Lower bounds for sums of powers of low degree univariate polynomials

Pascal Koiran
Joint work with:
Neeraj Kayal, Timothée Pecatte and Chandan Saha

WACT 2015, Saarbrücken

Why univariate polynomials?

- Open problem 1.4 in survey by Chen, Kayal and Wigderson: Find explicit family (f_n) of univariate polynomials of degree n and lower bound on circuit size $> (\log n)^{O(1)}$.

Why univariate polynomials?

- Open problem 1.4 in survey by Chen, Kayal and Wigderson: Find explicit family (f_n) of univariate polynomials of degree n and lower bound on circuit size $> (\log n)^{O(1)}$.
- Our model: representations of the form

$$f(x) = \sum_{i=1}^{s} \alpha_i . Q_i(x)^{e_i},$$

where $\deg(Q_i) \leq t$. **Wanted:** lower bound on s.

Why univariate polynomials?

- Open problem 1.4 in survey by Chen, Kayal and Wigderson: Find explicit family (f_n) of univariate polynomials of degree n and lower bound on circuit size $> (\log n)^{O(1)}$.
- Our model: representations of the form

$$f(x) = \sum_{i=1}^{s} \alpha_i . Q_i(x)^{e_i},$$

where $\deg(Q_i) \leq t$. **Wanted:** lower bound on s.

- This toy model is easier to analyze but still challenging, even for $t = 2$ or (!) $t = 1$.

Why univariate polynomials?

- Open problem 1.4 in survey by Chen, Kayal and Wigderson: Find explicit family (f_n) of univariate polynomials of degree n and lower bound on circuit size $> (\log n)^{O(1)}$.
- Our model: representations of the form

$$f(x) = \sum_{i=1}^{s} \alpha_i . Q_i(x)^{e_i},$$

where $\deg(Q_i) \leq t$. **Wanted:** lower bound on s.

- This toy model is easier to analyze but still challenging, even for $t = 2$ or (!) $t = 1$.
- A variation is closely connected to VP $\neq$ VNP.

Bounding sparsity(Q_i) instead of degree(Q_i)

Consider the model:

$$f(x) = \sum_{i=1}^{s} \alpha_i . Q_i(x)^{e_i},$$

where Q_i has at most t monomials. Candidate hard polynomials:

- $\prod_{i=1}^{2^n}(X + i)$. Probably hard for general arithmetic circuits.

Bounding sparsity(Q_i) instead of degree(Q_i)

Consider the model:

$$f(x) = \sum_{i=1}^{s} \alpha_i . Q_i(x)^{e_i},$$

where Q_i has at most t monomials. Candidate hard polynomials:

- $\prod_{i=1}^{2^n}(X + i)$. Probably hard for general arithmetic circuits.
- $\sum_{i=0}^{2^n-1} 2^{2i(2^n-i-1)} X^i$. Satisfies Kurz condition.

Bounding sparsity(Q_i) instead of degree(Q_i)

Consider the model:

$$f(x) = \sum_{i=1}^{s} \alpha_i . Q_i(x)^{e_i},$$

where Q_i has at most t monomials. Candidate hard polynomials:

- $\prod_{i=1}^{2^n} (X+i)$. Probably hard for general arithmetic circuits.
- $\sum_{i=0}^{2^n-1} 2^{2i(2^n-i-1)} X^i$. Satisfies Kurz condition.
- $(X+1)^{2^n}$. Seems hard if e_i required to be small.

Bounding sparsity(Q_i) instead of degree(Q_i)

Consider the model:

$$f(x) = \sum_{i=1}^{s} \alpha_i . Q_i(x)^{e_i},$$

where Q_i has at most t monomials. Candidate hard polynomials:

- $\prod_{i=1}^{2^n}(X+i)$. Probably hard for general arithmetic circuits.
- $\sum_{i=0}^{2^n-1} 2^{2i(2^n-i-1)}X^i$. Satisfies Kurz condition.
- $(X+1)^{2^n}$. Seems hard if e_i required to be small.

If VP = VNP, they can be represented with $t = n^{O(\sqrt{n})}$, $s = n^{O(\sqrt{n})}$ and $e_i = O(\sqrt{n})$.

Bounding sparsity(Q_i) instead of degree(Q_i)

Consider the model:

$$f(x) = \sum_{i=1}^{s} \alpha_i . Q_i(x)^{e_i},$$

where Q_i has at most t monomials. Candidate hard polynomials:

- $\prod_{i=1}^{2^n} (X + i)$. Probably hard for general arithmetic circuits.
- $\sum_{i=0}^{2^n-1} 2^{2i(2^n-i-1)} X^i$. Satisfies Kurz condition.
- $(X+1)^{2^n}$. Seems hard if e_i required to be small.

If VP = VNP, they can be represented with $t = n^{O(\sqrt{n})}$, $s = n^{O(\sqrt{n})}$ and $e_i = O(\sqrt{n})$.

- In 2 variables: $\sum_{i=1}^{2^n} X^i Y^{i^2}$ (Newton polygon).

Back to bounded degree

Recall:

$$f(x) = \sum_{i=1}^{s} \alpha_i . Q_i(x)^{e_i},$$

where $\deg(Q_i) \leq t$.

- Expected lower bound: $s = \Omega(d/t)$.
  Applies to "random" f by counting independent parameters.

Back to bounded degree

Recall:

$$f(x) = \sum_{i=1}^{s} \alpha_i . Q_i(x)^{e_i},$$

where $\deg(Q_i) \leq t$.

- Expected lower bound: $s = \Omega(d/t)$.
  Applies to "random" f by counting independent parameters.
- What we can prove:
  $s = \Omega(\sqrt{d/t})$ for some explicit polynomials f.

Upper bounds for bounded degree

Recall:

$$f(x) = \sum_{i=1}^{s} \alpha_i . Q_i(x)^{e_i},$$

where $\deg(Q_i) \leq t$.

- $s = O((d/t)^2)$ for any f (simple explicit construction).

Upper bounds for bounded degree

Recall:

$$f(x) = \sum_{i=1}^{s} \alpha_i . Q_i(x)^{e_i},$$

where $\deg(Q_i) \leq t$.

- $s = O((d/t)^2)$ for any f (simple explicit construction).
- $s = O(d/t)$ for most f
  [On the Waring problem for polynomial rings.
  Fröberg, Ottaviani, Shapiro, 2012]
  for $t = 1$: [Polynomial interpolation in several variables.
  Alexander - Hirschowitz, 1995]

Upper bounds for bounded degree

Recall:

$$f(x) = \sum_{i=1}^{s} \alpha_i . Q_i(x)^{e_i},$$

where $\deg(Q_i) \leq t$.

- $s = O((d/t)^2)$ for any f (simple explicit construction).
- $s = O(d/t)$ for most f
  [On the Waring problem for polynomial rings.
  Fröberg, Ottaviani, Shapiro, 2012]
  for $t = 1$: [Polynomial interpolation in several variables.
  Alexander - Hirschowitz, 1995]
- Worst case rank $\leq 2\times$(worst case border rank):
  [Blekherman - Teitler, 2014]
  simons.berkeley.edu/talks/grigoriy-blekherman-2014-11-10
  Hence $s = O(d/t)$ for any f (non-constructive).

The method of partial derivatives

To prove that f is hard to compute,
we seek a "complexity measure" Γ such that:

- $\Gamma(f)$ is high.
- $\Gamma(g)$ is low if g has small circuit complexity.

The method of partial derivatives

To prove that f is hard to compute,
we seek a "complexity measure" Γ such that:

- $\Gamma(f)$ is high.
- $\Gamma(g)$ is low if g has small circuit complexity.

One popular measure for multivariate polynomials:

- $\partial f =$ space spanned by all partial derivatives $\partial^\alpha f / \partial x^\alpha$.
- $\Gamma(f) = \dim(\partial f)$.

The method of partial derivatives

To prove that f is hard to compute,
we seek a "complexity measure" Γ such that:

- $\Gamma(f)$ is high.
- $\Gamma(g)$ is low if g has small circuit complexity.

One popular measure for multivariate polynomials:

- $\partial f =$ space spanned by all partial derivatives $\partial^\alpha f / \partial x^\alpha$.
- $\Gamma(f) = \dim(\partial f)$.

Abject failure for univariate polynomials!
Indeed, $\Gamma(f) = d + 1$ for all f of degree d.

The method of shifted derivatives

- To fix this: consider the shifted derivatives $x^i f^{(j)}(x)$.
- Degree is $\deg(f) + i - j \Rightarrow$ we can expect linear dependencies.
- This is just the "method of shifted partial derivatives" applied to univariate polynomials.

The Wronskian

Definition

The Wronskian $\mathrm{W}(f_1, \ldots, f_n)$ is defined by

$$\mathrm{W}(f_1, \ldots, f_n)(x) = \begin{vmatrix} f_1(x) & f_2(x) & \ldots & f_n(x) \\ f_1'(x) & f_2'(x) & \ldots & f_n'(x) \\ \vdots & \vdots & \ddots & \vdots \\ f_1^{(n-1)} & f_2^{(n-1)} & \ldots & f_n^{(n-1)} \end{vmatrix}$$

The Wronskian

Definition

The Wronskian $\mathrm{W}(f_1, \ldots, f_n)$ is defined by

$$\mathrm{W}(f_1, \ldots, f_n)(x) = \begin{vmatrix} f_1(x) & f_2(x) & \ldots & f_n(x) \\ f_1'(x) & f_2'(x) & \ldots & f_n'(x) \\ \vdots & \vdots & \ddots & \vdots \\ f_1^{(n-1)} & f_2^{(n-1)} & \ldots & f_n^{(n-1)} \end{vmatrix}$$

Proposition

For $f_1, \ldots, f_n \in \mathbb{K}(X)$, the functions are linearly dependent if and only if the Wronskian $\mathrm{W}(f_1, \ldots, f_n)$ vanishes everywhere.

We also use the Wronskian to bound multiplicities of roots.

Our results

- Hard polynomial: $\prod_{k=1}^{2t}(x-a_k)^{d/2t}$.
  Lower bound: $s=\Omega(\sqrt{d/t})$. Method: Wronskian.

Our results

- Hard polynomial: $\prod_{k=1}^{2t}(x-a_k)^{d/2t}$.
  Lower bound: $s = \Omega(\sqrt{d/t})$. Method: Wronskian.
- Hard polynomial: $f(x) = \sum_{i=1}^{m}(x-a_i)^d$.

Our results

- Hard polynomial: $\prod_{k=1}^{2t}(x-a_k)^{d/2t}$.
  Lower bound: $s=\Omega(\sqrt{d/t})$. Method: Wronskian.
- Hard polynomial: $f(x)=\sum_{i=1}^{m}(x-a_i)^d$.

deg Q_i	e_i	m	s	Method	Optimality

Our results

- Hard polynomial: $\prod_{k=1}^{2t}(x-a_k)^{d/2t}$.
  Lower bound: $s=\Omega(\sqrt{d/t})$. Method: Wronskian.
- Hard polynomial: $f(x)=\sum_{i=1}^{m}(x-a_i)^d$.

$\deg Q_i$	e_i	m	s	Method	Optimality
1	$= d$	$\frac{d}{2}$	$\Omega(d)$	Wronskian	Yes

Our results

- Hard polynomial: $\prod_{k=1}^{2t}(x-a_k)^{d/2t}$.
  Lower bound: $s=\Omega(\sqrt{d/t})$. Method: Wronskian.
- Hard polynomial: $f(x)=\sum_{i=1}^{m}(x-a_i)^d$.

deg Q_i	e_i	m	s	Method	Optimality
1	$=d$	$\frac{d}{2}$	$\Omega(d)$	Wronskian	Yes
2		$\frac{\sqrt{d}}{2}$	$\Omega\left(\sqrt{d}\right)$	Wronskian	Yes

Our results

- Hard polynomial: $\prod_{k=1}^{2t}(x-a_k)^{d/2t}$.
  Lower bound: $s=\Omega(\sqrt{d/t})$. Method: Wronskian.
- Hard polynomial: $f(x)=\sum_{i=1}^{m}(x-a_i)^d$.

deg Q_i	e_i	m	s	Method	Optimality
1	$=d$	$\frac{d}{2}$	$\Omega(d)$	Wronskian	Yes
2		$\frac{\sqrt{d}}{2}$	$\Omega\left(\sqrt{d}\right)$	Wronskian	Yes
t		$\frac{2}{3}\sqrt{\frac{d}{t}}$	$\Omega\left(\frac{1}{t}\sqrt{\frac{d}{t}}\right)$	Wronskian	

Our results

- Hard polynomial: $\prod_{k=1}^{2t}(x-a_k)^{d/2t}$.
  Lower bound: $s=\Omega(\sqrt{d/t})$. Method: Wronskian.
- Hard polynomial: $f(x)=\sum_{i=1}^{m}(x-a_i)^d$.

$\deg Q_i$	e_i	m	s	Method	Optimality
1	$=d$	$\frac{d}{2}$	$\Omega(d)$	Wronskian	Yes
2		$\frac{\sqrt{d}}{2}$	$\Omega\left(\sqrt{d}\right)$	Wronskian	Yes
t		$\frac{2}{3}\sqrt{\frac{d}{t}}$	$\Omega\left(\frac{1}{t}\sqrt{\frac{d}{t}}\right)$	Wronskian	
t	$\leq\frac{d}{t}$	$\frac{\sqrt{2}}{3}\sqrt{\frac{d}{t}}$	$\Omega\left(\sqrt{\frac{d}{t}}\right)$	Wronskian	Yes

Our results

- Hard polynomial: $\prod_{k=1}^{2t}(x-a_k)^{d/2t}$.
  Lower bound: $s=\Omega(\sqrt{d/t})$. Method: Wronskian.
- Hard polynomial: $f(x)=\sum_{i=1}^{m}(x-a_i)^d$.

$\deg Q_i$	e_i	m	s	Method	Optimality
1	$=d$	$\frac{d}{2}$	$\Omega(d)$	Wronskian	Yes
2		$\frac{\sqrt{d}}{2}$	$\Omega\left(\sqrt{d}\right)$	Wronskian	Yes
t		$\frac{2}{3}\sqrt{\frac{d}{t}}$	$\Omega\left(\frac{1}{t}\sqrt{\frac{d}{t}}\right)$	Wronskian	
t	$\leq\frac{d}{t}$	$\frac{\sqrt{2}}{3}\sqrt{\frac{d}{t}}$	$\Omega\left(\sqrt{\frac{d}{t}}\right)$	Wronskian	Yes
t		$\sqrt{\frac{d}{t}}$	$\Omega\left(\sqrt{\frac{d}{t}}\right)$	Shifted derivatives	Yes

Linear independence of powers of linear forms

For any distinct a_i's in $\mathbb{K}$, the family
$S = \{(x-a_1)^d, \dots, (x-a_{d+1})^d\}$ is a basis of $\mathbb{K}_d[X]$.
Proof.

$$\mathrm{Wr}(x) = \begin{vmatrix} (x-a_1)^d & \dots & (x-a_{d+1})^d \\ d(x-a_1)^{d-1} & \dots & d(x-a_{d+1})^{d-1} \\ \vdots & \ddots & \vdots \\ d! & \dots & d! \end{vmatrix}$$

For any $z \in \mathbb{C}$, define $b_i = z - a_i$ and we have:

$$\mathrm{Wr}(z) = \begin{vmatrix} b_1^d & \dots & b_{d+1}^d \\ d \cdot b_1^{d-1} & \dots & d \cdot b_{d+1}^{d-1} \\ \vdots & \ddots & \vdots \\ d! & \dots & d! \end{vmatrix} = c \cdot \begin{vmatrix} b_1^d & \dots & b_{d+1}^d \\ b_1^{d-1} & \dots & b_{d+1}^{d-1} \\ \vdots & \ddots & \vdots \\ 1 & \dots & 1 \end{vmatrix}$$

Vandermonde matrix: $|.| = \prod_{i \neq j}(b_i - b_j) = \prod_{i \neq j}(a_j - a_i) \neq 0$.
$\Rightarrow \mathrm{Wr} \not\equiv 0 \Rightarrow S$ is linearly independent.

Lower bound for $t = 1$

Theorem

For any d, the polynomial $f(x) = \sum_{i=1}^{m}(x - a_i)^d$, with distinct a_i's and $m = \left\lfloor \frac{d}{2} \right\rfloor$, is optimally hard in the following sense: any representation of f of the form $f = \sum_{i=1}^{s} \alpha_i \ell_i^d$, with each ℓ_i of degree 1, must satisfy $s \geq \left\lfloor \frac{d}{2} \right\rfloor$.

Lower bound for $t = 1$

Theorem

For any d, the polynomial $f(x) = \sum_{i=1}^{m}(x - a_i)^d$, with distinct a_i's and $m = \lfloor \frac{d}{2} \rfloor$, is optimally hard in the following sense: any representation of f of the form $f = \sum_{i=1}^{s} \alpha_i \ell_i^d$, with each ℓ_i of degree 1, must satisfy $s \geq \lfloor \frac{d}{2} \rfloor$.

Proof.

For contradiction, assume that $f(X) = \sum_{i=1}^{s} \alpha_i \ell_i^d$ with $s < m$.
We obtain the nontrivial linear relation

$$\sum_{i=1}^{m}(x - a_i)^d - \sum_{i=1}^{s} \alpha_i \ell_i^d = 0$$

between $m + s < d$ d-th powers: contradiction.

Lower bound for $t = 1$

Theorem

For any d, the polynomial $f(x) = \sum_{i=1}^{m}(x - a_i)^d$, with distinct a_i's and $m = \lfloor \frac{d}{2} \rfloor$, is optimally hard in the following sense: any representation of f of the form $f = \sum_{i=1}^{s} \alpha_i \ell_i^d$, with each ℓ_i of degree 1, must satisfy $s \geq \lfloor \frac{d}{2} \rfloor$.

Proof.

For contradiction, assume that $f(X) = \sum_{i=1}^{s} \alpha_i \ell_i^d$ with $s < m$. We obtain the nontrivial linear relation

$$\sum_{i=1}^{m}(x - a_i)^d - \sum_{i=1}^{s} \alpha_i \ell_i^d = 0$$

between $m + s < d$ d-th powers: contradiction.

Stronger bound by Johannes Kepple (*Candidatus Scientiarum*).

Bounding multiplicities with the Wronskian

Let $N_{z_0}(F)$ denote the multiplicity of z_0 as a root of F.

Lemma (Voorhoeve and Van Der Poorten, 1975)

Let $Q_1, \ldots, Q_m$ be linearly independent polynomials, and $F(z) = \sum_{i=1}^{m} Q_i(z)$. Then for any $z_0 \in K$:

$$\mathrm{N}_{z_0}(F) \leq m - 1 + \mathrm{N}_{z_0}(\mathrm{W}(Q_1, \ldots, Q_m))$$

Bounding multiplicities with the Wronskian

Let $N_{z_0}(F)$ denote the multiplicity of z_0 as a root of F.

Lemma (Voorhoeve and Van Der Poorten, 1975)

Let $Q_1, \ldots, Q_m$ be linearly independent polynomials, and $F(z) = \sum_{i=1}^{m} Q_i(z)$. Then for any $z_0 \in K$:

$$\mathrm{N}_{z_0}(F) \leq m - 1 + \mathrm{N}_{z_0}(\mathrm{W}(Q_1, \ldots, Q_m))$$

Proof.

Note that $\mathrm{W}(Q_1, \ldots, Q_m) = \mathrm{W}(Q_1, \ldots, Q_{m-1}, F)$.
Expand along last column:

$$\mathrm{W}(Q_1, \ldots, Q_{m-1}, F) = \sum_{i=0}^{m-1} B_i F^{(i)}$$

and $N_{z_0}(F^{(i)}) \geq N_{z_0}(F) - (m-1)$.

Lower bound for $t = 2$

Theorem

For any t, d, the polynomial $f(x) = \sum_{i=1}^{m}(x - a_i)^d$, with distinct a_i's and $m = \left\lfloor \frac{\sqrt{d}}{2} \right\rfloor$, is hard in the following sense: any representation of f of the form $f = \sum_{i=1}^{s} \alpha_i Q_i^{e_i}$, with each Q_i of degree ≤ 2, must satisfy:

$$s = \Omega\left(\sqrt{d}\right)$$

Sketch of the proof

- Remember $f(x) = \sum_{i=1}^{m}(x - a_i)^d$ where $m = \left\lfloor \frac{\sqrt{d}}{2} \right\rfloor$,

Sketch of the proof

- Remember $f(x) = \sum_{i=1}^{m}(x - a_i)^d$ where $m = \left\lfloor \frac{\sqrt{d}}{2} \right\rfloor$,
- For contradiction, assume $f = \sum_{i=1}^{s} \alpha_i Q_i^{e_i}$ with $s < m/2$.

Sketch of the proof

- Remember $f(x) = \sum_{i=1}^{m}(x - a_i)^d$ where $m = \left\lfloor \frac{\sqrt{d}}{2} \right\rfloor$,
- For contradiction, assume $f = \sum_{i=1}^{s} \alpha_i Q_i^{e_i}$ with $s < m/2$.
- Pick an a_i which isn't a root of any Q_j, wlog a_1.

Sketch of the proof

- Remember $f(x) = \sum_{i=1}^{m}(x - a_i)^d$ where $m = \left\lfloor \frac{\sqrt{d}}{2} \right\rfloor$,
- For contradiction, assume $f = \sum_{i=1}^{s} \alpha_i Q_i^{e_i}$ with $s < m/2$.
- Pick an a_i which isn't a root of any Q_j, wlog a_1.
- Rewrite $(x - a_1)^d = \sum_{i=1}^{l} \alpha_i R_i^{e_i}(x)$
  with linearly independent R_i of degree ≤ 2 and $l \leq s + m - 1 < 3m/2$.

Sketch of the proof

- Remember $f(x) = \sum_{i=1}^{m}(x - a_i)^d$ where $m = \left\lfloor \frac{\sqrt{d}}{2} \right\rfloor$,
- For contradiction, assume $f = \sum_{i=1}^{s} \alpha_i Q_i^{e_i}$ with $s < m/2$.
- Pick an a_i which isn't a root of any Q_j, wlog a_1.
- Rewrite $(x - a_1)^d = \sum_{i=1}^{l} \alpha_i R_i^{e_i}(x)$
  with linearly independent R_i of degree ≤ 2 and $l \leq s + m - 1 < 3m/2$.
- Use Voorhoeve - Van Der Poorten lemma to bound multiplicity of a_1:

$$d = \mathrm{N}_{a_1}\left((x - a_1)^d\right) \leq l - 1 + \mathrm{N}_{a_1}\left(\mathrm{W}\left(R_1^{e_1}, \ldots, R_l^{l}\right)\right)$$

Sketch of the proof

- Remember $f(x) = \sum_{i=1}^{m} (x - a_i)^d$ where $m = \left\lfloor \frac{\sqrt{d}}{2} \right\rfloor$,
- For contradiction, assume $f = \sum_{i=1}^{s} \alpha_i Q_i^{e_i}$ with $s < m/2$.
- Pick an a_i which isn't a root of any Q_j, wlog a_1.
- Rewrite $(x - a_1)^d = \sum_{i=1}^{l} \alpha_i R_i^{e_i}(x)$
  with linearly independent R_i of degree ≤ 2 and $l \leq s + m - 1 < 3m/2$.
- Use Voorhoeve - Van Der Poorten lemma to bound multiplicity of a_1:

$$d = \mathrm{N}_{a_1}\left((x - a_1)^d\right) \leq l - 1 + \mathrm{N}_{a_1}\left(\mathrm{W}\left(R_1^{e_1}, \ldots, R_l^{l}\right)\right)$$

- Factor out $R_i^{e_i - (l-1)}$ from each column of the Wronskian.

Sketch of the proof

- Remember $f(x) = \sum_{i=1}^{m}(x - a_i)^d$ where $m = \left\lfloor \frac{\sqrt{d}}{2} \right\rfloor$,
- For contradiction, assume $f = \sum_{i=1}^{s} \alpha_i Q_i^{e_i}$ with $s < m/2$.
- Pick an a_i which isn't a root of any Q_j, wlog a_1.
- Rewrite $(x - a_1)^d = \sum_{i=1}^{l} \alpha_i R_i^{e_i}(x)$
  with linearly independent R_i of degree ≤ 2 and $l \leq s + m - 1 < 3m/2$.
- Use Voorhoeve - Van Der Poorten lemma to bound multiplicity of a_1:

$$d = \mathrm{N}_{a_1}\left((x - a_1)^d\right) \leq l - 1 + \mathrm{N}_{a_1}\left(\mathrm{W}\left(R_1^{e_1}, \ldots, R_l^{l}\right)\right)$$

- Factor out $R_i^{e_i-(l-1)}$ from each column of the Wronskian.
- Remaining determinant: degree bounded by $3l(l-1)/2$.

Sketch of the proof

- Remember $f(x) = \sum_{i=1}^{m} (x - a_i)^d$ where $m = \left\lfloor \frac{\sqrt{d}}{2} \right\rfloor$,
- For contradiction, assume $f = \sum_{i=1}^{s} \alpha_i Q_i^{e_i}$ with $s < m/2$.
- Pick an a_i which isn't a root of any Q_j, wlog a_1.
- Rewrite $(x - a_1)^d = \sum_{i=1}^{l} \alpha_i R_i^{e_i}(x)$ with linearly independent R_i of degree ≤ 2 and $l \leq s + m - 1 < 3m/2$.
- Use Voorhoeve - Van Der Poorten lemma to bound multiplicity of a_1:

$$d = \mathrm{N}_{a_1}\left((x - a_1)^d\right) \leq l - 1 + \mathrm{N}_{a_1}\left(\mathrm{W}\left(R_1^{e_1}, \ldots, R_l^{l}\right)\right)$$

- Factor out $R_i^{e_i - (l-1)}$ from each column of the Wronskian.
- Remaining determinant: degree bounded by $3l(l-1)/2$.
- Combine to obtain :

$$d \leq l - 1 + 3l(l-1)/2 < 27m^2/8 \leq 27d/32.$$

A closer look

Take for example $l = 2$:

$$\mathrm{W}\left(R_1^{e_1}, R_2^{e_2}\right) = \begin{vmatrix} R_1^{e_1} & R_2^{e_2} \\ e_1 R_1^{e_1 - 1} R_1' & e_2 R_2^{e_2 - 1} R_2' \end{vmatrix} = R_1^{e_1 - 1} R_2^{e_2 - 1} \Delta$$

where $\Delta = \begin{vmatrix} R_1 & R_2 \\ e_1 R_1' & e_2 R_2' \end{vmatrix}$

- $\mathrm{N}_{a_1}\left(R_1^{e_1 - 1}\right) = \mathrm{N}_{a_1}\left(R_2^{e_2 - 1}\right) = 0.$
- The entries of Δ have low degree (here, at most 2); we bound $\mathrm{N}_{a_1}(\Delta)$ by the degree of Δ.
- Possible room for improvement: better bound on $\mathrm{N}_{a_1}(\Delta)$?

Shifted derivatives

Definition

Let $f(x) \in \mathbb{K}[x]$ be a polynomial.
The *span of the l-shifted k-th order derivatives* of f is defined as:

$$\left\langle x^{\leq i+l} \cdot f^{(i)} \right\rangle_{i \leq k} \stackrel{\text{def}}{=} \mathbb{K}\text{-span} \left\{ x^j \cdot f^{(i)}(x) \;\; : \;\; i \leq k, \; j \leq i + l \right\}$$

This forms a $\mathbb{K}$-vector space and we denote its dimension by:

$$\dim \left\langle x^{\leq i+l} \cdot f^{(i)} \right\rangle_{i \leq k}$$

This complexity measure is subadditive.

An upper bound for sums of powers

Proposition

For any polynomial f of degree d of the form $f = \sum_{i=1}^{s} \alpha_i Q_i^{e_i}$ with $\deg Q_i \leq t$ we have:

$$\dim \left\langle x^{\leq i+l} \cdot f^{(i)} \right\rangle_{i \leq k} \leq s \cdot (l + kt + 1).$$

An upper bound for sums of powers

Proposition

For any polynomial f of degree d of the form $f = \sum_{i=1}^{s} \alpha_i Q_i^{e_i}$ with $\deg Q_i \le t$ we have:

$$\dim \left\langle x^{\le i+l} \cdot f^{(i)} \right\rangle_{i \le k} \le s \cdot (l + kt + 1).$$

Proof.

- By subadditivity, it's enough to show that for $f = Q^{e_i}$ with $\deg Q \le t$, we have $\dim \left\langle x^{\le i+l} \cdot f^{(i)} \right\rangle_{i \le k} \le l + kt + 1$.

An upper bound for sums of powers

Proposition

For any polynomial f of degree d of the form $f = \sum_{i=1}^{s} \alpha_i Q_i^{e_i}$ with $\deg Q_i \le t$ we have:

$$\dim \left\langle x^{\le i+l} \cdot f^{(i)} \right\rangle_{i \le k} \le s \cdot (l + kt + 1).$$

Proof.

- By subadditivity, it's enough to show that for $f = Q^{e_i}$ with $\deg Q \le t$, we have $\dim \left\langle x^{\le i+l} \cdot f^{(i)} \right\rangle_{i \le k} \le l + kt + 1$.
- Any $g \in \left\langle x^{\le i+l} \cdot f^{(i)} \right\rangle_{i \le k}$ is of the form $g = Q^{e_i - k} \cdot R$. Since $\deg g \le e_i \cdot t + l$ we have $\deg R \le l + kt$.

Shifted Differential Equations

Definition (SDE)

This is an equation: $\sum_{i=0}^{k} P_i(x) f^{(i)}(x) = 0$
for some polynomials $P_i \in \mathbb{K}[X]$ with $\deg P_i \leq i + l$.
k is called the *order* and l is called the *shift*.

Shifted Differential Equations

Definition (SDE)

This is an equation: $\sum_{i=0}^{k} P_i(x) f^{(i)}(x) = 0$

for some polynomials $P_i \in \mathbb{K}[X]$ with $\deg P_i \leq i + l$.
k is called the *order* and l is called the *shift*.

Proposition

If $f \in \mathbb{K}[X]$ doesn't satisfy any SDE of order k and shift l then $\langle x^{\leq i+l} \cdot f^{(i)} \rangle_{i \leq k}$ is of full dimension , i.e.,

$$\dim \left\langle x^{\leq i+l} \cdot f^{(i)} \right\rangle_{i \leq k} = \sum_{i=0}^{k} (l + i + 1) = (k+1)l + k(k+1)/2.$$

The key lemma

Lemma

Let $f(x) = \sum_{i=1}^{m} (x - a_i)^d$ *where the* a_i*'s are distinct and* $m \leq d$*.*
If f *satisfies a SDE of order* k *and shift* l *then:*

i) $k \geq m$, *or*

ii) $l > \frac{d}{m} - 3m/2$

The key lemma

Lemma

Let $f(x) = \sum_{i=1}^{m} (x - a_i)^d$ *where the* a_i*'s are distinct and* $m \leq d$*.*
If f *satisfies a SDE of order* k *and shift* l *then:*

i) $k \geq m$, *or*

ii) $l > \frac{d}{m} - 3m/2$

Proof.

- Transform the SDE into a relation of the form:

$$-Q_1(x)(x - a_1)^{d-k} = \sum_{i=2}^{m} Q_i(x)(x - a_i)^{d-k}$$

It is nontrivial if $k < m$.

The key lemma

Lemma

Let $f(x) = \sum_{i=1}^{m} (x - a_i)^d$ *where the* a_i*'s are distinct and* $m \leq d$*.*
If f *satisfies a SDE of order* k *and shift* l *then:*

i) $k \geq m$, *or*

ii) $l > \frac{d}{m} - 3m/2$

Proof.

- Transform the SDE into a relation of the form:

$$-Q_1(x)(x - a_1)^{d-k} = \sum_{i=2}^{m} Q_i(x)(x - a_i)^{d-k}$$

  It is nontrivial if $k < m$.

- Use the Wronskian (again!) to obtain:

$$d - k \leq m - 2 + (m - 1)(l + k) + \binom{m-1}{2}$$

The lower bound

Theorem

For any $d, t \geq 2$ such that $t < \frac{d}{4}$, the polynomial $f(x) = \sum_{i=1}^{m} (x - a_i)^d$ with distinct a_i's and $m = \left\lfloor \sqrt{\frac{d}{t}} \right\rfloor$ is hard:

If $f = \sum_{i=1}^{s} \alpha_i Q_i^{e_i}$ with each Q_i of degree $\leq t$ then $s = \Omega\left(\sqrt{\frac{d}{t}}\right)$.

The lower bound

Theorem

For any $d, t \geq 2$ such that $t < \frac{d}{4}$, the polynomial $f(x) = \sum_{i=1}^{m}(x - a_i)^d$ with distinct a_i's and $m = \left\lfloor \sqrt{\frac{d}{t}} \right\rfloor$ is hard:

If $f = \sum_{i=1}^{s} \alpha_i Q_i^{e_i}$ with each Q_i of degree $\leq t$ then $s = \Omega\left(\sqrt{\frac{d}{t}}\right)$.

Proof.

- Pick $k = m - 1$ and $l = (d/m) - 3m/2$: $\langle x^{\leq i+l} \cdot f^{(i)} \rangle_{i \leq k}$ is full.

The lower bound

Theorem

For any $d, t \geq 2$ such that $t < \frac{d}{4}$, the polynomial $f(x) = \sum_{i=1}^{m}(x - a_i)^d$ with distinct a_i's and $m = \left\lfloor \sqrt{\frac{d}{t}} \right\rfloor$ is hard:

If $f = \sum_{i=1}^{s} \alpha_i Q_i^{e_i}$ with each Q_i of degree $\leq t$ then $s = \Omega\left(\sqrt{\frac{d}{t}}\right)$.

Proof.

- Pick $k = m - 1$ and $l = (d/m) - 3m/2$: $\left\langle x^{\leq i+l} \cdot f^{(i)} \right\rangle_{i \leq k}$ is full.
- Hence $\dim \left\langle x^{\leq i+l} \cdot f^{(i)} \right\rangle_{i \leq k} = (k+1)l + k(k+1)/2 = \Omega(d)$.

The lower bound

Theorem

For any $d, t \geq 2$ such that $t < \frac{d}{4}$, the polynomial $f(x) = \sum_{i=1}^{m} (x - a_i)^d$ with distinct a_i's and $m = \left\lfloor \sqrt{\frac{d}{t}} \right\rfloor$ is hard:

If $f = \sum_{i=1}^{s} \alpha_i Q_i^{e_i}$ with each Q_i of degree $\leq t$ then $s = \Omega\left(\sqrt{\frac{d}{t}}\right)$.

Proof.

- Pick $k = m - 1$ and $l = (d/m) - 3m/2$: $\left\langle x^{\leq i+l} \cdot f^{(i)} \right\rangle_{i \leq k}$ is full.
- Hence $\dim \left\langle x^{\leq i+l} \cdot f^{(i)} \right\rangle_{i \leq k} = (k+1)l + k(k+1)/2 = \Omega(d)$.
- Upper bound for sums of powers:
  $\dim \left\langle x^{\leq i+l} \cdot f^{(i)} \right\rangle_{i \leq k} \leq s \cdot (l + kt + 1)$.

The lower bound

Theorem

For any $d, t \geq 2$ such that $t < \frac{d}{4}$, the polynomial $f(x) = \sum_{i=1}^{m} (x - a_i)^d$ with distinct a_i's and $m = \left\lfloor \sqrt{\frac{d}{t}} \right\rfloor$ is hard:

If $f = \sum_{i=1}^{s} \alpha_i Q_i^{e_i}$ with each Q_i of degree $\leq t$ then $s = \Omega\left(\sqrt{\frac{d}{t}}\right)$.

Proof.

- Pick $k = m - 1$ and $l = (d/m) - 3m/2$: $\left\langle x^{\leq i+l} \cdot f^{(i)} \right\rangle_{i \leq k}$ is full.
- Hence $\dim \left\langle x^{\leq i+l} \cdot f^{(i)} \right\rangle_{i \leq k} = (k+1)l + k(k+1)/2 = \Omega(d)$.
- Upper bound for sums of powers:
  $\dim \left\langle x^{\leq i+l} \cdot f^{(i)} \right\rangle_{i \leq k} \leq s \cdot (l + kt + 1)$.
- This gives $s = \Omega\left(\frac{d}{l+kt+1}\right)$

Limitations of Shifted Derivatives

- Recall we wish to find f hard to write as:

$$f(x) = \sum_{i=1}^{s} \alpha_i . Q_i(x)^{e_i}$$

Limitations of Shifted Derivatives

- Recall we wish to find f hard to write as:

$$f(x) = \sum_{i=1}^{s} \alpha_i . Q_i(x)^{e_i}$$

- For **any** f of degree d,
  shifted derivatives cannot give a better bound than:

$$s = \Omega\left(\sqrt{\frac{d}{t}}\right)$$

Limitations of Shifted Derivatives

- Recall we wish to find f hard to write as:

$$f(x) = \sum_{i=1}^{s} \alpha_i . Q_i(x)^{e_i}$$

- For **any** f of degree d,
  shifted derivatives cannot give a better bound than:

$$s = \Omega\left(\sqrt{\frac{d}{t}}\right)$$

- Can the Wronskian do better?

Limitations of Shifted Derivatives

- Recall we wish to find f hard to write as:

$$f(x) = \sum_{i=1}^{s} \alpha_i . Q_i(x)^{e_i}$$

- For **any** f of degree d,
  shifted derivatives cannot give a better bound than:

$$s = \Omega\left(\sqrt{\frac{d}{t}}\right)$$

- Can the Wronskian do better?
- When are the $(x - a_i)^{e_i}$ linearly independent?

A natural first step?

We are looking for an f which does not belong to any subspace of the form:

$$\mathrm{Span}(Q_1^{e_1}, \dots, Q_s^{e_s}).$$

First step: find s-dimensional subspace of $\mathbb{K}_d[X]$ which is not of the form

$$\mathrm{Span}(Q_1^{e_1}, \dots, Q_s^{e_s}).$$