

An elementary recursive bound for the Positivstellensatz

Daniel Perrucci

Universidad de Buenos Aires, Argentina

joint work with

Henri Lombardi

Université de Franche-Comté, France

and

Marie-Françoise Roy

IRMAR CNRS / Université de Rennes 1, France

Mathematics, Algorithms and Proofs 2012
Universität Konstanz, Germany

Positivstellensatz (Krivine '64, Stengle '74)

- \mathbf{K} an ordered field, \mathbf{R} a real closed extension of \mathbf{K} ,
- $P_1, \dots, P_s \in \mathbf{K}[x_1, \dots, x_k]$, • $I_{\neq}, I_{\geq}, I_{=} \subset \{1, \dots, s\}$,

$$\mathcal{H}(x) : \begin{cases} P_i(x) \neq 0 & \text{for } i \in I_{\neq} \\ P_i(x) \geq 0 & \text{for } i \in I_{\geq} \\ P_i(x) = 0 & \text{for } i \in I_{=} \end{cases} \quad \text{no solution in } \mathbf{R}^k \quad \iff$$

$$\exists \quad S = \prod_{i \in I_{\neq}} P_i^{2e_i}, \quad N = \sum_{I \subset I_{\geq}} \left(\sum_j k_{I,j} Q_{I,j}^2 \right) \prod_{i \in I} P_i \quad (k_{I,j} > 0),$$

$$Z \in \langle P_i \mid i \in I_{=} \rangle \subset \mathbf{K}[x]$$

such that

$$\underbrace{S}_{> 0} + \underbrace{N}_{\geq 0} + \underbrace{Z}_{= 0} = 0. \quad \leftarrow \quad \downarrow \mathcal{H} \downarrow$$

Example:

$$\begin{cases} x & \neq 0 \\ y - x^2 - 1 & \geq 0 \\ xy & = 0 \end{cases} \quad \text{no solution in } \mathbf{R}^2$$

$\downarrow x \neq 0, y - x^2 - 1 \geq 0, xy = 0 \downarrow$:

$$\underbrace{x^2}_{> 0} + \underbrace{x^2(y - x^2 - 1) + x^4}_{\geq 0} + \underbrace{(-x^2y)}_{= 0} = 0.$$

Considered systems:

$$\begin{cases} P_i(x) \neq 0 & \text{for } i \in I_{\neq} \\ P_i(x) \geq 0 & \text{for } i \in I_{\geq} \\ P_i(x) = 0 & \text{for } i \in I_{=} \end{cases}$$

For any given system:

$$P \leq 0 \longrightarrow -P \geq 0,$$

$$P > 0 \longrightarrow P \neq 0, \quad P \geq 0$$

$$P < 0 \longrightarrow -P \neq 0, \quad -P \geq 0$$

Algebraically closed case: Nullstellensatz

- \mathbf{K} a field, \mathbf{C} an algebraically closed extension of \mathbf{K} ,
- $P_1, \dots, P_s \in \mathbf{K}[x_1, \dots, x_k]$, • $I_{\neq}, I_{=} \subset \{1, \dots, s\}$,

$$\begin{cases} P_i(x) \neq 0 & \text{for } i \in I_{\neq} \\ P_i(x) = 0 & \text{for } i \in I_{=} \end{cases} \quad \text{no solution in } \mathbf{C}^k \quad \iff$$

$$\exists S = \prod_{i \in I_{\neq}} P_i^{e_i}, \quad Z \in \langle P_i \mid i \in I_{=} \rangle \subset \mathbf{K}[x] \quad \text{such that}$$

$$\underbrace{S}_{\neq 0} + \underbrace{Z}_{= 0} = 0.$$

Algebraically closed case: Nullstellensatz

$$S + Z = 0.$$

- Optimal bound (Jelonek '05):

$$S = \prod_{i \in I_{\neq}} P_i^{e_i} \quad \text{with} \quad e_i \leq d^k \quad (\deg P_i \leq d).$$

$$Z = \sum_{i \in I_{=}} P_i Q_i \quad \text{with} \quad \deg P_i Q_i \leq (1 + d|I_{\neq}|)d^k.$$

- from the degree bound, $Z = \sum_{i \in I_{=}} P_i Q_i$ can be obtained solving a linear system.

Real closed case: Positivstellensatz

$$S + N + Z = 0.$$

- Constructive proof ([Lombardi '90](#)) based in [Hörmander algorithm](#):
degree bound \rightarrow primitive recursive in k, s and d .
- [Our work \(in progress\)](#): New constructive proof based in [cylindrical decomposition](#):
degree bound \rightarrow elementary recursive in k, s and d .
(exponential tower of height 5)

Hilbert 17th problem

$$P \geq 0 \text{ in } \mathbb{R}^k \implies \exists P = \sum_i G_i^2, \quad G_i \in \mathbb{R}(x_1, \dots, x_k) ?$$

- Artin '27: Affirmative answer.
- Positivstellensatz implies Hilbert 17th problem:

$$\{ P(x) < 0 \text{ no solution} \iff \begin{cases} -P(x) \neq 0 \\ -P(x) \geq 0 \end{cases} \text{ no solution}$$

$$\iff P^{2e} + \sum_i Q_i^2 - (\sum_j R_j^2)P = 0 \iff$$

$$P = \frac{P^{2e} + \sum_i Q_i^2}{\sum_j R_j^2} = \frac{(P^{2e} + \sum_i Q_i^2)(\sum_j R_j^2)}{(\sum_j R_j^2)^2}.$$

Incompatibilities

$$\mathcal{H}(x) : \begin{cases} P_i(x) \neq 0 & \text{for } i \in I_{\neq} \\ P_i(x) \geq 0 & \text{for } i \in I_{\geq} \\ P_i(x) = 0 & \text{for } i \in I_{=} \end{cases}$$

$$\downarrow \mathcal{H} \downarrow : \quad \underbrace{S}_{> 0} + \underbrace{N}_{\geq 0} + \underbrace{Z}_{= 0} = 0$$

with

$$S \in \left\{ \prod_{i \in I_{\neq}} P_i^{2\theta_i} \right\} \quad \leftarrow \text{monoid associated to } \mathcal{H}$$

$$N \in \left\{ \sum_{I \subset I_{\geq}} \left(\sum_j k_{I,j} Q_{I,j}^2 \right) \prod_{i \in I} P_i \right\} \quad \leftarrow \text{cone associated to } \mathcal{H}$$

$$Z \in \langle P_i \mid i \in I_{=} \rangle \quad \leftarrow \text{ideal associated to } \mathcal{H}$$

monoid
part

cone
part

ideal
part

$$\downarrow \mathcal{H} \downarrow: \quad \underbrace{S}_{> 0} + \underbrace{N}_{\geq 0} + \underbrace{Z}_{= 0} = 0$$

$$\downarrow \mathcal{H}, A \neq 0 \downarrow: \quad \underbrace{A^{2e}S}_{> 0} + \underbrace{N}_{\geq 0} + \underbrace{Z}_{= 0} = 0$$

$$\downarrow \mathcal{H}, A \geq 0 \downarrow: \quad \underbrace{S}_{> 0} + \underbrace{N + N'A}_{\geq 0} + \underbrace{Z}_{= 0} = 0$$

$$\downarrow \mathcal{H}, A = 0 \downarrow: \quad \underbrace{S}_{> 0} + \underbrace{N}_{\geq 0} + \underbrace{Z + WA}_{= 0} = 0$$

Weak inferences

$$A > 0, \quad B \geq 0 \quad \Longrightarrow \quad A + B > 0.$$

Let \mathcal{H} be a system of sign conditions.

$$\downarrow \mathcal{H}, \quad A + B > 0 \quad \downarrow \quad \longrightarrow \quad \begin{cases} \mathcal{H}(x) \\ A(x) + B(x) > 0 \end{cases} \quad \text{no solution}$$

$$\downarrow \mathcal{H}, \quad A > 0, \quad B \geq 0 \quad \downarrow \quad \longleftarrow \quad \begin{cases} \mathcal{H}(x) \\ A(x) > 0 \\ B(x) \geq 0 \end{cases} \quad \text{no solution}$$

$$A > 0, \quad B \geq 0 \quad \vdash \quad A + B > 0$$

$$A > 0, AB \geq 0 \vdash B \geq 0$$

$$\downarrow \mathcal{H}, B \geq 0 \downarrow$$

$$\underbrace{S}_{> 0} + \underbrace{N + N'B}_{\geq 0} + \underbrace{Z}_{= 0} = 0$$

↓

$$\underbrace{A^2 S}_{> 0} + \underbrace{NA^2 + N'A(AB)}_{\geq 0} + \underbrace{ZA^2}_{= 0} = 0$$

$$\downarrow \mathcal{H}, A \neq 0, A \geq 0, AB \geq 0 \downarrow \rightarrow \downarrow \mathcal{H}, A > 0, AB \geq 0 \downarrow$$

$$A \neq 0 \quad \vdash \quad A < 0 \quad \vee \quad A > 0$$

Let \mathcal{H} be a system of sign conditions.

$$\downarrow \mathcal{H}, A < 0 \downarrow \longrightarrow \left\{ \begin{array}{l} \mathcal{H}(x) \\ A(x) < 0 \end{array} \right. \text{ no solution}$$

$$\downarrow \mathcal{H}, A > 0 \downarrow \longrightarrow \left\{ \begin{array}{l} \mathcal{H}(x) \\ A(x) > 0 \end{array} \right. \text{ no solution}$$

$$\downarrow \mathcal{H}, A \neq 0 \downarrow \longleftarrow \left\{ \begin{array}{l} \mathcal{H}(x) \\ A(x) \neq 0 \end{array} \right. \text{ no solution}$$

$$A \neq 0 \vdash A < 0 \vee A > 0$$

$\downarrow \mathcal{H}, A < 0 \downarrow$

$\downarrow \mathcal{H}, A > 0 \downarrow$

$$\underbrace{A^{2e_1} S_1}_{>0} + \underbrace{N_1 - N'_1 A}_{\geq 0} + \underbrace{Z_1}_{=0} = 0$$

$$A^{2e_1} S_1 + N_1 + Z_1 = N'_1 A$$

$$\underbrace{A^{2e_2} S_2}_{>0} + \underbrace{N_2 + N'_2 A}_{\geq 0} + \underbrace{Z_2}_{=0} = 0$$

$$A^{2e_2} S_2 + N_2 + Z_2 = -N'_2 A$$



$$A^{2e_1+2e_2} S_1 S_2 + N_3 + Z_3 = -N'_1 N'_2 A^2$$

$$\underbrace{A^{2e_1+2e_2} S_1 S_2}_{>0} + \underbrace{N'_1 N'_2 A^2 + N_3}_{\geq 0} + \underbrace{Z_3}_{=0} = 0$$

$\downarrow \mathcal{H}, A \neq 0 \downarrow$

$$A \neq 0 \implies A = 0 \vee A < 0 \vee A > 0$$

$$A = 0 \vee A < 0 \vee A > 0$$

Similarly,

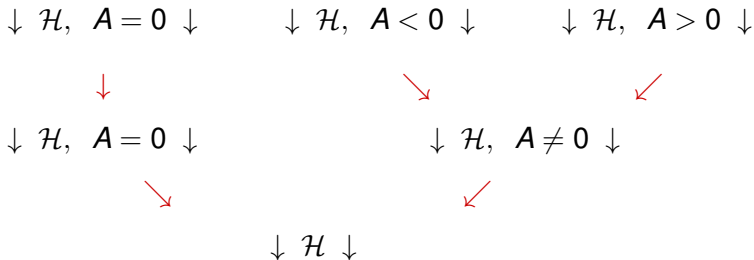
$$A \neq 0 \vdash A = 0 \vee A < 0 \vee A > 0$$

$$\vdash A = 0 \vee A < 0 \vee A > 0$$

$$\begin{array}{l} \vdash A = 0 \vee A \neq 0 \\ A \neq 0 \vdash A < 0 \vee A > 0 \end{array}$$

$$\vdash A = 0 \vee A < 0 \vee A > 0$$

as follows:



Weak Existence

$$\exists t \mid tA = 1 \vdash A \neq 0$$

$$\downarrow \mathcal{H}, A \neq 0 \downarrow$$

$$\underbrace{A^{2e}S}_{>0} + \underbrace{N}_{\geq 0} + \underbrace{Z}_{=0} = 0$$



$$\underbrace{S}_{>0} + \underbrace{t^{2e}N}_{\geq 0} + \underbrace{t^{2e}Z + ((tA)^{2e} - 1)S}_{=0} = 0$$

$$\downarrow \mathcal{H}, tA = 1 \downarrow \quad \leftarrow \text{involves the new variable } t$$

$$A \neq 0 \quad \vdash \quad \exists t \quad | \quad tA = 1$$

$\downarrow \mathcal{H}, tA = 1 \downarrow$ \leftarrow involves variable t

$$\underbrace{S}_{>0} + \underbrace{\sum (\sum k_{l,j} Q_{l,j}^2(t)) \prod P_i}_{\geq 0} + \underbrace{\sum W_j(t) P_j + W(t)(tA - 1)}_{=0} = 0$$

\downarrow

$$\underbrace{A^{2e} S}_{>0} + \underbrace{N}_{\geq 0} + \underbrace{Z}_{=0} = 0$$

$\downarrow \mathcal{H}, A \neq 0 \downarrow$ \leftarrow variable t is **eliminated**

Obtaining the incompatibility: example

$$P_0(x_1, x_2) = x_1^2 + x_2^2, \quad P_1(x_1, x_2) = x_1^2 + x_2^2 - 1.$$

$$\mathcal{H} = \begin{cases} P_0(x_1, x_2) = 0 \\ P_1(x_1, x_2) \geq 0 \end{cases} \quad \text{no solution in } \mathbf{R}^2.$$

Realizable systems of **strict** sign conditions for P_0, P_1 :

$$\begin{cases} P_0(x_1, x_2) > 0 \\ P_1(x_1, x_2) > 0 \end{cases} \quad \begin{cases} P_0(x_1, x_2) > 0 \\ P_1(x_1, x_2) = 0 \end{cases}$$

$$\begin{cases} P_0(x_1, x_2) > 0 \\ P_1(x_1, x_2) < 0 \end{cases} \quad \begin{cases} P_0(x_1, x_2) = 0 \\ P_1(x_1, x_2) < 0 \end{cases}$$

$$P_0(x_1, x_2) = x_1^2 + x_2^2, \quad P_1(x_1, x_2) = x_1^2 + x_2^2 - 1.$$

$$\mathcal{H} = \begin{cases} P_0(x_1, x_2) = 0 \\ P_1(x_1, x_2) \geq 0 \end{cases}$$

$$\vdash (P_0 > 0, P_1 > 0) \vee (P_0 > 0, P_1 = 0) \vee \\ (P_0 > 0, P_1 < 0) \vee (P_0 = 0, P_1 < 0).$$

- $\downarrow \mathcal{H}, P_0 > 0, P_1 > 0 \downarrow:$ $P_0^2 + 0 + (-P_0^2) = 0.$
- $\downarrow \mathcal{H}, P_0 > 0, P_1 = 0 \downarrow:$ $P_0^2 + 0 + (-P_0^2) = 0.$
- $\downarrow \mathcal{H}, P_0 > 0, P_1 < 0 \downarrow:$ $P_0^2 + 0 + (-P_0^2) = 0.$
- $\downarrow \mathcal{H}, P_0 = 0, P_1 < 0 \downarrow:$ $(-P_1)^2 + P_1(-P_1) + 0 = 0.$

$$P_0(x_1, x_2) = x_1^2 + x_2^2, \quad P_1(x_1, x_2) = x_1^2 + x_2^2 - 1.$$

$$\begin{aligned} & x_1 < -1 \quad \vee \quad x_1 = -1 \quad \vee \quad -1 < x_1 < 0 \quad \vee \\ \vdash & x_1 = 0 \quad \vee \quad 0 < x_1 < 1 \quad \vee \quad x_1 = 1 \quad \vee \\ & 1 < x_1. \end{aligned}$$

$$x_1 < -1 \quad \vdash \quad P_0 > 0, \quad P_1 > 0.$$

$$x_1 = -1 \quad \vdash \quad (P_0 > 0, \quad P_1 > 0) \quad \vee \quad (P_0 > 0, \quad P_1 = 0).$$

$$\begin{aligned} -1 < x_1 < 0 \quad \vdash & (P_0 > 0, \quad P_1 > 0) \quad \vee \quad (P_0 > 0, \quad P_1 = 0) \quad \vee \\ & (P_0 > 0, \quad P_1 < 0). \end{aligned}$$

⋮

$$P_0(x_1, x_2) = x_1^2 + x_2^2, \quad P_1(x_1, x_2) = x_1^2 + x_2^2 - 1.$$

$$-1 < x_1 < 0 \quad \vdash \quad \exists(a, b, t_1, t_2) \quad \left| \quad \begin{array}{l} -2ax_1 = 0, \quad a^2 + b^2 = x_1^2, \\ -(t_1 + t_2) = 0, \quad t_1 t_2 = x_1^2 - 1, \\ b \neq 0, \quad t_1 < t_2. \end{array} \right.$$

- $P_0(x_1, x_2) = (x_2 - a)^2 + b^2$ with $b \neq 0$,
- $P_1(x_1, x_2) = (x_2 - t_1)(x_2 - t_2)$ with $t_1 < t_2$.

Obtaining the incompatibility: general case

- $\mathcal{P} = P_1, \dots, P_s \subset \mathbf{R}[x_1, \dots, x_k]$,
- $I_{\neq}, I_{\geq}, I_{=} \subset \{1, \dots, s\}$,

$$\mathcal{H} = \begin{cases} P_i(x) \neq 0 & \text{for } i \in I_{\neq} \\ P_i(x) \geq 0 & \text{for } i \in I_{\geq} \\ P_i(x) = 0 & \text{for } i \in I_{=} \end{cases} \quad \text{no solution in } \mathbf{R}^k.$$

- For any realizable strict sign condition σ on \mathcal{P} ,

$$\downarrow \mathcal{H}, \text{ sign}(\mathcal{P}) = \sigma \downarrow$$

- a weak inference

$$\vdash \bigvee_{\sigma \text{ realizable for } \mathcal{P}} \text{sign}(\mathcal{P}) = \sigma.$$

- For any realizable strict sign condition σ on \mathcal{P} ,

$$\downarrow \mathcal{H}, \text{ sign}(\mathcal{P}) = \sigma \downarrow$$

\mathcal{H} is given by a **non realizable** sign condition on \mathcal{P} . We have at least one conflict of signs:

\mathcal{H}	$\text{sign}(\mathcal{P}) = \sigma$	\mathcal{H}	$\text{sign}(\mathcal{P}) = \sigma$
$P_i > 0$	$P_i = 0$	$P_i \leq 0$	$P_i > 0$
$P_i > 0$	$P_i < 0$	$P_i < 0$	$P_i > 0$
$P_i \geq 0$	$P_i < 0$	$P_i < 0$	$P_i = 0$
$P_i = 0$	$P_i > 0$	$P_i \neq 0$	$P_i = 0$
$P_i = 0$	$P_i < 0$		

$$P_i^2 - P_i^2 = 0$$

- $\vdash \bigvee_{\sigma \text{ realizable for } \mathcal{P}} \text{sign}(\mathcal{P}) = \sigma.$

$$\mathcal{P} = \mathcal{P}_k \subset \mathbf{R}[x_1, \dots, x_k]$$

$$\mathcal{P}_{k-1} \subset \mathbf{R}[x_1, \dots, x_{k-1}]$$

$$\vdots$$

$$\mathcal{P}_1 \subset \mathbf{R}[x_1]$$

$$\mathcal{P}_0 = \emptyset$$

For every realizable strict sign condition τ for \mathcal{P}_{j-1} ,

$$\text{sign}(\mathcal{P}_{j-1}) = \tau \vdash \bigvee_{\substack{\sigma \text{ realizable for } \mathcal{P}_j \\ \text{with } \text{sign}(\mathcal{P}_{j-1}) = \tau}} \text{sign}(\mathcal{P}_j) = \sigma.$$

Factorization of family \mathcal{P}_j and for

- 1) $\text{sign}(\mathcal{P}_{j-1}) = \tau \vdash$ all $Q_1, Q_2 \in \mathcal{P}_j$, sign of every derivative of Q_2 at real roots of Q_1 .

Factorization of family \mathcal{P}_j and for

- 2) all $Q_1, Q_2 \in \mathcal{P}_j$, sign of every derivative of Q_2 at real roots of Q_1 .

Factorization of

- \vdash family \mathcal{P}_j and order of real roots.

Factorization of

- 3) family \mathcal{P}_j and order of real roots. \vdash

$\bigvee_{\substack{\sigma \text{ realizable for } \mathcal{P}_j \\ \text{with } \text{sign}(\mathcal{P}_{j-1})=\tau}} \text{sign}(\mathcal{P}_j) = \sigma.$

Factorization of family \mathcal{P}_j and for

- 1) $\text{sign}(\mathcal{P}_{j-1}) = \tau \quad \vdash$ all $Q_1, Q_2 \in \mathcal{P}_j$, sign of every derivative of Q_2 at real roots of Q_1 .

Hermite Theory: $q = \deg_{x_j} Q_1$, $\text{Her}(Q_1, Q_2) \in \mathbf{K}[x_1, \dots, x_{j-1}]^{q \times q}$

$\text{Her}(Q_1, Q_2)_{\ell_1, \ell_2} = \text{Trace of mult. by } x_j^{\ell_1 + \ell_2} Q_2 \text{ in } \mathbf{K}[x] / \langle Q_1 \rangle.$

$$\begin{aligned} \text{Signature}(\text{Her}(Q_1, Q_2)_{\ell_1, \ell_2}) &= \\ &= \#\{t \in \mathbf{R} \mid Q_1(t) = 0, Q_2(t) > 0\} - \\ &\quad - \#\{t \in \mathbf{R} \mid Q_1(t) = 0, Q_2(t) < 0\}. \end{aligned}$$

Factorization of family \mathcal{P}_j and for

- 2) all $Q_1, Q_2 \in \mathcal{P}_j$, sign of every derivative of Q_2 at real roots of Q_1 .

Factorization of

- family \mathcal{P}_j and order of real roots.

Thom encoding of real algebraic numbers:

Example: P monic, $\deg P = 4$.

$$\begin{array}{ll} P(t_1) < 0, & P(t_2) = 0, \\ P'(t_1) = 0, & P'(t_2) > 0, \\ P''(t_1) > 0, & P''(t_2) > 0, \\ P'''(t_1) < 0, & P'''(t_2) < 0, \end{array} \implies t_1 < t_2$$

Factorization of

- 3) family \mathcal{P}_j and order \vdash of real roots. $\bigvee_{\substack{\sigma \text{ realizable for } \mathcal{P}_j \\ \text{with } \text{sign}(\mathcal{P}_{j-1})=\tau}} \text{sign}(\mathcal{P}_j) = \sigma.$

Partition of the real line according to real roots.

Thanks!