Progress on the Real τ-Conjecture

Pascal Koiran
LIP, Ecole Normale Supérieure de Lyon

Fields Institute, May 2012

The τ-Conjecture [Shub-Smale'95]

$\tau(f)$ = length of smallest straight-line program for $f \in \mathbb{Z}[X]$.
No constants are allowed.
Conjecture: f has at most $\tau(f)^c$ integer zeros (for a constant c).
Theorem [Shub-Smale'95]: τ-conjecture $\Rightarrow$ $\mathrm{P}_{\mathbb{C}} \neq \mathrm{NP}_{\mathbb{C}}$.
Theorem [Bürgisser'07]:
τ-conjecture $\Rightarrow$ no polynomial-size arithmetic circuits for the permanent.

Remarks:

- What if constants are allowed?
- We must have $c \geq 2$.
- Conjecture becomes false for real roots:
  Shub-Smale (Chebyshev's polynomials), Borodin-Cook'76.

The τ-Conjecture [Shub-Smale'95]

$\tau(f)$ = length of smallest straight-line program for $f \in \mathbb{Z}[X]$.
No constants are allowed.
Conjecture: f has at most $\tau(f)^c$ integer zeros (for a constant c).
Theorem [Shub-Smale'95]: τ-conjecture $\Rightarrow \mathrm{P}_{\mathbb{C}} \neq \mathrm{NP}_{\mathbb{C}}$.
Theorem [Bürgisser'07]:
τ-conjecture $\Rightarrow$ no polynomial-size arithmetic circuits for the permanent.

Remarks:

- What if constants are allowed?
- We must have $c \geq 2$.
- Conjecture becomes false for real roots:
  Shub-Smale (Chebyshev's polynomials), Borodin-Cook'76.

The τ-Conjecture [Shub-Smale'95]

$\tau(f) =$ length of smallest straight-line program for $f \in \mathbb{Z}[X]$.
No constants are allowed.
Conjecture: f has at most $\tau(f)^c$ integer zeros (for a constant c).
Theorem [Shub-Smale'95]: τ-conjecture $\Rightarrow \mathrm{P}_{\mathbb{C}} \neq \mathrm{NP}_{\mathbb{C}}$.
Theorem [Bürgisser'07]:
τ-conjecture $\Rightarrow$ no polynomial-size arithmetic circuits for the permanent.

Remarks:

- What if constants are allowed?
- We must have $c \geq 2$.
- Conjecture becomes false for real roots: Shub-Smale (Chebyshev's polynomials), Borodin-Cook'76.

The τ-Conjecture [Shub-Smale'95]

$\tau(f)$ = length of smallest straight-line program for $f \in \mathbb{Z}[X]$.
No constants are allowed.
Conjecture: f has at most $\tau(f)^c$ integer zeros (for a constant c).
Theorem [Shub-Smale'95]: τ-conjecture $\Rightarrow \mathrm{P}_{\mathbb{C}} \neq \mathrm{NP}_{\mathbb{C}}$.
Theorem [Bürgisser'07]:
τ-conjecture $\Rightarrow$ no polynomial-size arithmetic circuits for the permanent.

Remarks:

- What if constants are allowed?
- We must have $c \geq 2$.
- Conjecture becomes false for real roots:
  Shub-Smale (Chebyshev's polynomials), Borodin-Cook'76.

The Real τ-Conjecture

Conjecture: Consider $f(X) = \sum_{i=1}^{k} \prod_{j=1}^{m} f_{ij}(X)$,
where the f_{ij} are t-sparse.
If f is nonzero, its number of **real roots** is polynomial in kmt.
Theorem: If the conjecture is true then the permanent is hard.
Remarks:

- It is enough to bound the number of integer roots.
  Could techniques from real analysis be helpful?
- Case $k = 1$ of the conjecture follows from Descartes' rule.
- By expanding the products, f has at most $2kt^m - 1$ zeros.
- $k = 2$ is open. An even more basic question
  (courtesy of Arkadev Chattopadhyay):
  how many real solutions to $fg = 1$?
  Descartes' bound is $O(t^2)$ but true bound could be $O(t)$.

The Real τ-Conjecture

Conjecture: Consider $f(X) = \sum_{i=1}^{k} \prod_{j=1}^{m} f_{ij}(X)$,
where the f_{ij} are t-sparse.
If f is nonzero, its number of **real roots** is polynomial in kmt.
Theorem: If the conjecture is true then the permanent is hard.
Remarks:

- It is enough to bound the number of integer roots.
  Could techniques from real analysis be helpful?
- Case $k = 1$ of the conjecture follows from Descartes' rule.
- By expanding the products, f has at most $2kt^m - 1$ zeros.
- $k = 2$ is open. An even more basic question
  (courtesy of Arkadev Chattopadhyay):
  how many real solutions to $fg = 1$?
  Descartes' bound is $O(t^2)$ but true bound could be $O(t)$.

The Real τ-Conjecture

Conjecture: Consider $f(X) = \sum_{i=1}^{k} \prod_{j=1}^{m} f_{ij}(X)$,
where the f_{ij} are t-sparse.
If f is nonzero, its number of **real roots** is polynomial in kmt.
Theorem: If the conjecture is true then the permanent is hard.
Remarks:

- It is enough to bound the number of integer roots.
  Could techniques from real analysis be helpful?
- Case $k = 1$ of the conjecture follows from Descartes' rule.
- By expanding the products, f has at most $2kt^m - 1$ zeros.
- $k = 2$ is open. An even more basic question
  (courtesy of Arkadev Chattopadhyay):
  how many real solutions to $fg = 1$?
  Descartes' bound is $O(t^2)$ but true bound could be $O(t)$.

The Real τ-Conjecture

Conjecture: Consider $f(X) = \sum_{i=1}^{k} \prod_{j=1}^{m} f_{ij}(X)$,
where the f_{ij} are t-sparse.
If f is nonzero, its number of **real roots** is polynomial in kmt.
Theorem: If the conjecture is true then the permanent is hard.
Remarks:

- It is enough to bound the number of integer roots.
  Could techniques from real analysis be helpful?
- Case $k = 1$ of the conjecture follows from Descartes' rule.
- By expanding the products, f has at most $2kt^m - 1$ zeros.
- $k = 2$ is open. An even more basic question
  (courtesy of Arkadev Chattopadhyay):
  how many real solutions to $fg = 1$?
  Descartes' bound is $O(t^2)$ but true bound could be $O(t)$.

The Real τ-Conjecture

Conjecture: Consider $f(X) = \sum_{i=1}^{k} \prod_{j=1}^{m} f_{ij}(X)$,
where the f_{ij} are t-sparse.
If f is nonzero, its number of **real roots** is polynomial in kmt.
Theorem: If the conjecture is true then the permanent is hard.
Remarks:

- It is enough to bound the number of integer roots.
  Could techniques from real analysis be helpful?
- Case $k = 1$ of the conjecture follows from Descartes' rule.
- By expanding the products, f has at most $2kt^m - 1$ zeros.
- $k = 2$ is open. An even more basic question
  (courtesy of Arkadev Chattopadhyay):
  how many real solutions to $fg = 1$?
  Descartes' bound is $O(t^2)$ but true bound could be $O(t)$.

Descartes's rule without signs

Theorem:
If f has t monomials then f at most $t-1$ positive real roots.
Proof: Induction on t. No positive root for $t=1$.
For $t>1$: let $a_\alpha X^\alpha$ = lowest degree monomial.
We can assume $\alpha = 0$ (divide by X^α if not). Then:

(i) f' has $t-1$ monomials $\Rightarrow \leq t-2$ positive real roots.
(ii) There is a positive root of f' between 2 consecutive positive roots of f (Rolle's theorem).

Descartes's rule without signs

Theorem:
If f has t monomials then f at most $t - 1$ positive real roots.
Proof: Induction on t. No positive root for $t = 1$.
For $t > 1$: let $a_\alpha X^\alpha =$ lowest degree monomial.
We can assume $\alpha = 0$ (divide by X^α if not). Then:

(i) f' has $t - 1$ monomials $\Rightarrow \leq t - 2$ positive real roots.
(ii) There is a positive root of f' between 2 consecutive positive roots of f (Rolle's theorem).

Real τ-Conjecture $\Rightarrow$ Permanent is hard

The 2 main ingredients:

- The Pochhammer-Wilkinson polynomials:
  $PW_n(X) = \prod_{i=1}^{n}(X - i)$.
  Theorem [Bürgisser'07-09]: If the permanent is easy, PW_n has circuits size $(\log n)^{O(1)}$.
- Reduction to depth 4 for arithmetic circuits (Agrawal and Vinay, 2008).

The second ingredient: reduction to depth 4

Depth reduction theorem (Agrawal and Vinay, 2008):
Any multilinear polynomial in n variables with an arithmetic circuit of size $2^{o(n)}$ also has a depth four ($\Sigma\Pi\Sigma\Pi$) circuit of size $2^{o(n)}$.

Our polynomials are far from multilinear, but:

Depth-4 circuit with inputs of the form X^{2^i}, or constants
(Shallow circuit with high-powered inputs)

$\Updownarrow$

Sum of Products of Sparse Polynomials

How the proof does *not* go

Assume by contradiction that the permanent is easy.
Goal:
Show that SPS polynomials of size $2^{o(n)}$ can compute $\prod_{i=1}^{2^n}(X - i)$
$\Rightarrow$ contradiction with real τ-conjecture.

1. From assumption: $\prod_{i=1}^{2^n}(X - i)$ has circuits of polynomial in n (Bürgisser).
2. Reduction to depth 4 $\Rightarrow$ SPS polynomials of size $2^{o(n)}$.

What's wrong with this argument:

How the proof does *not* go

Assume by contradiction that the permanent is easy.
Goal:
Show that SPS polynomials of size $2^{o(n)}$ can compute $\prod_{i=1}^{2^n}(X-i)$
$\Rightarrow$ contradiction with real τ-conjecture.

1. From assumption: $\prod_{i=1}^{2^n}(X-i)$ has circuits of polynomial in n (Bürgisser).
2. Reduction to depth 4 $\Rightarrow$ SPS polynomials of size $2^{o(n)}$.

What's wrong with this argument:
No high-degree analogue of reduction to depth 4
(think of Chebyshev's polynomials).

How the proof goes (more or less)

Assume that the permanent is easy.
Goal:
Show that SPS polynomials of size $2^{o(n)}$ can compute $\prod_{i=1}^{2^n}(X-i)$
$\Rightarrow$ contradiction with real τ-conjecture.

1. From assumption: $\prod_{i=1}^{2^n}(X-i)$ has circuits of polynomial in n (Bürgisser).
2. Reduction to depth 4 $\Rightarrow$ SPS polynomials of size $2^{o(n)}$.

For step 2: need to use again the assumption that perm is easy.

The limited power of powering (a tractable special case)

What if the number of distinct f_{ij} is very small (even constant)?
Consider $f(X) = \sum_{i=1}^{k} \prod_{j=1}^{m} f_j^{\alpha_{ij}}(X)$,
where the f_j are t-sparse.

Theorem [with Grenet, Portier and Strozecki]:
If f is nonzero, it has at most $t^{O(m.2^k)}$ real roots.

Remarks:

- For this model we also give a permanent lower bound and a polynomial identity testing algorithm ($f \equiv 0$?). See also [Agrawal-Saha-Saptharishi-Saxena, STOC'2012].
- Bounds from Khovanskii's theory of fewnomials are exponential in k, m, t.

Today's result:

Theorem [with Portier and Tavenas]:
If f is nonzero, it has at most $t^{O(m.k^2)}$ real roots.
The main tool is...

The limited power of powering (a tractable special case)

What if the number of distinct f_{ij} is very small (even constant)?
Consider $f(X) = \sum_{i=1}^{k} \prod_{j=1}^{m} f_j^{\alpha_{ij}}(X)$,
where the f_j are t-sparse.

Theorem [with Grenet, Portier and Strozecki]:
If f is nonzero, it has at most $t^{O(m.2^k)}$ real roots.

Remarks:

- For this model we also give a permanent lower bound and a polynomial identity testing algorithm ($f \equiv 0$?). See also [Agrawal-Saha-Saptharishi-Saxena, STOC'2012].
- Bounds from Khovanskii's theory of fewnomials are exponential in k, m, t.

Today's result:

Theorem [with Portier and Tavenas]:
If f is nonzero, it has at most $t^{O(m.k^2)}$ real roots.
The main tool is...

The limited power of powering (a tractable special case)

What if the number of distinct f_{ij} is very small (even constant)?
Consider $f(X) = \sum_{i=1}^{k} \prod_{j=1}^{m} f_j^{\alpha_{ij}}(X)$,
where the f_j are t-sparse.

Theorem [with Grenet, Portier and Strozecki]:
If f is nonzero, it has at most $t^{O(m.2^k)}$ real roots.

Remarks:

- For this model we also give a permanent lower bound and a polynomial identity testing algorithm ($f \equiv 0$?). See also [Agrawal-Saha-Saptharishi-Saxena, STOC'2012].
- Bounds from Khovanskii's theory of fewnomials are exponential in k, m, t.

Today's result:

Theorem [with Portier and Tavenas]:
If f is nonzero, it has at most $t^{O(m.k^2)}$ real roots.

The main tool is...

The limited power of powering (a tractable special case)

What if the number of distinct f_{ij} is very small (even constant)?
Consider $f(X) = \sum_{i=1}^{k} \prod_{j=1}^{m} f_j^{\alpha_{ij}}(X)$,
where the f_j are t-sparse.

Theorem [with Grenet, Portier and Strozecki]:
If f is nonzero, it has at most $t^{O(m.2^k)}$ real roots.

Remarks:

- For this model we also give a permanent lower bound and a polynomial identity testing algorithm ($f \equiv 0$?). See also [Agrawal-Saha-Saptharishi-Saxena, STOC'2012].
- Bounds from Khovanskii's theory of fewnomials are exponential in k, m, t.

Today's result:

Theorem [with Portier and Tavenas]:
If f is nonzero, it has at most $t^{O(m.k^2)}$ real roots.

The main tool is...

The limited power of powering (a tractable special case)

What if the number of distinct f_{ij} is very small (even constant)?
Consider $f(X) = \sum_{i=1}^{k} \prod_{j=1}^{m} f_j^{\alpha_{ij}}(X)$,
where the f_j are t-sparse.

Theorem [with Grenet, Portier and Strozecki]:
If f is nonzero, it has at most $t^{O(m.2^k)}$ real roots.

Remarks:

- For this model we also give a permanent lower bound and a polynomial identity testing algorithm ($f \equiv 0$?). See also [Agrawal-Saha-Saptharishi-Saxena, STOC'2012].
- Bounds from Khovanskii's theory of fewnomials are exponential in k, m, t.

Today's result:

Theorem [with Portier and Tavenas]:
If f is nonzero, it has at most $t^{O(m.k^2)}$ real roots.
The main tool is...

The Wronskian

Definition: Let $f_1, \ldots, f_k : I \to \mathbb{R}$. Their *Wronskian* is the determinant of the *Wronskian matrix*

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

- Linear dependence $\Rightarrow W(f_1, \ldots, f_k) \equiv 0$.
- Converse is not always true (Peano, 1889):
  Let $f_1(x) = x^2$, $f_2(x) = x|x|$. Then

$$W(f_1, f_2) = \det \begin{bmatrix} x^2 & \mathrm{sign}(x)x^2 \\ 2x & 2\mathrm{sign}(x)x \end{bmatrix} \equiv 0.$$

- Converse *is* true for analytic functions (Bôcher, 1900).

The Wronskian and Real Roots

Upper Bound Theorem: Assume that the k wronskians

$$W(f_1), W(f_1, f_2), W(f_1, f_2, f_3), \ldots, W(f_1, \ldots, f_k)$$

have no zeros on I.
Let $f = a_1 f_1 + \cdots + a_k f_k$ where $a_i \neq 0$ for some i.
Then f has at most $k-1$ zeros on I, counted with multiplicities.
Remark:
Connections between real roots and the Wronksian were known.
Typical application:
Divide $\mathbb{R}$ into intervals where the k wronskians have no zeros.
Case $k = 2$:

1. If $a_2 = 0$, $f = a_1 f_1$ has no zero on I.
2. If $a_2 \neq 0$, write $f = f_1 g$ where $g = a_1 + a_2 f_2 / f_1$.
   $g' = a_2(f_2' f_1 - f_2 f_1')/f_1^2 = a_2 \mathrm{W}(f_1, f_2)/f_1^2$ has no zero $\Rightarrow$
   by Rolle's theorem, g has at most 1 zero, and f too.

The Wronskian and Real Roots

Upper Bound Theorem: Assume that the k wronskians

$$W(f_1), W(f_1, f_2), W(f_1, f_2, f_3), \dots, W(f_1, \dots, f_k)$$

have no zeros on I.
Let $f = a_1 f_1 + \cdots + a_k f_k$ where $a_i \neq 0$ for some i.
Then f has at most $k-1$ zeros on I, counted with multiplicities.
Remark:
Connections between real roots and the Wronksian were known.
Typical application:
Divide $\mathbb{R}$ into intervals where the k wronskians have no zeros.
Case $k = 2$:

1. If $a_2 = 0$, $f = a_1 f_1$ has no zero on I.
2. If $a_2 \neq 0$, write $f = f_1 g$ where $g = a_1 + a_2 f_2 / f_1$.
   $g' = a_2 (f_2' f_1 - f_2 f_1')/f_1^2 = a_2 \mathrm{W}(f_1, f_2)/f_1^2$ has no zero $\Rightarrow$
   by Rolle's theorem, g has at most 1 zero, and f too.

The Wronskian and Real Roots

Upper Bound Theorem: Assume that the k wronskians

$$W(f_1), W(f_1, f_2), W(f_1, f_2, f_3), \ldots, W(f_1, \ldots, f_k)$$

have no zeros on I.
Let $f = a_1 f_1 + \cdots + a_k f_k$ where $a_i \neq 0$ for some i.
Then f has at most $k-1$ zeros on I, counted with multiplicities.
Remark:
Connections between real roots and the Wronksian were known.
Typical application:
Divide $\mathbb{R}$ into intervals where the k wronskians have no zeros.
Case $k = 2$:

1. If $a_2 = 0$, $f = a_1 f_1$ has no zero on I.
2. If $a_2 \neq 0$, write $f = f_1 g$ where $g = a_1 + a_2 f_2 / f_1$.
   $g' = a_2(f_2' f_1 - f_2 f_1')/f_1^2 = a_2 \mathrm{W}(f_1, f_2)/f_1^2$ has no zero $\Rightarrow$
   by Rolle's theorem, g has at most 1 zero, and f too.

The Wronskian and Real Roots

Upper Bound Theorem: Assume that the k wronskians

$$W(f_1), W(f_1, f_2), W(f_1, f_2, f_3), \dots, W(f_1, \dots, f_k)$$

have no zeros on I.
Let $f = a_1 f_1 + \cdots + a_k f_k$ where $a_i \neq 0$ for some i.
Then f has at most $k-1$ zeros on I, counted with multiplicities.
Remark:
Connections between real roots and the Wronksian were known.
Typical application:
Divide $\mathbb{R}$ into intervals where the k wronskians have no zeros.
Case $k = 2$**:**

1. If $a_2 = 0$, $f = a_1 f_1$ has no zero on I.
2. If $a_2 \neq 0$, write $f = f_1 g$ where $g = a_1 + a_2 f_2 / f_1$.
   $g' = a_2(f_2' f_1 - f_2 f_1')/f_1^2 = a_2 \mathrm{W}(f_1, f_2)/f_1^2$ has no zero $\Rightarrow$
   by Rolle's theorem, g has at most 1 zero, and f too.

The Wronskian and Real Roots

Upper Bound Theorem: Assume that the k wronskians

$$W(f_1), W(f_1, f_2), W(f_1, f_2, f_3), \dots, W(f_1, \dots, f_k)$$

have no zeros on I.
Let $f = a_1 f_1 + \cdots + a_k f_k$ where $a_i \neq 0$ for some i.
Then f has at most $k-1$ zeros on I, counted with multiplicities.
Remark:
Connections between real roots and the Wronksian were known.
Typical application:
Divide $\mathbb{R}$ into intervals where the k wronskians have no zeros.
Case $k = 2$**:**

1. If $a_2 = 0$, $f = a_1 f_1$ has no zero on I.
2. If $a_2 \neq 0$, write $f = f_1 g$ where $g = a_1 + a_2 f_2 / f_1$.
   $g' = a_2(f_2' f_1 - f_2 f_1')/f_1^2 = a_2 \mathrm{W}(f_1, f_2)/f_1^2$ has no zero $\Rightarrow$
   by Rolle's theorem, g has at most 1 zero, and f too.

Linear Dependence for Analytic Functions (1/3)

Theorem [Bôcher]: If $f_1, \ldots, f_k : I \to \mathbb{R}$ are analytic and $\mathrm{W}(f_1, \ldots, f_k) \equiv 0$, these functions are linearly dependent.

Proof: By induction on k. Pick $J \subseteq I$ where $f_1 \neq 0$. On J:

$$\begin{aligned} & a_1 f_1 + \cdots + a_k f_k \equiv 0 \\ \Leftrightarrow \quad & a_1 + a_2(f_2/f_1) + \cdots + a_k(f_k/f_1) \equiv 0 \\ \Leftrightarrow \quad & a_2(f_2/f_1)' + \cdots + a_k(f_k/f_1)' \equiv 0. \qquad (*) \end{aligned}$$

(*) follows from induction hypothesis and the recursive formula:

$$\mathrm{W}(f_1, \ldots, f_k) = f_1^k \mathrm{W}((f_2/f_1)', \ldots, (f_k/f_1)').$$

To conclude: for analytic functions,
if $f = a_1 f_1 + \cdots + a_k f_k \equiv 0$ on J, then $f \equiv 0$ on I.

Linear Dependence for Analytic Functions (1/3)

Theorem [Bôcher]: If $f_1, \ldots, f_k : I \to \mathbb{R}$ are analytic and $\mathrm{W}(f_1, \ldots, f_k) \equiv 0$, these functions are linearly dependent.
Proof: By induction on k. Pick $J \subseteq I$ where $f_1 \neq 0$. On J:

$$\begin{aligned} & a_1 f_1 + \cdots + a_k f_k \equiv 0 \\ \Leftrightarrow \quad & a_1 + a_2(f_2/f_1) + \cdots + a_k(f_k/f_1) \equiv 0 \\ \Leftrightarrow \quad & a_2(f_2/f_1)' + \cdots + a_k(f_k/f_1)' \equiv 0. \qquad (*) \end{aligned}$$

(*) follows from induction hypothesis and the recursive formula:

$$\mathrm{W}(f_1, \ldots, f_k) = f_1^k \mathrm{W}((f_2/f_1)', \ldots, (f_k/f_1)').$$

To conclude: for analytic functions,
if $f = a_1 f_1 + \cdots + a_k f_k \equiv 0$ on J, then $f \equiv 0$ on I.

Linear Dependence for Analytic Functions (1/3)

Theorem [Bôcher]: If $f_1, \ldots, f_k : I \to \mathbb{R}$ are analytic and $\mathrm{W}(f_1, \ldots, f_k) \equiv 0$, these functions are linearly dependent.
Proof: By induction on k. Pick $J \subseteq I$ where $f_1 \neq 0$. On J:

$$\begin{aligned} & a_1 f_1 + \cdots + a_k f_k \equiv 0 \\ \Leftrightarrow \quad & a_1 + a_2(f_2/f_1) + \cdots + a_k(f_k/f_1) \equiv 0 \\ \Leftrightarrow \quad & a_2(f_2/f_1)' + \cdots + a_k(f_k/f_1)' \equiv 0. \qquad (*) \end{aligned}$$

(*) follows from induction hypothesis and the recursive formula:

$$\mathrm{W}(f_1, \ldots, f_k) = f_1^k \mathrm{W}((f_2/f_1)', \ldots, (f_k/f_1)').$$

To conclude: for analytic functions,
if $f = a_1 f_1 + \cdots + a_k f_k \equiv 0$ on J, then $f \equiv 0$ on I.

Linear Dependence for Analytic Functions (1/3)

Theorem [Bôcher]: If $f_1, \ldots, f_k : I \to \mathbb{R}$ are analytic and $\mathrm{W}(f_1, \ldots, f_k) \equiv 0$, these functions are linearly dependent.

Proof: By induction on k. Pick $J \subseteq I$ where $f_1 \neq 0$. On J:

$$\begin{aligned} & a_1 f_1 + \cdots + a_k f_k \equiv 0 \\ \Leftrightarrow \quad & a_1 + a_2(f_2/f_1) + \cdots + a_k(f_k/f_1) \equiv 0 \\ \Leftrightarrow \quad & a_2(f_2/f_1)' + \cdots + a_k(f_k/f_1)' \equiv 0. \qquad (*) \end{aligned}$$

(*) follows from induction hypothesis and the recursive formula:

$$\mathrm{W}(f_1, \ldots, f_k) = f_1^k \mathrm{W}((f_2/f_1)', \ldots, (f_k/f_1)').$$

To conclude: for analytic functions, if $f = a_1 f_1 + \cdots + a_k f_k \equiv 0$ on J, then $f \equiv 0$ on I.

Linear Dependence for Analytic Functions (1/3)

Theorem [Bôcher]: If $f_1, \ldots, f_k : I \to \mathbb{R}$ are analytic and $\mathrm{W}(f_1, \ldots, f_k) \equiv 0$, these functions are linearly dependent.
Proof: By induction on k. Pick $J \subseteq I$ where $f_1 \neq 0$. On J:

$$\begin{aligned} & a_1 f_1 + \cdots + a_k f_k \equiv 0 \\ \Leftrightarrow \quad & a_1 + a_2(f_2/f_1) + \cdots + a_k(f_k/f_1) \equiv 0 \\ \Leftrightarrow \quad & a_2(f_2/f_1)' + \cdots + a_k(f_k/f_1)' \equiv 0. \qquad (*) \end{aligned}$$

(*) follows from induction hypothesis and the recursive formula:

$$\mathrm{W}(f_1, \ldots, f_k) = f_1^k \mathrm{W}((f_2/f_1)', \ldots, (f_k/f_1)').$$

To conclude: for analytic functions,
if $f = a_1 f_1 + \cdots + a_k f_k \equiv 0$ on J, then $f \equiv 0$ on I.

Linear Dependence for Analytic Functions (1/3)

Theorem [Bôcher]: If $f_1, \ldots, f_k : I \to \mathbb{R}$ are analytic and $\mathrm{W}(f_1, \ldots, f_k) \equiv 0$, these functions are linearly dependent.
Proof: By induction on k. Pick $J \subseteq I$ where $f_1 \neq 0$. On J:

$$\begin{aligned} & a_1 f_1 + \cdots + a_k f_k \equiv 0 \\ \Leftrightarrow \quad & a_1 + a_2(f_2/f_1) + \cdots + a_k(f_k/f_1) \equiv 0 \\ \Leftrightarrow \quad & a_2(f_2/f_1)' + \cdots + a_k(f_k/f_1)' \equiv 0. \qquad (*) \end{aligned}$$

(*) follows from induction hypothesis and the recursive formula:

$$\mathrm{W}(f_1, \ldots, f_k) = f_1^k \mathrm{W}((f_2/f_1)', \ldots, (f_k/f_1)').$$

To conclude: for analytic functions,
if $f = a_1 f_1 + \cdots + a_k f_k \equiv 0$ on J, then $f \equiv 0$ on I.

Linear Dependence for Analytic Functions (1/3)

Theorem [Bôcher]: If $f_1, \ldots, f_k : I \to \mathbb{R}$ are analytic and $\mathrm{W}(f_1, \ldots, f_k) \equiv 0$, these functions are linearly dependent.
Proof: By induction on k. Pick $J \subseteq I$ where $f_1 \neq 0$. On J:

$$\begin{aligned} & a_1 f_1 + \cdots + a_k f_k \equiv 0 \\ \Leftrightarrow \quad & a_1 + a_2(f_2/f_1) + \cdots + a_k(f_k/f_1) \equiv 0 \\ \Leftrightarrow \quad & a_2(f_2/f_1)' + \cdots + a_k(f_k/f_1)' \equiv 0. \qquad (*) \end{aligned}$$

(*) follows from induction hypothesis and the recursive formula:

$$\mathrm{W}(f_1, \ldots, f_k) = f_1^k \mathrm{W}((f_2/f_1)', \ldots, (f_k/f_1)').$$

To conclude: for analytic functions,
if $f = a_1 f_1 + \cdots + a_k f_k \equiv 0$ on J, then $f \equiv 0$ on I.

Linear Dependence for Analytic Functions (2/3)

Lemma: $W(f_1 g, f_2 g, \ldots, f_k g) = g^k W(f_1, f_2, \ldots, f_k)$.
For instance:

$$W(f_1 g, f_2 g, f_3 g) = \begin{vmatrix} f_1 g & f_2 g & f_3 g \\ (f_1 g)' & (f_2 g)' & (f_3 g)'' \\ (f_1 g)'' & (f_2 g)'' & (f_3 g)'' \end{vmatrix}$$

$$= g \begin{vmatrix} f_1 & f_2 & f_3 \\ f_1' g + f_1 g' & f_2' g + f_2 g' & f_3' g + f_3 g' \\ f_1'' g + 2 f_1' g' + f_1 g'' & f_2'' g + 2 f_2' g' + f_2 g'' & f_3'' g + 2 f_3' g' + f_3 g'' \end{vmatrix}$$

$$= g \begin{vmatrix} f_1 & f_2 & f_3 \\ f_1' g & f_2' g & f_3' g \\ f_1'' g + 2 f_1' g' & f_2'' g + 2 f_2' g' & f_3'' g + 2 f_3' g' \end{vmatrix}$$

$$= g^2 \begin{vmatrix} f_1 & f_2 & f_3 \\ f_1' & f_2' & f_3' \\ f_1'' g + 2 f_1' g' & f_2'' g + 2 f_2' g' & f_3'' g + 2 f_3' g' \end{vmatrix} = g^3 W(f_1, f_2, f_3).$$

Linear Dependence for Analytic Functions (2/3)

Lemma: $W(f_1 g, f_2 g, \ldots, f_k g) = g^k W(f_1, f_2, \ldots, f_k)$.
For instance:

$$W(f_1 g, f_2 g, f_3 g) = \begin{vmatrix} f_1 g & f_2 g & f_3 g \\ (f_1 g)' & (f_2 g)' & (f_3 g)'' \\ (f_1 g)'' & (f_2 g)'' & (f_3 g)'' \end{vmatrix}$$

$$= g \begin{vmatrix} f_1 & f_2 & f_3 \\ f_1' g + f_1 g' & f_2' g + f_2 g' & f_3' g + f_3 g' \\ f_1'' g + 2 f_1' g' + f_1 g'' & f_2'' g + 2 f_2' g' + f_2 g'' & f_3'' g + 2 f_3' g' + f_3 g'' \end{vmatrix}$$

$$= g \begin{vmatrix} f_1 & f_2 & f_3 \\ f_1' g & f_2' g & f_3' g \\ f_1'' g + 2 f_1' g' & f_2'' g + 2 f_2' g' & f_3'' g + 2 f_3' g' \end{vmatrix}$$

$$= g^2 \begin{vmatrix} f_1 & f_2 & f_3 \\ f_1' & f_2' & f_3' \\ f_1'' g + 2 f_1' g' & f_2'' g + 2 f_2' g' & f_3'' g + 2 f_3' g' \end{vmatrix} = g^3 W(f_1, f_2, f_3).$$

Linear Dependence for Analytic Functions (2/3)

Lemma: $W(f_1 g, f_2 g, \ldots, f_k g) = g^k W(f_1, f_2, \ldots, f_k)$.

For instance:

$$W(f_1 g, f_2 g, f_3 g) = \begin{vmatrix} f_1 g & f_2 g & f_3 g \\ (f_1 g)' & (f_2 g)' & (f_3 g)'' \\ (f_1 g)'' & (f_2 g)'' & (f_3 g)'' \end{vmatrix}$$

$$= g \begin{vmatrix} f_1 & f_2 & f_3 \\ f_1' g + f_1 g' & f_2' g + f_2 g' & f_3' g + f_3 g' \\ f_1'' g + 2 f_1' g' + f_1 g'' & f_2'' g + 2 f_2' g' + f_2 g'' & f_3'' g + 2 f_3' g' + f_3 g'' \end{vmatrix}$$

$$= g \begin{vmatrix} f_1 & f_2 & f_3 \\ f_1' g & f_2' g & f_3' g \\ f_1'' g + 2 f_1' g' & f_2'' g + 2 f_2' g' & f_3'' g + 2 f_3' g' \end{vmatrix}$$

$$= g^2 \begin{vmatrix} f_1 & f_2 & f_3 \\ f_1' & f_2' & f_3' \\ f_1'' g + 2 f_1' g' & f_2'' g + 2 f_2' g' & f_3'' g + 2 f_3' g' \end{vmatrix} = g^3 W(f_1, f_2, f_3).$$

Linear Dependence for Analytic Functions (2/3)

Lemma: $\mathrm{W}(f_1 g, f_2 g, \dots, f_k g) = g^k \mathrm{W}(f_1, f_2, \dots, f_k)$.
For instance:

$$\mathrm{W}(f_1 g, f_2 g, f_3 g) = \begin{vmatrix} f_1 g & f_2 g & f_3 g \\ (f_1 g)' & (f_2 g)' & (f_3 g)'' \\ (f_1 g)'' & (f_2 g)'' & (f_3 g)'' \end{vmatrix}$$

$$= g \begin{vmatrix} f_1 & f_2 & f_3 \\ f_1' g + f_1 g' & f_2' g + f_2 g' & f_3' g + f_3 g' \\ f_1'' g + 2 f_1' g' + f_1 g'' & f_2'' g + 2 f_2' g' + f_2 g'' & f_3'' g + 2 f_3' g' + f_3 g'' \end{vmatrix}$$

$$= g \begin{vmatrix} f_1 & f_2 & f_3 \\ f_1' g & f_2' g & f_3' g \\ f_1'' g + 2 f_1' g' & f_2'' g + 2 f_2' g' & f_3'' g + 2 f_3' g' \end{vmatrix}$$

$$= g^2 \begin{vmatrix} f_1 & f_2 & f_3 \\ f_1' & f_2' & f_3' \\ f_1'' g + 2 f_1' g' & f_2'' g + 2 f_2' g' & f_3'' g + 2 f_3' g' \end{vmatrix} = g^3 \mathrm{W}(f_1, f_2, f_3).$$

Linear Dependence for Analytic Functions (3/3): The Recursive Formula for the Wronskian

Proposition [Hesse - Christoffel - Frobenius]:
$W(f_1, \ldots, f_k) = f_1^k W((f_2/f_1)', \ldots, (f_k/f_1)')$.
From previous lemma:

$$W(f_1, f_2, f_3) = f_1^3 W(1, f_2/f_1, f_3/f_1) = f_1^3 \begin{vmatrix} 1 & f_2/f_1 & f_3/f_1 \\ 0 & (f_2/f_1)' & (f_3/f_1)' \\ 0 & (f_2/f_1)'' & (f_3/f_1)'' \end{vmatrix}$$

Hence

$$W(f_1, f_2, f_3) = f_1^3 \begin{vmatrix} (f_2/f_1)' & (f_3/f_1)' \\ (f_2/f_1)'' & (f_3/f_1)'' \end{vmatrix} = f_1^3 W((f_2/f_1)', (f_3/f_1)').$$

Linear Dependence for Analytic Functions (3/3): The Recursive Formula for the Wronskian

Proposition [Hesse - Christoffel - Frobenius]:
$W(f_1, \ldots, f_k) = f_1^k W((f_2/f_1)', \ldots, (f_k/f_1)')$.
From previous lemma:

$$W(f_1, f_2, f_3) = f_1^3 W(1, f_2/f_1, f_3/f_1) = f_1^3 \begin{vmatrix} 1 & f_2/f_1 & f_3/f_1 \\ 0 & (f_2/f_1)' & (f_3/f_1)' \\ 0 & (f_2/f_1)'' & (f_3/f_1)'' \end{vmatrix}$$

Hence

$$W(f_1, f_2, f_3) = f_1^3 \begin{vmatrix} (f_2/f_1)' & (f_3/f_1)' \\ (f_2/f_1)'' & (f_3/f_1)'' \end{vmatrix} = f_1^3 W((f_2/f_1)', (f_3/f_1)').$$

Linear Dependence for Analytic Functions (3/3): The Recursive Formula for the Wronskian

Proposition [Hesse - Christoffel - Frobenius]:
$W(f_1, \ldots, f_k) = f_1^k W((f_2/f_1)', \ldots, (f_k/f_1)')$.
From previous lemma:

$$W(f_1, f_2, f_3) = f_1^3 W(1, f_2/f_1, f_3/f_1) = f_1^3 \begin{vmatrix} 1 & f_2/f_1 & f_3/f_1 \\ 0 & (f_2/f_1)' & (f_3/f_1)' \\ 0 & (f_2/f_1)'' & (f_3/f_1)'' \end{vmatrix}$$

Hence

$$W(f_1, f_2, f_3) = f_1^3 \begin{vmatrix} (f_2/f_1)' & (f_3/f_1)' \\ (f_2/f_1)'' & (f_3/f_1)'' \end{vmatrix} = f_1^3 W((f_2/f_1)', (f_3/f_1)').$$

Proof of Upper Bound Theorem

Theorem: Assume that the k wronskians

$$W(f_1), W(f_1, f_2), W(f_1, f_2, f_3), \dots, W(f_1, \dots, f_k)$$

have no zeros on I.
Let $f = a_1 f_1 + \cdots + a_k f_k$ where $a_i \neq 0$ for some i.
Then f has at most $k - 1$ zeros on I, counted with multiplicities.
Proof: By induction on k.
Assume $k \geq 2$ and $a_2, \dots, a_k$ not all 0.
Write $f = f_1 g$ where $g = a_1 + a_2 f_2/f_1 + \cdots + a_k f_k/f_1$.
To apply induction hypothesis to $g' = a_2(f_2/f_1)' + \cdots + a_k(f_k/f_1)'$:
Note

$$\mathrm{W}((f_2/f_1)', \dots, (f_i/f_1)') = \mathrm{W}(f_1, \dots, f_i)/f_1^i$$

has no zero on I.
Hence g' has at most $k - 2$ zeros on I,
g and f at most $k - 1$ by Rolle's theorem.

Proof of Upper Bound Theorem

Theorem: Assume that the k wronskians

$$W(f_1), W(f_1, f_2), W(f_1, f_2, f_3), \ldots, W(f_1, \ldots, f_k)$$

have no zeros on I.
Let $f = a_1 f_1 + \cdots + a_k f_k$ where $a_i \neq 0$ for some i.
Then f has at most $k - 1$ zeros on I, counted with multiplicities.
Proof: By induction on k.
Assume $k \geq 2$ and $a_2, \ldots, a_k$ not all 0.
Write $f = f_1 g$ where $g = a_1 + a_2 f_2/f_1 + \cdots + a_k f_k/f_1$.
To apply induction hypothesis to $g' = a_2(f_2/f_1)' + \cdots + a_k(f_k/f_1)'$:
Note

$$\mathrm{W}((f_2/f_1)', \ldots, (f_i/f_1)') = \mathrm{W}(f_1, \ldots, f_i)/f_1^i$$

has no zero on I.
Hence g' has at most $k - 2$ zeros on I,
g and f at most $k - 1$ by Rolle's theorem.

Proof of Upper Bound Theorem

Theorem: Assume that the k wronskians

$$W(f_1), W(f_1, f_2), W(f_1, f_2, f_3), \ldots, W(f_1, \ldots, f_k)$$

have no zeros on I.
Let $f = a_1 f_1 + \cdots + a_k f_k$ where $a_i \neq 0$ for some i.
Then f has at most $k - 1$ zeros on I, counted with multiplicities.
Proof: By induction on k.
Assume $k \geq 2$ and $a_2, \ldots, a_k$ not all 0.
Write $f = f_1 g$ where $g = a_1 + a_2 f_2/f_1 + \cdots + a_k f_k/f_1$.
To apply induction hypothesis to $g' = a_2(f_2/f_1)' + \cdots + a_k(f_k/f_1)'$:
Note

$$\mathrm{W}((f_2/f_1)', \ldots, (f_i/f_1)') = \mathrm{W}(f_1, \ldots, f_i)/f_1^i$$

has no zero on I.
Hence g' has at most $k - 2$ zeros on I,
g and f at most $k - 1$ by Rolle's theorem.

Proof of Upper Bound Theorem

Theorem: Assume that the k wronskians

$$W(f_1), W(f_1, f_2), W(f_1, f_2, f_3), \ldots, W(f_1, \ldots, f_k)$$

have no zeros on I.
Let $f = a_1 f_1 + \cdots + a_k f_k$ where $a_i \neq 0$ for some i.
Then f has at most $k-1$ zeros on I, counted with multiplicities.
Proof: By induction on k.
Assume $k \geq 2$ and $a_2, \ldots, a_k$ not all 0.
Write $f = f_1 g$ where $g = a_1 + a_2 f_2/f_1 + \cdots + a_k f_k/f_1$.
To apply induction hypothesis to $g' = a_2(f_2/f_1)' + \cdots + a_k(f_k/f_1)'$:
Note

$$\mathrm{W}((f_2/f_1)', \ldots, (f_i/f_1)') = \mathrm{W}(f_1, \ldots, f_i)/f_1^i$$

has no zero on I.
Hence g' has at most $k-2$ zeros on I,
g and f at most $k-1$ by Rolle's theorem.

Application: Intersection of a plane curve and a line (1/2)

Theorem (Avendano'09):
Let $g = \sum_{j=1}^{k} a_j x^{\alpha_j} y^{\beta_j}$ and $f(x) = f(x, ax+b)$. Assume $f \not\equiv 0$.
If $b/a > 0$ then f has at most $2k-2$ in each of the 3 intervals $]-\infty, -b/a[$, $]-b/a, 0[$, $]0, +\infty[$.
Remark: This bound is *provably false* for rational exponents.

Set $a = b = 1$ and $f_j(X) = X^{\alpha_j}(1+X)^{\beta_j}$.
The entries of the wronskians are of the form:

$$f_j^{(i)}(X) = \sum_{t=0}^{i} c_{ijt} X^{\alpha_j - t}(1+X)^{\beta_j - i + t}.$$

Factorizing common factors in rows and columns shows

$$\mathrm{W}(f_1, \ldots, f_k) = X^{\sum_j \alpha_j - \binom{k}{2}}(1+X)^{\sum_j \beta_j - \binom{k}{2}} \det M$$

where $\det M$ has degree $\leq \binom{k}{2}$.

Application: Intersection of a plane curve and a line (1/2)

Theorem (Avendano'09):
Let $g = \sum_{j=1}^{k} a_j x^{\alpha_j} y^{\beta_j}$ and $f(x) = f(x, ax+b)$. Assume $f \not\equiv 0$.
If $b/a > 0$ then f has at most $2k-2$ in each of the 3 intervals
$]-\infty, -b/a[$, $]-b/a, 0[$, $]0, +\infty[$.
Remark: This bound is *provably false* for rational exponents.

Set $a = b = 1$ and $f_j(X) = X^{\alpha_j}(1+X)^{\beta_j}$.
The entries of the wronskians are of the form:

$$f_j^{(i)}(X) = \sum_{t=0}^{i} c_{ijt} X^{\alpha_j - t}(1+X)^{\beta_j - i + t}.$$

Factorizing common factors in rows and columns shows

$$\mathrm{W}(f_1, \ldots, f_k) = X^{\sum_j \alpha_j - \binom{k}{2}}(1+X)^{\sum_j \beta_j - \binom{k}{2}} \det M$$

where $\det M$ has degree $\leq \binom{k}{2}$.

Application: Intersection of a plane curve and a line (2/2)

Conclusion:
$f(x) = \sum_{j=1}^{k} a_j x^{\alpha_j}(1+x)^{\beta_j}$ has $O(k^4)$ zeros in $]0, +\infty[$.

Proof:
Assume $\mathrm{W}(f_1, \ldots, f_k) \not\equiv 0$ (otherwise, there is a linear dependence).
We have k Wronskians, each with $O(k^2)$ zeros in $]0, +\infty[$.
$\Rightarrow O(k^3)$ intervals containing $\leq k-1$ zeros each.

Remark: This can be adapted to a number of different models.

Application: Intersection of a plane curve and a line (2/2)

Conclusion:
$f(x) = \sum_{j=1}^{k} a_j x^{\alpha_j}(1+x)^{\beta_j}$ has $O(k^4)$ zeros in $]0,+\infty[$.

Proof:
Assume $\mathrm{W}(f_1,\ldots,f_k) \not\equiv 0$ (otherwise, there is a linear dependence).
We have k Wronskians, each with $O(k^2)$ zeros in $]0,+\infty[$.
$\Rightarrow O(k^3)$ intervals containing $\leq k-1$ zeros each.

Remark: This can be adapted to a number of different models.

Application: Intersection of a plane curve and a line (2/2)

Conclusion:
$f(x) = \sum_{j=1}^{k} a_j x^{\alpha_j}(1+x)^{\beta_j}$ has $O(k^4)$ zeros in $]0, +\infty[$.

Proof:
Assume $\mathrm{W}(f_1, \ldots, f_k) \not\equiv 0$ (otherwise, there is a linear dependence).
We have k Wronskians, each with $O(k^2)$ zeros in $]0, +\infty[$.
$\Rightarrow O(k^3)$ intervals containing $\leq k-1$ zeros each.

Remark: This can be adapted to a number of different models.

To learn more about the Wronskian

- M. Krusemeyer. Why does the Wronskian work?
  American Math. Monthly, 1988.
  (Recursive formula for the Wronskian)
- A. Bostan and P. Dumas.
  Wronskians and Linear Independence.
  American Math. Monthly, 2010. *(New non-recursive proof for analytic functions and power series)*
- G. Pólya and G. Szegö.
  Problems and Theorems in Analysis II.
  (Includes connection to Descartes' rule of signs,
  pointed out by Saugata Basu)

§ 7. What is the Basis of Descartes' Rule of Signs?

We see from **36, 41, 77, 84, 85** that the sequences of functions

$$1,\quad x,\quad x^2,\quad x^3,\ \ldots,$$
$$1,\quad x-\xi_1,\quad (x-\xi_1)(x-\xi_2),\ \ldots,$$
$$e^{\lambda_1 x},\quad e^{\lambda_2 x},\quad e^{\lambda_3 x},\ \ldots,$$
$$1,\quad \frac{1}{x},\quad \frac{1}{x(x+1)},\quad \frac{1}{x(x+1)(x+2)},\ \ldots,$$
$$F(\alpha_1 x),\quad F(\alpha_2 x),\quad F(\alpha_3 x),\ \ldots$$

considered there have a common property: The number of zeros lying in a certain interval of their linear combinations with constant coefficients never exceeds the number of changes of sign of these coefficients. What is the basis for this frequent validity of Descartes' rule of signs?

87. Let the sequence of functions

$$h_1(x),\ h_2(x),\ h_3(x),\ \ldots,\ h_n(x)$$

obey Descartes' rule of signs in the open inerval $a<x<b$. More precisely: If $a_1, a_2, \ldots, a_n$ denote any real numbers which are not all zero, then the number of zeros lying in $a<x<b$ of the linear combination

$$a_1h_1(x)+a_2h_2(x)+\cdots+a_nh_n(x)$$

never exceeds the number of changes of sign of the sequence

$$a_1,\ a_2,\ \ldots,\ a_n.$$

and sufficient

For this to hold, the following property of the sequence $h_1(x), h_2(x), \ldots, h_n(x)$ is a necessary condition: If $\nu_1, \nu_2, \ldots, \nu_l$ denote integers with $1 \leq \nu_1 < \nu_2 < \nu_3 < \cdots < \nu_l \leq n$, then the Wronskian determinants [VII, §5]

$$W[h_{\nu_1}(x),\ h_{\nu_2}(x),\ h_{\nu_3}(x),\ \ldots,\ h_{\nu_l}(x)]$$

do not vanish in the interval (a, b) and further any two Wronskian determinants with the same number l of rows have the same sign, where $l=1, 2, 3, \ldots, n-1$. [Look at multiple zeros!]

88 (continued). In particular for the validity of Descartes' rule of signs it is necessary that in the interval $a<x<b$ the quotients

$$\frac{h_2(x)}{h_1(x)},\quad \frac{h_3(x)}{h_2(x)},\quad \ldots,\quad \frac{h_n(x)}{h_{n-1}(x)}$$

are all positive and are either all monotonically decreasing or all monotonically increasing.

89 (continued). Let $1 \leq \alpha \leq n$. If $h_1(x), h_2(x), \ldots, h_n(x)$ satisfy the determinantal conditions stated in **87**, then so do the $n-1$ functions

$$H_1=-\frac{d}{dx}\frac{h_1}{h_\alpha},\quad H_2=-\frac{d}{dx}\frac{h_2}{h_\alpha},\ldots,\quad H_{\alpha-1}=-\frac{d}{dx}\frac{h_{\alpha-1}}{h_\alpha},$$
$$H_\alpha=\frac{d}{dx}\frac{h_{\alpha+1}}{h_\alpha},\ldots,\quad H_{n-2}=\frac{d}{dx}\frac{h_{n-1}}{h_\alpha},\quad H_{n-1}=\frac{d}{dx}\frac{h_n}{h_\alpha}.$$

[VII **58**.]

A lower bound for restricted depth 4 circuits, or: the limited power of powering.

Consider representations of the permanent of the form:

$$\mathrm{PER}(X) = \sum_{i=1}^{k} \prod_{j=1}^{m} f_j^{\alpha_{ij}}(X) \qquad (1)$$

where

- X is a $n \times n$ matrix of indeterminates.
- k and m are bounded, and the α_{ij} are of polynomial bit size.
- The f_j are polynomials in n^2 variables, with at most t monomials.

Theorem [with Grenet, Portier and Strozecki]:
No such representation if t is polynomially bounded in n.
Remark: The point is that the α_{ij} may be nonconstant.
Otherwise, the number of monomials in (1) is polynomial in t.

Lower Bound Proof

- Assume otherwise:

$$\mathrm{PER}(X) = \sum_{i=1}^{k} \prod_{j=1}^{m} f_j^{\alpha_{ij}}(X). \tag{2}$$

- Since PER is easy, $P_n = \prod_{i=1}^{2^n}(x - i)$ is easy too.
  In fact [Bürgisser], $P_n(x) = \mathrm{PER}(X)$ where X is of size $n^{O(1)}$, with entries that are constants or powers of x.
- By (2) and upper bound theorem, P_n should have only $n^{O(1)}$ real roots.
  But P_n has 2^n integer roots!

Remark:
The current proof requires the Generalized Riemann Hypothesis (to handle arbitrary complex coefficients in the f_j).

Lower Bound Proof

- Assume otherwise:

$$\mathrm{PER}(X) = \sum_{i=1}^{k} \prod_{j=1}^{m} f_j^{\alpha_{ij}}(X). \tag{2}$$

- Since PER is easy, $P_n = \prod_{i=1}^{2^n}(x - i)$ is easy too.
  In fact [Bürgisser], $P_n(x) = \mathrm{PER}(X)$ where X is of size $n^{O(1)}$, with entries that are constants or powers of x.
- By (2) and upper bound theorem, P_n should have only $n^{O(1)}$ real roots.
  But P_n has 2^n integer roots!

Remark:
The current proof requires the Generalized Riemann Hypothesis (to handle arbitrary complex coefficients in the f_j).

Lower Bound Proof

- Assume otherwise:

$$\mathrm{PER}(X) = \sum_{i=1}^{k} \prod_{j=1}^{m} f_j^{\alpha_{ij}}(X). \tag{2}$$

- Since PER is easy, $P_n = \prod_{i=1}^{2^n}(x-i)$ is easy too.
  In fact [Bürgisser], $P_n(x) = \mathrm{PER}(X)$ where X is of size $n^{O(1)}$, with entries that are constants or powers of x.
- By (2) and upper bound theorem, P_n should have only $n^{O(1)}$ real roots.
  But P_n has 2^n integer roots!

Remark:
The current proof requires the Generalized Riemann Hypothesis (to handle arbitrary complex coefficients in the f_j).

Lower Bound Proof

- Assume otherwise:

$$\mathrm{PER}(X) = \sum_{i=1}^{k} \prod_{j=1}^{m} f_j^{\alpha_{ij}}(X). \qquad (2)$$

- Since PER is easy, $P_n = \prod_{i=1}^{2^n}(x - i)$ is easy too.
  In fact [Bürgisser], $P_n(x) = \mathrm{PER}(X)$ where X is of size $n^{O(1)}$, with entries that are constants or powers of x.
- By (2) and upper bound theorem, P_n should have only $n^{O(1)}$ real roots.
  But P_n has 2^n integer roots!

Remark:
The current proof requires the Generalized Riemann Hypothesis (to handle arbitrary complex coefficients in the f_j).