}]$ 6. $L_y(p_{v_i}) > 0$. $[\text{since } p_{v_i} - (p_{v_i})^2 \in I]$
- 7. $\sum_{i=1}^{r} L_y(p_{v_i}) = 1.$ [since $1 \sum_{i=1}^{r} p_{v_i} \in I$]
- 8. $v_1, \dots, v_r \in K$. [since $0 \le L_y(g_j(p_{v_i})^2) = L_y(p_{v_i})g_j(v_i)$]

We are done:

$$y=\sum_{i=1}^r L_y(p_{v_i})[v_i]_\infty\in \mathcal{C}_\infty(K).$$

Polynomial optimization: Stopping criterion (flatness condition) Extracting global minimizers

Flat extension of matrices

Lemma 1: Consider a matrix in block form: $X = \begin{pmatrix} A & B \\ B^T & C \end{pmatrix}$. Assume rank X = rank A (call X a flat extension of A). Then

 $\ker X = \ker(A \ B)$

Lemma 2: Given $y \in \mathbb{R}^{\mathbb{N}_{2s}^n}$, assume rank $M_s(y) = \operatorname{rank} M_{s-1}(y)$, i.e., $M_s(y)$ is a **flat extension of** $M_{s-1}(y)$ (then call y **flat**). Then, for any polynomials f, g:

 $f \in \ker M_s(y), \ \deg(fg) \leq s \implies fg \in \ker M_s(y).$

Proof:

- Suffices to show the result for $g = x_i$ (then iterate).
- Suffices to show $L(u(f_{x_i})) = 0 \quad \forall u \in \mathbb{R}[x]_{s-1}$. [by Lemma 1]

Indeed: $L(u(fx_i)) = L((x_iu)f) = 0$ as deg $(x_iu) \le s$ and $f \in \ker M_s(y)$.

Hence: ker $M_s(y)$ behaves like a **'truncated' ideal**.

Flat extension of moment matrices

Theorem 1: [Flat extension theorem of Curto-Fialkow 1996] Given $y \in \mathbb{R}^{\mathbb{N}_{2s}^{n}}$, assume:

 $\operatorname{rank} M_s(y) = \operatorname{rank} M_{s-1}(y).$

Then one can extend y to a sequence $\tilde{y} \in \mathbb{R}^{\mathbb{N}^n}$ satisfying: rank $M(\tilde{y}) = \operatorname{rank} M_s(y)$.

Moreover, the ideal $I = \ker M(\tilde{y})$ satisfies:

(1) If $\{\alpha_1, \cdots, \alpha_r\} \subseteq \mathbb{N}_{s-1}^n$ indexes a column base of $M_{s-1}(y)$, then $\{[x^{\alpha_1}], \cdots, [x^{\alpha_r}]\}$ is a base of $\mathbb{R}[x]/I$.

(2) I is generated by the polynomials in ker $M_s(y)$:

 $I = (\ker M_s(y)).$

Sketch of proof of Theorem 1

Goal: Find a matrix $M = \begin{pmatrix} M_s(y) & B \\ B^T & C \end{pmatrix}$, indexed by \mathbb{N}_{s+1}^n , satisfying: (1) M is a flat extension of $M_s(y)$: rank $M = \operatorname{rank} M_s(y) =: r$ (2) M is a moment matrix: $M_{\alpha,\beta} = M_{\alpha',\beta'}$ for all $\alpha, \beta, \alpha', \beta' \in \mathbb{N}_{s+1}^n$

Key ideas:

- Let B = {x^{α1},..., x^{αr}} ⊆ ℝ[x]_{s-1} index a maximum linearly independent set of columns of M_s(y).
- Let $|\gamma| = t + 1$. Say, $\gamma_i \ge 1$. If such M exists it must satisfy: $x^{\gamma-e_i} - r(x) \in \ker M_s(y) \subseteq \ker M$, for some $r \in \operatorname{Span}(\mathcal{B})$ and thus $x_i^{\gamma} - x_i r(x) = x_i (x^{\gamma-e_i} - r(x)) \in \ker M$. [by Lemma 2] This permits to define the γ th column of M in terms of columns of $M_s(y)$ (and thus to define B and C).
- Remains to verify that this is a **good** definition:
 - it does not depend on the choice of index *i* such that $\gamma_i \geq 1$,
 - and the matrix M obtained in this way is a moment matrix.

Stopping criterion and extracting global minimizers

- K_p^* : set of all **global minimizers** of p in K.
- $d_p = \lceil \deg(p)/2 \rceil$, $d_K = \max\{\lceil \deg(g_j)/2 \rceil : j \in [m]\}$.

Theorem 2: [Lasserre 2001] Let *L* be an optimal solution to

 $p_{\text{mom},t} = \inf\{L(p) : L \in (\mathbb{R}[x]_{2t})^*, L(1) = 1, L \ge 0 \text{ on } \mathcal{M}(\mathbf{g})_{2t}\}$

with associated sequence $y = (L(x^{\alpha}))_{\alpha \in \mathbb{N}_{2s}^{n}}$. Assume:

rank $M_s(y) = \text{rank } M_{s-d_K}(y)$ for some s with $\max\{d_p, d_K\} \le s \le t$. Then:

- (1) The relaxation is exact: $p_{\text{mom},t} = p_{\text{min}}$.
- (2) All common roots of the polynomials in ker $M_s(y)$ are real and they are global minimizers: $V_{\mathbb{C}}(\ker M_s(y)) \subseteq K_p^*$.
- (3) If L is an optimal solution for which the matrix $M_t(y)$ has maximum possible rank, then:

$$V_{\mathbb{C}}(\ker M_s(y)) = K_p^*$$

Proof of Theorem 2

1. Apply the 'flat extension theorem': There exists a sequence $\tilde{y} \in \mathbb{R}^{\mathbb{N}^n}$ extending the subsequence $(y_\alpha)_{|\alpha| \leq 2s}$ satisfying:

2. Apply the 'finite rank moment matrix theorem':

(a)
$$V_{\mathbb{C}}(I) = V_{\mathbb{C}}(\ker M_s(y)) = \{v_1, \cdots, v_r\} \subseteq \mathbb{R}^n$$
.
(b) $\tilde{y} = \sum_{i=1}^r \lambda_i [v_i]_{\infty}$, where $v_i \in K$, $\lambda_i > 0$, $\sum_i \lambda_i = 1$.
(c) $(y_{\alpha})_{|\alpha| \leq 2s} = \sum_{i=1}^r \lambda_i [v_i]_{2s}$ where $v_i \in K$, $\lambda_i > 0$, $\sum_i \lambda_i = 1$.

3. Hence: $p_{\text{mom},t} = p_{\text{min}}$ and v_1, \dots, v_r are global minimizers.

Proof of Theorem 2 (continued)

Assume now L_y is an optimal solution for which rank $M_t(y)$ is maximum.

That is, for any other optimal solution z to $p_{\text{mom},t}$, we have rank $M_t(z) \leq \text{rank } M_t(y)$.

This implies ker $M_t(y) \subseteq \ker M_t(z)$, and thus ker $M_s(y) \subseteq \ker M_s(z)$, $V_{\mathbb{C}}(\ker M_s(z)) \subseteq V_{\mathbb{C}}(\ker M_s(y)) = V_{\mathbb{C}}(I) = \{v_1, \dots, v_r\}$. Let $x^* \in K$ be a global minimizer of p. Then $z = [x^*]_{2t}$ is an optimal solution of $p_{\text{mom},t}$. Therefore, $\{x^*\} = V_{\mathbb{C}}(\ker M_s(z)) \subseteq \{v_1, \dots, v_r\}$.

Some observations

• Use the 'eigenvalue method' to extract the global minimizers: via the eigenvectors of the multiplication matrix M_h for $h = \sum_{i=1}^n h_i x_i$.

All needed information is contained in $M_s(y)$: the entries of $M_h = \sum_{i=1}^n h_i M_{x_i}$ can be derived directly by expressing each $[x_i x^{\alpha_j}]$ in the basis $\mathcal{B} = \{[x^{\alpha_1}], \dots, [x^{\alpha_r}]\}.$

• If the flatness condition holds then *p* has **finitely many global minimizers** in *K*.

The converse is **not** true!

Example: Let $K = \{x : \sum_{i=1}^{n} x_i^2 \le 1\}$ and assume p is homogeneous, p > 0 on $\mathbb{R}^n \setminus \{0\}$, p is not SOS. Then, $p_{\min} = 0$, attained **only at** 0. But, $p_{\text{sos},t} = p_{\text{mom},t} < p_{\min} = 0$ for all $t \ge d_p$. **Fact:** $p \in \mathcal{M}(1 - \sum_i x_i^2) \implies p \in \Sigma$

• The flatness condition holds generically.

[Nie 2014]