Upper and Lower Bounds for Arithmetic Circuits

Sébastien Tavenas

supervised by Pascal Koiran and Natacha Portier

July 9, 2014

Title: "Upper and Lower Bounds for Arithmetic Circuits"

- A problem: multiply 12345 by 378267

Title: "Upper and Lower Bounds for Arithmetic Circuits"

- A problem: multiply 12345 by 378267
- Algorithm with 40 operations.

Title: “Upper and Lower Bounds for Arithmetic Circuits”

- A problem: multiply 12345 by 378267
- Algorithm with 40 operations.
  $\Rightarrow$ Upper bound on the minimal cost.

Title: "Upper and Lower Bounds for Arithmetic Circuits"

- A problem: multiply 12345 by 378267
- Algorithm with 40 operations.
  $\Rightarrow$ Upper bound on the minimal cost.
- Proof: it is not possible with 10 operations.

Title: "Upper and Lower Bounds for Arithmetic Circuits"

- A problem: multiply 12345 by 378267
- Algorithm with 40 operations.
  $\Rightarrow$ Upper bound on the minimal cost.
- Proof: it is not possible with 10 operations.
  $\Rightarrow$ Lower bound on the minimal cost.

Title: "Upper and Lower Bounds for Arithmetic Circuits"

- A problem: multiply 12345 by 378267
- Algorithm with 40 operations.
  $\Rightarrow$ Upper bound on the minimal cost.
- Proof: it is not possible with 10 operations.
  $\Rightarrow$ Lower bound on the minimal cost.
- Easier model of computation: Arithmetic circuits.

Outline

1. Arithmetic circuits
2. Depth Reduction
3. Real τ-conjecture
4. Sevostyanov's problem

Outline

Arithmetic circuits

Polynomials

$f(x, y) = 4x^2 - 2xy$

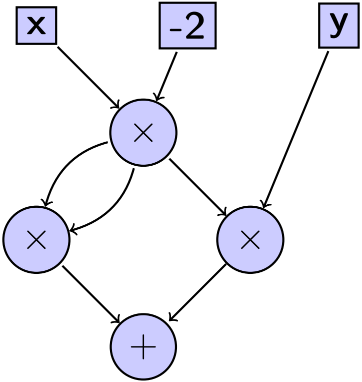
Representation by circuits (gates: $+$, $\times$, variables and real constants):

Arithmetic circuits

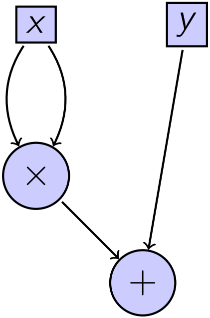
Polynomials

$f(x, y) = 4x^2 - 2xy$

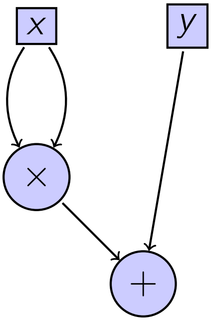
Representation by circuits (gates: $+$, $\times$, variables and real constants):



Complexity of the circuits - Examples



Complexity of the circuits - Examples



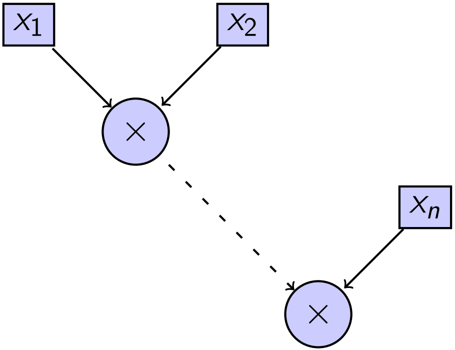
- Computed polynomial: $P(x) = x^2 + y$.
- Size: $s = 4$.
- Depth: $l = 2$.

Complexity of the circuits - Examples

- Example:
  $P_n(x_1, \ldots, x_n) = x_1 \cdot x_2 \cdot \ldots \cdot x_n$

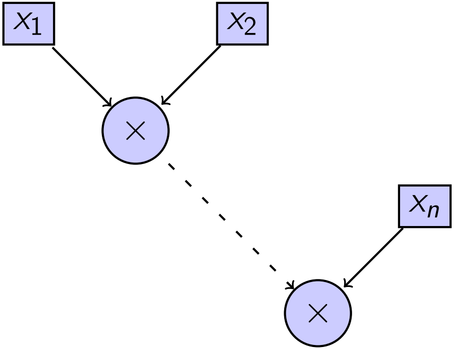
Complexity of the circuits - Examples

- Example:
  $P_n(x_1, \ldots, x_n) = x_1 \cdot x_2 \cdot \ldots \cdot x_n$



Complexity of the circuits - Examples

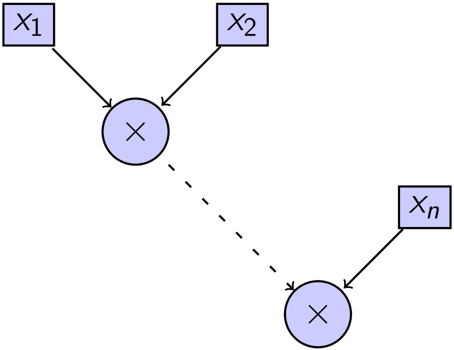
- Example:
  $P_n(x_1, \dots, x_n) = x_1 \cdot x_2 \cdot \dots \cdot x_n$



- Size: $s = 2n - 1$.
- Depth: $l = n - 1$.

Complexity of the circuits - Examples

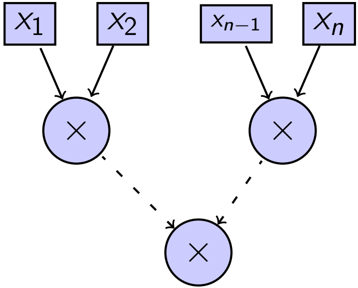
- Example:
  $P_n(x_1, \ldots, x_n) = x_1 \cdot x_2 \cdot \ldots \cdot x_n$



- Size: $s = 2n - 1$.
- Depth: $l = n - 1$.
- Sequence: homogeneous polynomials
  - $x^3 - 2xy^2 \rightarrow$ hom.
  - $x^2y^2 + y^4 - 3 \rightarrow$ not hom.
- Homogeneous circuit: all gates compute homogeneous polynomials.

Complexity of the circuits - Examples

- Example:
  $P_n(x_1, \ldots, x_n) = x_1 \cdot x_2 \cdot \ldots \cdot x_n$



- Size: $s = 2n - 1$.
- Depth: $l = \log n$.

Valiant's conjecture

Class VP

(f_n) : there exists c s.t. for every $n \geq 2$

- f_n is computed by circuits of size $\leq n^c$
- 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

(f_n) : there exists c s.t. for every $n \geq 2$

- f_n is computed by circuits of size $\leq n^c$
- degree is bounded by n^c.

Class VNP

(g_n) : there exists $(f_n) \in \mathrm{VP}$ s.t. for every 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

(f_n) : there exists c s.t. for every $n \geq 2$

- f_n is computed by circuits of size $\leq n^c$
- degree is bounded by n^c.

Class VNP

(g_n) : there exists $(f_n) \in \mathrm{VP}$ s.t. for every n

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

Valiant's conjecture (1979)

$\mathrm{VP} \neq \mathrm{VNP}$.

Outline

1. Arithmetic circuits
2. Depth Reduction
3. Real τ-conjecture
4. Sevostyanov's problem

Reduction of the depth

Theorem (Valiant,Skyum,Berkowitz,Rackoff (1983))

f: homogeneous, of degree d, circuits of size s.
Then f computed by homogeneous circuits of size $(sd)^{O(1)}$ and of depth $O(\log s \log d)$.

Reduction of the depth

Theorem (Valiant,Skyum,Berkowitz,Rackoff (1983))

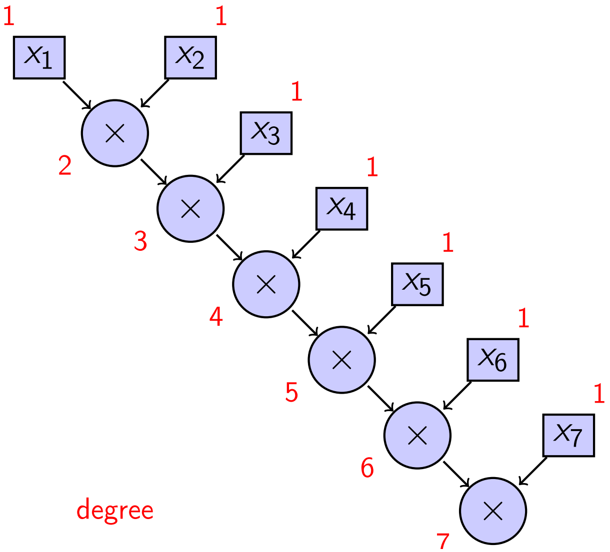
f: homogeneous, of degree d, circuits of size s.
Then f computed by homogeneous circuits of size $(sd)^{O(1)}$ and of depth $O(\log s \log d)$.

Theorem (Valiant,Skyum,Berkowitz,Rackoff/Agrawal,Vinay (2008))

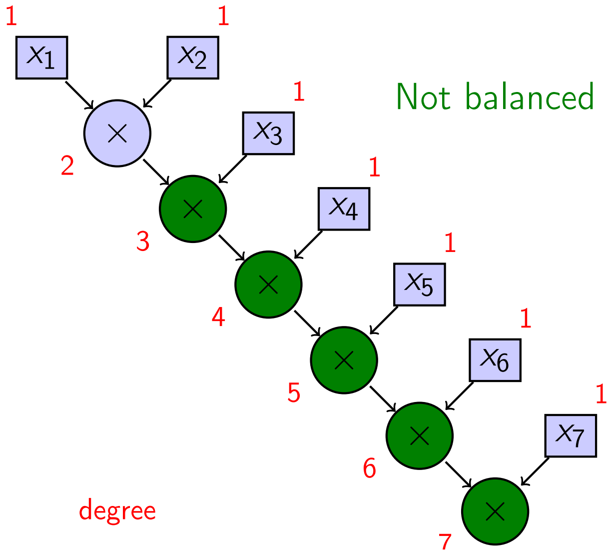
f: homogeneous, degree d, circuits of size s.
Then f computed by homogeneous circuits of size $(sd)^{O(1)}$
such that

- *Fan-in of $\times$-gates bounded by 5,*
- *If α is a $\times$-gate of degree d and of children $\alpha_1, \ldots, \alpha_r$ ($r \leq 5$), then $\forall i, d^\circ(\alpha_i) \leq \frac{d}{2}$.*

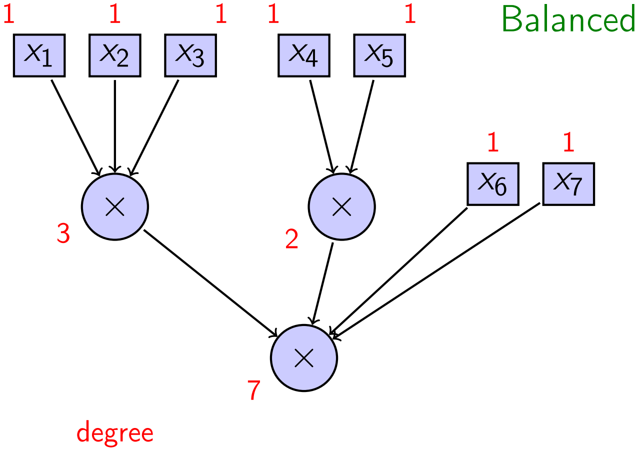
Reduction of the depth



Reduction of the depth



Reduction of the depth



Reduction of the depth

Theorem (Valiant,Skyum,Berkowitz,Rackoff (1983))

f: homogeneous, of degree d, circuits of size s.
Then f computed by homogeneous circuits of size $(sd)^{O(1)}$ and of depth $O(\log s \log d)$.

Theorem (Valiant,Skyum,Berkowitz,Rackoff/Agrawal,Vinay (2008))

f: homogeneous, degree d, circuits of size s.
Then f computed by homogeneous circuits of size $(sd)^{O(1)}$
such that

- *Fan-in of $\times$-gates bounded by 5,*
- *If α is a $\times$-gate of degree d and of children $\alpha_1, \dots, \alpha_r$ ($r \leq 5$), then $\forall i, d^\circ(\alpha_i) \leq \frac{d}{2}$.*

In the following, $s, d = n^{O(1)}$.

Reduction of the depth

Theorem (Valiant,Skyum,Berkowitz,Rackoff (1983))

f: homogeneous, of degree d, circuits of size s.
Then f computed by homogeneous circuits of size $(sd)^{O(1)}$ and of depth $O(\log s \log d)$.

Theorem (Valiant,Skyum,Berkowitz,Rackoff/Agrawal,Vinay (2008))

f: homogeneous, degree d, circuits of size s.
Then f computed by homogeneous circuits of size $(sd)^{O(1)}$
such that

- *Fan-in of $\times$-gates bounded by 5,*
- *If α is a $\times$-gate of degree d and of children $\alpha_1, \ldots, \alpha_r$ ($r \leq 5$), then $\forall i, d^\circ(\alpha_i) \leq \frac{d}{2}$.*

In the following, $s, d = n^{O(1)}$.
Is it possible to reduce the depth?

Reduction to depth 4

Unbounded fan-in for the gates.

Reduction to depth 4

Unbounded fan-in for the gates.

Theorem (Agrawal,Vinay (2008))

If f has subexponential-size circuits ($n^{o(d)}$),
then f has depth-4 circuits of subexponential size.

Reduction to depth 4

Unbounded fan-in for the gates.

Theorem (Agrawal,Vinay (2008))

If f has subexponential-size circuits ($n^{o(d)}$), then f has depth-4 circuits of subexponential size.

Remarks:

- Depth 2 $\rightarrow$ the polynomial is expanded as a sum of monomials.

Reduction to depth 4

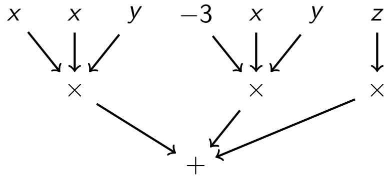
Unbounded fan-in for the gates.

Theorem (Agrawal,Vinay (2008))

If f has subexponential-size circuits ($n^{o(d)}$), then f has depth-4 circuits of subexponential size.

Remarks:

- Depth 2 $\rightarrow$ the polynomial is expanded as a sum of monomials.
  - $x^2y - 3xy + z \rightarrow$



Reduction to depth 4

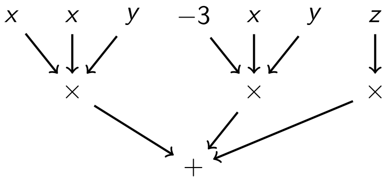
Unbounded fan-in for the gates.

Theorem (Agrawal,Vinay (2008))

If f has subexponential-size circuits ($n^{o(d)}$),
then f has depth-4 circuits of subexponential size.

Remarks:

- Depth 2 $\rightarrow$ the polynomial is expanded as a sum of monomials.
  - $x^2y - 3xy + z \rightarrow$



- Depth 3 $\rightarrow$ a subexponential reduction to depth 3 using the reduction to depth 4.

Reduction to depth 4

Theorem (Koiran (2012))

If f has polynomial-size (homogeneous) circuits,
then f has depth 4 (homogeneous) circuits of size $2^{O(\sqrt{d}\log^2 n)}$.

Idea:

$$\underset{s,d}{\mathcal{C}} \longrightarrow \underset{2^{O(\log d \log s)}}{\text{Iterated matrix product}} \longrightarrow \underset{2^{O(\sqrt{d}\log d \log s)}}{\text{Depth 4 circuits}}$$

Reduction to depth 4

Theorem (Koiran (2012))

If f has polynomial-size (homogeneous) circuits, then f has depth 4 (homogeneous) circuits of size $2^{O(\sqrt{d}\log^2 n)}$.

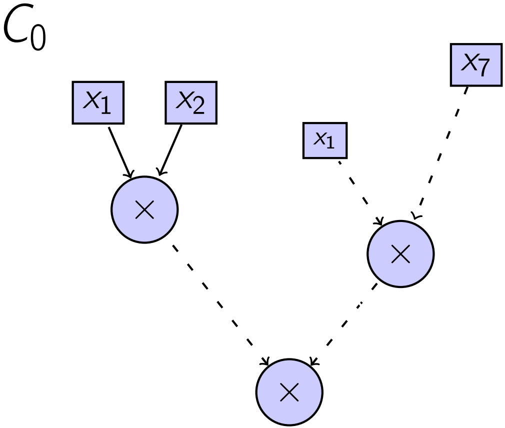
Idea:

$$\underset{s,d}{\mathcal{C}} \longrightarrow \underset{2^{O(\log d \log s)}}{\text{Iterated matrix product}} \longrightarrow \underset{2^{O(\sqrt{d}\log d \log s)}}{\text{Depth 4 circuits}}$$

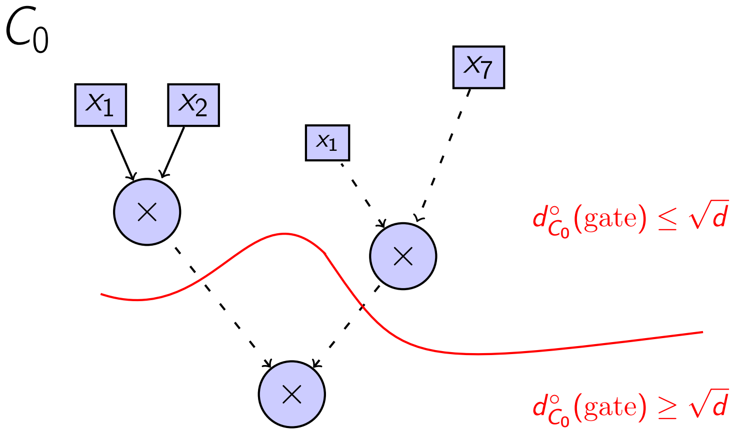
Theorem (T. *MFCS 2013*)

If f has polynomial-size (homogeneous) circuits, then f has depth 4 (homogeneous) circuits of size $2^{O(\sqrt{d}\log n)}$.

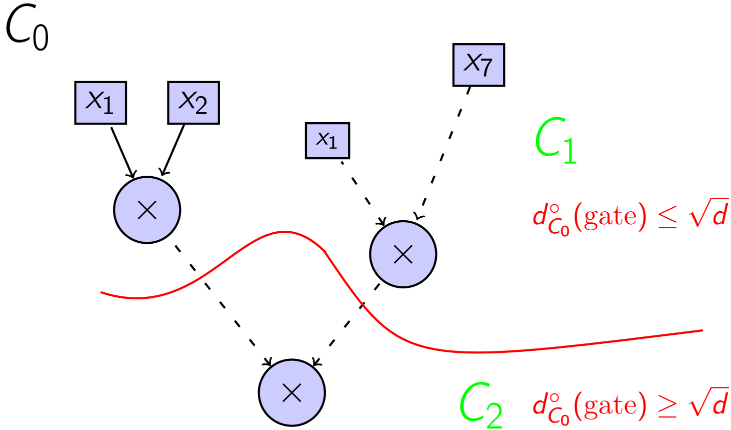
Idea of the proof 1/5



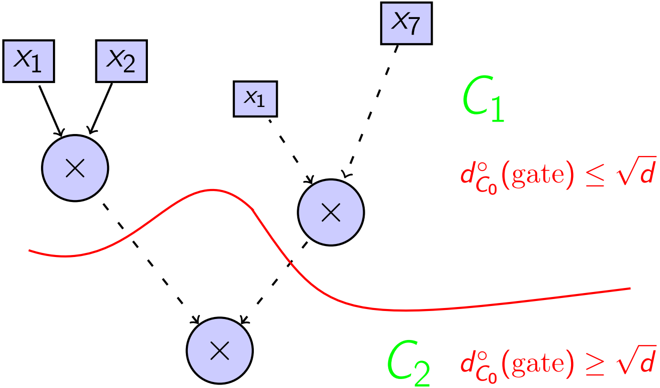
Idea of the proof 1/5



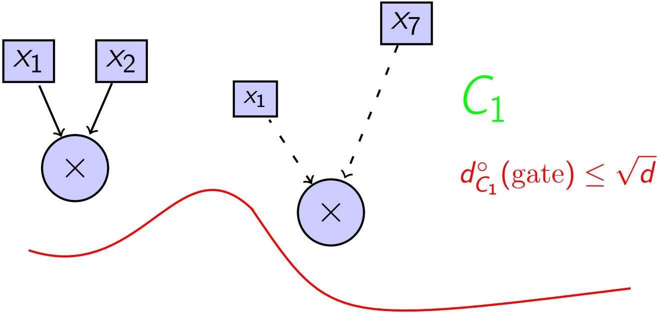
Idea of the proof 1/5



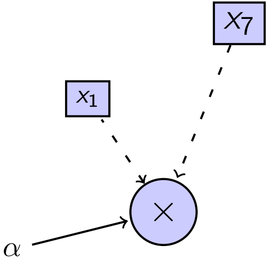
Idea of the proof 2/5



Idea of the proof 2/5



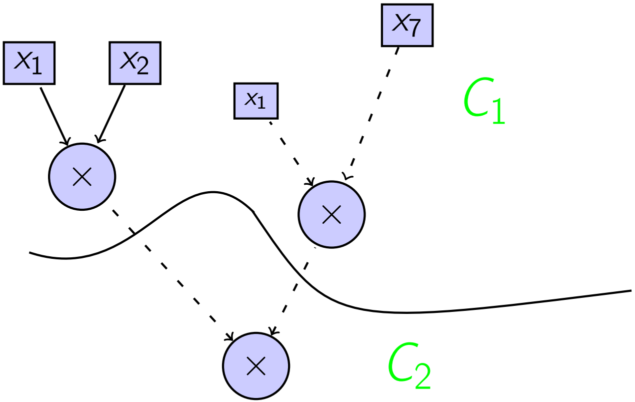
Idea of the proof 2/5



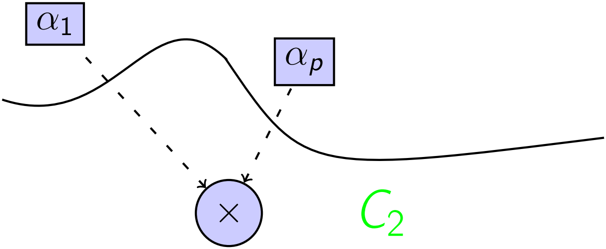
$d^{\circ}_{C_1}(\text{gate}) \leq \sqrt{d}$

α computed by a depth-2 circuit of size $n^{O(\sqrt{d})}$

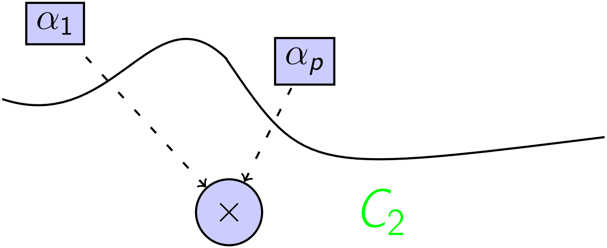
Idea of the proof 3/5: Let us suppose...



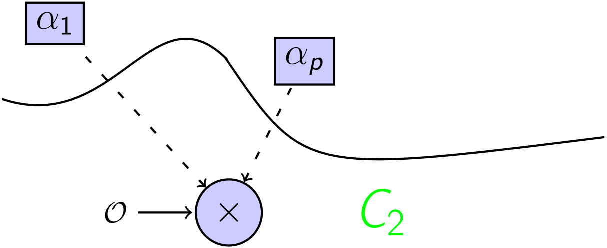
Idea of the proof 3/5: Let us suppose...



Idea of the proof 3/5: Let us suppose...

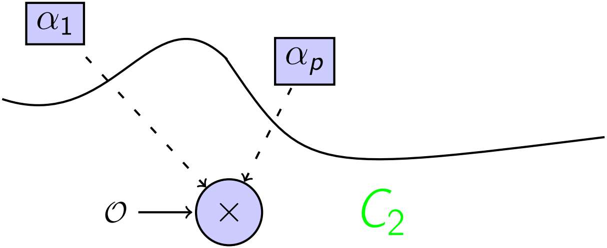


Idea of the proof 3/5: Let us suppose...



Let us suppose that $d^{\circ}_{C_2}(\mathcal{O}) = O(\sqrt{d})$

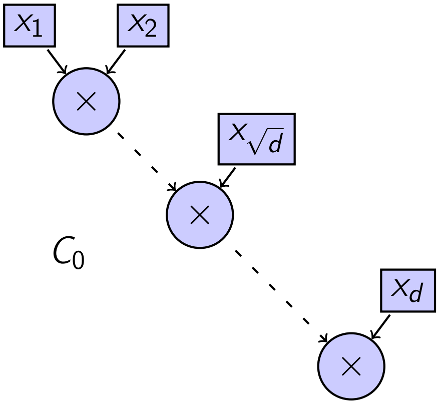
Idea of the proof 3/5: Let us suppose...



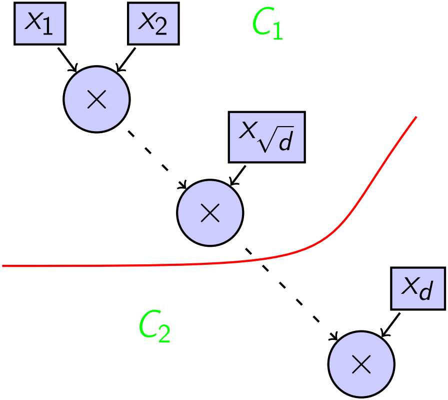
Let us suppose that $d^{\circ}_{C_2}(\mathcal{O}) = O(\sqrt{d})$

depth-2 circuit of size $n^{O(\sqrt{d})}$ for C_2 $\rightarrow$ QED

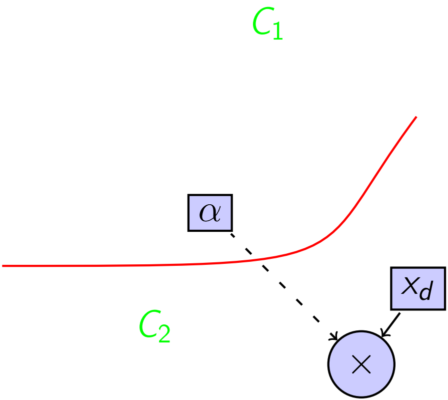
Idea of the proof 4/5: but ...



Idea of the proof 4/5: but ...



Idea of the proof 4/5: but ...



C_2 computes $\alpha \cdot x_{\sqrt{d}+1} \cdot \ldots \cdot x_d$

of degree $d - \sqrt{d} + 1 >> \sqrt{d}$

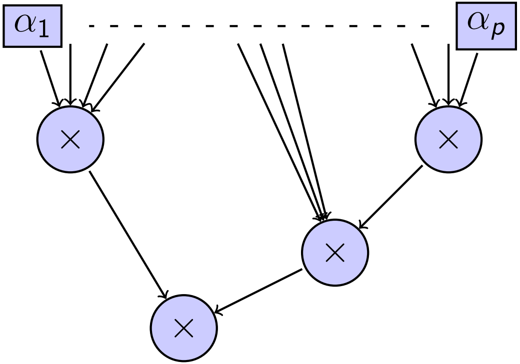
Idea of the proof 5/5: ... and if C_0 is balanced.

Lemma

If C_0 is balanced, then the degree of $C_2 \leq O(\sqrt{d})$.

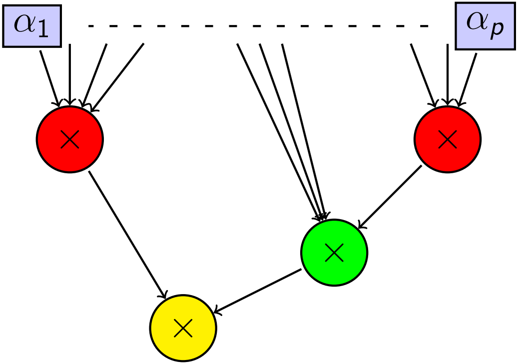
Idea of the proof 5/5: ... and if C_0 is balanced.

A monomial in C_2

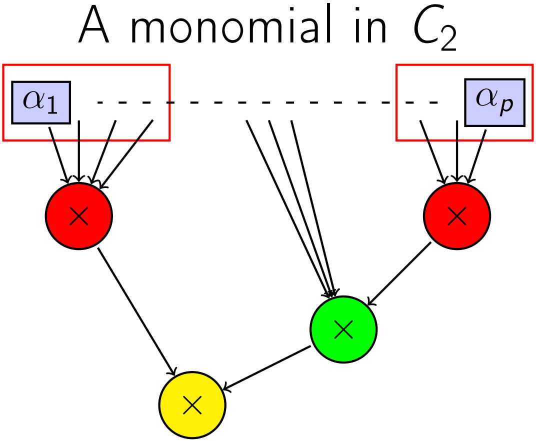


Idea of the proof 5/5: ... and if C_0 is balanced.

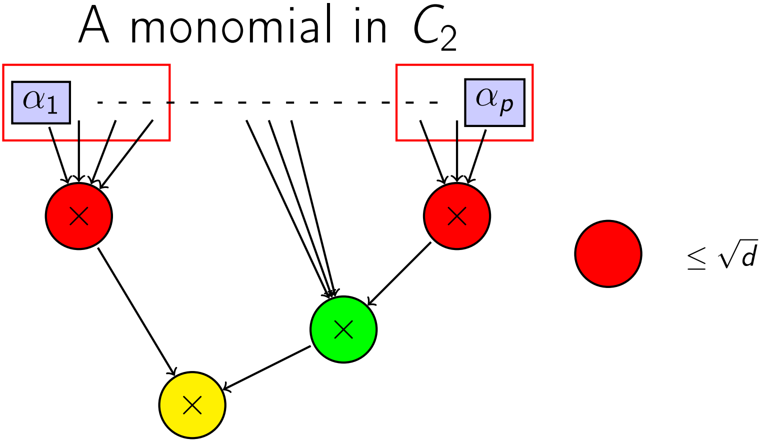
A monomial in C_2



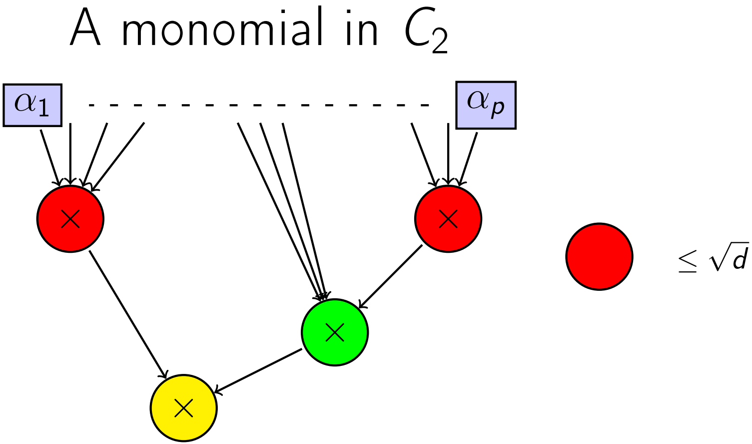
Idea of the proof 5/5: ... and if C_0 is balanced.



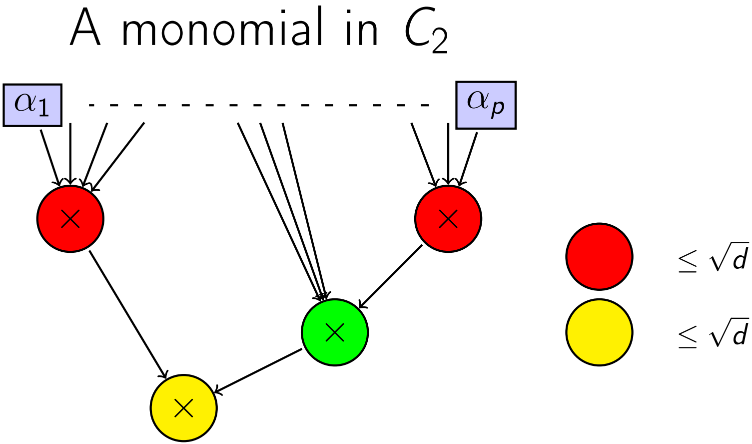
Idea of the proof 5/5: ... and if C_0 is balanced.



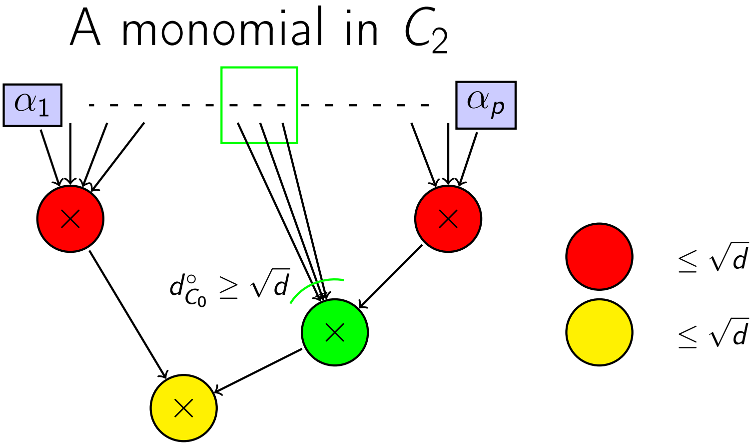
Idea of the proof 5/5: ... and if C_0 is balanced.



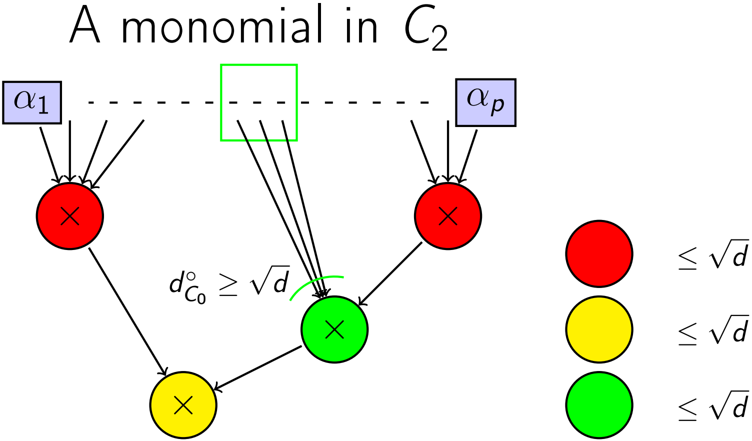
Idea of the proof 5/5: ... and if C_0 is balanced.



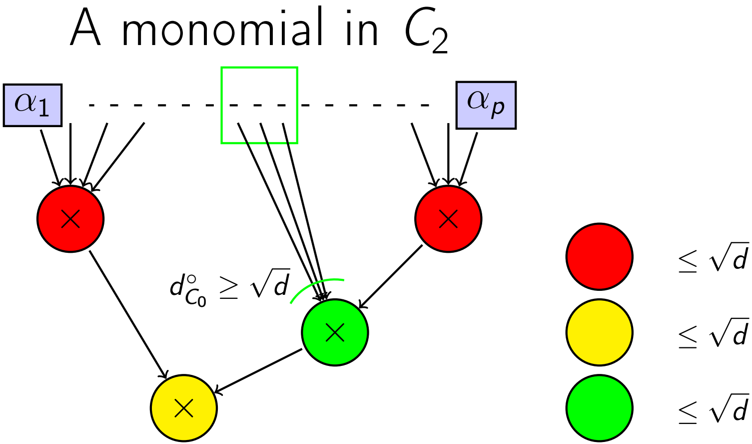
Idea of the proof 5/5: ... and if C_0 is balanced.



Idea of the proof 5/5: ... and if C_0 is balanced.



Idea of the proof 5/5: ... and if C_0 is balanced.



So $d^\circ(C_2) \leq 15\sqrt{d}$ $\Rightarrow$ theorem is proved.

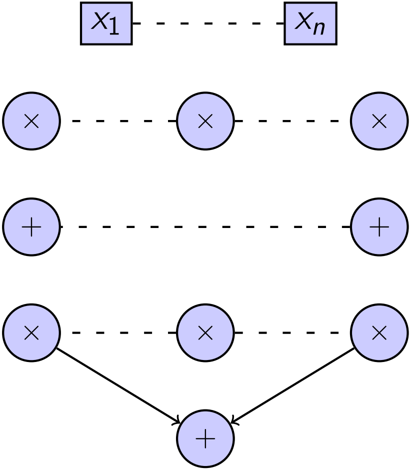
Case of the Permanent

Corollary

If Perm_n *has no depth-4 homogeneous circuits of size* $2^{O(\sqrt{n}\log n)}$, *then* $\mathsf{VP} \neq \mathsf{VNP}$.

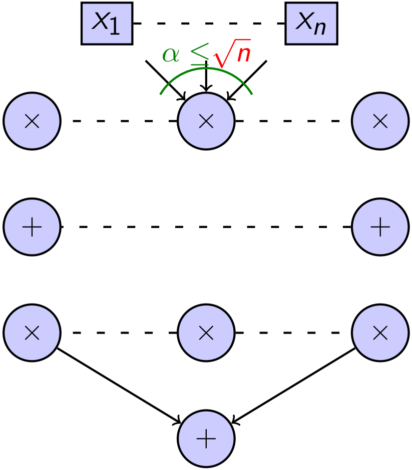
Lower bounds for Perm_n in depth 4

Homogeneous circuits:



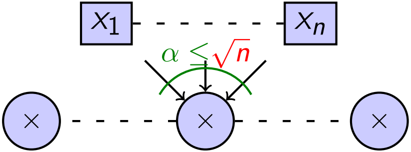
Lower bounds for Perm_n in depth 4

Homogeneous circuits:



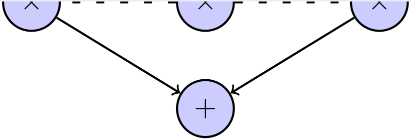
Lower bounds for Perm_n in depth 4

Homogeneous circuits:



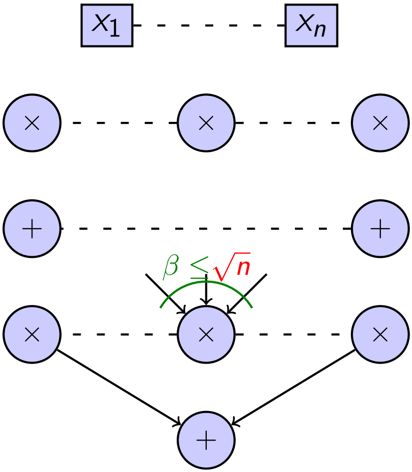
Theorem (Gupta,Kamath,Kayal,Saptharishi (2013))

If C is an homogeneous depth-4 circuit with $\alpha \leq O(\sqrt{n})$ which computes Perm_n*,*
then, $size(C) \geq 2^{\Omega(\sqrt{n})}$.



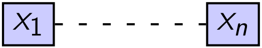
Lower bounds for Perm_n in depth 4

Homogeneous circuits:



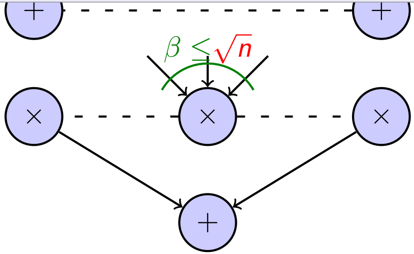
Lower bounds for Perm_n in depth 4

Homogeneous circuits:



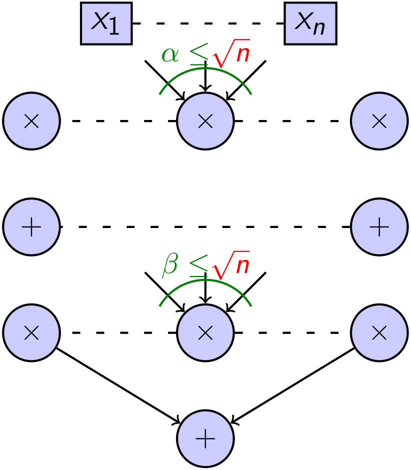
Proposition (Monomials counting)

If C is an homogeneous depth-4 circuit with $\beta \leq O(\sqrt{n})$ which computes Perm_n,
then, $size(C) \geq 2^{\Omega(\sqrt{n}\log n)}$.



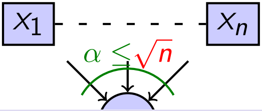
Lower bounds for Det_n in depth 4

Homogeneous circuits:



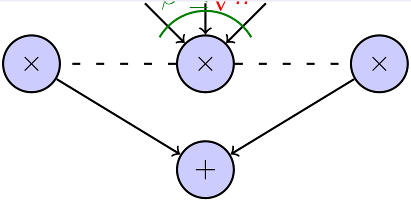
Lower bounds for Det_n in depth 4

Homogeneous circuits:



Corollary

If C is a minimal homogeneous depth-4 circuit with α and $\beta \leq O(\sqrt{n})$ computing Det_n,
then, $size(C) = 2^{\Theta(\sqrt{n}\log n)}$.



Generalization to constant depth

Theorem (T.)

If f_n has polynomial-size homogeneous circuits,
then f_n has depth $2p$ homogeneous circuits of size $2^{O(d^{1/p} \log n)}$.

Generalization to constant depth

Theorem (T.)

If f_n has polynomial-size homogeneous circuits,
then f_n has depth $2p$ homogeneous circuits of size $2^{O(d^{1/p} \log n)}$.

Application (Adaptation of Gupta, Kamath, Kayal and Saptharishi's proof):

Generalization to constant depth

Theorem (T.)

If f_n has polynomial-size homogeneous circuits, then f_n has depth $2p$ homogeneous circuits of size $2^{O(d^{1/p}\log n)}$.

Application (Adaptation of Gupta, Kamath, Kayal and Saptharishi's proof):

Proposition (T.)

If f_n has polynomial-size homogeneous circuits, then f_n has depth-4 non-homogeneous circuits of size $2^{O(\sqrt[3]{d}\log n)}$.

Outline

τ-conjecture

Conjecture (τ-conjecture, Shub-Smale (1995))

There exists an universal constant c such that if $P(X)$ is an **univariate** *polynomial computed by a circuit of size s, then the number of integer roots of P is bounded by s^c.*

τ-conjecture

Conjecture (τ-conjecture, Shub-Smale (1995))

There exists an universal constant c such that if $P(X)$ is an **univariate** *polynomial computed by a circuit of size s, then the number of integer roots of P is bounded by s^c.*

Theorem (Bürgisser (2007), almost...)

If the τ-conjecture is true, then $\mathsf{VP} \neq \mathsf{VNP}$*.*

τ-conjecture

Conjecture (τ-conjecture, Shub-Smale (1995))

There exists an universal constant c such that if $P(X)$ is an **univariate** *polynomial computed by a circuit of size s, then the number of integer roots of P is bounded by s^c.*

Theorem (Bürgisser (2007))

If the τ-conjecture is true, then $\mathsf{VP}^0 \neq \mathsf{VNP}^0$.

- VP^0, VNP^0 classes using only the constant -1.

Bürgisser's proof

Let us assume $\mathsf{VP}^0 = \mathsf{VNP}^0$.

Bürgisser's proof

Let us assume $\mathsf{VP}^0 = \mathsf{VNP}^0$.

- $\mathsf{PW}_n(X) = \prod_{i=0}^{2^n-1}(X - i)$

Bürgisser's proof

Let us assume $\mathsf{VP}^0 = \mathsf{VNP}^0$.

- $\mathrm{PW}_n(X) = \prod_{i=0}^{2^n-1}(X - i)$
- $\mathrm{PW}_n(X) = F_n\left(X, X^2, X^{2^2}, \ldots, X^{2^{n-1}}\right)$

Bürgisser's proof

Let us assume $\mathsf{VP}^0 = \mathsf{VNP}^0$.

- $\mathsf{PW}_n(X) = \prod_{i=0}^{2^n-1}(X - i)$
- $\mathsf{PW}_n(X) = F_n\left(X, X^2, X^{2^2}, \ldots, X^{2^{n-1}}\right)$
- $F_n(X_1, \ldots, X_n) = \sum_{\boldsymbol{\alpha}} a(n, \boldsymbol{\alpha})\mathbf{X}^{\boldsymbol{\alpha}}$

Bürgisser's proof

Let us assume $\mathsf{VP}^0 = \mathsf{VNP}^0$.

- $\mathsf{PW}_n(X) = \prod_{i=0}^{2^n-1}(X - i)$
- $\mathsf{PW}_n(X) = F_n\left(X, X^2, X^{2^2}, \ldots, X^{2^{n-1}}\right)$
- $F_n(X_1, \ldots, X_n) = \sum_{\boldsymbol{\alpha}} a(n, \boldsymbol{\alpha})\mathbf{X}^{\boldsymbol{\alpha}}$
- If $a(n, \boldsymbol{\alpha})$ is not too difficult to compute
  (digits computable in the counting hierarchy)
  $\Rightarrow F_n(X_1, \ldots, X_n)$ is computed by a circuit of size n^c.

Bürgisser's proof

Let us assume $\mathsf{VP}^0 = \mathsf{VNP}^0$.

- $\mathrm{PW}_n(X) = \prod_{i=0}^{2^n-1}(X - i)$
- $\mathrm{PW}_n(X) = F_n\left(X, X^2, X^{2^2}, \dots, X^{2^{n-1}}\right)$
- $F_n(X_1, \dots, X_n) = \sum_{\alpha} a(n, \alpha)\mathbf{X}^{\alpha}$
- If $a(n, \alpha)$ is not too difficult to compute
  (digits computable in the counting hierarchy)
  $\Rightarrow F_n(X_1, \dots, X_n)$ is computed by a circuit of size n^c.
- $\mathrm{PW}_n(X)$ computed by a circuit of size $n^c + n$.

Bürgisser's proof

Let us assume $\mathsf{VP}^0 = \mathsf{VNP}^0$.

- $\mathrm{PW}_n(X) = \prod_{i=0}^{2^n-1}(X-i)$
- $\mathrm{PW}_n(X) = F_n\left(X, X^2, X^{2^2}, \ldots, X^{2^{n-1}}\right)$
- $F_n(X_1, \ldots, X_n) = \sum_{\boldsymbol{\alpha}} a(n, \boldsymbol{\alpha})\mathbf{X}^{\boldsymbol{\alpha}}$
- If $a(n, \boldsymbol{\alpha})$ is not too difficult to compute (digits computable in the counting hierarchy) $\Rightarrow F_n(X_1, \ldots, X_n)$ is computed by a circuit of size n^c.
- $\mathrm{PW}_n(X)$ computed by a circuit of size $n^c + n$.
- By τ-conjecture, its number of integer roots is polynomial in n.

Bürgisser's proof

Let us assume $\mathsf{VP}^0 = \mathsf{VNP}^0$.

- $\mathrm{PW}_n(X) = \prod_{i=0}^{2^n-1}(X-i)$
- $\mathrm{PW}_n(X) = F_n\left(X, X^2, X^{2^2}, \ldots, X^{2^{n-1}}\right)$
- $F_n(X_1, \ldots, X_n) = \sum_{\alpha} a(n, \alpha)\mathbf{X}^{\alpha}$
- If $a(n, \alpha)$ is not too difficult to compute (digits computable in the counting hierarchy) $\Rightarrow F_n(X_1, \ldots, X_n)$ is computed by a circuit of size n^c.
- $\mathrm{PW}_n(X)$ computed by a circuit of size $n^c + n$.
- By τ-conjecture, its number of integer roots is polynomial in n.
- Contradiction.

Adaptation for depth-4 (Koiran)

Let us assume $\mathsf{VP}^0 = \mathsf{VNP}^0$.

- $\mathrm{PW}_n(X) = \prod_{i=0}^{2^n-1}(X - i)$
- $\mathrm{PW}_n(X) = F_n\left(X, X^2, X^{2^2}, \ldots, X^{2^{n-1}}\right)$
- $F_n(X_1, \ldots, X_n) = \sum_{\alpha} a(n, \alpha)\mathbf{X}^{\alpha}$
- If $a(n, \alpha)$ is not too difficult to compute
  (digits computable in the counting hierarchy)
  $\Rightarrow F_n(X_1, \ldots, X_n)$ is computed by a circuit of size n^c.
- $\mathrm{PW}_n(X)$ computed by a circuit of size $n^c + n$.
- By τ-conjecture, its number of integer roots is polynomial in n.
- Contradiction.

Adaptation for depth-4 (Koiran)

Let us assume $\mathsf{VP}^0 = \mathsf{VNP}^0$.

- $\mathrm{PW}_n(X) = \prod_{i=0}^{2^n-1}(X - i)$
- $\mathrm{PW}_n(X) = F_n\left(X, X^2, X^{2^2}, \ldots, X^{2^{n-1}}\right)$
- $F_n(X_1, \ldots, X_n) = \sum_{\alpha} a(n, \alpha)\mathbf{X}^{\alpha}$
- If $a(n, \alpha)$ is not too difficult to compute (digits computable in the counting hierarchy) $\Rightarrow F_n(X_1, \ldots, X_n)$ is computed by a circuit of size n^c.

Adaptation for depth-4 (Koiran)

Let us assume $\mathsf{VP}^0 = \mathsf{VNP}^0$.

- $\mathrm{PW}_n(X) = \prod_{i=0}^{2^n-1}(X-i)$
- $\mathrm{PW}_n(X) = F_n\left(X, X^2, X^{2^2}, \ldots, X^{2^{n-1}}\right)$
- $F_n(X_1, \ldots, X_n) = \sum_{\alpha} a(n,\alpha)\mathbf{X}^{\alpha}$
- If $a(n,\alpha)$ is not too difficult to compute (digits computable in the counting hierarchy) $\Rightarrow F_n(X_1, \ldots, X_n)$ is computed by a circuit of size n^c.

$\Rightarrow F_n(X_1, \ldots, X_n) = \sum_{k=1}^{n\sqrt{n}} \prod_{m=1}^{\sqrt{n}} \sum_{t=1}^{n\sqrt{n}} \prod_{v=1}^{\sqrt{n}} c_{k,m,t,v} X_{k,m,t,v}$

Adaptation for depth-4 (Koiran)

Let us assume $\mathsf{VP}^0 = \mathsf{VNP}^0$.

- $\mathrm{PW}_n(X) = \prod_{i=0}^{2^n-1}(X - i)$
- $\mathrm{PW}_n(X) = F_n\left(X, X^2, X^{2^2}, \ldots, X^{2^{n-1}}\right)$
- $F_n(X_1, \ldots, X_n) = \sum_{\alpha} a(n, \alpha)\mathbf{X}^{\alpha}$
- If $a(n, \alpha)$ is not too difficult to compute
  (digits computable in the counting hierarchy)
  $\Rightarrow F_n(X_1, \ldots, X_n)$ is computed by a circuit of size n^c.

$\Rightarrow F_n(X_1, \ldots, X_n) = \sum_{k=1}^{n\sqrt{n}} \prod_{m=1}^{\sqrt{n}} \sum_{t=1}^{n\sqrt{n}} \prod_{v=1}^{\sqrt{n}} c_{k,m,t,v} X_{k,m,t,v}$

$\mathrm{PW}_n(X) = \sum_{k=1}^{n\sqrt{n}} \prod_{m=1}^{\sqrt{n}} \sum_{t=1}^{n\sqrt{n}} c_{k,m,t} X^{\gamma_{k,m,t}}$.

Koiran's version (2013)

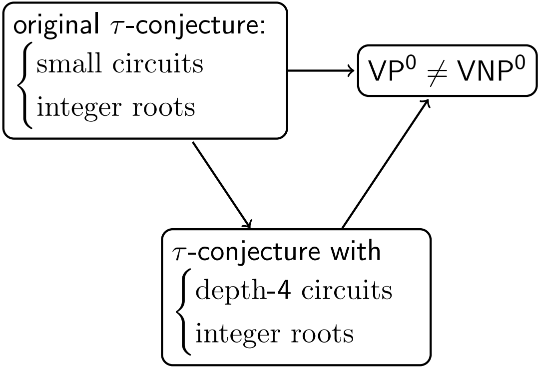
Conjecture

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

Koiran's version (2013)

Conjecture

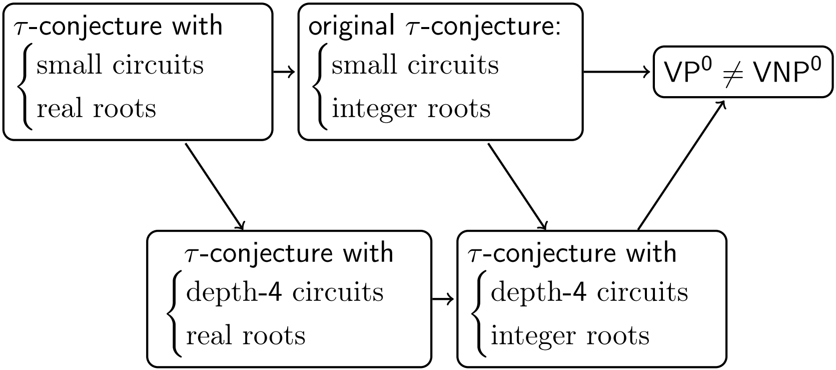
There exists c such that the univariate polynomial $\sum_{i=1}^{k} \prod_{j=1}^{m} f_{i,j}$ *(with* $f_{i,j}$ *t-sparse) has at most* $(m+k+t)^c$ *integer roots.*



Koiran's version (2013)

Conjecture (Real τ-conjecture (2013))

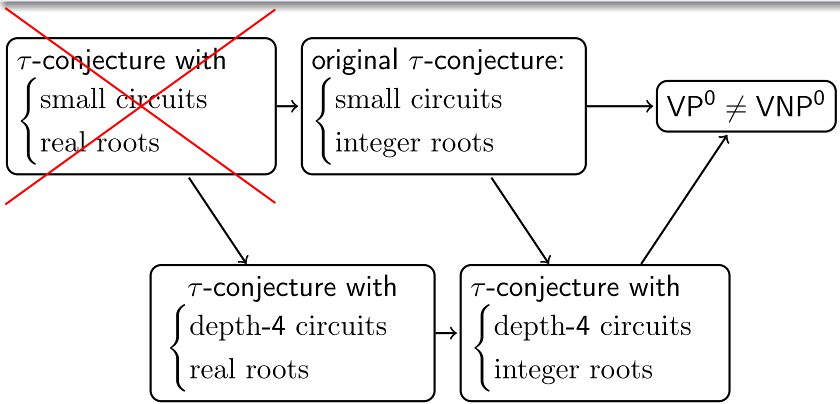
There exists c such that the univariate polynomial $\sum_{i=1}^{k}\prod_{j=1}^{m} f_{i,j}$ (with $f_{i,j}$ t-sparse) has at most $(m+k+t)^c$ **real** *roots.*



Koiran's version (2013)

Conjecture (Real τ-conjecture (2013))

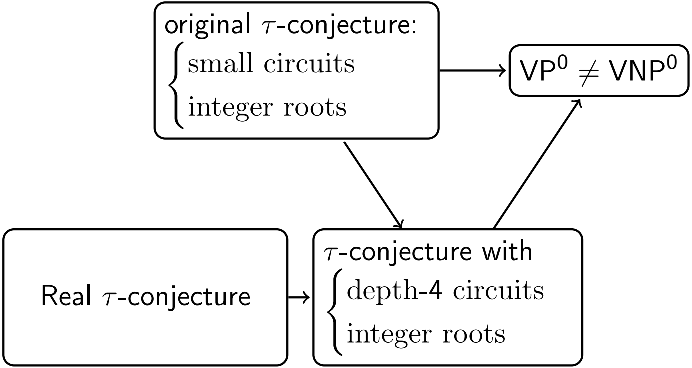
There exists c such that the univariate polynomial $\sum_{i=1}^{k} \prod_{j=1}^{m} f_{i,j}$ (with $f_{i,j}$ t-sparse) has at most $(m + k + t)^c$ **real** *roots.*



Koiran's version (2013)

Conjecture (Real τ-conjecture (2013))

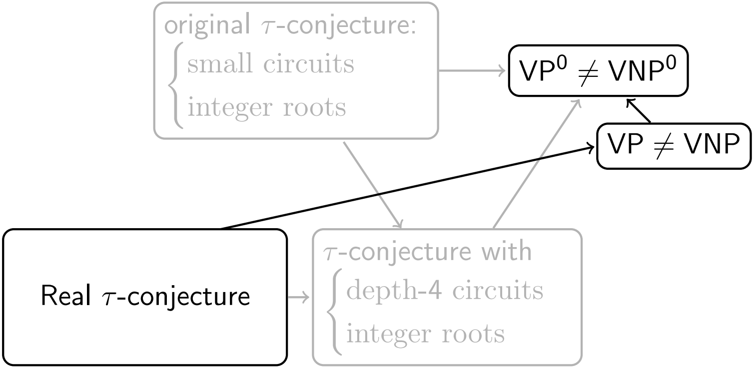
There exists c such that the univariate polynomial $\sum_{i=1}^{k} \prod_{j=1}^{m} f_{i,j}$ (with $f_{i,j}$ t-sparse) has at most $(m+k+t)^c$ **real** *roots.*



Koiran's version (2013)

Conjecture (Real τ-conjecture (2013))

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



Outline

Descartes' rule

Fundamental theorem of algebra

A complex polynomial P of degree d has exactly d roots counted with multiplicity.

Descartes' rule

Fundamental theorem of algebra

A complex polynomial P of degree d has exactly d roots counted with multiplicity.

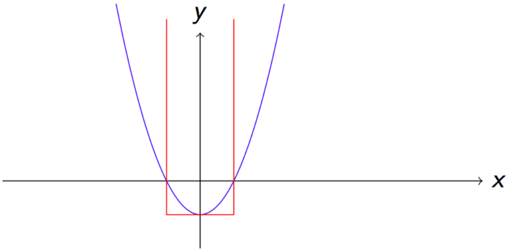
- In the real world?

Descartes' rule

Fundamental theorem of algebra

A complex polynomial P of degree d has exactly d roots counted with multiplicity.

- In the real world?
- $f(x) = x^2 - 1$ and $g(x) = x^{200} - 1$?



Descartes' rule

Fundamental theorem of algebra

A complex polynomial P of degree d has exactly d roots counted with multiplicity.

- In the real world?
- $f(x) = x^2 - 1$ and $g(x) = x^{200} - 1$?

Descartes' estimate

If P is a real t-sparse polynomial, then P has at most $t - 1$ positive roots (counted with multiplicity).
So, at most $2t - 1$ distinct roots on $\mathbb{R}$.

In fact Descartes' rule is more precise.

Bézout's Theorem

Bézout's Theorem

The following $n \times n$ system

$$\begin{cases} f_1(x_1, \dots, x_n) = 0 \\ \dots \\ f_n(x_1, \dots, x_n) = 0 \end{cases}$$

has at most $d_1 d_2 \dots d_n$ nondegenerate complex solutions.

Bézout's Theorem

Bézout's Theorem

The following $n \times n$ system

$$\begin{cases} f_1(x_1, \dots, x_n) = 0 \\ \dots \\ f_n(x_1, \dots, x_n) = 0 \end{cases}$$

has at most $d_1 d_2 \dots d_n$ nondegenerate complex solutions.

- Similar result for sparse polynomials and real solutions?

Bézout's Theorem

Bézout's Theorem

The following $n \times n$ system

$$\begin{cases} f_1(x_1, \ldots, x_n) = 0 \\ \ldots \\ f_n(x_1, \ldots, x_n) = 0 \end{cases}$$

has at most $d_1 d_2 \ldots d_n$ nondegenerate complex solutions.

- Similar result for sparse polynomials and real solutions?
- Kushnirenko's question (1977): bounded by a function $N(t_1, \ldots, t_n)$? What is the optimal bound?

An initial case

Sevostyanov's problem (1977)

Let f and g be two real bivariate polynomials.
f is of degree d and g is t-sparse.
Is the number of distinct isolated real solutions of the system

$$\begin{cases} f(x, y) = 0 \\ g(x, y) = 0 \end{cases}$$

bounded by a function $N(d, t)$? If so, what is this function?

An initial case

Sevostyanov's problem (1977)

Let f and g be two real bivariate polynomials.
f is of degree d and g is t-sparse.
Is the number of distinct isolated real solutions of the system

$$\begin{cases} f(x,y) = 0 \\ g(x,y) = 0 \end{cases}$$

bounded by a function $N(d,t)$? If so, what is this function?

According to Kushnirenko, Sevostyanov proved the existence of $N(d,t)$ in 1978.

Fewnomial bounds

Theorem (Khovanskiĭ (1983))

System of n equations and n variables
with ony $n + l + 1$ distinct monomials.
Then, number of positive real solutions bounded by

$$2^{\binom{l+n}{2}}(n+1)^{l+n}$$

Fewnomial bounds

Theorem (Khovanskiĭ (1983))

System of n equations and n variables
with ony $n + l + 1$ distinct monomials.
Then, number of positive real solutions bounded by

$$2^{\binom{l+n}{2}}(n+1)^{l+n}$$

In particular,

- Kushnirenko's question: $N(t_1, \ldots, t_n) \leq 2^{\binom{t_1+\ldots+t_n}{2}}(n+1)^{t_1+\ldots+t_n}$

Improvement

Khovanskiĭ's Theorem was improved by Bihan and Sottile.

Theorem (Bihan, Sottile (2007))

System of n equations and n variables
with only $n + l + 1$ distinct monomials.
Then, number of positive real solutions bounded by

$$\frac{e^2 + 3}{4} 2^{\binom{l}{2}} n^l.$$

Intersection of a trinomial curve with a sparse curve

Theorem (Li, Rojas, Wang (2003))

$f(x, y)$ is a trinomial and $g(x, y)$ is t-sparse.
Then the system $f(x, y) = g(x, y) = 0$ has at most $2^t - 2$ real solutions.

Intersection of a trinomial curve with a sparse curve

Theorem (Li, Rojas, Wang (2003))

$f(x, y)$ is a trinomial and $g(x, y)$ is t-sparse.
Then the system $f(x, y) = g(x, y) = 0$ has at most $2^t - 2$ real solutions.

Theorem (Li, Rojas, Wang (2003))

$f_1, \ldots, f_{n-1}$ are trinomials. f_n is t-sparse.
Then the system $f_1 = \ldots = f_n = 0$ has at most $n + n^2 + \ldots + n^{t-1}$ positive real roots.

Intersection of a trinomial curve with a sparse curve

Theorem (Li, Rojas, Wang (2003))

$f(x, y)$ is a trinomial and $g(x, y)$ is t-sparse.
Then the system $f(x, y) = g(x, y) = 0$ has at most $2^t - 2$ real solutions.

Theorem (Li, Rojas, Wang (2003))

$f_1, \ldots, f_{n-1}$ are trinomials. f_n is t-sparse.
Then the system $f_1 = \ldots = f_n = 0$ has at most $n + n^2 + \ldots + n^{t-1}$ positive real roots.

Theorem (Koiran, Portier, T. *MEGA* 2013)

$f(x, y)$ is a trinomial and $g(x, y)$ is t-sparse.
Then the system $f(x, y) = g(x, y) = 0$ has at most $\frac{2}{3}t^3 + 5t$ positive real solutions.

Sevostyanov's problem

Theorem (Koiran, Portier, T. *Discrete & Computational Geometry*, to appear)

*$f(x, y)$ non-zero polynomial of degree d and $g(x, y)$ t-sparse.
Then the system $f(x, y) = g(x, y) = 0$ has at most $O(d^3 t + d^2 t^3)$ real solutions.*

Sevostyanov's problem

Theorem (Koiran, Portier, T. *Discrete & Computational Geometry*, to appear)

$f(x,y)$ non-zero polynomial of degree d and $g(x,y)$ t-sparse.
Then the system $f(x,y) = g(x,y) = 0$ has at most $O(d^3 t + d^2 t^3)$ real solutions.

The best previous bound was $d(2+d)^{t+1} 2^{\binom{t+1}{2}}$.

Sevostyanov's problem

Theorem (Koiran, Portier, T. *Discrete & Computational Geometry*, to appear)

$f(x, y)$ non-zero polynomial of degree d and $g(x, y)$ t-sparse.
Then the system $f(x, y) = g(x, y) = 0$ has at most $O(d^3 t + d^2 t^3)$ real solutions.

The best previous bound was $d(2 + d)^{t+1} 2^{\binom{t+1}{2}}$.
The constraint $f \neq 0$ is important.

Stronger hypothesis

Theorem

*$f(x, y)$ non-zero polynomial of degree d and $g(x, y)$ t-sparse.
Then the system $f(x, y) = g(x, y) = 0$ has at most $O(d^3 t + d^2 t^3)$ real solutions.*

Stronger hypothesis

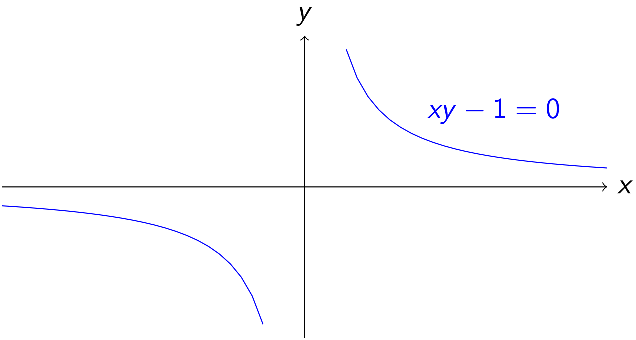
Theorem

$f(x,y)$ non-zero polynomial of degree d and $g(x,y)$ t-sparse.
Then the system $f(x,y) = g(x,y) = 0$ has at most $O(d^3t + d^2t^3)$ real connected components.

Stronger hypothesis

Theorem

$f(x, y)$ non-zero polynomial of degree d and $g(x, y)$ t-sparse.
Then the system $f(x, y) = g(x, y) = 0$ has at most $O(d^3 t + d^2 t^3)$ real connected components.



Stronger hypothesis

Theorem

$f(x,y)$ non-zero polynomial of degree d and $g(x,y)$ t-sparse.
Then the system $f(x,y) = g(x,y) = 0$ has at most $O(d^3t + d^2t^3)$ real connected components.

Lemma

$f(x,y)$ non-zero polynomial of degree d and $g(x,y)$ t-sparse.
Assume that:

- *f irreducible in $\mathbb{C}[X,Y]$*
- *and finite number of solutions.*

Then the system $f(x,y) = g(x,y) = 0$ has at most $O(d^3t + d^2t^3)$ distinct real solutions.

From the lemma to the theorem

Hypothesis

- finite number of solutions
- and f irreducible in $\mathbb{C}[X, Y]$.

From the lemma to the theorem

Hypothesis

- finite number of solutions
- and f irreducible in $\mathbb{C}[X, Y]$.

1. If the number of solutions is infinite then f divides g.
   $\Rightarrow 2d(d-1)$ connected components.

From the lemma to the theorem

Hypothesis

- finite number of solutions
- and f irreducible in $\mathbb{C}[X, Y]$.

1. If the number of solutions is infinite then f divides g.
   $\Rightarrow 2d(d-1)$ connected components.
2. Irreducibility of f.

From the lemma to the theorem

Hypothesis

- finite number of solutions
- and f irreducible in $\mathbb{C}[X, Y]$.

1. If the number of solutions is infinite then f divides g.
   $\Rightarrow 2d(d-1)$ connected components.
2. Irreducibility of f.
   - $f = f_1 f_2 \dots f_k$

$$\bigcup_i \text{solutions of } \begin{cases} f_i = 0 \\ g = 0 \end{cases}$$

Outline of the proof

Lemma

$f(x, y)$ irreducible polynomial of degree d and $g(x, y)$ t-sparse. Then if the system $f(x, y) = g(x, y) = 0$ has a finite number of real solutions, it is at most $O(d^3 t + d^2 t^3)$ solutions.

Outline of the proof

Lemma

$f(x, y)$ irreducible polynomial of degree d and $g(x, y)$ t-sparse. Then if the system $f(x, y) = g(x, y) = 0$ has a finite number of real solutions, it is at most $O(d^3 t + d^2 t^3)$ solutions.

1. Rewrite $f(x, y) = 0$ as $y = h(x)$ (h nice).
   To bound the number of roots of $g(x, (h(x))) = \sum^k a_i x^{\alpha_i} h(x)^{\beta_i}$.

Outline of the proof

Lemma

$f(x,y)$ irreducible polynomial of degree d and $g(x,y)$ t-sparse. Then if the system $f(x,y) = g(x,y) = 0$ has a finite number of real solutions, it is at most $O(d^3t + d^2t^3)$ solutions.

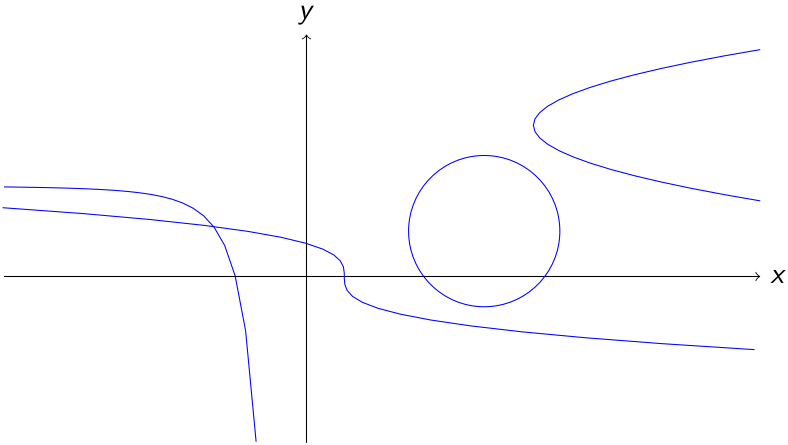
1. Rewrite $f(x,y) = 0$ as $y = h(x)$ (h nice).
   To bound the number of roots of $g(x,(h(x))) = \sum^k a_i x^{\alpha_i} h(x)^{\beta_i}$.
2. To bound the number of roots of a sum.

Cylindrical algebraic decomposition

- Solutions of $f(x, y) = 0$.

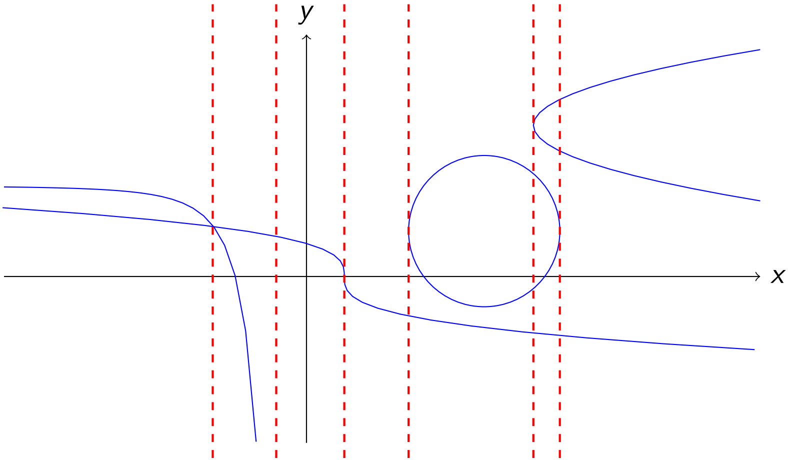
Cylindrical algebraic decomposition

- Solutions of $f(x, y) = 0$.



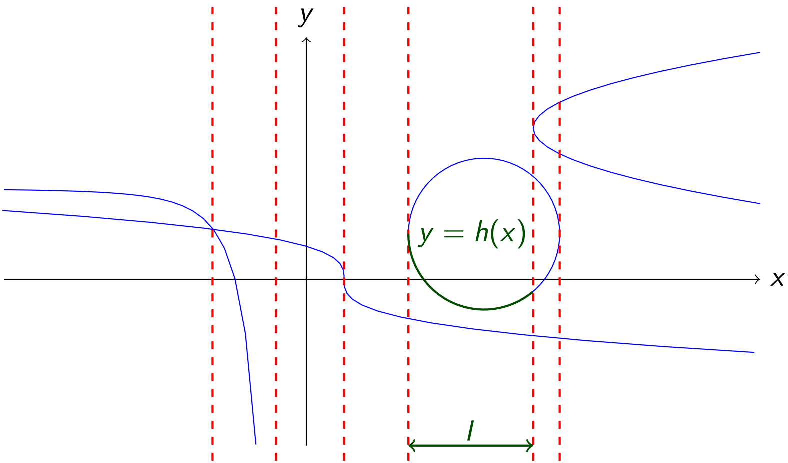
Cylindrical algebraic decomposition

- Solutions of $f(x, y) = 0$.



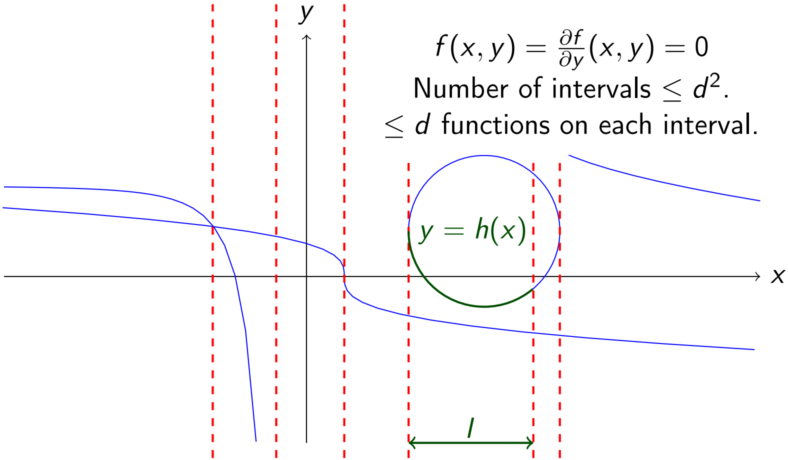
Cylindrical algebraic decomposition

- Solutions of $f(x, y) = 0$.



Cylindrical algebraic decomposition

- Solutions of $f(x, y) = 0$.



To bound the number of roots of a sum

To bound the number of roots of

$$g(x, h(x)) = \sum_{i=1}^{t} a_i x^{\alpha_i} h(x)^{\beta_i}.$$

To bound the number of roots of a sum

To bound the number of roots of

$$g(x, h(x)) = \sum_{i=1}^{t} a_i x^{\alpha_i} h(x)^{\beta_i}.$$

We will use the Wronskian.

The key of the proof: the Wronskian

- Pólya, Szegö (1925) used it for proving Descartes' rule.

The key of the proof: the Wronskian

- Pólya, Szegö (1925) used it for proving Descartes' rule.
- Some connections with the number of roots of a sum already known by Voorhoeve and van der Poorten (1975).

The key of the proof: the Wronskian

- Pólya, Szegö (1925) used it for proving Descartes' rule.
- Some connections with the number of roots of a sum already known by Voorhoeve and van der Poorten (1975).

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

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

The key of the proof: the Wronskian

- Pólya, Szegö (1925) used it for proving Descartes' rule.
- Some connections with the number of roots of a sum already known by Voorhoeve and van der Poorten (1975).

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

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

- Idea: upper bound the number of roots of a sum by the number of roots of some particular Wronskians.

From sum to Wronskians

Lemma

Let I be a real interval.
If $W(f_1), W(f_1, f_2), \ldots, W(f_1, f_2, \ldots, f_k)$ have no zero on I, then $Z_I(f_1 + \ldots + f_k) \leq k - 1$.

From sum to Wronskians

Lemma

Let I be a real interval.
If $W(f_1), W(f_1, f_2), \ldots, W(f_1, f_2, \ldots, f_k)$ have no zero on I, then $Z_I(f_1 + \ldots + f_k) \leq k - 1$.

- $f_1 + f_2 =$

From sum to Wronskians

Lemma

Let I be a real interval.
If $W(f_1), W(f_1, f_2), \ldots, W(f_1, f_2, \ldots, f_k)$ have no zero on I, then $Z_I(f_1 + \ldots + f_k) \leq k - 1$.

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

From sum to Wronskians

Lemma

Let I be a real interval.
If $W(f_1), W(f_1, f_2), \ldots, W(f_1, f_2, \ldots, f_k)$ have no zero on I, then $Z_I(f_1 + \ldots + f_k) \leq k - 1$.

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

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

From sum to Wronskians

Lemma

Let I be a real interval.
If $W(f_1), W(f_1, f_2), \ldots, W(f_1, f_2, \ldots, f_k)$ have no zero on I, then $Z_I(f_1 + \ldots + f_k) \leq k - 1$.

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

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

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

From sum to Wronskians

Lemma

Let I be a real interval.
If $W(f_1), W(f_1, f_2), \ldots, W(f_1, f_2, \ldots, f_k)$ have no zero on I, then $Z_I(f_1 + \ldots + f_k) \leq k - 1$.

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

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

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

$$W\left(\left(\frac{f_2}{f_1}\right)', \ldots, \left(\frac{f_q}{f_1}\right)'\right) = \left(\frac{1}{f_1}\right)^p W(f_1, \ldots, f_q).$$

From sum to Wronskians

Theorem (Koiran, Portier, T. *MFCS 2013*)

$$Z(f_1 + \ldots + f_k) \leq k - 1 + 2\sum_{j=1}^{k-2} Z(W(f_1, \ldots, f_j))$$

What remains to be done

Theorem

$f(x, y)$ polynomial of degree d and $g(x, y)$ t-sparse.
Then the system $f(x, y) = g(x, y) = 0$ has at most $O(d^3 t + d^2 t^3)$ real solutions.

What remains to be done

Theorem

*$f(x, y)$ polynomial of degree d and $g(x, y)$ t-sparse.
Then the system $f(x, y) = g(x, y) = 0$ has at most $O(d^3 t + d^2 t^3)$ real solutions.*

1. We have rewritten $f(x, y) = 0$ as $y = h(x)$ (h nice).
   We have bounded the number of roots of
   $g(x, h(x)) = \sum^t a_i x^{\alpha_i} h(x)^{\beta_i}$.

What remains to be done

Theorem

$f(x,y)$ polynomial of degree d and $g(x,y)$ t-sparse.
Then the system $f(x,y) = g(x,y) = 0$ has at most $O(d^3t + d^2t^3)$ real solutions.

1. We have rewritten $f(x,y) = 0$ as $y = h(x)$ (h nice).
   We have bounded the number of roots of
   $g(x, h(x)) = \sum^t a_i x^{\alpha_i} h(x)^{\beta_i}$.
2. To bound the number of roots of
   $W_s = W(a_1 x^{\alpha_1} h^{\beta_1}(x), \dots, a_s x^{\alpha_s} h^{\beta_s}(x))$.

Bounds for W_3

$$\det \begin{bmatrix} x^{\alpha_1} h^{\beta_1} & x^{\alpha_2} h^{\beta_2} & x^{\alpha_3} h^{\beta_3} \\ \left(x^{\alpha_1} h^{\beta_1}\right)' & \left(x^{\alpha_2} h^{\beta_2}\right)' & \left(x^{\alpha_3} h^{\beta_3}\right)' \\ \left(x^{\alpha_1} h^{\beta_1}\right)'' & \left(x^{\alpha_2} h^{\beta_2}\right)'' & \left(x^{\alpha_3} h^{\beta_3}\right)'' \end{bmatrix}$$

Bounds for W_3

$$\det \begin{bmatrix} x^{\alpha_1} h^{\beta_1} & x^{\alpha_2} h^{\beta_2} & x^{\alpha_3} h^{\beta_3} \\ \left(x^{\alpha_1} h^{\beta_1}\right)' & \left(x^{\alpha_2} h^{\beta_2}\right)' & \left(x^{\alpha_3} h^{\beta_3}\right)' \\ \left(x^{\alpha_1} h^{\beta_1}\right)'' & \left(x^{\alpha_2} h^{\beta_2}\right)'' & \left(x^{\alpha_3} h^{\beta_3}\right)'' \end{bmatrix}$$

$$\det \begin{bmatrix} x^{\alpha_1} h^{\beta_1} & x^{\alpha_2} h^{\beta_2} & x^{\alpha_3} h^{\beta_3} \\ \left(x^{\alpha_1 - 1} h^{\beta_1 - 1}\right)\left(\alpha_1 h + \beta_1 x h'\right) & \dots & \dots \\ \left(x^{\alpha_1 - 2} h^{\beta_1 - 2}\right)\left(P_2(x, h, h', h'')\right) & \dots & \dots \end{bmatrix}$$

Bounds for W_3

$$\det \begin{bmatrix} x^{\alpha_1} h^{\beta_1} & x^{\alpha_2} h^{\beta_2} & x^{\alpha_3} h^{\beta_3} \\ \left(x^{\alpha_1} h^{\beta_1}\right)' & \left(x^{\alpha_2} h^{\beta_2}\right)' & \left(x^{\alpha_3} h^{\beta_3}\right)' \\ \left(x^{\alpha_1} h^{\beta_1}\right)'' & \left(x^{\alpha_2} h^{\beta_2}\right)'' & \left(x^{\alpha_3} h^{\beta_3}\right)'' \end{bmatrix}$$

$$\det \begin{bmatrix} x^{\alpha_1} h^{\beta_1} & x^{\alpha_2} h^{\beta_2} & x^{\alpha_3} h^{\beta_3} \\ \left(x^{\alpha_1 - 1} h^{\beta_1 - 1}\right)(\alpha_1 h + \beta_1 x h') & \dots & \dots \\ \left(x^{\alpha_1 - 2} h^{\beta_1 - 2}\right)(P_2(x, h, h', h'')) & \dots & \dots \end{bmatrix}$$

$$x^{\alpha_1+\alpha_2+\alpha_3-6} h^{\beta_1+\beta_2+\beta_3-6} \det \begin{bmatrix} x^2 h^2 & x^2 h^2 & x^2 h^2 \\ xh(\alpha_1 h + \beta_1 x h') & \dots & \dots \\ P_2(x, h, h', h'') & \dots & \dots \end{bmatrix}$$

Consequently

Theorem

$f(x, y)$ non-zero polynomial of degree d and $g(x, y)$ t-sparse.
Then the system $f(x, y) = g(x, y) = 0$ has at most $O(d^3 t + d^2 t^3)$ real connected components.

Consequently

Theorem

$f(x, y)$ non-zero polynomial of degree d and $g(x, y)$ t-sparse.
Then the system $f(x, y) = g(x, y) = 0$ has at most $O(d^3 t + d^2 t^3)$ real connected components.

Case of the real τ-conjecture? $\sum^k \prod^m f_{i,j}(x)$?

Consequently

Theorem

$f(x,y)$ non-zero polynomial of degree d and $g(x,y)$ t-sparse.
Then the system $f(x,y) = g(x,y) = 0$ has at most $O(d^3t + d^2t^3)$ real connected components.

Case of the real τ-conjecture? $\sum^k \prod^m f_{i,j}(x)$?
If the number of distinct $f_{i,j}$ is very small (constant?)?

Consequently

Theorem

$f(x, y)$ non-zero polynomial of degree d and $g(x, y)$ t-sparse.
Then the system $f(x, y) = g(x, y) = 0$ has at most $O(d^3 t + d^2 t^3)$ real connected components.

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

Consequently

Theorem

$f(x,y)$ non-zero polynomial of degree d and $g(x,y)$ t-sparse. Then the system $f(x,y) = g(x,y) = 0$ has at most $O(d^3t + d^2t^3)$ real connected components.

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

- Bound given by Grenet,Koiran,Portier and Strozecki: $t^{O(m2^k)}$
- Bound given by Khovanskiĭ: $2^{O((k+t)^2m^2)}$

Consequently

Theorem

*$f(x, y)$ non-zero polynomial of degree d and $g(x, y)$ t-sparse.
Then the system $f(x, y) = g(x, y) = 0$ has at most $O(d^3 t + d^2 t^3)$ real connected components.*

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

- Bound given by Grenet,Koiran,Portier and Strozecki: $t^{O(m2^k)}$
- Bound given by Khovanskiĭ: $2^{O((k+t)^2 m^2)}$

Theorem (Koiran, Portier, T.)

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

Perspectives

- Fournier, Limaye, Malod, Srinivasan 2013: If a circuit $\sum^{[s]}\prod^{[O(D)]}\sum\prod^{[\sqrt{d}]}$ computes $\mathsf{IMM}_{n,d}$, then $s \geq 2^{\Omega(\sqrt{d}\log(n/D))}$.
- Approach for VP $\neq$ VNP: shifted partial derivatives.

Perspectives

- Fournier, Limaye, Malod, Srinivasan 2013: If a circuit $\sum^{[s]}\prod^{[O(D)]}\sum\prod^{[\sqrt{d}]}$ computes $\mathsf{IMM}_{n,d}$, then $s \geq 2^{\Omega(\sqrt{d}\log(n/D))}$.
- Approach for VP $\neq$ VNP: shifted partial derivatives.
- Variants of the τ-conjecture:
  - Bounds on multiplicities (Hrubeš 2013)
  - Combinatorial version: Newton polygons.
    A non trivial upper bound (Koiran, Portier, T., Thomassé)

Perspectives

- Fournier, Limaye, Malod, Srinivasan 2013: If a circuit $\sum^{[s]}\prod^{[O(D)]}\sum\prod^{[\sqrt{d}]}$ computes $\mathrm{IMM}_{n,d}$, then $s \geq 2^{\Omega(\sqrt{d}\log(n/D))}$.
- Approach for VP $\neq$ VNP: shifted partial derivatives.
- Variants of the τ-conjecture:
  - Bounds on multiplicities (Hrubeš 2013)
  - Combinatorial version: Newton polygons.
    A non trivial upper bound (Koiran, Portier, T., Thomassé)
- Generalisations of Sevostyanov's problem
  - $f_1 = \ldots = f_n = g = 0$ (f_i dense, g sparse)
  - $f = g = 0$ (f and g sparse)

Thank you!

Publications

- Improved Bounds for Reduction to Depth 4 and Depth 3. *MFCS* 813-824, 2013. To appear in a Special Issue of *Information and Computation*.
- With P. Koiran, N. Portier: A Wronskian Approach to the real τ-conjecture. *MEGA*, 2013. To appear in a Special Issue of *Journal of Symbolic Computation*.
- With P. Koiran, N. Portier, S. Thomassé: A τ-conjecture for Newton polygons. To appear in the Special Issue of *Foundations of Computational Mathematics honoring Mike Shub's 70th birthday*.
- With P. Koiran, N. Portier: On the intersection of a sparse curve and a low-degree curve : A polynomial version of the lost theorem. To appear in *Discrete & Computational Geometry*.
- With E. Diot, N. Trotignon: Detecting wheels. *Applicable Analysis and Discrete Mathematics*, 8:111–122, 2014.