A Wronskian approach to the real τ-conjecture

Pascal Koiran, Natacha Portier and Sébastien Tavenas

September 18, 2012

Plan

1. Introduction
   - Arithmetic circuits
   - τ-conjecture
2. real τ-conjecture
   - SPS
   - Conjecture
3. Results
   - Main tool
   - Upper bound
   - Application for different models

Plan

1. Introduction
   - Arithmetic circuits
   - τ-conjecture
2. real τ-conjecture
   - SPS
   - Conjecture
3. Results
   - Main tool
   - Upper bound
   - Application for different models

Arithmetic circuits

Polynomial

$f(x, y) = x^2 - xy$

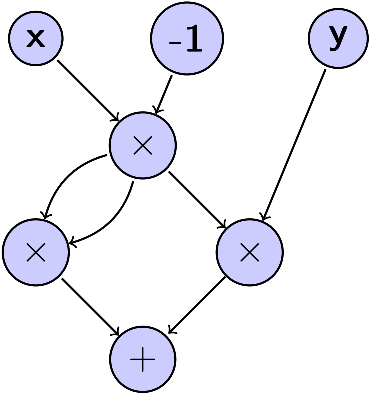
Representation by circuits (gates: $+$, $*$, $-$, variables and constants $0, 1, -1$):

Arithmetic circuits

Polynomial

$f(x,y) = x^2 - xy$

Representation by circuits (gates: $+$, $*$, $-$, variables and constants $0, 1, -1$):



Circuits complexity

Complexity of a polynomial

$\tau(P)$ = size of the smallest circuit computing P.

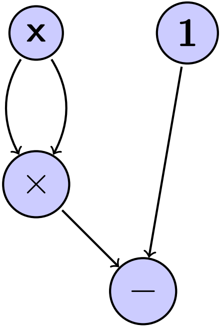
Example: $P(x) = x^2 - 1$: we get $\tau(P) = 4$

Circuits complexity

Complexity of a polynomial

$\tau(P) =$ size of the smallest circuit computing P.

Example: $P(x) = x^2 - 1$: we get $\tau(P) = 4$



Circuits complexity

Complexity of a polynomial

$\tau(P)$ = size of the smallest circuit computing P.

Example: $P(x) = x^2 - 1$: we get $\tau(P) = 4$

Complexity of a sequence of polynomials

$Q_n(x_1, \ldots, x_n) = (x_1 x_2 \ldots x_n)^2$ then $\tau(Q_n) = 2n$

Circuits complexity

Complexity of a polynomial

$\tau(P) =$ size of the smallest circuit computing P.

Example: $P(x) = x^2 - 1$: we get $\tau(P) = 4$

Complexity of a sequence of polynomials

$Q_n(x_1, \ldots, x_n) = (x_1 x_2 \ldots x_n)^2$ then $\tau(Q_n) = 2n$

- Example: $Det_n\left((x_{i,j})_{i,j \leq n}\right)$

Valiant's Conjecture

Class VP^0

(f_n): there exists c such that for all $n \geq 2$

- at most n^c variables
- $\tau(f_n) \leq n^c$
- formal degree is bounded by n^c

$$\mathrm{Det}_n((x_{i,j})_{i,j\leq n}) = \sum_{\sigma\in\mathfrak{S}_n} (-1)^{\epsilon(\sigma)} \prod_{i=1}^{n} x_{i,\sigma(i)}$$

Valiant's Conjecture

Class VP^0

(f_n): there exists c such that for all $n \geq 2$

- at most n^c variables
- $\tau(f_n) \leq n^c$
- formal degree is bounded by n^c

Class VNP^0

(g_n): there exists $(f_n) \in \mathrm{VP}^0$ such that for all n

- $g_n(x) = \sum_{\epsilon \in \{0,1\}^{n^c}} f_n(x, \epsilon)$

$$\mathrm{Per}_n((x_{i,j})_{i,j \leq n}) = \sum_{\sigma \in \mathfrak{S}_n} \prod_{i=1}^{n} x_{i,\sigma(i)}$$

Valiant's Conjecture

Class VP^0

(f_n): there exists c such that for all $n \geq 2$

- at most n^c variables
- $\tau(f_n) \leq n^c$
- formal degree is bounded by n^c

Class VNP^0

(g_n): there exists $(f_n) \in VP^0$ such that for all n

- $g_n(x) = \sum_{\epsilon \in \{0,1\}^{n^c}} f_n(x, \epsilon)$

Valiant's Conjecture

$VP^0 \neq VNP^0$

τ-conjecture [Shub & Smale, 95]

Conjecture

There exists a constant c such that $f(x)$ has at most $\tau(f)^c$ integer roots.

τ-conjecture [Shub & Smale, 95]

Conjecture

There exists a constant c such that $f(x)$ has at most $\tau(f)^c$ integer roots.

Theorem [Shub-Smale, 95]

τ-conjecture $\Rightarrow \mathrm{P}_{\mathbb{C}} \neq \mathrm{NP}_{\mathbb{C}}$.

τ-conjecture [Shub & Smale, 95]

Conjecture

There exists a constant c such that $f(x)$ has at most $\tau(f)^c$ integer roots.

Theorem [Shub-Smale, 95]

τ-conjecture $\Rightarrow \mathrm{P}_{\mathbb{C}} \neq \mathrm{NP}_{\mathbb{C}}$.

Theorem [Bürgisser, 07]

τ-conjecture $\Rightarrow \mathrm{VP}^0 \neq \mathrm{VNP}^0$

τ-conjecture [Shub & Smale, 95]

Conjecture

There exists a constant c such that $f(x)$ has at most $\tau(f)^c$ integer roots.

Theorem [Shub-Smale, 95]

τ-conjecture $\Rightarrow \mathrm{P}_{\mathbb{C}} \neq \mathrm{NP}_{\mathbb{C}}$.

Theorem [Bürgisser, 07]

τ-conjecture $\Rightarrow \mathrm{VP}^0 \neq \mathrm{VNP}^0$

Remark:

- The conjecture is wrong for real roots:
  Chebyshev polynomials

Plan

1. Introduction
   - Arithmetic circuits
   - τ-conjecture

2. real τ-conjecture
   - SPS
   - Conjecture

3. Results
   - Main tool
   - Upper bound
   - Application for different models

Sum of products of sparse polynomials

To bound the number of distinct real roots:

- t-sparse polynomial: $\sum_{p=1}^{t} a_p X^{\alpha_p}$?

Sum of products of sparse polynomials

To bound the number of distinct real roots:

- t-sparse polynomial: $\sum_{p=1}^{t} a_p X^{\alpha_p}$:
  Descartes' rule of signs $\Rightarrow$ at most $2t-1$

Sum of products of sparse polynomials

To bound the number of distinct real roots:

- t-sparse polynomial: $\sum_{p=1}^{t} a_p X^{\alpha_p}$:
  Descartes' rule of signs $\Rightarrow$ at most $2t-1$
- product of m t-sparse polynomials: $\prod_{j=1}^{m}\left(\sum_{p=1}^{t} a_{j,p} X^{\alpha_{j,p}}\right)$?

Sum of products of sparse polynomials

To bound the number of distinct real roots:

- t-sparse polynomial: $\sum_{p=1}^{t} a_p X^{\alpha_p}$:
  Descartes' rule of signs $\Rightarrow$ at most $2t-1$
- product of m t-sparse polynomials: $\prod_{j=1}^{m}\left(\sum_{p=1}^{t} a_{j,p} X^{\alpha_{j,p}}\right)$:
  at most $m(2t-1)$

Sum of products of sparse polynomials

To bound the number of distinct real roots:

- t-sparse polynomial: $\sum_{p=1}^{t} a_p X^{\alpha_p}$:
  Descartes' rule of signs $\Rightarrow$ at most $2t-1$
- product of m t-sparse polynomials: $\prod_{j=1}^{m} \left(\sum_{p=1}^{t} a_{j,p} X^{\alpha_{j,p}} \right)$:
  at most $m(2t-1)$
- sum of k products of m t-sparse polynomials:
  $\sum_{i=1}^{k} \left(\prod_{j=1}^{m} \left(\sum_{p=1}^{t} a_{i,j,p} X^{\alpha_{i,j,p}} \right) \right)$?

Sum of products of sparse polynomials

To bound the number of distinct real roots:

- t-sparse polynomial: $\sum_{p=1}^{t} a_p X^{\alpha_p}$:
  Descartes' rule of signs $\Rightarrow$ at most $2t-1$
- product of m t-sparse polynomials: $\prod_{j=1}^{m}\left(\sum_{p=1}^{t} a_{j,p} X^{\alpha_{j,p}}\right)$:
  at most $m(2t-1)$
- sum of k products of m t-sparse polynomials:
  $\sum_{i=1}^{k}\left(\prod_{j=1}^{m}\left(\sum_{p=1}^{t} a_{i,j,p} X^{\alpha_{i,j,p}}\right)\right)$:
  at most ???

Sum of products of sparse polynomials

To bound the number of distinct real roots:

- t-sparse polynomial: $\sum_{p=1}^{t} a_p X^{\alpha_p}$:
  Descartes' rule of signs $\Rightarrow$ at most $2t-1$
- product of m t-sparse polynomials: $\prod_{j=1}^{m}\left(\sum_{p=1}^{t} a_{j,p} X^{\alpha_{j,p}}\right)$:
  at most $m(2t-1)$
- sum of k products of m t-sparse polynomials:
  $\sum_{i=1}^{k}\left(\prod_{j=1}^{m}\left(\sum_{p=1}^{t} a_{i,j,p} X^{\alpha_{i,j,p}}\right)\right)$:
  at most ???
  Bounded by $O(kt^m)$ by expanding

Real τ-Conjecture

τ-Conjecture

There exists a constant c such that for all polynomials f, f has at most $\tau(f)^c$ integer roots.

Real τ-Conjecture

τ-Conjecture

There exists a constant c such that for all polynomials f, f has at most $\tau(f)^c$ **integer** roots.

Real τ-Conjecture

There exists c such that $\sum_{i=1}^{k}\prod_{j=1}^{m} f_{i,j}$ (with $f_{i,j}$ t-sparse) has at most $(m+k+t)^c$ **real** roots.

Real τ-Conjecture

τ-Conjecture

There exists a constant c such that for all polynomials f, f has at most $\tau(f)^c$ **integer** roots.

Real τ-Conjecture

There exists c such that $\sum_{i=1}^{k}\prod_{j=1}^{m} f_{i,j}$ (with $f_{i,j}$ t-sparse) has at most $(m+k+t)^c$ **real** roots.

Theorem [Koiran, 11]

Real τ-conjecture $\Rightarrow \mathrm{VP}^0 \neq \mathrm{VNP}^0$

Real τ-Conjecture

τ-Conjecture

There exists a constant c such that for all polynomials f, f has at most $\tau(f)^c$ **integer** roots.

Real τ-Conjecture

There exists c such that $\sum_{i=1}^{k}\prod_{j=1}^{m} f_{i,j}$ (with $f_{i,j}$ t-sparse) has at most $(m+k+t)^c$ **real** roots.

Theorem [Koiran, 11]

Real τ-conjecture $\Rightarrow \mathrm{VP}^0 \neq \mathrm{VNP}^0$

Use of real analysis

The limited power of powering

And if the number of distinct f_{ij} is very small (constant?)?
Let us consider $f(X) = \sum_{i=1}^{k} \prod_{j=1}^{m} f_j^{\alpha_{ij}}(X)$ with f_j t-sparse polynomial.

Theorem (Grenet, Koiran, Portier and Strozecki)

If f is not zero, then it has at most $t^{O(m.2^k)}$ real roots.

The limited power of powering

And if the number of distinct f_{ij} is very small (constant?)?
Let us consider $f(X) = \sum_{i=1}^{k} \prod_{j=1}^{m} f_j^{\alpha_{ij}}(X)$ with f_j t-sparse polynomial.

Theorem (Grenet, Koiran, Portier and Strozecki)

If f is not zero, then it has at most $t^{O(m.2^k)}$ real roots.

- Bound given by Khovanskiĭ: $2^{O((k+t)^2 m^2)}$

The limited power of powering

And if the number of distinct f_{ij} is very small (constant?)?
Let us consider $f(X) = \sum_{i=1}^{k} \prod_{j=1}^{m} f_j^{\alpha_{ij}}(X)$ with f_j t-sparse polynomial.

Theorem (Grenet, Koiran, Portier and Strozecki)

If f is not zero, then it has at most $t^{O(m.2^k)}$ real roots.

- Bound given by Khovanskiĭ: $2^{O((k+t)^2 m^2)}$

Theorem (with Koiran and Portier)

If f is not zero, then it has at most $t^{O(m.k^2)}$ real roots.

The limited power of powering

And if the number of distinct f_{ij} is very small (constant?)?
Let us consider $f(X) = \sum_{i=1}^{k} \prod_{j=1}^{m} f_j^{\alpha_{ij}}(X)$ with f_j t-sparse polynomial.

Theorem (Grenet, Koiran, Portier and Strozecki)

If f is not zero, then it has at most $t^{O(m.2^k)}$ real roots.

- Bound given by Khovanskiĭ: $2^{O((k+t)^2 m^2)}$

Theorem (with Koiran and Portier)

If f is not zero, then it has at most $t^{O(m.k^2)}$ real roots.

The main tool is...

Plan

1. Introduction
   - Arithmetic circuits
   - τ-conjecture
2. real τ-conjecture
   - SPS
   - Conjecture
3. Results
   - Main tool
   - Upper bound
   - Application for different models

The Wronskian

Definition: Let $f_1, \ldots, f_k \in C^{k-1}(I)$ with $I \subset \mathbb{R}$. The *Wronskian* of the family is the determinant of the matrix:

$$W(f_1, \ldots, f_k) = \det \begin{bmatrix} f_1 & f_2 & \cdots & f_k \\ f_1' & f_2' & \cdots & f_k' \\ \vdots & \vdots & & \vdots \\ f_1^{(k-1)} & f_2^{(k-1)} & \ldots & f_k^{(k-1)} \end{bmatrix}$$

The Wronskian

Definition: Let $f_1, \ldots, f_k \in C^{k-1}(I)$ with $I \subset \mathbb{R}$. The *Wronskian* of the family is the determinant of the matrix:

$$W(f_1, \ldots, f_k) = \det \begin{bmatrix} f_1 & f_2 & \cdots & f_k \\ f_1' & f_2' & \cdots & f_k' \\ \vdots & \vdots & & \vdots \\ f_1^{(k-1)} & f_2^{(k-1)} & \ldots & f_k^{(k-1)} \end{bmatrix}$$

- Upper bound the number of roots of a sum by the number of roots of Wronskians

The Wronskian

Definition: Let $f_1, \ldots, f_k \in C^{k-1}(I)$ with $I \subset \mathbb{R}$. The *Wronskian* of the family is the determinant of the matrix:

$$W(f_1, \ldots, f_k) = \det \begin{bmatrix} f_1 & f_2 & \cdots & f_k \\ f_1' & f_2' & \cdots & f_k' \\ \vdots & \vdots & & \vdots \\ f_1^{(k-1)} & f_2^{(k-1)} & \cdots & f_k^{(k-1)} \end{bmatrix}$$

- Upper bound the number of roots of a sum by the number of roots of Wronskians
- Upper bound the number of roots of Wronskians

First step

Goal

With conditions over zeros of $W(f_1), W(f_1, f_2), \ldots, W(f_1, f_2, \ldots, f_k)$, find an upper bound of the number of zeros of $f_1 + \ldots + f_k$

First step

Goal

With conditions over zeros of $W(f_1), W(f_1, f_2), \ldots, W(f_1, f_2, \ldots, f_k)$, find an upper bound of the number of zeros of $f_1 + \ldots + f_k$

- $f_1 + f_2 =$

First step

Goal

With conditions over zeros of $W(f_1), W(f_1, f_2), \ldots, W(f_1, f_2, \ldots, f_k)$, find an upper bound of the number of zeros of $f_1 + \ldots + f_k$

- $f_1 + f_2 = f_1(1 + \frac{f_2}{f_1})$

First step

Goal

With conditions over zeros of $W(f_1), W(f_1, f_2), \ldots, W(f_1, f_2, \ldots, f_k)$, find an upper bound of the number of zeros of $f_1 + \ldots + f_k$

- $f_1 + f_2 = f_1(1 + \frac{f_2}{f_1})$

$$\left(1 + \frac{f_2}{f_1}\right)' = \frac{W(f_1, f_2)}{f_1^2}$$

First step

Goal

With conditions over zeros of $W(f_1), W(f_1, f_2), \ldots, W(f_1, f_2, \ldots, f_k)$, find an upper bound of the number of zeros of $f_1 + \ldots + f_k$

- $f_1 + f_2 = f_1(1 + \frac{f_2}{f_1})$

$$\left(1 + \frac{f_2}{f_1}\right)' = \frac{W(f_1, f_2)}{f_1^2}$$

- $f_1 + f_2 + \ldots f_p = f_1(1 + \frac{f_2}{f_1} + \ldots + \frac{f_p}{f_1})$

First step

Goal

With conditions over zeros of $W(f_1), W(f_1, f_2), \dots, W(f_1, f_2, \dots, f_k)$, find an upper bound of the number of zeros of $f_1 + \dots + f_k$

- $f_1 + f_2 = f_1(1 + \frac{f_2}{f_1})$

$$\left(1 + \frac{f_2}{f_1}\right)' = \frac{W(f_1, f_2)}{f_1^2}$$

- $f_1 + f_2 + \dots f_p = f_1(1 + \frac{f_2}{f_1} + \dots + \frac{f_p}{f_1})$

$$W\left(\left(\frac{f_2}{f_1}\right)', \dots, \left(\frac{f_q}{f_1}\right)'\right) = \left(\frac{1}{f_1}\right)^q W(f_1, \dots, f_q)$$

Results

Theorem (1, with P.Koiran and N.Portier)

Let $\Upsilon = \{x \in I | \exists s, W(f_1, \ldots, f_s)(x) = 0\}$.
Then

$$Z(a_1 f_1 + \ldots + a_k f_k) \leq (1 + |\Upsilon|)k - 1$$

Results

Theorem (1, with P.Koiran and N.Portier)

Let $\Upsilon = \{x \in I | \exists s, W(f_1, \dots, f_s)(x) = 0\}$.
Then

$$Z(a_1 f_1 + \dots + a_k f_k) \leq (1 + |\Upsilon|)k - 1$$

- Voorhoeve's results

Results

Theorem (1, with P.Koiran and N.Portier)

Let $\Upsilon = \{x \in I | \exists s, W(f_1, \ldots, f_s)(x) = 0\}$.
Then

$$Z(a_1 f_1 + \ldots + a_k f_k) \leq (1 + |\Upsilon|)k - 1$$

- Voorhoeve's results

Theorem (2, with P.Koiran and N.Portier)

$$Z(f_1 + \ldots + f_k) \leq k - 1 + Z(W_k) + Z(W_{k-1}) + 2\sum_{j=1}^{k-2} Z(W_j)$$

Application: $\sum_{i=1}^{k}\prod_{j=1}^{m}(f_j)^{\alpha_{i,j}}$ with f_j sparse

Let us consider $f(X)=\sum_{i=1}^{k}\prod_{j=1}^{m}f_j^{\alpha_{ij}}(X)$ with f_j t-sparse polynomial.

Theorem (Grenet, Koiran, Portier and Strozecki)

If f is not zero, then it has at most $t^{O(m.2^k)}$ distinct real roots.

Application: $\sum_{i=1}^{k} \prod_{j=1}^{m} (f_j)^{\alpha_{i,j}}$ with f_j sparse

Let us consider $f(X) = \sum_{i=1}^{k} \prod_{j=1}^{m} f_j^{\alpha_{ij}}(X)$ with f_j t-sparse polynomial.

Theorem (Grenet, Koiran, Portier and Strozecki)

If f is not zero, then it has at most $t^{O(m.2^k)}$ distinct real roots.

Theorem

If f is not zero, then it has at most $4ktm + 4\left(\mathrm{e}(1+t)\right)^{\frac{mk^2}{2}} = t^{O(mk^2)}$ distinct real roots.

Application: $\sum_{i=1}^{k}\prod_{j=1}^{m}(f_j)^{\alpha_{i,j}}$ with f_j of small degree

Theorem

$$f = \sum_{i=1}^{k}\prod_{j=1}^{m} f_j^{\alpha_{i,j}}$$

Then, $Z(f) \leq \frac{1}{3}k^3md + 2kmd + k = \frac{k^3md}{3}(1 + o(1))$

Some particular models

Avendaño's model

Corollary

Let $f = \sum_{i=1}^{k} c_i x^{\alpha_i}(ax+b)^{\beta_i}$*.*
Then $Z(f) = O(k^3)$*.*

Some particular models

Avendaño's model

Corollary

Let $f = \sum_{i=1}^{k} c_i x^{\alpha_i} (ax+b)^{\beta_i}$.
Then $Z(f) = O(k^3)$.

Li, Rojas and Wang's model

Corollary

Let $f = \sum_{i=1}^{k} a_i \prod_{j=1}^{m} (c_j x + d_j)^{\alpha_{i,j}}$.
Then $Z(f) = O(mk^3)$.

Open questions

- $Z(f_1 + \ldots + f_k) \overset{?}{\leq} k - 1 + \sum_{j=1}^{k} Z(W_j)$

Open questions

- $Z(f_1 + \ldots + f_k) \overset{?}{\leq} k - 1 + \sum_{j=1}^{k} Z(W_j)$
- Is the real τ-conjecture true?

Open questions

- $Z(f_1 + \ldots + f_k) \overset{?}{\leq} k - 1 + \sum_{j=1}^{k} Z(W_j)$
- Is the real τ-conjecture true?
- What about fg ? If f and g are t-sparse.

Open questions

- $Z(f_1 + \ldots + f_k) \overset{?}{\leq} k - 1 + \sum_{j=1}^{k} Z(W_j)$
- Is the real τ-conjecture true?
- What about $fg + 1$? If f and g are t-sparse.

Thanks!