# Zeros of structured polynomials over the reals and p-adics

Peter Bürgisser

WACT 2023

Warwick University, 28 March 2023

# Real zeros of sparse polynomials

- Study number $N(f)$ of positive real zeros of univariate polynomial $f$.
- If $f$ has at most $t$ monomial terms, call it $t$-sparse.
- Descartes rule (sharp): $N(f) \leq t - 1$ if $f$ is $t$-sparse.
- Clearly,

$$N(f_1 \cdots f_k) \leq k(t-1) \text{ if } f_1, \ldots, f_k \text{ are } t\text{-sparse.}$$

- How about

$$f_1 \cdots f_k - 1 \quad ?$$

- Expanding and Descartes give $N(f_1 \cdots f_k - 1) \leq t^k$.
- Is this bound pessimistic?

# Real zeros of sparse polynomials

- Study number $N(f)$ of positive real zeros of univariate polynomial $f$.
- If $f$ has at most $t$ monomial terms, call it $t$-sparse.
- Descartes rule (sharp): $N(f) \leq t-1$ if $f$ is $t$-sparse.
- Clearly,

$$N(f_1 \cdots f_k) \leq k(t-1) \text{ if } f_1, \ldots, f_k \text{ are } t\text{-sparse.}$$

- How about

$$f_1 \cdots f_k - 1 \quad ?$$

- Expanding and Descartes give $N(f_1 \cdots f_k - 1) \leq t^k$.
- Is this bound pessimistic?

# Polynomials given by ΣΠΣΠ-circuits

- For a support $S \subseteq \mathbb{N}$ with $|S| \leq t$ define

$$f_S(X) := \sum_{s \in S} u_s X^s, \qquad \text{where } u_s \in \mathbb{R}.$$

- Fix a system of supports $S_{ij} \subseteq \mathbb{N}$, where $1 \leq i \leq m$ and $1 \leq j \leq k_i$. We assume $|S_{ij}| \leq t$ and $k_i \leq k$.
- Consider the sum of products of sparse polynomials

$$F(X) := \sum_{i=1}^{m} f_{i1}(X) \cdot \ldots \cdot f_{ik_i}(X) X^{d_i},$$

where $f_{ij} := f_{S_{ij}}$ and $d_1 \leq d_2 \leq \ldots \leq d_m$, $d_i \in \mathbb{N}$.

- Using $f_{d+S}(X) = X^d f_S(X)$, can w.l.o.g. assume $0 \in S_{ij}$ and $d_1 = 0$.
- Upper bounds on $NF$ by Grenet, Koiran, Portier, Strozeki, Tavenas (2011, 2014) showed via Wronskian.

# Polynomials given by ΣΠΣΠ-circuits

- For a support $S \subseteq \mathbb{N}$ with $|S| \leq t$ define

$$f_S(X) := \sum_{s \in S} u_s X^s, \quad \text{where } u_s \in \mathbb{R}.$$

- Fix a system of supports $S_{ij} \subseteq \mathbb{N}$, where $1 \leq i \leq m$ and $1 \leq j \leq k_i$. We assume $|S_{ij}| \leq t$ and $k_i \leq k$.
- Consider the sum of products of sparse polynomials

$$F(X) := \sum_{i=1}^{m} f_{i1}(X) \cdot \ldots \cdot f_{ik_i}(X) X^{d_i},$$

where $f_{ij} := f_{S_{ij}}$ and $d_1 \leq d_2 \leq \ldots \leq d_m$, $d_i \in \mathbb{N}$.
- Using $f_{d+S}(X) = X^d f_S(X)$, can w.l.o.g. assume $0 \in S_{ij}$ and $d_1 = 0$.
- Upper bounds on $NF$ by Grenet, Koiran, Portier, Strozeki, Tavenas (2011, 2014) showed via Wronskian.

# Koiran's Real Tau Conjecture

## Real Tau Conjecture

The number of real zeros of $F$ is bounded by a polynomial in $m, k, t$.

Surprisingly, it is related to Valiant's Conjecture in characteristic zero.

**Thm** (Koiran 2011)

The Real Tau Conjecture implies $\mathrm{VP}^0 \neq \mathrm{VNP}^0$.

Tavenas (2014):

- The Real Tau Conjecture also implies $\mathrm{VP} \neq \mathrm{VNP}$ (allow circuits using any complex constants).
- $\mathrm{VP} \neq \mathrm{VNP}$ can even be derived from weaker bound

$$N(F) \leq \mathrm{poly}(m, t, 2^{k \log k})$$

Note: $N(F) \leq mt^k = m2^{k \log t}$ since $F$ is $mt^k$-sparse.

# Koiran's Real Tau Conjecture

## Real Tau Conjecture

The number of real zeros of $F$ is bounded by a polynomial in $m, k, t$.

Surprisingly, it is related to Valiant's Conjecture in characteristic zero.

## Thm (Koiran 2011)

The Real Tau Conjecture implies $\mathrm{VP}^0 \neq \mathrm{VNP}^0$.

Tavenas (2014):

- The Real Tau Conjecture also implies $\mathrm{VP} \neq \mathrm{VNP}$ (allow circuits using any complex constants).
- $\mathrm{VP} \neq \mathrm{VNP}$ can even be derived from weaker bound

$$N(F) \leq \mathrm{poly}(m, t, 2^{k \log k})$$

Note: $N(F) \leq mt^k = m2^{k \log t}$ since $F$ is $mt^k$-sparse.

# Koiran's Real Tau Conjecture

## Real Tau Conjecture

The number of real zeros of $F$ is bounded by a polynomial in $m, k, t$.

Surprisingly, it is related to Valiant's Conjecture in characteristic zero.

## Thm (Koiran 2011)

The Real Tau Conjecture implies $\mathrm{VP}^0 \neq \mathrm{VNP}^0$.

Tavenas (2014):

- The Real Tau Conjecture also implies $\mathrm{VP} \neq \mathrm{VNP}$ (allow circuits using any complex constants).
- $\mathrm{VP} \neq \mathrm{VNP}$ can even be derived from weaker bound

$$N(F) \leq \mathrm{poly}(m, t, 2^{k \log k})$$

Note: $N(F) \leq mt^k = m2^{k \log t}$ since $F$ is $mt^k$-sparse.

# Related results

Tau Conjecture: The number of integer zeros of $f \in \mathbb{Z}[X]$ is bounded by a polynomial in the arithmetic circuit size of $f$.

**Thm** (Shub & Smale 1995)

The Tau Conjecture implies $\mathrm{P}_{\mathbb{C}} \neq \mathrm{NP}_{\mathbb{C}}$.

**Thm** (B 2009)

The Tau Conjecture implies $\mathrm{VP}^0 \neq \mathrm{VNP}^0$.

Koiran's implication is based on refining my proof of this result, combined with reduction to depth 4 (Agrawal and Vinay 2008).

# Related results

Tau Conjecture: The number of integer zeros of $f \in \mathbb{Z}[X]$ is bounded by a polynomial in the arithmetic circuit size of $f$.

**Thm** (Shub & Smale 1995)

The Tau Conjecture implies $\mathrm{P}_{\mathbb{C}} \neq \mathrm{NP}_{\mathbb{C}}$.

**Thm** (B 2009)

The Tau Conjecture implies $\mathrm{VP}^0 \neq \mathrm{VNP}^0$.

Koiran's implication is based on refining my proof of this result, combined with reduction to depth 4 (Agrawal and Vinay 2008).

# A *p*-adic Tau Conjecture

- Completing the field $\mathbb{Q}$ with respect to absolute value $|\ |$ leads to $\mathbb{R}$.
- There are also the *p*-adic absolute values (nonarchimedean):

$$|x|_p = p^{-\nu} \text{ if } x = p^\nu \tfrac{a}{b} \text{ with } a, b \in \mathbb{Z} \text{ not divisible by } p$$

- E.g., $|12|_2 = |2^2 \cdot 3|_2 = 2^{-2}$ and $|2^\nu|_2 = 2^{-\nu} \to 0$ for $\nu \to \infty$.
- Can formulate *p*-adic Tau Conjecture. Similarly as over $\mathbb{R}$ one shows:

$$p\text{-adic Tau Conjecture} \Longrightarrow \mathrm{VP}^0 \neq \mathrm{VNP}^0$$

- Over $\mathbb{Q}_p$ this conjecture may be easier to cope with than over $\mathbb{R}$!
- Smaller question: Can one infer $\mathrm{VP} \neq \mathrm{VNP}$?
- Encouragement: Recent insights (especially on on random polynomials) show that the situation over $\mathbb{Q}_p$ is much easier to understand than over $\mathbb{R}$.

# A $p$-adic Tau Conjecture

- Completing the field $\mathbb{Q}$ with respect to absolute value $|\ |$ leads to $\mathbb{R}$.
- There are also the $p$-adic absolute values (nonarchimedean):

$$|x|_p = p^{-\nu} \text{ if } x = p^{\nu}\frac{a}{b} \text{ with } a, b \in \mathbb{Z} \text{ not divisible by } p$$

- E.g., $|12|_2 = |2^2 \cdot 3|_2 = 2^{-2}$ and $|2^{\nu}|_2 = 2^{-\nu} \to 0$ for $\nu \to \infty$.
- Can formulate $p$-adic Tau Conjecture. Similarly as over $\mathbb{R}$ one shows:

$$p\text{-adic Tau Conjecture} \Longrightarrow \mathrm{VP}^0 \neq \mathrm{VNP}^0$$

- Over $\mathbb{Q}_p$ this conjecture may be easier to cope with than over $\mathbb{R}$!
- Smaller question: Can one infer $\mathrm{VP} \neq \mathrm{VNP}$?
- Encouragement: Recent insights (especially on on random polynomials) show that the situation over $\mathbb{Q}_p$ is much easier to understand than over $\mathbb{R}$.

# Some known facts on zeros of $p$-adic polynomials

- $p$-adic Descartes' rule (Lenstra 1999): $t$-sparse univariate polynomial $f \in \mathbb{Q}_p[X]$ has at most $O(pt^2 \log t)$ zeros in $\mathbb{Q}_p$.
- There are $f \in \mathbb{Q}_p[X]$ with $\Theta(t^2)$ many zeros
- Some improvements by Krick and Avendano (2011).

- Rojas 2004: Bound on number of $p$-adic zeros for fewnomial systems

$$f_i(x_1, \ldots, x_n) = 0, \quad i = 1, \ldots, n.$$

of the form

$$N_{\mathbb{Q}_p}(f_1, \ldots, f_n) = O(pt)^{O(n)}.$$

Can be seen as $p$-adic version of Kushnirenko's Conjecture, which is unknown over $\mathbb{R}$.

# Some known facts on zeros of $p$-adic polynomials

- $p$-adic Descartes' rule (Lenstra 1999): $t$-sparse univariate polynomial $f \in \mathbb{Q}_p[X]$ has at most $O(pt^2 \log t)$ zeros in $\mathbb{Q}_p$.
- There are $f \in \mathbb{Q}_p[X]$ with $\Theta(t^2)$ many zeros
- Some improvements by Krick and Avendano (2011).

- Rojas 2004: Bound on number of $p$-adic zeros for fewnomial systems

$$f_i(x_1, \ldots, x_n) = 0, \quad i = 1, \ldots, n.$$

of the form

$$N_{\mathbb{Q}_p}(f_1, \ldots, f_n) = O(pt)^{O(n)}.$$

Can be seen as $p$-adic version of Kushnirenko's Conjecture, which is unknown over $\mathbb{R}$.

# Bounds for random polynomials

# The Real Tau Conjecture is true on average

- Recall the sum of products of sparse polynomials:

$$F(X) := \sum_{i=1}^{m} f_{i1}(X) \cdot \ldots \cdot f_{ik_i}(X) X^{d_i},$$

where $f_{ij} := f_{S_{ij}}$ and $S_{ij}$ with $|S_{ij}| \leq t$ is a support system as before.

- We assume $f_{ij}(X)$ has independent standard gaussian coefficients:

$$f_{ij}(X) := \sum_{s \in S_{ij}} u_{ijs} X^s, \quad u_{ijs} \sim N(0,1).$$

**Thm** (Briquel & B, Random Structures & Algorithms 2020)

$$\mathbb{E}\#\{x \in \mathbb{R} \mid F(x) = 0\} = O(mk^2 t)$$

Note this is an almost linear upper bound on the number of real zeros! So typically, there are only very few real zeros.

# The Kac-Rice formula

- Assume parametrization $\mathbb{R}^N \to \mathbb{R}[X]_{\leq D}, u \mapsto F(u,X)$ of family of structured polynomials.
- Fix prob. density on $\mathbb{R}^N$, so that $F(u,X)$ becomes random polynomial.
- For $x \in \mathbb{R}$, suppose the random variable $u \mapsto F(u,x)$ has density $\rho_{F(x)}$.

**Kac-Rice Formula**

Under some technical assumptions (see Azaïs & Wschebor)

$$\mathbb{E}_u \#\{x \in [0,1] \mid F(u,x) = 0\} = \int_0^1 \mathbb{E}\left(|F'(x)| \middle| F(x) = 0\right) \rho_{F(x)}(0)\, dx.$$

- The conditional expectation is not easy to deal with.
- Technical assumptions hard to verify, but can can infer $\leq$ under less assumptions.

# The Kac-Rice formula

- Assume parametrization $\mathbb{R}^N \to \mathbb{R}[X]_{\le D}, u \mapsto F(u, X)$ of family of structured polynomials.
- Fix prob. density on $\mathbb{R}^N$, so that $F(u, X)$ becomes random polynomial.
- For $x \in \mathbb{R}$, suppose the random variable $u \mapsto F(u, x)$ has density $\rho_{F(x)}$.

## Kac-Rice Formula

Under some technical assumptions (see Azaïs & Wschebor)

$$\mathbb{E}_u \#\{x \in [0,1] \mid F(u,x) = 0\} = \int_0^1 \mathbb{E}\left(|F'(x)| \,\middle|\, F(x) = 0\right) \rho_{F(x)}(0)\, dx.$$

- The conditional expectation is not easy to deal with.
- Technical assumptions hard to verify, but can can infer $\le$ under less assumptions.

# Simple application: random linear combinations

- Fix $C^1$ weight functions $w_i : \mathbb{R} \to \mathbb{R}$ with variation

$$V(w_i) := \int_0^1 |w_i'(x)|\, dx$$

- Note $V(w_i) = |w_i(1) - w_i(0)|$ if $w_i$ is monotonous.
- Consider random linear combination

$$F(x) := \sum_{i=1}^{t} u_i w_i(x), \qquad u_i \text{ independent r.v.}$$

where density $\varphi_i$ of $u_i$ satisfies $\sup \varphi_i \le A$ and $\int_{\mathbb{R}} |u_i| \varphi_i(u_i)\, du_i \le B$.

- The Kac-Rice formula implies (assume $w_1(x) = 1$)

$$\mathbb{E}_u \#\{x \in [0,1] \mid F(u,x) = 0\} \le AB \sum_{i=2}^{t} V(w_i)$$

- Probabilistic version of Descartes rule obtained for $w_i(x) = x^{d_i}$. The expectation bound is $AB(t-1)$.
- Optimal bound on expectation is $O(\sqrt{t})$ for standard gaussian $u_i$: [B, Erguer, Tonelli-Cueto] and [Jindal, Pandey, Shukla, Zisopoulos 2020].

# Simple application: random linear combinations

- Fix $C^1$ weight functions $w_i\colon \mathbb{R} \to \mathbb{R}$ with variation

$$V(w_i) := \int_0^1 |w_i'(x)|\, dx$$

- Note $V(w_i) = |w_i(1) - w_i(0)|$ if $w_i$ is monotonous.
- Consider random linear combination

$$F(x) := \sum_{i=1}^{t} u_i w_i(x), \qquad u_i \text{ independent r.v.}$$

  where density $\varphi_i$ of $u_i$ satisfies $\sup \varphi_i \le A$ and $\int_{\mathbb{R}} |u_i| \varphi_i(u_i)\, du_i \le B$.
- The Kac-Rice formula implies (assume $w_1(x) = 1$)

$$\mathbb{E}_u \#\{x \in [0,1] \mid F(u,x) = 0\} \le AB \sum_{i=2}^{t} V(w_i)$$

- Probabilistic version of Descartes rule obtained for $w_i(x) = x^{d_i}$. The expectation bound is $AB(t-1)$.
- Optimal bound on expectation is $O(\sqrt{t})$ for standard gaussian $u_i$: [B, Erguer, Tonelli-Cueto] and [Jindal, Pandey, Shukla, Zisopoulos 2020].

# Special case: all $f_{ij}(x)$ have constant term

- Consider $F(X)$ from before where all $d_i = 0$, i.e.,

$$F(X) := \sum_{i=1}^{m} f_{i1}(X) \cdot \ldots \cdot f_{ik_i}(X).$$

  The $f_{ij}(X)$ has support $S_{ij}$ and $0 \in S_{ij}$; hence all $f_{ij}$ have a.s. nonzero constant term

- Kac-Rice formula implies with some work

$$\mathbb{E}_u \#\{x \in [0,1] \mid F(x) = 0\} \leq AB \sum_{i=1}^{m} \sum_{j=1}^{k_i} \int_0^1 y_{ij}'(x)\, dx \leq AB\, mk(t-1),$$

  where $y_{ij}(x) := \sum_{s \in S_{ij}} x^s$.

- This bound only makes few assumptions on distribution of coefficients.

$$\boxed{\text{Considerable difficulty: remove assumption } 0 \in S_{ij}}$$

# Dealing with singularities

- Now assume $f_{ij}$ has standard gaussian coefficients.
- Define $\alpha_{ij}(x) := \mathbb{E} f_{ij}(x)^2 = \sum_{s \in S_{ij}} x^{2s}$.
- Reduce to counting zeros of random linear combinations

$$R(x) = \sum_{i=1}^{m} v_i q_i(x) x^{d_i}$$

  with independent random $v_i$, whose distribution is the one of a product of $k_i$ standard gaussians.
- The weight functions

$$q_i(x) := \prod_{j=1}^{k_i} \left( \frac{\alpha_{ij}(x)}{\alpha_{1j}(x)} \right)^{\frac{1}{2}},$$

  are obtained by multiplying and dividing sparse sums of squares in a way reflecting the build-up of the arithmetic circuit forming $F$.
- Key technical idea: introduce logarithmic variation of $p$

$$LV(q) := \int_0^1 \left| \frac{d}{dx} \ln q(x) \right| dx = \int_0^1 \left| \frac{q'(x)}{q(x)} \right| dx.$$

# Open problems

- Prove à la Tavenas that (allow circuits with any constants)

$$p\text{-adic Tau Conjecture} \Longrightarrow \mathrm{VP} \neq \mathrm{VNP}$$

- Is the $p$-adic Tau Conjecture true on average?
- (Dis)prove the $p$-adic Tau Conjecture.

Thank you for your attention!