Low-depth algebraic circuit lower bounds over any field

Michael A. Forbes
`miforbes@illinois.edu`
University of Illinois at Urbana-Champaign

Appeared in CCC 2024 (*Best Paper*)

April 4, 2025

Theorem

Theorem

Let $\mathbb{F}$ be a field.

Theorem

Let $\mathbb{F}$ be a field. There is an *n-variate degree-d polynomial*

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-d polynomial

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-d polynomial requiring size

$$n^{d^{\frac{1}{\exp(\Theta(\Delta))}}},$$

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-d polynomial requiring size

$$n^{d^{\frac{1}{\exp(\Theta(\Delta))}}},$$

to be computed by algebraic circuits over $\mathbb{F}$,

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-d polynomial requiring size

$$n^{d^{\frac{1}{\exp(\Theta(\Delta))}}},$$

to be computed by algebraic circuits over $\mathbb{F}$, when the depth is Δ;

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-d polynomial requiring size

$$n^{d^{\frac{1}{\exp(\Theta(\Delta))}}},$$

to be computed by algebraic circuits over $\mathbb{F}$, when the depth is Δ; for $d \lesssim \log n$.

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-d polynomial requiring size

$$n^{d^{\frac{1}{\exp(\Theta(\Delta))}}},$$

to be computed by algebraic circuits over $\mathbb{F}$, when the depth is Δ; for $d \lesssim \log n$.

Remark

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-d polynomial requiring size

$$n^{d^{\frac{1}{\exp(\Theta(\Delta))}}},$$

to be computed by algebraic circuits over $\mathbb{F}$, when the depth is Δ; for $d \lesssim \log n$.

Remark

- *extends breakthrough of Limaye, Srinivasan, Tavenas 22*

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-d polynomial requiring size

$$n^{d^{\frac{1}{\exp(\Theta(\Delta))}}},$$

to be computed by algebraic circuits over $\mathbb{F}$, when the depth is Δ; for $d \lesssim \log n$.

Remark

- *extends breakthrough of Limaye, Srinivasan, Tavenas 22 to* **any** *field,*

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-d polynomial requiring size

$$n^{d^{\frac{1}{\exp(\Theta(\Delta))}}},$$

to be computed by algebraic circuits over $\mathbb{F}$, when the depth is Δ; for $d \lesssim \log n$.

Remark

- *extends breakthrough of Limaye, Srinivasan, Tavenas 22 to* **any** *field, not just when* $\mathrm{char}(F) > d$

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-d polynomial requiring size

$$n^{d^{\frac{1}{\exp(\Theta(\Delta))}}},$$

to be computed by algebraic circuits over $\mathbb{F}$, when the depth is Δ; for $d \lesssim \log n$.

Remark

- *extends breakthrough of Limaye, Srinivasan, Tavenas 22 to* **any** *field, not just when $\mathrm{char}(F) > d$ (or $\mathrm{char}(\mathbb{F}) = 0$)*

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-d polynomial requiring size

$$n^{d^{\frac{1}{\exp(\Theta(\Delta))}}},$$

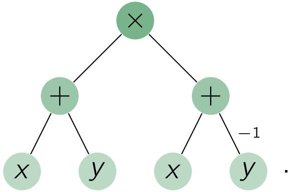
to be computed by algebraic circuits over $\mathbb{F}$, when the depth is Δ; for $d \lesssim \log n$.

Remark

- *extends breakthrough of Limaye, Srinivasan, Tavenas 22 to* **any** *field, not just when $\mathrm{char}(F) > d$ (or $\mathrm{char}(\mathbb{F}) = 0$)*
- *matches best known quantitative parameters [BDS22].*

Multivariate polynomials can be computed by small algebraic circuits, e.g.

$$x^2 - y^2 = (x + y)(x - y) \quad \sim$$



- size 7
- depth 2
- any $\mathbb{F}$
- (total) degree 2

The **size** is the number of nodes.

Goal (Algebraic Complexity Theory)

Find explicit polynomials requiring algebraic circuits of super-polynomial size.

parameters:

- depth: maximum length of input-output path
- $\mathbb{F}$: domain of constants appearing in circuit

Goal

Find explicit polynomials requiring algebraic circuits of super-polynomial size.

Goal

Find explicit polynomials requiring depth-3 algebraic circuits of super-polynomial size.

Goal

Find explicit polynomials requiring depth-3 algebraic circuits of super-polynomial size.

e.g.

$$f(x_1, \ldots, x_n) =$$

Goal

Find explicit polynomials requiring depth-3 algebraic circuits of super-polynomial size.

e.g.

$$f(x_1, \ldots, x_n) = \sum_{i=1}^{s} \prod_{j=1}^{D} \left(\alpha_{i,j,0} + \sum_{k=1}^{n} \alpha_{i,j,k} x_k \right),$$

Goal

Find explicit polynomials requiring depth-3 algebraic circuits of super-polynomial size.

e.g.

$$f(x_1,\ldots,x_n) = \sum_{i=1}^{s}\prod_{j=1}^{D}\left(\alpha_{i,j,0} + \sum_{k=1}^{n}\alpha_{i,j,k}x_k\right), \qquad \alpha_{i,j,k}\in\mathbb{F}$$

Goal

Find explicit polynomials requiring depth-3 algebraic circuits of super-polynomial size.

e.g.

$$f(x_1,\dots,x_n) = \sum_{i=1}^{s}\prod_{j=1}^{D}\left(\alpha_{i,j,0} + \sum_{k=1}^{n}\alpha_{i,j,k}x_k\right), \qquad \alpha_{i,j,k}\in\mathbb{F}$$

$$= \sum_{i}\prod_{j}\ell_{i,j}(\overline{x}),$$

Goal

Find explicit polynomials requiring depth-3 algebraic circuits of super-polynomial size.

e.g.

$$f(x_1, \ldots, x_n) = \sum_{i=1}^{s} \prod_{j=1}^{D} \left(\alpha_{i,j,0} + \sum_{k=1}^{n} \alpha_{i,j,k} x_k \right), \qquad \alpha_{i,j,k} \in \mathbb{F}$$

$$= \sum_{i} \prod_{j} \ell_{i,j}(\overline{x}), \qquad \deg \ell_{i,j} \leq 1$$

Goal

Find explicit polynomials requiring depth-3 algebraic circuits of super-polynomial size.

e.g.

$$f(x_1, \ldots, x_n) = \sum_{i=1}^{s} \prod_{j=1}^{D} \left(\alpha_{i,j,0} + \sum_{k=1}^{n} \alpha_{i,j,k} x_k \right), \qquad \alpha_{i,j,k} \in \mathbb{F}$$

$$= \sum_{i} \prod_{j} \ell_{i,j}(\overline{x}), \qquad \deg \ell_{i,j} \leq 1$$

size $\approx sDn$.

Goal

Find explicit polynomials requiring depth-3 algebraic circuits of super-polynomial size.

e.g.

$$f(x_1,\ldots,x_n) = \sum_{i=1}^{s}\prod_{j=1}^{D}\left(\alpha_{i,j,0} + \sum_{k=1}^{n}\alpha_{i,j,k}x_k\right), \qquad \alpha_{i,j,k} \in \mathbb{F}$$

$$= \sum_{i}\prod_{j}\ell_{i,j}(\overline{x}), \qquad \deg \ell_{i,j} \le 1$$

size $\approx sDn$.

known results:

Goal

Find explicit polynomials requiring depth-3 algebraic circuits of super-polynomial size.

e.g.

$$f(x_1, \ldots, x_n) = \sum_{i=1}^{s} \prod_{j=1}^{D} \left(\alpha_{i,j,0} + \sum_{k=1}^{n} \alpha_{i,j,k} x_k \right), \qquad \alpha_{i,j,k} \in \mathbb{F}$$

$$= \sum_{i} \prod_{j} \ell_{i,j}(\overline{x}), \qquad \deg \ell_{i,j} \leq 1$$

size $\approx sDn$.

known results:

- $\Omega(n^2)$ [SW01],

Goal

Find explicit polynomials requiring depth-3 algebraic circuits of super-polynomial size.

e.g.

$$f(x_1,\dots,x_n) = \sum_{i=1}^{s}\prod_{j=1}^{D}\left(\alpha_{i,j,0} + \sum_{k=1}^{n}\alpha_{i,j,k}x_k\right), \qquad \alpha_{i,j,k}\in\mathbb{F}$$

$$= \sum_i \prod_j \ell_{i,j}(\overline{x}), \qquad \deg \ell_{i,j} \le 1$$

size $\approx sDn$.

known results:

- $\Omega(n^2)$ [SW01], in large characteristic

Goal

Find explicit polynomials requiring depth-3 algebraic circuits of super-polynomial size.

e.g.

$$f(x_1, \dots, x_n) = \sum_{i=1}^{s} \prod_{j=1}^{D} \left(\alpha_{i,j,0} + \sum_{k=1}^{n} \alpha_{i,j,k} x_k \right), \qquad \alpha_{i,j,k} \in \mathbb{F}$$

$$= \sum_i \prod_j \ell_{i,j}(\overline{x}), \qquad \deg \ell_{i,j} \le 1$$

size $\approx sDn$.

known results:

- $\Omega(n^2)$ [SW01], in large characteristic
- $\tilde{\Omega}(n^3)$ [KST16]

Goal

Find explicit polynomials requiring depth-3 algebraic circuits of super-polynomial size.

e.g.

$$f(x_1, \ldots, x_n) = \sum_{i=1}^{s} \prod_{j=1}^{D} \left(\alpha_{i,j,0} + \sum_{k=1}^{n} \alpha_{i,j,k} x_k \right), \qquad \alpha_{i,j,k} \in \mathbb{F}$$

$$= \sum_{i} \prod_{j} \ell_{i,j}(\overline{x}), \qquad \deg \ell_{i,j} \leq 1$$

size $\approx sDn$.

known results:

- $\Omega(n^2)$ [SW01], in large characteristic
- $\tilde{\Omega}(n^3)$ [KST16]
- $n^{\Omega(\sqrt{\log n})}$ [LST22],

Goal

Find explicit polynomials requiring depth-3 algebraic circuits of super-polynomial size.

e.g.

$$f(x_1,\ldots,x_n) = \sum_{i=1}^{s}\prod_{j=1}^{D}\left(\alpha_{i,j,0} + \sum_{k=1}^{n}\alpha_{i,j,k}x_k\right), \qquad \alpha_{i,j,k}\in\mathbb{F}$$

$$= \sum_i \prod_j \ell_{i,j}(\overline{x}), \qquad \deg \ell_{i,j} \le 1$$

size $\approx sDn$.

known results:

- $\Omega(n^2)$ [SW01], in large characteristic
- $\tilde{\Omega}(n^3)$ [KST16]
- $n^{\Omega(\sqrt{\log n})}$ [LST22], in large characteristic

Goal

Goal

Super-polynomial depth-3 algebraic circuit lower bounds, over <u>every</u> field.

Goal

Super-polynomial depth-3 algebraic circuit lower bounds, over every field.

Definition

The **characteristic** $\mathrm{char}(F)$ of the field $\mathbb{F}$

Goal

Super-polynomial depth-3 algebraic circuit lower bounds, over every field.

Definition

The **characteristic** $\mathrm{char}(F)$ of the field $\mathbb{F}$ is the minimum $p \geq 1$ such that $\underbrace{1 + 1 + \cdots + 1}_{p} =$

Goal

Super-polynomial depth-3 algebraic circuit lower bounds, over <u>every</u> field.

Definition

The **characteristic** $\mathrm{char}(F)$ of the field $\mathbb{F}$ is the minimum $p \geq 1$ such that $\underbrace{1 + 1 + \cdots + 1}_{p} = 0$,

Goal

Super-polynomial depth-3 algebraic circuit lower bounds, over every field.

Definition

The **characteristic** $\mathrm{char}(F)$ of the field $\mathbb{F}$ is the minimum $p \geq 1$ such that $\underbrace{1 + 1 + \cdots + 1}_{p} = 0$, or 0 if no such p exists.

Goal

Super-polynomial depth-3 algebraic circuit lower bounds, over <u>every</u> field.

Definition

The **characteristic** $\mathrm{char}(F)$ of the field $\mathbb{F}$ is the minimum $p \geq 1$ such that $\underbrace{1 + 1 + \cdots + 1}_{p} = 0$, or 0 if no such p exists. **fact**:

Goal

Super-polynomial depth-3 algebraic circuit lower bounds, over <u>every</u> field.

Definition

The **characteristic** $\mathrm{char}(F)$ of the field $\mathbb{F}$ is the minimum $p \geq 1$ such that $\underbrace{1+1+\cdots+1}_{p} = 0$, or 0 if no such p exists. **fact**: $\mathrm{char}(F) = 0$

Goal

Super-polynomial depth-3 algebraic circuit lower bounds, over <u>every</u> field.

Definition

The **characteristic** $\mathrm{char}(F)$ of the field $\mathbb{F}$ is the minimum $p \geq 1$ such that $\underbrace{1+1+\cdots+1}_{p} = 0$, or 0 if no such p exists. **fact**: $\mathrm{char}(F) = 0$ or $\mathrm{char}(F)$ is prime.

Goal

Super-polynomial depth-3 algebraic circuit lower bounds, over every field.

Definition

The **characteristic** $\mathrm{char}(F)$ of the field $\mathbb{F}$ is the minimum $p \geq 1$ such that $\underbrace{1 + 1 + \cdots + 1}_{p} = 0$, or 0 if no such p exists. **fact**: $\mathrm{char}(F) = 0$ or $\mathrm{char}(F)$ is prime.

e.g.

Goal

Super-polynomial depth-3 algebraic circuit lower bounds, over every field.

Definition

The **characteristic** $\mathrm{char}(F)$ of the field $\mathbb{F}$ is the minimum $p \geq 1$ such that $\underbrace{1 + 1 + \cdots + 1}_{p} = 0$, or 0 if no such p exists. **fact**: $\mathrm{char}(F) = 0$ or $\mathrm{char}(F)$ is prime.

e.g.

- $\mathbb{Q}$,

Goal

Super-polynomial depth-3 algebraic circuit lower bounds, over every field.

Definition

The **characteristic** $\mathrm{char}(F)$ of the field $\mathbb{F}$ is the minimum $p \geq 1$ such that $\underbrace{1 + 1 + \cdots + 1}_{p} = 0$, or 0 if no such p exists. **fact**: $\mathrm{char}(F) = 0$ or $\mathrm{char}(F)$ is prime.

e.g.

- $\mathbb{Q}$, $\mathbb{R}$,

Goal

Super-polynomial depth-3 algebraic circuit lower bounds, over <u>every</u> field.

Definition

The **characteristic** $\text{char}(F)$ of the field $\mathbb{F}$ is the minimum $p \geq 1$ such that $\underbrace{1 + 1 + \cdots + 1}_{p} = 0$, or 0 if no such p exists. **fact**: $\text{char}(F) = 0$ or $\text{char}(F)$ is prime.

e.g.

- $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$

Goal

Super-polynomial depth-3 algebraic circuit lower bounds, over <u>every</u> field.

Definition

The **characteristic** $\mathrm{char}(F)$ of the field $\mathbb{F}$ is the minimum $p \geq 1$ such that $\underbrace{1+1+\cdots+1}_{p} = 0$, or 0 if no such p exists. **fact**: $\mathrm{char}(F) = 0$ or $\mathrm{char}(F)$ is prime.

e.g.

- $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are of characteristic 0

Goal

Super-polynomial depth-3 algebraic circuit lower bounds, over <u>every</u> field.

Definition

The **characteristic** $\mathrm{char}(F)$ of the field $\mathbb{F}$ is the minimum $p \geq 1$ such that $\underbrace{1 + 1 + \cdots + 1}_{p} = 0$, or 0 if no such p exists. **fact**: $\mathrm{char}(F) = 0$ or $\mathrm{char}(F)$ is prime.

e.g.

- $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are of characteristic 0
- $\mathbb{F}_p = \{0, 1 \ldots, p - 1\}$

Goal

Super-polynomial depth-3 algebraic circuit lower bounds, over every field.

Definition

The **characteristic** $\mathrm{char}(F)$ of the field $\mathbb{F}$ is the minimum $p \geq 1$ such that $\underbrace{1 + 1 + \cdots + 1}_{p} = 0$, or 0 if no such p exists. **fact**: $\mathrm{char}(F) = 0$ or $\mathrm{char}(F)$ is prime.

e.g.

- $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are of characteristic 0
- $\mathbb{F}_p = \{0, 1 \ldots, p-1\}$ is of characteristic p

Goal

Super-polynomial depth-3 algebraic circuit lower bounds, over every field.

Definition

The **characteristic** $\mathrm{char}(F)$ of the field $\mathbb{F}$ is the minimum $p \geq 1$ such that $\underbrace{1 + 1 + \cdots + 1}_{p} = 0$, or 0 if no such p exists. **fact**: $\mathrm{char}(F) = 0$ or $\mathrm{char}(F)$ is prime.

e.g.

- $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are of characteristic 0
- $\mathbb{F}_p = \{0, 1 \ldots, p-1\}$ is of characteristic p
- $\mathbb{Q}(x, y, z) =$

Goal

Super-polynomial depth-3 algebraic circuit lower bounds, over every field.

Definition

The **characteristic** $\mathrm{char}(F)$ of the field $\mathbb{F}$ is the minimum $p \geq 1$ such that $\underbrace{1 + 1 + \cdots + 1}_{p} = 0$, or 0 if no such p exists. **fact**: $\mathrm{char}(F) = 0$ or $\mathrm{char}(F)$ is prime.

e.g.

- $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are of characteristic 0
- $\mathbb{F}_p = \{0, 1 \ldots, p-1\}$ is of characteristic p
- $\mathbb{Q}(x, y, z) = \left\{ \frac{f(x,y,z)}{g(x,y,z)} : \right.$

Goal

Super-polynomial depth-3 algebraic circuit lower bounds, over every field.

Definition

The **characteristic** $\mathrm{char}(F)$ of the field $\mathbb{F}$ is the minimum $p \geq 1$ such that $\underbrace{1+1+\cdots+1}_{p} = 0$, or 0 if no such p exists. **fact**: $\mathrm{char}(F) = 0$ or $\mathrm{char}(F)$ is prime.

e.g.

- $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are of characteristic 0
- $\mathbb{F}_p = \{0, 1 \ldots, p-1\}$ is of characteristic p
- $\mathbb{Q}(x,y,z) = \left\{\frac{f(x,y,z)}{g(x,y,z)} : f, g \in \mathbb{Q}[x,y,z],\right.$

Goal

Super-polynomial depth-3 algebraic circuit lower bounds, over every field.

Definition

The **characteristic** $\mathrm{char}(F)$ of the field $\mathbb{F}$ is the minimum $p \geq 1$ such that $\underbrace{1 + 1 + \cdots + 1}_{p} = 0$, or 0 if no such p exists. **fact**: $\mathrm{char}(F) = 0$ or $\mathrm{char}(F)$ is prime.

e.g.

- $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are of characteristic 0
- $\mathbb{F}_p = \{0, 1 \ldots, p-1\}$ is of characteristic p
- $\mathbb{Q}(x, y, z) = \left\{\frac{f(x,y,z)}{g(x,y,z)} : f, g \in \mathbb{Q}[x, y, z], g \neq 0\right\}$

Goal

Super-polynomial depth-3 algebraic circuit lower bounds, over every field.

Definition

The **characteristic** $\mathrm{char}(F)$ of the field $\mathbb{F}$ is the minimum $p \geq 1$ such that $\underbrace{1+1+\cdots+1}_{p} = 0$, or 0 if no such p exists. **fact**: $\mathrm{char}(F) = 0$ or $\mathrm{char}(F)$ is prime.

e.g.

- $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are of characteristic 0
- $\mathbb{F}_p = \{0, 1 \ldots, p-1\}$ is of characteristic p
- $\mathbb{Q}(x,y,z) = \left\{ \frac{f(x,y,z)}{g(x,y,z)} : f, g \in \mathbb{Q}[x,y,z], g \neq 0 \right\}$ is of characteristic 0

Goal

Super-polynomial depth-3 algebraic circuit lower bounds, over every field.

Definition

The **characteristic** $\mathrm{char}(F)$ of the field $\mathbb{F}$ is the minimum $p \geq 1$ such that $\underbrace{1 + 1 + \cdots + 1}_{p} = 0$, or 0 if no such p exists. **fact**: $\mathrm{char}(F) = 0$ or $\mathrm{char}(F)$ is prime.

e.g.

- $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are of characteristic 0
- $\mathbb{F}_p = \{0, 1 \ldots, p - 1\}$ is of characteristic p
- $\mathbb{Q}(x, y, z) = \left\{ \frac{f(x,y,z)}{g(x,y,z)} : f, g \in \mathbb{Q}[x, y, z], g \neq 0 \right\}$ is of characteristic 0

regimes:

Goal

Super-polynomial depth-3 algebraic circuit lower bounds, over every field.

Definition

The **characteristic** $\mathrm{char}(F)$ of the field $\mathbb{F}$ is the minimum $p \geq 1$ such that $\underbrace{1 + 1 + \cdots + 1}_{p} = 0$, or 0 if no such p exists. **fact**: $\mathrm{char}(F) = 0$ or $\mathrm{char}(F)$ is prime.

e.g.

- $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are of characteristic 0
- $\mathbb{F}_p = \{0, 1 \ldots, p-1\}$ is of characteristic p
- $\mathbb{Q}(x, y, z) = \left\{ \frac{f(x,y,z)}{g(x,y,z)} : f, g \in \mathbb{Q}[x, y, z], g \neq 0 \right\}$ is of characteristic 0

regimes:

- **large** characteristic:

Goal

Super-polynomial depth-3 algebraic circuit lower bounds, over <u>every</u> field.

Definition

The **characteristic** $\mathrm{char}(F)$ of the field $\mathbb{F}$ is the minimum $p \geq 1$ such that $\underbrace{1 + 1 + \cdots + 1}_{p} = 0$, or 0 if no such p exists. **fact**: $\mathrm{char}(F) = 0$ or $\mathrm{char}(F)$ is prime.

e.g.

- $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are of characteristic 0
- $\mathbb{F}_p = \{0, 1 \ldots, p-1\}$ is of characteristic p
- $\mathbb{Q}(x, y, z) = \left\{ \frac{f(x,y,z)}{g(x,y,z)} : f, g \in \mathbb{Q}[x, y, z], g \neq 0 \right\}$ is of characteristic 0

regimes:

- **large** characteristic: $\mathrm{char}(F) \gg 0$

Goal

Super-polynomial depth-3 algebraic circuit lower bounds, over every field.

Definition

The **characteristic** $\mathrm{char}(F)$ of the field $\mathbb{F}$ is the minimum $p \geq 1$ such that $\underbrace{1+1+\cdots+1}_{p} = 0$, or 0 if no such p exists. **fact**: $\mathrm{char}(F) = 0$ or $\mathrm{char}(F)$ is prime.

e.g.

- $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are of characteristic 0
- $\mathbb{F}_p = \{0, 1 \ldots, p-1\}$ is of characteristic p
- $\mathbb{Q}(x, y, z) = \left\{ \frac{f(x,y,z)}{g(x,y,z)} : f, g \in \mathbb{Q}[x, y, z], g \neq 0 \right\}$ is of characteristic 0

regimes:

- **large** characteristic: $\mathrm{char}(F) \gg 0$ (or $\mathrm{char}(F) = 0$)

Goal

Super-polynomial depth-3 algebraic circuit lower bounds, over every field.

Definition

The **characteristic** $\mathrm{char}(F)$ of the field $\mathbb{F}$ is the minimum $p \geq 1$ such that $\underbrace{1+1+\cdots+1}_{p} = 0$, or 0 if no such p exists. **fact**: $\mathrm{char}(F) = 0$ or $\mathrm{char}(F)$ is prime.

e.g.

- $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are of characteristic 0
- $\mathbb{F}_p = \{0, 1 \ldots, p-1\}$ is of characteristic p
- $\mathbb{Q}(x, y, z) = \left\{ \frac{f(x,y,z)}{g(x,y,z)} : f, g \in \mathbb{Q}[x, y, z], g \neq 0 \right\}$ is of characteristic 0

regimes:

- **large** characteristic: $\mathrm{char}(F) \gg 0$ (or $\mathrm{char}(F) = 0$)
- **small** characteristic

Question

Question

How does the power of algebraic circuits depend on the characteristic?

Question

How does the power of algebraic circuits depend on the characteristic?

some algebraic reasoning requires *large* characteristic:

Question

How does the power of algebraic circuits depend on the characteristic?

some algebraic reasoning requires *large* characteristic:

- notable polynomial identities

Question

How does the power of algebraic circuits depend on the characteristic?

some algebraic reasoning requires *large* characteristic:

- notable polynomial identities
  - Fischer's identity

Question

How does the power of algebraic circuits depend on the characteristic?

some algebraic reasoning requires *large* characteristic:

- notable polynomial identities
  - Fischer's identity
  - $\sqrt{1+x} =$

Question

How does the power of algebraic circuits depend on the characteristic?

some algebraic reasoning requires *large* characteristic:

- notable polynomial identities
  - Fischer's identity
  - $\sqrt{1+x} = 1 + \frac{1}{2}x - \frac{1}{8}x^2 + \frac{1}{16}x^3 + \cdots.$

Question

How does the power of algebraic circuits depend on the characteristic?

some algebraic reasoning requires *large* characteristic:

- notable polynomial identities
  - Fischer's identity
  - $\sqrt{1+x} = 1 + \frac{1}{2}x - \frac{1}{8}x^2 + \frac{1}{16}x^3 + \cdots$.
  - Newton identities,

Question

How does the power of algebraic circuits depend on the characteristic?

some algebraic reasoning requires *large* characteristic:

- notable polynomial identities
  - Fischer's identity
  - $\sqrt{1+x} = 1 + \frac{1}{2}x - \frac{1}{8}x^2 + \frac{1}{16}x^3 + \cdots$.
  - Newton identities, e.g. $\mathrm{esym}_{n,2} =$

Question

How does the power of algebraic circuits depend on the characteristic?

some algebraic reasoning requires *large* characteristic:

- notable polynomial identities
  - Fischer's identity
  - $\sqrt{1+x} = 1 + \frac{1}{2}x - \frac{1}{8}x^2 + \frac{1}{16}x^3 + \cdots.$
  - Newton identities, e.g. $\mathrm{esym}_{n,2} = \sum_{i<j} x_i x_j =$

Question

How does the power of algebraic circuits depend on the characteristic?

some algebraic reasoning requires *large* characteristic:

- notable polynomial identities
  - Fischer's identity
  - $\sqrt{1+x} = 1 + \frac{1}{2}x - \frac{1}{8}x^2 + \frac{1}{16}x^3 + \cdots$.
  - Newton identities, e.g. $\mathrm{esym}_{n,2} = \sum_{i<j} x_i x_j = \frac{\left(\sum_i x_i\right)^2 - \left(\sum_i x_i^2\right)}{2}$.

Question

How does the power of algebraic circuits depend on the characteristic?

some algebraic reasoning requires *large* characteristic:

- notable polynomial identities
  - Fischer's identity
  - $\sqrt{1+x} = 1 + \frac{1}{2}x - \frac{1}{8}x^2 + \frac{1}{16}x^3 + \cdots$.
  - Newton identities, e.g. $\mathrm{esym}_{n,2} = \sum_{i<j} x_i x_j = \frac{\left(\sum_i x_i\right)^2 - \left(\sum_i x_i^2\right)}{2}$.
- applications of polynomial identities to algebraic complexity theory

Question

How does the power of algebraic circuits depend on the characteristic?

some algebraic reasoning requires *large* characteristic:

- notable polynomial identities
  - Fischer's identity
  - $\sqrt{1+x} = 1 + \frac{1}{2}x - \frac{1}{8}x^2 + \frac{1}{16}x^3 + \cdots$.
  - Newton identities, e.g. $\mathrm{esym}_{n,2} = \sum_{i<j} x_i x_j = \frac{\left(\sum_i x_i\right)^2 - \left(\sum_i x_i^2\right)}{2}$.
- applications of polynomial identities to algebraic complexity theory
  - reduction to depth-3 [GKKS13]

Question

How does the power of algebraic circuits depend on the characteristic?

some algebraic reasoning requires *large* characteristic:

- notable polynomial identities
  - Fischer's identity
  - $\sqrt{1+x} = 1 + \frac{1}{2}x - \frac{1}{8}x^2 + \frac{1}{16}x^3 + \cdots$.
  - Newton identities, e.g. $\mathrm{esym}_{n,2} = \sum_{i<j} x_i x_j = \frac{\left(\sum_i x_i\right)^2 - \left(\sum_i x_i^2\right)}{2}$.
- applications of polynomial identities to algebraic complexity theory
  - reduction to depth-3 [GKKS13]
  - small algebraic circuits can be factored efficiently [Kal89]

Question

How does the power of algebraic circuits depend on the characteristic?

some algebraic reasoning requires *large* characteristic:

- notable polynomial identities
  - Fischer's identity
  - $\sqrt{1+x} = 1 + \frac{1}{2}x - \frac{1}{8}x^2 + \frac{1}{16}x^3 + \cdots$.
  - Newton identities, e.g. $\mathrm{esym}_{n,2} = \sum_{i<j} x_i x_j = \frac{\left(\sum_i x_i\right)^2 - \left(\sum_i x_i^2\right)}{2}$.
- applications of polynomial identities to algebraic complexity theory
  - reduction to depth-3 [GKKS13]
  - small algebraic circuits can be factored efficiently [Kal89]
  - lower bounds for constant-depth circuits [LST22]

Question

How does the power of algebraic circuits depend on the characteristic?

some algebraic reasoning requires *large* characteristic:

- notable polynomial identities
  - Fischer's identity
  - $\sqrt{1+x} = 1 + \frac{1}{2}x - \frac{1}{8}x^2 + \frac{1}{16}x^3 + \cdots$.
  - Newton identities, e.g. $\mathrm{esym}_{n,2} = \sum_{i<j} x_i x_j = \frac{\left(\sum_i x_i\right)^2 - \left(\sum_i x_i^2\right)}{2}$.
- applications of polynomial identities to algebraic complexity theory
  - reduction to depth-3 [GKKS13]
  - small algebraic circuits can be factored efficiently [Kal89]
  - lower bounds for constant-depth circuits [LST22]

some algebraic reasoning requires *small* characteristic:

Question

How does the power of algebraic circuits depend on the characteristic?

some algebraic reasoning requires *large* characteristic:

- notable polynomial identities
  - Fischer's identity
  - $\sqrt{1+x} = 1 + \frac{1}{2}x - \frac{1}{8}x^2 + \frac{1}{16}x^3 + \cdots$.
  - Newton identities, e.g. $\mathrm{esym}_{n,2} = \sum_{i<j} x_i x_j = \frac{\left(\sum_i x_i\right)^2 - \left(\sum_i x_i^2\right)}{2}$.
- applications of polynomial identities to algebraic complexity theory
  - reduction to depth-3 [GKKS13]
  - small algebraic circuits can be factored efficiently [Kal89]
  - lower bounds for constant-depth circuits [LST22]

some algebraic reasoning requires *small* characteristic:

- $(x+y)^p = x^p + y^p$

Question

How does the power of algebraic circuits depend on the characteristic?

some algebraic reasoning requires *large* characteristic:

- notable polynomial identities
  - Fischer's identity
  - $\sqrt{1+x} = 1 + \frac{1}{2}x - \frac{1}{8}x^2 + \frac{1}{16}x^3 + \cdots$.
  - Newton identities, e.g. $\mathrm{esym}_{n,2} = \sum_{i<j} x_i x_j = \frac{\left(\sum_i x_i\right)^2 - \left(\sum_i x_i^2\right)}{2}$.
- applications of polynomial identities to algebraic complexity theory
  - reduction to depth-3 [GKKS13]
  - small algebraic circuits can be factored efficiently [Kal89]
  - lower bounds for constant-depth circuits [LST22]

some algebraic reasoning requires *small* characteristic:

- $(x+y)^p = x^p + y^p$
- permanent efficiently computable in characteristic 2.

Question

How does the power of algebraic circuits depend on the characteristic?

some algebraic reasoning requires *large* characteristic:

- notable polynomial identities
  - Fischer's identity
  - $\sqrt{1+x} = 1 + \frac{1}{2}x - \frac{1}{8}x^2 + \frac{1}{16}x^3 + \cdots$.
  - Newton identities, e.g. $\mathrm{esym}_{n,2} = \sum_{i<j} x_i x_j = \frac{\left(\sum_i x_i\right)^2 - \left(\sum_i x_i^2\right)}{2}$.
- applications of polynomial identities to algebraic complexity theory
  - reduction to depth-3 [GKKS13]
  - small algebraic circuits can be factored efficiently [Kal89]
  - lower bounds for constant-depth circuits [LST22]

some algebraic reasoning requires *small* characteristic:

- $(x+y)^p = x^p + y^p$
- permanent efficiently computable in characteristic 2.

$\Longrightarrow$ small and large characteristic fields are incomparable in difficulty

lower bounds in small characteristic have several applications:

lower bounds in small characteristic have several applications:

- $\mathrm{AC}^0[p]$-Frege proofs

lower bounds in small characteristic have several applications:

- $\mathrm{AC}^0[p]$-Frege proofs can be simulated by $O(1)$-depth algebraic-circuit (IPS) proofs

lower bounds in small characteristic have several applications:

- $\mathrm{AC}^0[p]$-Frege proofs can be simulated by $O(1)$-depth algebraic-circuit (IPS) proofs over $\mathbb{F}_p$ [GP14]

lower bounds in small characteristic have several applications:

- $\mathsf{AC}^0[p]$-Frege proofs can be simulated by $O(1)$-depth algebraic-circuit (IPS) proofs over $\mathbb{F}_p$ [GP14]

$\implies$ "strong enough" $O(1)$-depth algebraic "circuit lower bounds" over $\mathbb{F}_p$

lower bounds in small characteristic have several applications:

- $\mathrm{AC}^0[p]$-Frege proofs can be simulated by $O(1)$-depth algebraic-circuit (IPS) proofs over $\mathbb{F}_p$ [GP14]

$\Longrightarrow$ "strong enough" $O(1)$-depth algebraic "circuit lower bounds" over $\mathbb{F}_p$ yield breakthrough $\mathrm{AC}^0[p]$-Frege lower bounds

lower bounds in small characteristic have several applications:

- $\mathsf{AC}^0[p]$-Frege proofs can be simulated by $O(1)$-depth algebraic-circuit (IPS) proofs over $\mathbb{F}_p$ [GP14]

  $\Longrightarrow$ "strong enough" $O(1)$-depth algebraic "circuit lower bounds" over $\mathbb{F}_p$ yield breakthrough $\mathsf{AC}^0[p]$-Frege lower bounds

- polynomial identity testing over $\mathbb{F}_p$

lower bounds in small characteristic have several applications:

- $\mathsf{AC}^0[p]$-Frege proofs can be simulated by $O(1)$-depth algebraic-circuit (IPS) proofs over $\mathbb{F}_p$ [GP14]

  $\Longrightarrow$ "strong enough" $O(1)$-depth algebraic "circuit lower bounds" over $\mathbb{F}_p$ yield breakthrough $\mathsf{AC}^0[p]$-Frege lower bounds

- polynomial identity testing over $\mathbb{F}_p$ from "strong enough" algebraic circuit lower bounds over $\mathbb{F}_p$,

lower bounds in small characteristic have several applications:

- $\mathrm{AC}^0[p]$-Frege proofs can be simulated by $O(1)$-depth algebraic-circuit (IPS) proofs over $\mathbb{F}_p$ [GP14]

  $\Longrightarrow$ "strong enough" $O(1)$-depth algebraic "circuit lower bounds" over $\mathbb{F}_p$ yield breakthrough $\mathrm{AC}^0[p]$-Frege lower bounds

- polynomial identity testing over $\mathbb{F}_p$ from "strong enough" algebraic circuit lower bounds over $\mathbb{F}_p$, via algebraic hardness-vs-randomness

lower bounds in small characteristic have several applications:

- $\mathsf{AC}^0[p]$-Frege proofs can be simulated by $O(1)$-depth algebraic-circuit (IPS) proofs over $\mathbb{F}_p$ [GP14]
  - $\Longrightarrow$ "strong enough" $O(1)$-depth algebraic "circuit lower bounds" over $\mathbb{F}_p$ yield breakthrough $\mathsf{AC}^0[p]$-Frege lower bounds
- polynomial identity testing over $\mathbb{F}_p$ from "strong enough" algebraic circuit lower bounds over $\mathbb{F}_p$, via algebraic hardness-vs-randomness
- settling whether notable polynomial identities (e.g., the Newton identities) have analogues over fields of small characteristic.

lower bounds in small characteristic have several applications:

- $AC^0[p]$-Frege proofs can be simulated by $O(1)$-depth algebraic-circuit (IPS) proofs over $\mathbb{F}_p$ [GP14]

  $\Longrightarrow$ "strong enough" $O(1)$-depth algebraic "circuit lower bounds" over $\mathbb{F}_p$ yield breakthrough $AC^0[p]$-Frege lower bounds

- polynomial identity testing over $\mathbb{F}_p$ from "strong enough" algebraic circuit lower bounds over $\mathbb{F}_p$, via algebraic hardness-vs-randomness
- settling whether notable polynomial identities (e.g., the Newton identities) have analogues over fields of small characteristic.
- "better understand" LST22

Theorem (**F**24)

Theorem (**F**24)

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-d polynomial requiring size

$$n^{d^{\frac{1}{\exp(\Theta(\Delta))}}},$$

to be computed by algebraic circuits over $\mathbb{F}$, when the depth is Δ ; for $d \approx \log n$,

Theorem (LST22)

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-d polynomial requiring size

$$n^{d^{\frac{1}{\exp(\Theta(\Delta))}}},$$

to be computed by algebraic circuits over $\mathbb{F}$, when the depth is Δ ; for $d \approx \log n$,

$\boxed{\textit{if } \mathrm{char}(F) > d \ \textit{(or } \mathrm{char}(F) = 0.\textit{)}}$

Theorem (LST22)

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-d polynomial requiring size

$$n^{\Omega(\sqrt{\log n})},$$

to be computed by algebraic circuits over $\mathbb{F}$, when the depth is $\Delta = 3$; for $d \approx \log n$,

$\boxed{\textit{if } \operatorname{char}(F) > d \ (\textit{or } \operatorname{char}(F) = 0.)}$

Theorem (LST22)

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-d polynomial requiring size

$$n^{\Omega(\sqrt{\log n})},$$

to be computed by algebraic circuits over $\mathbb{F}$, when the depth is $\Delta = 3$; for $d \approx \log n$,

$\boxed{\textit{if } \operatorname{char}(F) > d \ \textit{(or } \operatorname{char}(F) = 0.)}$

Proof.

Theorem (LST22)

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-d polynomial requiring size

$$n^{\Omega(\sqrt{\log n})},$$

to be computed by algebraic circuits over $\mathbb{F}$, when the depth is $\Delta = 3$; for $d \approx \log n$, $\boxed{\textit{if } \mathrm{char}(F) > d \ \textit{(or } \mathrm{char}(F) = 0.\textit{)}}$

Proof.

1. small depth-3 circuit

Theorem (LST22)

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-d polynomial requiring size

$$n^{\Omega(\sqrt{\log n})},$$

to be computed by algebraic circuits over $\mathbb{F}$, when the depth is $\Delta = 3$; for $d \approx \log n$, $\boxed{\textit{if } \mathrm{char}(F) > d \ (\textit{or } \mathrm{char}(F) = 0.)}$

Proof.

1. small depth-3 circuit $\implies$ small *homogeneous* depth-5 circuit

Theorem (LST22)

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-d polynomial requiring size

$$n^{\Omega(\sqrt{\log n})},$$

to be computed by algebraic circuits over $\mathbb{F}$, when the depth is $\Delta = 3$; for $d \approx \log n$, $\boxed{\textit{if } \mathrm{char}(F) > d \ \textit{(or } \mathrm{char}(F) = 0\textit{.)}}$

Proof.

1. small depth-3 circuit $\implies$ small *homogeneous* depth-5 circuit
2. small homogeneous depth-5 circuit

Theorem (LST22)

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-d polynomial requiring size

$$n^{\Omega(\sqrt{\log n})},$$

to be computed by algebraic circuits over $\mathbb{F}$, when the depth is $\Delta = 3$; for $d \approx \log n$, $\boxed{\textit{if } \mathrm{char}(F) > d \ \textit{(or } \mathrm{char}(F) = 0.\textit{)}}$

Proof.

1. small depth-3 circuit $\implies$ small *homogeneous* depth-5 circuit
2. small homogeneous depth-5 circuit $\implies$ small *set-multilinear* depth-5 circuit

Theorem (LST22)

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-d polynomial requiring size

$$n^{\Omega(\sqrt{\log n})},$$

to be computed by algebraic circuits over $\mathbb{F}$, when the depth is $\Delta = 3$; for $d \approx \log n$, $\boxed{\textit{if } \mathrm{char}(F) > d \ \textit{(or } \mathrm{char}(F) = 0.\textit{)}}$

Proof.

1. small depth-3 circuit $\implies$ small *homogeneous* depth-5 circuit
2. small homogeneous depth-5 circuit $\implies$ small *set-multilinear* depth-5 circuit
3. find explicit f that has no small set-multilinear depth-5 circuit $\square$

Theorem (LST22)

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-d polynomial requiring size

$$n^{\Omega(\sqrt{\log n})},$$

to be computed by algebraic circuits over $\mathbb{F}$, when the depth is $\Delta = 3$; for $d \approx \log n$, $\boxed{\textit{if } \mathrm{char}(F) > d \ \textit{(or } \mathrm{char}(F) = 0.\textit{)}}$

Proof.

1. small depth-3 circuit $\implies$ small *homogeneous* depth-5 circuit
2. small homogeneous depth-5 circuit $\implies$ small *set-multilinear* depth-5 circuit
3. find explicit f that has no small set-multilinear depth-5 circuit $\square$

Remark

Theorem (LST22)

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-d polynomial requiring size

$$n^{\Omega(\sqrt{\log n})},$$

to be computed by algebraic circuits over $\mathbb{F}$, when the depth is $\Delta = 3$; for $d \approx \log n$, $\boxed{\textit{if } \mathrm{char}(F) > d \textit{ (or } \mathrm{char}(F) = 0.)}$

Proof.

1. small depth-3 circuit $\implies$ small *homogeneous* depth-5 circuit
2. small homogeneous depth-5 circuit $\implies$ small *set-multilinear* depth-5 circuit
3. find explicit f that has no small set-multilinear depth-5 circuit $\square$

Remark

(1) requires large characteristic,

Theorem (LST22)

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-d polynomial requiring size

$$n^{\Omega(\sqrt{\log n})},$$

to be computed by algebraic circuits over $\mathbb{F}$, when the depth is $\Delta = 3$; for $d \approx \log n$,
$\boxed{\textit{if } \mathrm{char}(F) > d \ \textit{(or } \mathrm{char}(F) = 0.\textit{)}}$

Proof.

1. small depth-3 circuit $\implies$ small *homogeneous* depth-5 circuit
2. small homogeneous depth-5 circuit $\implies$ small *set-multilinear* depth-5 circuit
3. find explicit f that has no small set-multilinear depth-5 circuit $\square$

Remark

(1) requires large characteristic, while (2) and (3) work over any field.

Definition

Definition

A polynomial is **homogeneous** if all monomials that appear have the same degree d.

Definition

A polynomial is **homogeneous** if all monomials that appear have the same degree d.
A circuit is **homogeneous** if all gates compute homogeneous polynomials.

Definition

A polynomial is **homogeneous** if all monomials that appear have the same degree d.
A circuit is **homogeneous** if all gates compute homogeneous polynomials.

e.g. the **elementary symmetric polynomial**

Definition

A polynomial is **homogeneous** if all monomials that appear have the same degree d.
A circuit is **homogeneous** if all gates compute homogeneous polynomials.

e.g. the **elementary symmetric polynomial**

$$\mathrm{esym}_{n,d} =$$

Definition

A polynomial is **homogeneous** if all monomials that appear have the same degree d.
A circuit is **homogeneous** if all gates compute homogeneous polynomials.

e.g. the **elementary symmetric polynomial**

$$\mathrm{esym}_{n,d} = \sum_{S \subseteq [n],}$$

Definition

A polynomial is **homogeneous** if all monomials that appear have the same degree d.
A circuit is **homogeneous** if all gates compute homogeneous polynomials.

e.g. the **elementary symmetric polynomial**

$$\mathrm{esym}_{n,d} = \sum_{S \subseteq [n], |S| = d}$$

Definition

A polynomial is **homogeneous** if all monomials that appear have the same degree d.
A circuit is **homogeneous** if all gates compute homogeneous polynomials.

e.g. the **elementary symmetric polynomial**

$$\mathrm{esym}_{n,d} = \sum_{S \subseteq [n], |S|=d} \prod_{i \in S} x_i \ ,$$

Definition

A polynomial is **homogeneous** if all monomials that appear have the same degree d.
A circuit is **homogeneous** if all gates compute homogeneous polynomials.

e.g. the **elementary symmetric polynomial**

$$\mathrm{esym}_{n,d} = \sum_{S \subseteq [n], |S| = d} \prod_{i \in S} x_i \ ,$$

is homogeneous of degree d.

Definition

A polynomial is **homogeneous** if all monomials that appear have the same degree d.
A circuit is **homogeneous** if all gates compute homogeneous polynomials.

e.g. the **elementary symmetric polynomial**

$$\mathrm{esym}_{n,d} = \sum_{S\subseteq[n],|S|=d} \prod_{i\in S} x_i \ ,$$

is homogeneous of degree d.

Definition

Definition

A polynomial is **homogeneous** if all monomials that appear have the same degree d. A circuit is **homogeneous** if all gates compute homogeneous polynomials.

e.g. the **elementary symmetric polynomial**

$$\mathrm{esym}_{n,d} = \sum_{S \subseteq [n], |S| = d} \prod_{i \in S} x_i \ ,$$

is homogeneous of degree d.

Definition

Let the variables be partitioned into $x_{1,1}, \ldots, x_{1,n}$,

Definition

A polynomial is **homogeneous** if all monomials that appear have the same degree d.
A circuit is **homogeneous** if all gates compute homogeneous polynomials.

e.g. the **elementary symmetric polynomial**

$$\mathrm{esym}_{n,d} = \sum_{S \subseteq [n], |S| = d} \prod_{i \in S} x_i \ ,$$

is homogeneous of degree d.

Definition

Let the variables be partitioned into $x_{1,1}, \ldots, x_{1,n}, \ \ldots \ , x_{d,1}, \ldots, x_{d,n} =$

Definition

A polynomial is **homogeneous** if all monomials that appear have the same degree d. A circuit is **homogeneous** if all gates compute homogeneous polynomials.

e.g. the **elementary symmetric polynomial**

$$\mathrm{esym}_{n,d} = \sum_{S \subseteq [n], |S|=d} \prod_{i \in S} x_i \ ,$$

is homogeneous of degree d.

Definition

Let the variables be partitioned into $x_{1,1}, \ldots, x_{1,n}, \ \ldots \ , x_{d,1}, \ldots, x_{d,n} = \overline{x}_1, \ldots, \overline{x}_d$.

Definition

A polynomial is **homogeneous** if all monomials that appear have the same degree d.
A circuit is **homogeneous** if all gates compute homogeneous polynomials.

e.g. the **elementary symmetric polynomial**

$$\mathrm{esym}_{n,d} = \sum_{S \subseteq [n], |S| = d} \prod_{i \in S} x_i \ ,$$

is homogeneous of degree d.

Definition

Let the variables be partitioned into $x_{1,1}, \ldots, x_{1,n}, \ \ldots \ , x_{d,1}, \ldots, x_{d,n} = \overline{x}_1, \ldots, \overline{x}_d$.
A monomial is **set-multilinear** if is a product of one variable per $\overline{x}_i$,

Definition

A polynomial is **homogeneous** if all monomials that appear have the same degree d.
A circuit is **homogeneous** if all gates compute homogeneous polynomials.

e.g. the **elementary symmetric polynomial**

$$\mathrm{esym}_{n,d} = \sum_{S \subseteq [n], |S| = d} \prod_{i \in S} x_i \ ,$$

is homogeneous of degree d.

Definition

Let the variables be partitioned into $x_{1,1}, \ldots, x_{1,n}, \ \ldots \ , x_{d,1}, \ldots, x_{d,n} = \overline{x}_1, \ldots, \overline{x}_d$.
A monomial is **set-multilinear** if is a product of one variable per $\overline{x}_i$, e.g. $\prod_{i=1}^{d} x_{i,j_i}$.

Definition

A polynomial is **homogeneous** if all monomials that appear have the same degree d.
A circuit is **homogeneous** if all gates compute homogeneous polynomials.

e.g. the **elementary symmetric polynomial**

$$\mathrm{esym}_{n,d} = \sum_{S \subseteq [n], |S|=d} \prod_{i \in S} x_i \; ,$$

is homogeneous of degree d.

Definition

Let the variables be partitioned into $x_{1,1}, \ldots, x_{1,n}, \;\ldots\;, x_{d,1}, \ldots, x_{d,n} = \overline{x}_1, \ldots, \overline{x}_d$.
A monomial is **set-multilinear** if is a product of one variable per $\overline{x}_i$, e.g. $\prod_{i=1}^{d} x_{i,j_i}$. A polynomial is **set-multilinear** if all monomials are set-multilinear.

Definition

A polynomial is **homogeneous** if all monomials that appear have the same degree d. A circuit is **homogeneous** if all gates compute homogeneous polynomials.

e.g. the **elementary symmetric polynomial**

$$\mathrm{esym}_{n,d} = \sum_{S \subseteq [n], |S| = d} \prod_{i \in S} x_i \ ,$$

is homogeneous of degree d.

Definition

Let the variables be partitioned into $x_{1,1}, \ldots, x_{1,n}, \ \ldots \ , x_{d,1}, \ldots, x_{d,n} = \overline{x}_1, \ldots, \overline{x}_d$. A monomial is **set-multilinear** if is a product of one variable per $\overline{x}_i$, e.g. $\prod_{i=1}^{d} x_{i,j_i}$. A polynomial is **set-multilinear** if all monomials are set-multilinear. A circuit is **set-multilinear** if all gates compute set-multilinear polynomials.

Definition

A polynomial is **homogeneous** if all monomials that appear have the same degree d. A circuit is **homogeneous** if all gates compute homogeneous polynomials.

e.g. the **elementary symmetric polynomial**

$$\mathrm{esym}_{n,d} = \sum_{S \subseteq [n], |S|=d} \prod_{i \in S} x_i \ ,$$

is homogeneous of degree d.

Definition

Let the variables be partitioned into $x_{1,1}, \ldots, x_{1,n}, \ \ldots \ , x_{d,1}, \ldots, x_{d,n} = \overline{x}_1, \ldots, \overline{x}_d$. A monomial is **set-multilinear** if is a product of one variable per $\overline{x}_i$, e.g. $\prod_{i=1}^{d} x_{i,j_i}$. A polynomial is **set-multilinear** if all monomials are set-multilinear. A circuit is **set-multilinear** if all gates compute set-multilinear polynomials.

e.g.

Definition

A polynomial is **homogeneous** if all monomials that appear have the same degree d. A circuit is **homogeneous** if all gates compute homogeneous polynomials.

e.g. the **elementary symmetric polynomial**

$$\mathrm{esym}_{n,d} = \sum_{S \subseteq [n], |S| = d} \prod_{i \in S} x_i \ ,$$

is homogeneous of degree d.

Definition

Let the variables be partitioned into $x_{1,1}, \ldots, x_{1,n}, \ \ldots \ , x_{d,1}, \ldots, x_{d,n} = \overline{x}_1, \ldots, \overline{x}_d$. A monomial is **set-multilinear** if is a product of one variable per $\overline{x}_i$, e.g. $\prod_{i=1}^{d} x_{i,j_i}$. A polynomial is **set-multilinear** if all monomials are set-multilinear. A circuit is **set-multilinear** if all gates compute set-multilinear polynomials.

e.g. the **rectangular permanent**

Definition

A polynomial is **homogeneous** if all monomials that appear have the same degree d. A circuit is **homogeneous** if all gates compute homogeneous polynomials.

e.g. the **elementary symmetric polynomial**

$$\mathrm{esym}_{n,d} = \sum_{S \subseteq [n], |S| = d} \prod_{i \in S} x_i \ ,$$

is homogeneous of degree d.

Definition

Let the variables be partitioned into $x_{1,1}, \ldots, x_{1,n}, \ \ldots \ , x_{d,1}, \ldots, x_{d,n} = \overline{x}_1, \ldots, \overline{x}_d$. A monomial is **set-multilinear** if is a product of one variable per $\overline{x}_i$, e.g. $\prod_{i=1}^{d} x_{i,j_i}$. A polynomial is **set-multilinear** if all monomials are set-multilinear. A circuit is **set-multilinear** if all gates compute set-multilinear polynomials.

e.g. the **rectangular permanent**

$$\mathrm{perm}_{n,d} =$$

Definition

A polynomial is **homogeneous** if all monomials that appear have the same degree d. A circuit is **homogeneous** if all gates compute homogeneous polynomials.

e.g. the **elementary symmetric polynomial**

$$\mathrm{esym}_{n,d} = \sum_{S\subseteq[n],|S|=d} \prod_{i\in S} x_i \ ,$$

is homogeneous of degree d.

Definition

Let the variables be partitioned into $x_{1,1},\ldots,x_{1,n}, \ \ldots \ ,x_{d,1},\ldots,x_{d,n} = \overline{x}_1,\ldots,\overline{x}_d$. A monomial is **set-multilinear** if is a product of one variable per $\overline{x}_i$, e.g. $\prod_{i=1}^{d} x_{i,j_i}$. A polynomial is **set-multilinear** if all monomials are set-multilinear. A circuit is **set-multilinear** if all gates compute set-multilinear polynomials.

e.g. the **rectangular permanent**

$$\mathrm{perm}_{n,d} = \sum_{\sigma:[d]\hookrightarrow[n]}$$

Definition

A polynomial is **homogeneous** if all monomials that appear have the same degree d. A circuit is **homogeneous** if all gates compute homogeneous polynomials.

e.g. the **elementary symmetric polynomial**

$$\mathrm{esym}_{n,d} = \sum_{S \subseteq [n], |S| = d} \prod_{i \in S} x_i \ ,$$

is homogeneous of degree d.

Definition

Let the variables be partitioned into $x_{1,1}, \ldots, x_{1,n}, \ \ldots \ , x_{d,1}, \ldots, x_{d,n} = \overline{x}_1, \ldots, \overline{x}_d$. A monomial is **set-multilinear** if is a product of one variable per $\overline{x}_i$, e.g. $\prod_{i=1}^{d} x_{i,j_i}$. A polynomial is **set-multilinear** if all monomials are set-multilinear. A circuit is **set-multilinear** if all gates compute set-multilinear polynomials.

e.g. the **rectangular permanent**

$$\mathrm{perm}_{n,d} = \sum_{\sigma : [d] \hookrightarrow [n]} \prod_{i=1}^{d} x_{i,\sigma(i)}$$

Definition

A polynomial is **homogeneous** if all monomials that appear have the same degree d. A circuit is **homogeneous** if all gates compute homogeneous polynomials.

e.g. the **elementary symmetric polynomial**

$$\mathrm{esym}_{n,d} = \sum_{S \subseteq [n], |S| = d} \prod_{i \in S} x_i ,$$

is homogeneous of degree d.

Definition

Let the variables be partitioned into $x_{1,1}, \ldots, x_{1,n}, \ \ldots \ , x_{d,1}, \ldots, x_{d,n} = \overline{x}_1, \ldots, \overline{x}_d$. A monomial is **set-multilinear** if is a product of one variable per $\overline{x}_i$, e.g. $\prod_{i=1}^{d} x_{i,j_i}$. A polynomial is **set-multilinear** if all monomials are set-multilinear. A circuit is **set-multilinear** if all gates compute set-multilinear polynomials.

e.g. the **rectangular permanent**

$$\mathrm{perm}_{n,d} = \sum_{\sigma : [d] \hookrightarrow [n]} \prod_{i=1}^{d} x_{i,\sigma(i)}$$

is set-multilinear.

Definition

A polynomial is **homogeneous** if all monomials that appear have the same degree d. A circuit is **homogeneous** if all gates compute homogeneous polynomials.

e.g. the **elementary symmetric polynomial**

$$\mathrm{esym}_{n,d} = \sum_{S \subseteq [n], |S| = d} \prod_{i \in S} x_i \ ,$$

is homogeneous of degree d.

Definition

Let the variables be partitioned into $x_{1,1}, \ldots, x_{1,n}, \ \ldots \ , x_{d,1}, \ldots, x_{d,n} = \overline{x}_1, \ldots, \overline{x}_d$. A monomial is **set-multilinear** if is a product of one variable per $\overline{x}_i$, e.g. $\prod_{i=1}^{d} x_{i,j_i}$. A polynomial is **set-multilinear** if all monomials are set-multilinear. A circuit is **set-multilinear** if all gates compute set-multilinear polynomials.

e.g. the **rectangular permanent**

$$\mathrm{perm}_{n,d} = \sum_{\sigma : [d] \hookrightarrow [n]} \prod_{i=1}^{d} x_{i,\sigma(i)}$$

is set-multilinear. When $d = n$ this is the standard permanent.

Question

Question

General circuits versus homogeneous circuits?

Question

General circuits versus homogeneous circuits?

fact:

Question

General circuits versus homogeneous circuits?

fact: small circuit

Question

General circuits versus homogeneous circuits?

fact: small circuit $\implies$ small homogeneous circuit;

Question

General circuits versus homogeneous circuits?

fact: small circuit $\implies$ small homogeneous circuit; but depth blows up.

Question

General circuits versus homogeneous circuits?

fact: small circuit $\implies$ small homogeneous circuit; but depth blows up.

Theorem (SW01,LST22)

Question

General circuits versus homogeneous circuits?

fact: small circuit $\implies$ small homogeneous circuit; but depth blows up.

Theorem (SW01,LST22)

size s depth-3 circuit

Question

General circuits versus homogeneous circuits?

fact: small circuit $\implies$ small homogeneous circuit; but depth blows up.

Theorem (SW01,LST22)

size s depth-3 circuit $\overset{\mathrm{char}(F)>d}{\Longrightarrow}$

Question

General circuits versus homogeneous circuits?

fact: small circuit $\implies$ small homogeneous circuit; but depth blows up.

Theorem (SW01,LST22)

size s depth-3 circuit $\overset{\mathrm{char}(F)>d}{\Longrightarrow}$ *homogeneous depth-5 circuit of size* $\mathrm{poly}(s, 2^{\sqrt{d}})$.

Question

General circuits versus homogeneous circuits?

fact: small circuit $\implies$ small homogeneous circuit; but depth blows up.

Theorem (SW01,LST22)

size s depth-3 circuit $\overset{\mathrm{char}(F)>d}{\Longrightarrow}$ *homogeneous depth-5 circuit of size* $\mathrm{poly}(s, 2^{\sqrt{d}})$.

Theorem (SW01)

Question

General circuits versus homogeneous circuits?

fact: small circuit $\implies$ small homogeneous circuit; but depth blows up.

Theorem (SW01,LST22)

size s depth-3 circuit $\overset{\text{char}(F)>d}{\implies}$ *homogeneous depth-5 circuit of size* $\text{poly}(s, 2^{\sqrt{d}})$.

Theorem (SW01)

The elementary symmetric polynomial $\text{esym}_{n,d} =$

Question

General circuits versus homogeneous circuits?

fact: small circuit $\implies$ small homogeneous circuit; but depth blows up.

Theorem (SW01,LST22)

size s depth-3 circuit $\overset{\mathrm{char}(F)>d}{\Longrightarrow}$ *homogeneous depth-5 circuit of size* $\mathrm{poly}(s, 2^{\sqrt{d}})$.

Theorem (SW01)

The elementary symmetric polynomial $\mathrm{esym}_{n,d} = \sum_{S\subseteq[n],|S|=d} \prod_{i\in S} x_i$

Question

General circuits versus homogeneous circuits?

fact: small circuit $\implies$ small homogeneous circuit; but depth blows up.

Theorem (SW01,LST22)

size s depth-3 circuit $\overset{\mathrm{char}(F)>d}{\Longrightarrow}$ *homogeneous depth-5 circuit of size* $\mathrm{poly}(s, 2^{\sqrt{d}})$.

Theorem (SW01)

The elementary symmetric polynomial $\mathrm{esym}_{n,d} = \sum_{S\subseteq[n],|S|=d} \prod_{i\in S} x_i$ *has a homogeneous depth-4 circuit of size* $\mathrm{poly}(n, 2^{\sqrt{d}})$,

Question

General circuits versus homogeneous circuits?

fact: small circuit $\implies$ small homogeneous circuit; but depth blows up.

Theorem (SW01,LST22)

size s depth-3 circuit $\overset{\mathrm{char}(F)>d}{\Longrightarrow}$ *homogeneous depth-5 circuit of size* $\mathrm{poly}(s, 2^{\sqrt{d}})$.

Theorem (SW01)

The elementary symmetric polynomial $\mathrm{esym}_{n,d} = \sum_{S \subseteq [n], |S|=d} \prod_{i \in S} x_i$ *has a homogeneous depth-4 circuit of size* $\mathrm{poly}(n, 2^{\sqrt{d}})$, *if* $\mathrm{char}(F) > d$ *(or* $\mathrm{char}(F) = 0$*).*

Question

General circuits versus homogeneous circuits?

fact: small circuit $\implies$ small homogeneous circuit; but depth blows up.

Theorem (SW01,LST22)

size s depth-3 circuit $\overset{\mathrm{char}(F)>d}{\implies}$ *homogeneous depth-5 circuit of size* $\mathrm{poly}(s, 2^{\sqrt{d}})$.

Theorem (SW01)

The elementary symmetric polynomial $\mathrm{esym}_{n,d} = \sum_{S\subseteq[n],|S|=d} \prod_{i\in S} x_i$ *has a homogeneous depth-4 circuit of size* $\mathrm{poly}(n, 2^{\sqrt{d}})$, *if* $\mathrm{char}(F) > d$ *(or* $\mathrm{char}(F) = 0$*).*

Proof.

Question

General circuits versus homogeneous circuits?

fact: small circuit $\implies$ small homogeneous circuit; but depth blows up.

Theorem (SW01,LST22)

size s depth-3 circuit $\overset{\mathrm{char}(F)>d}{\implies}$ *homogeneous depth-5 circuit of size* $\mathrm{poly}(s, 2^{\sqrt{d}})$.

Theorem (SW01)

The elementary symmetric polynomial $\mathrm{esym}_{n,d} = \sum_{S\subseteq[n],|S|=d} \prod_{i\in S} x_i$ *has a homogeneous depth-4 circuit of size* $\mathrm{poly}(n, 2^{\sqrt{d}})$, *if* $\mathrm{char}(F) > d$ *(or* $\mathrm{char}(F) = 0$*).*

Proof.

- use Newton identities relating $\mathrm{esym}_{n,d}$ and $\mathrm{pow}_{n,d} =$

Question

General circuits versus homogeneous circuits?

fact: small circuit $\implies$ small homogeneous circuit; but depth blows up.

Theorem (SW01,LST22)

size s depth-3 circuit $\overset{\mathrm{char}(F)>d}{\implies}$ *homogeneous depth-5 circuit of size* $\mathrm{poly}(s, 2^{\sqrt{d}})$.

Theorem (SW01)

The elementary symmetric polynomial $\mathrm{esym}_{n,d} = \sum_{S\subseteq[n],|S|=d} \prod_{i\in S} x_i$ *has a homogeneous depth-4 circuit of size* $\mathrm{poly}(n, 2^{\sqrt{d}})$, *if* $\mathrm{char}(F) > d$ *(or* $\mathrm{char}(F) = 0$*).*

Proof.

- use Newton identities relating $\mathrm{esym}_{n,d}$ and $\mathrm{pow}_{n,d} = \sum_{i=1}^{n} x_i^d$

Question

General circuits versus homogeneous circuits?

fact: small circuit $\implies$ small homogeneous circuit; but depth blows up.

Theorem (SW01,LST22)

size s depth-3 circuit $\overset{\mathrm{char}(F)>d}{\Longrightarrow}$ *homogeneous depth-5 circuit of size* $\mathrm{poly}(s, 2^{\sqrt{d}})$.

Theorem (SW01)

The elementary symmetric polynomial $\mathrm{esym}_{n,d} = \sum_{S\subseteq[n],|S|=d} \prod_{i\in S} x_i$ *has a homogeneous depth-4 circuit of size* $\mathrm{poly}(n, 2^{\sqrt{d}})$, *if* $\mathrm{char}(F) > d$ *(or* $\mathrm{char}(F) = 0$*).*

Proof.

- use Newton identities relating $\mathrm{esym}_{n,d}$ and $\mathrm{pow}_{n,d} = \sum_{i=1}^{n} x_i^d$ $(\mathrm{char}(F) > d)$

Question

General circuits versus homogeneous circuits?

fact: small circuit $\implies$ small homogeneous circuit; but depth blows up.

Theorem (SW01,LST22)

size s depth-3 circuit $\overset{\mathrm{char}(F)>d}{\implies}$ *homogeneous depth-5 circuit of size* $\mathrm{poly}(s, 2^{\sqrt{d}})$.

Theorem (SW01)

The elementary symmetric polynomial $\mathrm{esym}_{n,d} = \sum_{S\subseteq[n],|S|=d} \prod_{i\in S} x_i$ *has a homogeneous depth-4 circuit of size* $\mathrm{poly}(n, 2^{\sqrt{d}})$*, if* $\mathrm{char}(F) > d$ *(or* $\mathrm{char}(F) = 0$*).*

Proof.

- use Newton identities relating $\mathrm{esym}_{n,d}$ and $\mathrm{pow}_{n,d} = \sum_{i=1}^{n} x_i^d$ ($\mathrm{char}(F) > d$)
- count integer partitions

$\square$

Theorem (SW01,LST22)

size s depth-3 circuit $\overset{\mathrm{char}(F)>d}{\Longrightarrow}$ *homogeneous depth-5 circuit of size* $\mathrm{poly}(s, 2^{\sqrt{d}})$.

Theorem (SW01,LST22)

size s depth-3 circuit $\overset{\mathrm{char}(F)>d}{\Longrightarrow}$ *homogeneous depth-5 circuit of size* $\mathrm{poly}(s, 2^{\sqrt{d}})$.

idea:

Theorem (SW01,LST22)

size s depth-3 circuit $\stackrel{\mathrm{char}(F)>d}{\Longrightarrow}$ *homogeneous depth-5 circuit of size* $\mathrm{poly}(s, 2^{\sqrt{d}})$.

idea: elementary symmetric polynomials are "homogenization complete"

Theorem (SW01,LST22)

size s depth-3 circuit $\overset{\mathrm{char}(F)>d}{\Longrightarrow}$ *homogeneous depth-5 circuit of size* $\mathrm{poly}(s, 2^{\sqrt{d}})$.

idea: elementary symmetric polynomials are "homogenization complete"

Proof.

Theorem (SW01,LST22)

size s depth-3 circuit $\overset{\mathrm{char}(F)>d}{\Longrightarrow}$ *homogeneous depth-5 circuit of size* $\mathrm{poly}(s, 2^{\sqrt{d}})$.

idea: elementary symmetric polynomials are "homogenization complete"

Proof.

- f homogeneous degree d,

Theorem (SW01,LST22)

size s depth-3 circuit $\overset{\mathrm{char}(F)>d}{\Longrightarrow}$ *homogeneous depth-5 circuit of size* $\mathrm{poly}(s, 2^{\sqrt{d}})$.

idea: elementary symmetric polynomials are "homogenization complete"

Proof.

- f homogeneous degree d, $f = \sum_{i=1}^{s} \prod_{j=1}^{D} (\alpha_{i,j,0} + \sum_{k=1}^{n} \alpha_{i,j,k} x_k)$

Theorem (SW01,LST22)

size s depth-3 circuit $\overset{\mathrm{char}(F)>d}{\Longrightarrow}$ *homogeneous depth-5 circuit of size* $\mathrm{poly}(s, 2^{\sqrt{d}})$.

idea: elementary symmetric polynomials are "homogenization complete"

Proof.

- f homogeneous degree d, $f = \sum_{i=1}^{s} \prod_{j=1}^{D} (\alpha_{i,j,0} + \sum_{k=1}^{n} \alpha_{i,j,k} x_k)$
- suffices to homogenize each product gate individually

Theorem (SW01,LST22)

size s depth-3 circuit $\overset{\mathrm{char}(F)>d}{\Longrightarrow}$ *homogeneous depth-5 circuit of size* $\mathrm{poly}(s, 2^{\sqrt{d}})$.

idea: elementary symmetric polynomials are "homogenization complete"

Proof.

- f homogeneous degree d, $f = \sum_{i=1}^{s} \prod_{j=1}^{D} (\alpha_{i,j,0} + \sum_{k=1}^{n} \alpha_{i,j,k} x_k)$
- suffices to homogenize each product gate individually

$$\prod_{j=1}^{D} (\beta_{j,0} + \sum_{k=1}^{n} \beta_{j,k} x_k)$$

Theorem (SW01,LST22)

size s depth-3 circuit $\overset{\mathrm{char}(F)>d}{\Longrightarrow}$ *homogeneous depth-5 circuit of size* $\mathrm{poly}(s, 2^{\sqrt{d}})$.

idea: elementary symmetric polynomials are "homogenization complete"

Proof.

- f homogeneous degree d, $f = \sum_{i=1}^{s} \prod_{j=1}^{D} (\alpha_{i,j,0} + \sum_{k=1}^{n} \alpha_{i,j,k} x_k)$
- suffices to homogenize each product gate individually

$$\prod_{j=1}^{D} (\beta_{j,0} + \underbrace{\sum_{k=1}^{n} \beta_{j,k} x_k}_{y_j})$$

Theorem (SW01,LST22)

size s depth-3 circuit $\overset{\mathrm{char}(F)>d}{\Longrightarrow}$ *homogeneous depth-5 circuit of size* $\mathrm{poly}(s, 2^{\sqrt{d}})$.

idea: elementary symmetric polynomials are "homogenization complete"

Proof.

- f homogeneous degree d, $f = \sum_{i=1}^{s} \prod_{j=1}^{D} (\alpha_{i,j,0} + \sum_{k=1}^{n} \alpha_{i,j,k} x_k)$
- suffices to homogenize each product gate individually

$$\prod_{j=1}^{D} (\beta_{j,0} + \underbrace{\sum_{k=1}^{n} \beta_{j,k} x_k}_{y_j}) \approx \prod_{j=1}^{D} (1 + y_j)$$

Theorem (SW01,LST22)

size s depth-3 circuit $\overset{\mathrm{char}(F)>d}{\Longrightarrow}$ *homogeneous depth-5 circuit of size* $\mathrm{poly}(s, 2^{\sqrt{d}})$.

idea: elementary symmetric polynomials are “homogenization complete”

Proof.

- f homogeneous degree d, $f = \sum_{i=1}^{s} \prod_{j=1}^{D} (\alpha_{i,j,0} + \sum_{k=1}^{n} \alpha_{i,j,k} x_k)$
- suffices to homogenize each product gate individually

$$\begin{aligned} \prod_{j=1}^{D} (\beta_{j,0} + \underbrace{\textstyle\sum_{k=1}^{n} \beta_{j,k} x_k}_{y_j}) &\approx \prod_{j=1}^{D} (1 + y_j) \\ &= (1 + y_1)(1 + y_2) \cdots (1 + y_D) \end{aligned}$$

Theorem (SW01,LST22)

size s depth-3 circuit $\overset{\mathrm{char}(F)>d}{\Longrightarrow}$ *homogeneous depth-5 circuit of size* $\mathrm{poly}(s, 2^{\sqrt{d}})$.

idea: elementary symmetric polynomials are "homogenization complete"

Proof.

- f homogeneous degree d, $f = \sum_{i=1}^{s} \prod_{j=1}^{D} (\alpha_{i,j,0} + \sum_{k=1}^{n} \alpha_{i,j,k} x_k)$
- suffices to homogenize each product gate individually

$$\begin{aligned}\prod_{j=1}^{D}(\beta_{j,0} + \underbrace{\textstyle\sum_{k=1}^{n} \beta_{j,k} x_k}_{y_j}) &\approx \prod_{j=1}^{D}(1 + y_j) \\ &= (1+y_1)(1+y_2)\cdots(1+y_D) \\ &= \end{aligned}$$

Theorem (SW01,LST22)

size s depth-3 circuit $\overset{\mathrm{char}(F)>d}{\Longrightarrow}$ *homogeneous depth-5 circuit of size* $\mathrm{poly}(s, 2^{\sqrt{d}})$.

idea: elementary symmetric polynomials are "homogenization complete"

Proof.

- f homogeneous degree d, $f = \sum_{i=1}^{s} \prod_{j=1}^{D} (\alpha_{i,j,0} + \sum_{k=1}^{n} \alpha_{i,j,k} x_k)$
- suffices to homogenize each product gate individually

$$\begin{aligned}
\prod_{j=1}^{D} (\beta_{j,0} + \underbrace{\sum_{k=1}^{n} \beta_{j,k} x_k}_{y_j}) &\approx \prod_{j=1}^{D} (1 + y_j) \\
&= (1 + y_1)(1 + y_2) \cdots (1 + y_D) \\
&= 1 +
\end{aligned}$$

Theorem (SW01,LST22)

size s depth-3 circuit $\overset{\mathrm{char}(F)>d}{\Longrightarrow}$ *homogeneous depth-5 circuit of size* $\mathrm{poly}(s, 2^{\sqrt{d}})$.

idea: elementary symmetric polynomials are "homogenization complete"

Proof.

- f homogeneous degree d, $f = \sum_{i=1}^{s} \prod_{j=1}^{D} (\alpha_{i,j,0} + \sum_{k=1}^{n} \alpha_{i,j,k} x_k)$
- suffices to homogenize each product gate individually

$$\begin{aligned}\prod_{j=1}^{D} (\beta_{j,0} + \underbrace{\textstyle\sum_{k=1}^{n} \beta_{j,k} x_k}_{y_j}) &\approx \prod_{j=1}^{D} (1 + y_j) \\ &= (1 + y_1)(1 + y_2) \cdots (1 + y_D) \\ &= 1 + \mathrm{esym}_{D,1}(\overline{y}) +\end{aligned}$$

Theorem (SW01,LST22)

size s depth-3 circuit $\overset{\mathrm{char}(F)>d}{\Longrightarrow}$ *homogeneous depth-5 circuit of size* $\mathrm{poly}(s, 2^{\sqrt{d}})$.

idea: elementary symmetric polynomials are "homogenization complete"

Proof.

- f homogeneous degree d, $f = \sum_{i=1}^{s} \prod_{j=1}^{D} (\alpha_{i,j,0} + \sum_{k=1}^{n} \alpha_{i,j,k} x_k)$
- suffices to homogenize each product gate individually

$$\begin{aligned}
\prod_{j=1}^{D} (\beta_{j,0} + \underbrace{\textstyle\sum_{k=1}^{n} \beta_{j,k} x_k}_{y_j}) &\approx \prod_{j=1}^{D} (1 + y_j) \\
&= (1 + y_1)(1 + y_2) \cdots (1 + y_D) \\
&= 1 + \mathrm{esym}_{D,1}(\overline{y}) + \cdots + \mathrm{esym}_{D,d}(\overline{y}) + \cdots
\end{aligned}$$

Theorem (SW01,LST22)

size s depth-3 circuit $\overset{\mathrm{char}(F)>d}{\Longrightarrow}$ *homogeneous depth-5 circuit of size* $\mathrm{poly}(s, 2^{\sqrt{d}})$.

idea: elementary symmetric polynomials are "homogenization complete"

Proof.

- f homogeneous degree d, $f = \sum_{i=1}^{s} \prod_{j=1}^{D} (\alpha_{i,j,0} + \sum_{k=1}^{n} \alpha_{i,j,k} x_k)$
- suffices to homogenize each product gate individually

$$\begin{aligned}\prod_{j=1}^{D}(\beta_{j,0} + \underbrace{\textstyle\sum_{k=1}^{n} \beta_{j,k} x_k}_{y_j}) &\approx \prod_{j=1}^{D}(1 + y_j) \\ &= (1+y_1)(1+y_2)\cdots(1+y_D) \\ &= 1 + \mathrm{esym}_{D,1}(\overline{y}) + \cdots + \mathrm{esym}_{D,d}(\overline{y}) + \cdots\end{aligned}$$

- the relevant component is $\mathrm{esym}_{D,d}(\overline{y})$

Theorem (SW01,LST22)

size s depth-3 circuit $\overset{\mathrm{char}(F)>d}{\Longrightarrow}$ *homogeneous depth-5 circuit of size* $\mathrm{poly}(s, 2^{\sqrt{d}})$.

idea: elementary symmetric polynomials are "homogenization complete"

Proof.

- f homogeneous degree d, $f = \sum_{i=1}^{s} \prod_{j=1}^{D} (\alpha_{i,j,0} + \sum_{k=1}^{n} \alpha_{i,j,k} x_k)$
- suffices to homogenize each product gate individually

$$\begin{aligned}
\prod_{j=1}^{D} (\beta_{j,0} + \underbrace{\textstyle\sum_{k=1}^{n} \beta_{j,k} x_k}_{y_j}) &\approx \prod_{j=1}^{D} (1 + y_j) \\
&= (1 + y_1)(1 + y_2) \cdots (1 + y_D) \\
&= 1 + \mathrm{esym}_{D,1}(\overline{y}) + \cdots + \mathrm{esym}_{D,d}(\overline{y}) + \cdots
\end{aligned}$$

- the relevant component is $\mathrm{esym}_{D,d}(\overline{y})$
- apply depth-4 homog circuit for $\mathrm{esym}_{D,d}$ to homogeneous $y_j \leftarrow \sum_{k=1}^{n} \beta_{j,k} x_k$ □

Question (LST22b, GHT22, FLST23)

Question (LST22b, GHT22, FLST23)

Compute $\mathrm{esym}_{n,d}$

Question (LST22b, GHT22, FLST23)

Compute $\mathrm{esym}_{n,d}$ *by size* $\mathrm{poly}(n, 2^{\sqrt{d}})$ *homog depth-4 circuit,*

Question (LST22b, GHT22, FLST23)

Compute $\mathrm{esym}_{n,d}$ *by size* $\mathrm{poly}(n, 2^{\sqrt{d}})$ *homog depth-4 circuit, over* **any** *field?*

Question (LST22b, GHT22, FLST23)

Compute $\mathrm{esym}_{n,d}$ *by size* $\mathrm{poly}(n, 2^{\sqrt{d}})$ *homog depth-4 circuit, over* **any** *field?*
Compute $\mathrm{esym}_{n,d}$ *by size* $\mathrm{poly}(n, O_d(1))$

Question (LST22b, GHT22, FLST23)

Compute $\mathrm{esym}_{n,d}$ *by size* $\mathrm{poly}(n, 2^{\sqrt{d}})$ *homog depth-4 circuit, over* **any** *field?*
Compute $\mathrm{esym}_{n,d}$ *by size* $\mathrm{poly}(n, O_d(1))$ *homog* $O(1)$*-depth*

Question (LST22b, GHT22, FLST23)

Compute $\mathrm{esym}_{n,d}$ *by size* $\mathrm{poly}(n, 2^{\sqrt{d}})$ *homog depth-4 circuit, over* **any** *field?*
Compute $\mathrm{esym}_{n,d}$ *by size* $\mathrm{poly}(n, O_d(1))$ *homog* $O(1)$*-depth circuit, over* **any** *field?*

Question (LST22b, GHT22, FLST23)

Compute $\mathrm{esym}_{n,d}$ *by size* $\mathrm{poly}(n, 2^{\sqrt{d}})$ *homog depth-4 circuit, over* **any** *field?*
Compute $\mathrm{esym}_{n,d}$ *by size* $\mathrm{poly}(n, O_d(1))$ *homog* $O(1)$*-depth circuit, over* **any** *field?*

Answer

Question (LST22b, GHT22, FLST23)

Compute $\mathrm{esym}_{n,d}$ *by size* $\mathrm{poly}(n, 2^{\sqrt{d}})$ *homog depth-4 circuit, over* **any** *field?*
Compute $\mathrm{esym}_{n,d}$ *by size* $\mathrm{poly}(n, O_d(1))$ *homog* $O(1)$*-depth circuit, over* **any** *field?*

Answer

1. *I don't know.*

Question (LST22b, GHT22, FLST23)

Compute $\mathrm{esym}_{n,d}$ *by size* $\mathrm{poly}(n, 2^{\sqrt{d}})$ *homog depth-4 circuit, over* **any** *field?*
Compute $\mathrm{esym}_{n,d}$ *by size* $\mathrm{poly}(n, O_d(1))$ *homog* $O(1)$*-depth circuit, over* **any** *field?*

Answer

1. *I don't know.*
2. *no "Newton-like" identities for* $\mathrm{esym}_{n,d}$ *in small characteristic [FLST23]*

Question (LST22b, GHT22, FLST23)

Compute $\mathrm{esym}_{n,d}$ *by size* $\mathrm{poly}(n, 2^{\sqrt{d}})$ *homog depth-4 circuit, over* **any** *field?*
Compute $\mathrm{esym}_{n,d}$ *by size* $\mathrm{poly}(n, O_d(1))$ *homog* $O(1)$*-depth circuit, over* **any** *field?*

Answer

1. *I don't know.*
2. *no "Newton-like" identities for* $\mathrm{esym}_{n,d}$ *in small characteristic [FLST23]*

Question

Question (LST22b, GHT22, FLST23)

Compute $\mathrm{esym}_{n,d}$ *by size* $\mathrm{poly}(n, 2^{\sqrt{d}})$ *homog depth-4 circuit, over* **any** *field?*
Compute $\mathrm{esym}_{n,d}$ *by size* $\mathrm{poly}(n, O_d(1))$ *homog* $O(1)$*-depth circuit, over* **any** *field?*

Answer

1. *I don't know.*
2. *no "Newton-like" identities for* $\mathrm{esym}_{n,d}$ *in small characteristic [FLST23]*

Question

What **else** *can we do?*

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-$\Theta(\log n)$ polynomial requiring size $n^{\Omega(\sqrt{\log n})}$ to be computed by depth-3 algebraic circuits over $\mathbb{F}$.

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-$\Theta(\log n)$ polynomial requiring size $n^{\Omega(\sqrt{\log n})}$ to be computed by depth-3 algebraic circuits over $\mathbb{F}$.

idea:

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-$\Theta(\log n)$ polynomial requiring size $n^{\Omega(\sqrt{\log n})}$ to be computed by depth-3 algebraic circuits over $\mathbb{F}$.

idea: transfer the result over characteristic zero to arbitrary fields,

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-$\Theta(\log n)$ polynomial requiring size $n^{\Omega(\sqrt{\log n})}$ to be computed by depth-3 algebraic circuits over $\mathbb{F}$.

idea: transfer the result over characteristic zero to arbitrary fields, via "logic"

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-$\Theta(\log n)$ polynomial requiring size $n^{\Omega(\sqrt{\log n})}$ to be computed by depth-3 algebraic circuits over $\mathbb{F}$.

idea: transfer the result over characteristic zero to arbitrary fields, via "logic"

Lemma

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-$\Theta(\log n)$ polynomial requiring size $n^{\Omega(\sqrt{\log n})}$ to be computed by depth-3 algebraic circuits over $\mathbb{F}$.

idea: transfer the result over characteristic zero to arbitrary fields, via "logic"

Lemma

$p(\overline{x}) \in \mathbb{Z}[\overline{x}]$,

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-$\Theta(\log n)$ polynomial requiring size $n^{\Omega(\sqrt{\log n})}$ to be computed by depth-3 algebraic circuits over $\mathbb{F}$.

idea: <u>transfer</u> the result over characteristic zero to arbitrary fields, via "logic"

Lemma

$p(\overline{x}) \in \mathbb{Z}[\overline{x}]$, $\mathbb{F}$ any field.

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-$\Theta(\log n)$ polynomial requiring size $n^{\Omega(\sqrt{\log n})}$ to be computed by depth-3 algebraic circuits over $\mathbb{F}$.

idea: transfer the result over characteristic zero to arbitrary fields, via "logic"

Lemma

$p(\overline{x}) \in \mathbb{Z}[\overline{x}]$, $\mathbb{F}$ *any field.* $p(\overline{x}) = 0$

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-$\Theta(\log n)$ polynomial requiring size $n^{\Omega(\sqrt{\log n})}$ to be computed by depth-3 algebraic circuits over $\mathbb{F}$.

idea: transfer the result over characteristic zero to arbitrary fields, via "logic"

Lemma

$p(\overline{x}) \in \mathbb{Z}[\overline{x}]$, $\mathbb{F}$ *any field.* $p(\overline{x}) = 0$ *(in* $\mathbb{Z}[\overline{x}]$*)*

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-$\Theta(\log n)$ polynomial requiring size $n^{\Omega(\sqrt{\log n})}$ to be computed by depth-3 algebraic circuits over $\mathbb{F}$.

idea: transfer the result over characteristic zero to arbitrary fields, via "logic"

Lemma

$p(\overline{x}) \in \mathbb{Z}[\overline{x}]$, $\mathbb{F}$ any field. $p(\overline{x}) = 0$ (in $\mathbb{Z}[\overline{x}]$) $\implies$ $p(\overline{x}) = 0$,

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-$\Theta(\log n)$ polynomial requiring size $n^{\Omega(\sqrt{\log n})}$ to be computed by depth-3 algebraic circuits over $\mathbb{F}$.

idea: transfer the result over characteristic zero to arbitrary fields, via "logic"

Lemma

$p(\overline{x}) \in \mathbb{Z}[\overline{x}]$, $\mathbb{F}$ *any field.* $p(\overline{x}) = 0$ *(in $\mathbb{Z}[\overline{x}]$)* $\Longrightarrow$ $p(\overline{x}) = 0$, *in* $\mathbb{F}[\overline{x}]$.

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-$\Theta(\log n)$ polynomial requiring size $n^{\Omega(\sqrt{\log n})}$ to be computed by depth-3 algebraic circuits over $\mathbb{F}$.

idea: transfer the result over characteristic zero to arbitrary fields, via "logic"

Lemma

$p(\overline{x}) \in \mathbb{Z}[\overline{x}]$, $\mathbb{F}$ any field. $p(\overline{x}) = 0$ (in $\mathbb{Z}[\overline{x}]$) $\implies$ $p(\overline{x}) = 0$, in $\mathbb{F}[\overline{x}]$.

- $\det(X)\det(Y) = \det(XY)$

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-$\Theta(\log n)$ polynomial requiring size $n^{\Omega(\sqrt{\log n})}$ to be computed by depth-3 algebraic circuits over $\mathbb{F}$.

idea: transfer the result over characteristic zero to arbitrary fields, via "logic"

Lemma

$p(\overline{x}) \in \mathbb{Z}[\overline{x}]$, $\mathbb{F}$ any field. $p(\overline{x}) = 0$ (in $\mathbb{Z}[\overline{x}]$) $\implies$ $p(\overline{x}) = 0$, in $\mathbb{F}[\overline{x}]$.

- $\det(X)\det(Y) = \det(XY)$
- Cayley-Hamilton theorem

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-$\Theta(\log n)$ polynomial requiring size $n^{\Omega(\sqrt{\log n})}$ to be computed by depth-3 algebraic circuits over $\mathbb{F}$.

idea: transfer the result over characteristic zero to arbitrary fields, via "logic"

Lemma

$p(\overline{x}) \in \mathbb{Z}[\overline{x}]$, $\mathbb{F}$ any field. $p(\overline{x}) = 0$ (in $\mathbb{Z}[\overline{x}]$) $\implies$ $p(\overline{x}) = 0$, in $\mathbb{F}[\overline{x}]$.

- $\det(X)\det(Y) = \det(XY)$
- Cayley-Hamilton theorem
  - restate as identity in $\mathbb{Z}[X]$

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-$\Theta(\log n)$ polynomial requiring size $n^{\Omega(\sqrt{\log n})}$ to be computed by depth-3 algebraic circuits over $\mathbb{F}$.

idea: transfer the result over characteristic zero to arbitrary fields, via "logic"

Lemma

$p(\overline{x}) \in \mathbb{Z}[\overline{x}]$, $\mathbb{F}$ any field. $p(\overline{x}) = 0$ (in $\mathbb{Z}[\overline{x}]$) $\implies$ $p(\overline{x}) = 0$, in $\mathbb{F}[\overline{x}]$.

- $\det(X)\det(Y) = \det(XY)$
- Cayley-Hamilton theorem
  - restate as identity in $\mathbb{Z}[X]$
  - prove identity over $\mathbb{C}$ using *analytic* methods

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-$\Theta(\log n)$ polynomial requiring size $n^{\Omega(\sqrt{\log n})}$ to be computed by depth-3 algebraic circuits over $\mathbb{F}$.

idea: transfer the result over characteristic zero to arbitrary fields, via "logic"

Lemma

$p(\overline{x}) \in \mathbb{Z}[\overline{x}]$, $\mathbb{F}$ *any field.* $p(\overline{x}) = 0$ *(in* $\mathbb{Z}[\overline{x}]$*)* $\Longrightarrow$ $p(\overline{x}) = 0$, *in* $\mathbb{F}[\overline{x}]$.

- $\det(X)\det(Y) = \det(XY)$
- Cayley-Hamilton theorem
  - restate as identity in $\mathbb{Z}[X]$
  - prove identity over $\mathbb{C}$ using *analytic* methods

$\Longrightarrow$ proof over any $\mathbb{F}$

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-$\Theta(\log n)$ polynomial requiring size $n^{\Omega(\sqrt{\log n})}$ to be computed by depth-3 algebraic circuits over $\mathbb{F}$.

idea: transfer the result over characteristic zero to arbitrary fields, via "logic"

Lemma

$p(\overline{x}) \in \mathbb{Z}[\overline{x}]$, $\mathbb{F}$ any field. $p(\overline{x}) = 0$ (in $\mathbb{Z}[\overline{x}]$) $\implies$ $p(\overline{x}) = 0$, in $\mathbb{F}[\overline{x}]$.

- $\det(X)\det(Y) = \det(XY)$
- Cayley-Hamilton theorem
  - restate as identity in $\mathbb{Z}[X]$
  - prove identity over $\mathbb{C}$ using *analytic* methods

$\implies$ proof over any $\mathbb{F}$

Goal

Express LST as polynomial identity over $\mathbb{Z}$,

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-$\Theta(\log n)$ polynomial requiring size $n^{\Omega(\sqrt{\log n})}$ to be computed by depth-3 algebraic circuits over $\mathbb{F}$.

idea: transfer the result over characteristic zero to arbitrary fields, via "logic"

Lemma

$p(\overline{x}) \in \mathbb{Z}[\overline{x}]$, $\mathbb{F}$ any field. $p(\overline{x}) = 0$ (in $\mathbb{Z}[\overline{x}]$) $\implies$ $p(\overline{x}) = 0$, in $\mathbb{F}[\overline{x}]$.

- $\det(X)\det(Y) = \det(XY)$
- Cayley-Hamilton theorem
  - restate as identity in $\mathbb{Z}[X]$
  - prove identity over $\mathbb{C}$ using *analytic* methods

$\implies$ proof over any $\mathbb{F}$

Goal

Express LST as polynomial identity over $\mathbb{Z}$, then transfer identity to every $\mathbb{F}$.

Metafact

Metafact

Most algebraic circuit lower bounds proven through **rank methods**,

Metafact

Most algebraic circuit lower bounds proven through **rank methods**, *including LST.*

Metafact

Most algebraic circuit lower bounds proven through **rank methods**, *including LST.*

- $P(\overline{x})$ *has small ckt*

Metafact

Most algebraic circuit lower bounds proven through **rank methods**, *including LST.*

- $P(\overline{x})$ *has small ckt* $\implies$ *matrix* M_P

Metafact

Most algebraic circuit lower bounds proven through **rank methods**, *including LST.*

- $P(\overline{x})$ *has small ckt* $\implies$ *matrix* M_P *with* $\mathrm{rank}_{\mathbb{F}} M_P$ *small*

Metafact

Most algebraic circuit lower bounds proven through **rank methods**, *including LST.*

- $P(\overline{x})$ *has small ckt* $\implies$ *matrix* M_P *with* $\mathrm{rank}_{\mathbb{F}} M_P$ *small*

- *exhibit* $f(\overline{x})$ *with* $\mathrm{rank}_{\mathbb{F}} M_f$ *large*

Metafact

Most algebraic circuit lower bounds proven through **rank methods**, *including LST.*

- $P(\overline{x})$ *has small ckt* $\implies$ *matrix* M_P *with* $\operatorname{rank}_{\mathbb{F}} M_P$ *small*

- *exhibit* $f(\overline{x})$ *with* $\operatorname{rank}_{\mathbb{F}} M_f$ *large*

$\implies$ f *requires large circuits*

Metafact

Most algebraic circuit lower bounds proven through **rank methods**, *including LST.*

- $P(\overline{x})$ *has small ckt* $\implies$ *matrix* M_P *with* $\operatorname{rank}_{\mathbb{F}} M_P$ *small*
  - *each entry of* M_P *is a linear combination of the coefficients of* P
- *exhibit* $f(\overline{x})$ *with* $\operatorname{rank}_{\mathbb{F}} M_f$ *large*

$\implies$ f *requires large circuits*

Metafact

Most algebraic circuit lower bounds proven through **rank methods**, *including LST.*

- $P(\overline{x})$ *has small ckt* $\implies$ *matrix* M_P *with* $\operatorname{rank}_{\mathbb{F}} M_P$ *small*
  - *each entry of* M_P *is a (often* **integer***) linear combination of the coefficients of* P
- *exhibit* $f(\overline{x})$ *with* $\operatorname{rank}_{\mathbb{F}} M_f$ *large*

$\implies$ f *requires large circuits*

Metafact

Most algebraic circuit lower bounds proven through **rank methods**, *including LST.*

- $P(\overline{x})$ *has small ckt* $\implies$ *matrix* M_P *with* $\text{rank}_{\mathbb{F}} M_P$ *small*
  - *each entry of* M_P *is a (often* **integer***) linear combination of the coefficients of* P
    - $M_{g+h} = M_g + M_h$
- *exhibit* $f(\overline{x})$ *with* $\text{rank}_{\mathbb{F}} M_f$ *large*

$\implies$ f *requires large circuits*

Metafact

Most algebraic circuit lower bounds proven through **rank methods**, *including LST.*

- $P(\overline{x})$ *has small ckt* $\implies$ *matrix* M_P *with* $\operatorname{rank}_{\mathbb{F}} M_P$ *small*
  - *each entry of* M_P *is a (often* **integer***) linear combination of the coefficients of* P
    - $M_{g+h} = M_g + M_h$
    - $\operatorname{rank} M_{g+h} \le \operatorname{rank} M_g + \operatorname{rank} M_h$
- *exhibit* $f(\overline{x})$ *with* $\operatorname{rank}_{\mathbb{F}} M_f$ *large*

$\implies$ f *requires large circuits*

Metafact

Most algebraic circuit lower bounds proven through **rank methods**, *including LST.*

- $P(\overline{x})$ *has small ckt* $\implies$ *matrix* M_P *with* $\operatorname{rank}_{\mathbb{F}} M_P$ *small*
  - *each entry of* M_P *is a (often* **integer***) linear combination of the coefficients of* P
    - $M_{g+h} = M_g + M_h$
    - $\operatorname{rank} M_{g+h} \leq \operatorname{rank} M_g + \operatorname{rank} M_h$
- *exhibit* $f(\overline{x})$ *with* $\operatorname{rank}_{\mathbb{F}} M_f$ *large*

$\implies$ f *requires large circuits*

Example

Metafact

Most algebraic circuit lower bounds proven through **rank methods**, *including LST.*

- $P(\overline{x})$ *has small ckt* $\implies$ *matrix* M_P *with* $\operatorname{rank}_{\mathbb{F}} M_P$ *small*
  - *each entry of* M_P *is a (often* **integer***) linear combination of the coefficients of* P
    - $M_{g+h} = M_g + M_h$
    - $\operatorname{rank} M_{g+h} \leq \operatorname{rank} M_g + \operatorname{rank} M_h$
- *exhibit* $f(\overline{x})$ *with* $\operatorname{rank}_{\mathbb{F}} M_f$ *large*

$\implies$ f *requires large circuits*

Example

$P(x) = ax^2 + bx + c.$

Metafact

Most algebraic circuit lower bounds proven through **rank methods**, *including LST.*

- $P(\overline{x})$ *has small ckt* $\implies$ *matrix* M_P *with* $\operatorname{rank}_{\mathbb{F}} M_P$ *small*
    - *each entry of* M_P *is a (often* **integer***) linear combination of the coefficients of* P
        - $M_{g+h} = M_g + M_h$
        - $\operatorname{rank} M_{g+h} \leq \operatorname{rank} M_g + \operatorname{rank} M_h$
- *exhibit* $f(\overline{x})$ *with* $\operatorname{rank}_{\mathbb{F}} M_f$ *large*

$\implies$ f *requires large circuits*

Example

$P(x) = ax^2 + bx + c.$

$$M_P =$$

Metafact

Most algebraic circuit lower bounds proven through **rank methods**, *including LST.*

- $P(\overline{x})$ *has small ckt* $\implies$ *matrix* M_P *with* $\operatorname{rank}_{\mathbb{F}} M_P$ *small*
  - *each entry of* M_P *is a (often* **integer***) linear combination of the coefficients of* P
    - $M_{g+h} = M_g + M_h$
    - $\operatorname{rank} M_{g+h} \leq \operatorname{rank} M_g + \operatorname{rank} M_h$
- *exhibit* $f(\overline{x})$ *with* $\operatorname{rank}_{\mathbb{F}} M_f$ *large*

$\implies$ f *requires large circuits*

Example

$P(x) = ax^2 + bx + c.$

$$M_P = \begin{bmatrix} a & \\ & \end{bmatrix}$$

Metafact

Most algebraic circuit lower bounds proven through **rank methods**, *including LST.*

- $P(\overline{x})$ *has small ckt* $\implies$ *matrix* M_P *with* $\operatorname{rank}_{\mathbb{F}} M_P$ *small*
  - *each entry of* M_P *is a (often* **integer***) linear combination of the coefficients of* P
    - $M_{g+h} = M_g + M_h$
    - $\operatorname{rank} M_{g+h} \leq \operatorname{rank} M_g + \operatorname{rank} M_h$
- *exhibit* $f(\overline{x})$ *with* $\operatorname{rank}_{\mathbb{F}} M_f$ *large*

$\implies$ f *requires large circuits*

Example

$P(x) = ax^2 + bx + c.$

$$M_P = \begin{bmatrix} a & b/2 \\ b/2 & \end{bmatrix}$$

Metafact

Most algebraic circuit lower bounds proven through **rank methods**, *including LST.*

- $P(\overline{x})$ *has small ckt* $\implies$ *matrix* M_P *with* $\operatorname{rank}_{\mathbb{F}} M_P$ *small*
  - *each entry of* M_P *is a (often* **integer***) linear combination of the coefficients of* P
    - $M_{g+h} = M_g + M_h$
    - $\operatorname{rank} M_{g+h} \leq \operatorname{rank} M_g + \operatorname{rank} M_h$
- *exhibit* $f(\overline{x})$ *with* $\operatorname{rank}_{\mathbb{F}} M_f$ *large*

$\implies$ f *requires large circuits*

Example

$P(x) = ax^2 + bx + c.$

$$M_P = \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix}$$

Metafact

Most algebraic circuit lower bounds proven through **rank methods**, *including LST.*

- $P(\overline{x})$ *has small ckt* $\implies$ *matrix* M_P *with* $\operatorname{rank}_{\mathbb{F}} M_P$ *small*
  - *each entry of* M_P *is a (often* **integer***) linear combination of the coefficients of* P
    - $M_{g+h} = M_g + M_h$
    - $\operatorname{rank} M_{g+h} \leq \operatorname{rank} M_g + \operatorname{rank} M_h$
- *exhibit* $f(\overline{x})$ *with* $\operatorname{rank}_{\mathbb{F}} M_f$ *large*

$\implies$ f *requires large circuits*

Example

$P(x) = ax^2 + bx + c$.

$$M_P = \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix}$$

$P = \alpha(x - \beta)^2$ iff

Metafact

Most algebraic circuit lower bounds proven through **rank methods**, *including LST.*

- $P(\overline{x})$ *has small ckt* $\implies$ *matrix* M_P *with* $\operatorname{rank}_{\mathbb{F}} M_P$ *small*
    - *each entry of* M_P *is a (often* **integer***) linear combination of the coefficients of* P
        - $M_{g+h} = M_g + M_h$
        - $\operatorname{rank} M_{g+h} \leq \operatorname{rank} M_g + \operatorname{rank} M_h$
- *exhibit* $f(\overline{x})$ *with* $\operatorname{rank}_{\mathbb{F}} M_f$ *large*

$\implies$ f *requires large circuits*

Example

$P(x) = ax^2 + bx + c.$

$$M_P = \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix}$$

$P = \alpha(x-\beta)^2$ iff $b^2 - 4ac = 0$ iff

Metafact

Most algebraic circuit lower bounds proven through **rank methods**, *including LST.*

- $P(\overline{x})$ *has small ckt* $\implies$ *matrix* M_P *with* $\operatorname{rank}_{\mathbb{F}} M_P$ *small*
  - *each entry of* M_P *is a (often* **integer***) linear combination of the coefficients of* P
    - $M_{g+h} = M_g + M_h$
    - $\operatorname{rank} M_{g+h} \leq \operatorname{rank} M_g + \operatorname{rank} M_h$
- *exhibit* $f(\overline{x})$ *with* $\operatorname{rank}_{\mathbb{F}} M_f$ *large*

$\implies$ f *requires large circuits*

Example

$P(x) = ax^2 + bx + c.$

$$M_P = \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix}$$

$P = \alpha(x - \beta)^2$ iff $b^2 - 4ac = 0$ iff $\det M_P = 0$ iff

Metafact

Most algebraic circuit lower bounds proven through **rank methods**, *including LST.*

- $P(\overline{x})$ *has small ckt* $\implies$ *matrix* M_P *with* $\operatorname{rank}_{\mathbb{F}} M_P$ *small*
  - *each entry of* M_P *is a (often* **integer***) linear combination of the coefficients of* P
    - $M_{g+h} = M_g + M_h$
    - $\operatorname{rank} M_{g+h} \leq \operatorname{rank} M_g + \operatorname{rank} M_h$
- *exhibit* $f(\overline{x})$ *with* $\operatorname{rank}_{\mathbb{F}} M_f$ *large*

$\implies$ f *requires large circuits*

Example

$P(x) = ax^2 + bx + c.$

$$M_P = \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix}$$

$P = \alpha(x - \beta)^2$ iff $b^2 - 4ac = 0$ iff $\det M_P = 0$ iff $\operatorname{rank} M_P = 1$.

Question

Question

Phrase the rank method as a polynomial identity?

Question

Phrase the rank method as a polynomial identity?

Lemma

Question

Phrase the rank method as a polynomial identity?

Lemma

M matrix,

Question

Phrase the rank method as a polynomial identity?

Lemma

M matrix, $M \in \mathbb{F}^{n\times m}$.

Question

Phrase the rank method as a polynomial identity?

Lemma

M matrix, $M \in \mathbb{F}^{n\times m}$. $\operatorname{rank}_{\mathbb{F}} M \leq r$ iff

Question

Phrase the rank method as a polynomial identity?

Lemma

M matrix, $M \in \mathbb{F}^{n \times m}$. $\operatorname{rank}_{\mathbb{F}} M \leq r$ iff all $(r+1) \times (r+1)$ submatrices $M|_{S \times T}$

Question

Phrase the rank method as a polynomial identity?

Lemma

M matrix, $M \in \mathbb{F}^{n\times m}$. $\operatorname{rank}_{\mathbb{F}} M \leq r$ *iff all* $(r+1)\times(r+1)$ *submatrices* $M|_{S\times T}$ *have* $\det M|_{S\times T} = 0$,

Question

Phrase the rank method as a polynomial identity?

Lemma

M matrix, $M \in \mathbb{F}^{n\times m}$. $\operatorname{rank}_{\mathbb{F}} M \leq r$ *iff all* $(r+1)\times(r+1)$ *submatrices* $M|_{S\times T}$ *have* $\det M|_{S\times T} = 0$, $S \subseteq [n]$,

Question

Phrase the rank method as a polynomial identity?

Lemma

M matrix, $M \in \mathbb{F}^{n \times m}$. $\mathrm{rank}_{\mathbb{F}} M \leq r$ *iff all $(r+1) \times (r+1)$ submatrices $M|_{S \times T}$ have* $\det M|_{S \times T} = 0$, $S \subseteq [n]$, $T \subseteq [m]$,

Question

Phrase the rank method as a polynomial identity?

Lemma

M matrix, $M \in \mathbb{F}^{n \times m}$. $\operatorname{rank}_{\mathbb{F}} M \leq r$ *iff all* $(r+1) \times (r+1)$ *submatrices* $M|_{S \times T}$ *have* $\det M|_{S \times T} = 0$, $S \subseteq [n]$, $T \subseteq [m]$, $|S| = |T| = r + 1$.

Question

Phrase the rank method as a polynomial identity?

Lemma

M matrix, $M \in \mathbb{F}^{n\times m}$. $\operatorname{rank}_{\mathbb{F}} M \le r$ iff all $(r+1)\times(r+1)$ submatrices $M|_{S\times T}$ have $\det M|_{S\times T} = 0$, $S \subseteq [n]$, $T \subseteq [m]$, $|S| = |T| = r+1$.

Corollary

Question

Phrase the rank method as a polynomial identity?

Lemma

M matrix, $M \in \mathbb{F}^{n\times m}$. $\operatorname{rank}_{\mathbb{F}} M \le r$ iff all $(r+1)\times(r+1)$ submatrices $M|_{S\times T}$ have $\det M|_{S\times T} = 0$, $S \subseteq [n]$, $T \subseteq [m]$, $|S| = |T| = r+1$.

Corollary

M matrix,

Question

Phrase the rank method as a polynomial identity?

Lemma

M matrix, $M \in \mathbb{F}^{n \times m}$. $\operatorname{rank}_{\mathbb{F}} M \leq r$ iff all $(r+1) \times (r+1)$ submatrices $M|_{S \times T}$ have $\det M|_{S \times T} = 0$, $S \subseteq [n]$, $T \subseteq [m]$, $|S| = |T| = r + 1$.

Corollary

M matrix, $M \in \mathbb{Z}^{n \times m}$.

Question

Phrase the rank method as a polynomial identity?

Lemma

M matrix, $M \in \mathbb{F}^{n\times m}$. $\mathrm{rank}_{\mathbb{F}} M \leq r$ iff all $(r+1)\times(r+1)$ submatrices $M|_{S\times T}$ have $\det M|_{S\times T} = 0$, $S \subseteq [n]$, $T \subseteq [m]$, $|S| = |T| = r+1$.

Corollary

M matrix, $M \in \mathbb{Z}^{n\times m}$. $\mathbb{F}$ any field.

Question

Phrase the rank method as a polynomial identity?

Lemma

M matrix, $M \in \mathbb{F}^{n\times m}$. $\operatorname{rank}_{\mathbb{F}} M \leq r$ iff all $(r+1)\times(r+1)$ submatrices $M|_{S\times T}$ have $\det M|_{S\times T} = 0$, $S \subseteq [n]$, $T \subseteq [m]$, $|S| = |T| = r+1$.

Corollary

M matrix, $M \in \mathbb{Z}^{n\times m}$. $\mathbb{F}$ any field. $\operatorname{rank}_{\mathbb{Q}} M \leq r$

Question

Phrase the rank method as a polynomial identity?

Lemma

M matrix, $M \in \mathbb{F}^{n\times m}$. $\operatorname{rank}_{\mathbb{F}} M \le r$ iff all $(r+1)\times(r+1)$ submatrices $M|_{S\times T}$ have $\det M|_{S\times T} = 0$, $S \subseteq [n]$, $T \subseteq [m]$, $|S| = |T| = r+1$.

Corollary

M matrix, $M \in \mathbb{Z}^{n\times m}$. $\mathbb{F}$ any field. $\operatorname{rank}_{\mathbb{Q}} M \le r \implies \operatorname{rank}_{\mathbb{F}} M \le r$.

Question

Phrase the rank method as a polynomial identity?

Lemma

M matrix, $M \in \mathbb{F}^{n \times m}$. $\operatorname{rank}_{\mathbb{F}} M \leq r$ iff all $(r+1) \times (r+1)$ submatrices $M|_{S \times T}$ have $\det M|_{S \times T} = 0$, $S \subseteq [n]$, $T \subseteq [m]$, $|S| = |T| = r + 1$.

Corollary

M matrix, $M \in \mathbb{Z}^{n \times m}$. $\mathbb{F}$ any field. $\operatorname{rank}_{\mathbb{Q}} M \leq r \implies \operatorname{rank}_{\mathbb{F}} M \leq r$.

Proof.

Question

Phrase the rank method as a polynomial identity?

Lemma

M matrix, $M \in \mathbb{F}^{n \times m}$. $\operatorname{rank}_{\mathbb{F}} M \le r$ *iff all* $(r+1) \times (r+1)$ *submatrices* $M|_{S \times T}$ *have* $\det M|_{S \times T} = 0$, $S \subseteq [n]$, $T \subseteq [m]$, $|S| = |T| = r+1$.

Corollary

M matrix, $M \in \mathbb{Z}^{n \times m}$. $\mathbb{F}$ any field. $\operatorname{rank}_{\mathbb{Q}} M \le r \implies \operatorname{rank}_{\mathbb{F}} M \le r$.

Proof.

$\operatorname{rank}_{\mathbb{Q}} M \le r \implies$

Question

Phrase the rank method as a polynomial identity?

Lemma

M matrix, $M \in \mathbb{F}^{n\times m}$. $\operatorname{rank}_{\mathbb{F}} M \le r$ iff all $(r+1)\times(r+1)$ submatrices $M|_{S\times T}$ have $\det M|_{S\times T} = 0$, $S \subseteq [n]$, $T \subseteq [m]$, $|S| = |T| = r+1$.

Corollary

M matrix, $M \in \mathbb{Z}^{n\times m}$. $\mathbb{F}$ any field. $\operatorname{rank}_{\mathbb{Q}} M \le r \implies \operatorname{rank}_{\mathbb{F}} M \le r$.

Proof.

$\operatorname{rank}_{\mathbb{Q}} M \le r \implies \det(M|_{S\times T}) \overset{\mathbb{Q}}{=} 0$

Question

Phrase the rank method as a polynomial identity?

Lemma

M *matrix,* $M \in \mathbb{F}^{n\times m}$. $\operatorname{rank}_{\mathbb{F}} M \le r$ *iff all* $(r+1)\times(r+1)$ *submatrices* $M|_{S\times T}$ *have* $\det M|_{S\times T} = 0$, $S \subseteq [n]$, $T \subseteq [m]$, $|S| = |T| = r+1$.

Corollary

M *matrix,* $M \in \mathbb{Z}^{n\times m}$. $\mathbb{F}$ *any field.* $\operatorname{rank}_{\mathbb{Q}} M \le r \implies \operatorname{rank}_{\mathbb{F}} M \le r$.

Proof.

$\operatorname{rank}_{\mathbb{Q}} M \le r \implies \det(M|_{S\times T}) \stackrel{\mathbb{Q}}{=} 0 \implies \det(M|_{S\times T}) \stackrel{\mathbb{Z}}{=} 0$

Question

Phrase the rank method as a polynomial identity?

Lemma

M matrix, $M \in \mathbb{F}^{n\times m}$. $\operatorname{rank}_{\mathbb{F}} M \leq r$ iff all $(r+1)\times(r+1)$ submatrices $M|_{S\times T}$ have $\det M|_{S\times T} = 0$, $S \subseteq [n]$, $T \subseteq [m]$, $|S| = |T| = r+1$.

Corollary

M matrix, $M \in \mathbb{Z}^{n\times m}$. $\mathbb{F}$ any field. $\operatorname{rank}_{\mathbb{Q}} M \leq r \implies \operatorname{rank}_{\mathbb{F}} M \leq r$.

Proof.

$$\operatorname{rank}_{\mathbb{Q}} M \leq r \implies \det(M|_{S\times T}) \stackrel{\mathbb{Q}}{=} 0 \implies \det(M|_{S\times T}) \stackrel{\mathbb{Z}}{=} 0 \implies \det(M|_{S\times T}) \stackrel{\mathbb{F}}{=} 0$$

Question

Phrase the rank method as a polynomial identity?

Lemma

M *matrix,* $M \in \mathbb{F}^{n\times m}$. $\operatorname{rank}_{\mathbb{F}} M \leq r$ *iff all* $(r+1)\times(r+1)$ *submatrices* $M|_{S\times T}$ *have* $\det M|_{S\times T} = 0$, $S \subseteq [n]$, $T \subseteq [m]$, $|S| = |T| = r+1$.

Corollary

M *matrix,* $M \in \mathbb{Z}^{n\times m}$. $\mathbb{F}$ *any field.* $\operatorname{rank}_{\mathbb{Q}} M \leq r \implies \operatorname{rank}_{\mathbb{F}} M \leq r$.

Proof.

$$\operatorname{rank}_{\mathbb{Q}} M \leq r \underset{\text{all } S,T}{\iff} \det(M|_{S\times T}) \overset{\mathbb{Q}}{=} 0 \implies \det(M|_{S\times T}) \overset{\mathbb{Z}}{=} 0 \implies \det(M|_{S\times T}) \overset{\mathbb{F}}{=} 0$$

Question

Phrase the rank method as a polynomial identity?

Lemma

M *matrix,* $M \in \mathbb{F}^{n\times m}$. $\operatorname{rank}_{\mathbb{F}} M \le r$ *iff all* $(r+1)\times(r+1)$ *submatrices* $M|_{S\times T}$ *have* $\det M|_{S\times T} = 0$, $S \subseteq [n]$, $T \subseteq [m]$, $|S| = |T| = r+1$.

Corollary

M *matrix,* $M \in \mathbb{Z}^{n\times m}$. $\mathbb{F}$ *any field.* $\operatorname{rank}_{\mathbb{Q}} M \le r \implies \operatorname{rank}_{\mathbb{F}} M \le r$.

Proof.

$\operatorname{rank}_{\mathbb{Q}} M \le r \underset{\text{all } S,T}{\implies} \det(M|_{S\times T}) \overset{\mathbb{Q}}{=} 0 \implies \det(M|_{S\times T}) \overset{\mathbb{Z}}{=} 0 \implies \det(M|_{S\times T}) \overset{\mathbb{F}}{=} 0 \underset{\text{all } S,T}{\implies} \operatorname{rank}_{\mathbb{F}} M \le r$. $\square$

Question

Phrase the rank method as a polynomial identity?

Question

Phrase the rank method as a polynomial identity?

Corollary

M matrix,

Question

Phrase the rank method as a polynomial identity?

Corollary

M matrix, $M \in \mathbb{Z}[\overline{w}]^{n \times m}$.

Question

Phrase the rank method as a polynomial identity?

Corollary

M matrix, $M \in \mathbb{Z}[\overline{w}]^{n \times m}$. $\mathbb{F}$ any field.

Question

Phrase the rank method as a polynomial identity?

Corollary

M matrix, $M \in \mathbb{Z}[\overline{w}]^{n\times m}$. $\mathbb{F}$ any field. $\mathrm{rank}_{\mathbb{Q}(\overline{w})} M(\overline{w}) \leq r$

Question

Phrase the rank method as a polynomial identity?

Corollary

M matrix, $M \in \mathbb{Z}[\overline{w}]^{n\times m}$. $\mathbb{F}$ any field. $\operatorname{rank}_{\mathbb{Q}(\overline{w})} M(\overline{w}) \leq r \implies \operatorname{rank}_{\mathbb{F}(\overline{w})} M(\overline{w}) \leq r$.

Question

Phrase the rank method as a polynomial identity?

Corollary

M matrix, $M \in \mathbb{Z}[\overline{w}]^{n\times m}$. $\mathbb{F}$ any field. $\mathrm{rank}_{\mathbb{Q}(\overline{w})} M(\overline{w}) \leq r \implies \mathrm{rank}_{\mathbb{F}(\overline{w})} M(\overline{w}) \leq r$.

Corollary

M matrix,

Question

Phrase the rank method as a polynomial identity?

Corollary

M matrix, $M \in \mathbb{Z}[\overline{w}]^{n \times m}$. $\mathbb{F}$ any field. $\operatorname{rank}_{\mathbb{Q}(\overline{w})} M(\overline{w}) \leq r \implies \operatorname{rank}_{\mathbb{F}(\overline{w})} M(\overline{w}) \leq r$.

Corollary

M matrix, $M \in \mathbb{Z}[\overline{w}]^{n \times m}$.

Question

Phrase the rank method as a polynomial identity?

Corollary

M matrix, $M \in \mathbb{Z}[\overline{w}]^{n \times m}$. $\mathbb{F}$ any field. $\operatorname{rank}_{\mathbb{Q}(\overline{w})} M(\overline{w}) \leq r \implies \operatorname{rank}_{\mathbb{F}(\overline{w})} M(\overline{w}) \leq r$.

Corollary

M matrix, $M \in \mathbb{Z}[\overline{w}]^{n \times m}$. $\overline{\gamma}$ over field $\mathbb{F}$.

Question

Phrase the rank method as a polynomial identity?

Corollary

M *matrix,* $M \in \mathbb{Z}[\overline{w}]^{n \times m}$. $\mathbb{F}$ *any field.* $\operatorname{rank}_{\mathbb{Q}(\overline{w})} M(\overline{w}) \leq r \implies \operatorname{rank}_{\mathbb{F}(\overline{w})} M(\overline{w}) \leq r$.

Corollary

M *matrix,* $M \in \mathbb{Z}[\overline{w}]^{n \times m}$. $\overline{\gamma}$ *over field* $\mathbb{F}$. $\operatorname{rank}_{\mathbb{F}(\overline{w})} M(\overline{w}) \leq r$

Question

Phrase the rank method as a polynomial identity?

Corollary

M matrix, $M \in \mathbb{Z}[\overline{w}]^{n\times m}$. $\mathbb{F}$ any field. $\operatorname{rank}_{\mathbb{Q}(\overline{w})} M(\overline{w}) \leq r \implies \operatorname{rank}_{\mathbb{F}(\overline{w})} M(\overline{w}) \leq r$.

Corollary

M matrix, $M \in \mathbb{Z}[\overline{w}]^{n\times m}$. $\overline{\gamma}$ over field $\mathbb{F}$. $\operatorname{rank}_{\mathbb{F}(\overline{w})} M(\overline{w}) \leq r \implies \operatorname{rank}_{\mathbb{F}} M(\overline{\gamma}) \leq r$.

Proposition (existence of (depth-3) universal circuits [Raz10])

Proposition (existence of (depth-3) universal circuits [Raz10])

Exists $P(\overline{x}, \overline{w})$

Proposition (existence of (depth-3) universal circuits [Raz10])

Exists $P(\overline{x}, \overline{w})$ *with a size* $\mathrm{poly}(s)$*-size depth-3 circuit,*

Proposition (existence of (depth-3) universal circuits [Raz10])

Exists $P(\overline{x}, \overline{w})$ *with a size* $\mathrm{poly}(s)$*-size depth-3 circuit, over variables* $\overline{x}, \overline{w}$

Proposition (existence of (depth-3) universal circuits [Raz10])

Exists $P(\overline{x}, \overline{w})$ *with a size* $\mathrm{poly}(s)$*-size depth-3 circuit, over variables* $\overline{x}, \overline{w}$ *and coefficients from* $\mathbb{Z}$

Proposition (existence of (depth-3) universal circuits [Raz10])

Exists $P(\overline{x}, \overline{w})$ with a size $\mathrm{poly}(s)$*-size depth-3 circuit, over variables $\overline{x}, \overline{w}$ and coefficients from $\mathbb{Z}$ that is a* **universal** *depth-3 circuit.*

Proposition (existence of (depth-3) universal circuits [Raz10])

Exists $P(\overline{x}, \overline{w})$ *with a size* $\text{poly}(s)$*-size depth-3 circuit, over variables* $\overline{x}, \overline{w}$ *and coefficients from* $\mathbb{Z}$ *that is a* **universal** *depth-3 circuit. Any* f *with size-*s *depth-3 circuit*

Proposition (existence of (depth-3) universal circuits [Raz10])

Exists $P(\overline{x}, \overline{w})$ with a size $\mathrm{poly}(s)$*-size depth-3 circuit, over variables $\overline{x}, \overline{w}$ and coefficients from $\mathbb{Z}$ that is a* **universal** *depth-3 circuit. Any f with size-s depth-3 circuit has $f(\overline{x}) = P(\overline{x}, \overline{\gamma})$*

Proposition (existence of (depth-3) universal circuits [Raz10])

Exists $P(\overline{x}, \overline{w})$ *with a size* $\mathrm{poly}(s)$*-size depth-3 circuit, over variables* $\overline{x}, \overline{w}$ *and coefficients from* $\mathbb{Z}$ *that is a* **universal** *depth-3 circuit. Any* f *with size-*s *depth-3 circuit has* $f(\overline{x}) = P(\overline{x}, \overline{\gamma})$ *for some* $\overline{\gamma}$ *from* $\mathbb{F}$.

Proposition (existence of (depth-3) universal circuits [Raz10])

Exists $P(\overline{x}, \overline{w})$ with a size $\operatorname{poly}(s)$*-size depth-3 circuit, over variables $\overline{x}, \overline{w}$ and coefficients from $\mathbb{Z}$ that is a* **universal** *depth-3 circuit. Any f with size-s depth-3 circuit has $f(\overline{x}) = P(\overline{x}, \overline{\gamma})$ for some $\overline{\gamma}$ from $\mathbb{F}$.*

Corollary

Proposition (existence of (depth-3) universal circuits [Raz10])

Exists $P(\overline{x}, \overline{w})$ with a size $\mathrm{poly}(s)$*-size depth-3 circuit, over variables $\overline{x}, \overline{w}$ and coefficients from $\mathbb{Z}$ that is a* **universal** *depth-3 circuit. Any f with size-s depth-3 circuit has $f(\overline{x}) = P(\overline{x}, \overline{\gamma})$ for some $\overline{\gamma}$ from $\mathbb{F}$.*

Corollary

Rank method of LST

Proposition (existence of (depth-3) universal circuits [Raz10])

Exists $P(\overline{x}, \overline{w})$ *with a size* $\mathrm{poly}(s)$*-size depth-3 circuit, over variables* $\overline{x}, \overline{w}$ *and coefficients from* $\mathbb{Z}$ *that is a* **universal** *depth-3 circuit. Any* f *with size-*s *depth-3 circuit has* $f(\overline{x}) = P(\overline{x}, \overline{\gamma})$ *for some* $\overline{\gamma}$ *from* $\mathbb{F}$.

Corollary

Rank method of LST implies that $P(\overline{x}, \overline{w})$ *yields matrix* M_P

Proposition (existence of (depth-3) universal circuits [Raz10])

Exists $P(\overline{x}, \overline{w})$ with a size $\mathrm{poly}(s)$*-size depth-3 circuit, over variables $\overline{x}, \overline{w}$ and coefficients from $\mathbb{Z}$ that is a* **universal** *depth-3 circuit. Any f with size-s depth-3 circuit has $f(\overline{x}) = P(\overline{x}, \overline{\gamma})$ for some $\overline{\gamma}$ from $\mathbb{F}$.*

Corollary

Rank method of LST implies that $P(\overline{x}, \overline{w})$ yields matrix M_P with low rank.

Proposition (existence of (depth-3) universal circuits [Raz10])

Exists $P(\overline{x}, \overline{w})$ with a size $\mathrm{poly}(s)$*-size depth-3 circuit, over variables $\overline{x}, \overline{w}$ and coefficients from $\mathbb{Z}$ that is a* **universal** *depth-3 circuit. Any f with size-s depth-3 circuit has $f(\overline{x}) = P(\overline{x}, \overline{\gamma})$ for some $\overline{\gamma}$ from $\mathbb{F}$.*

Corollary

Rank method of LST implies that $P(\overline{x}, \overline{w})$ yields matrix M_P with low rank.

Proof.

- View P as polynomial in $\mathbb{Z}[\overline{w}][\overline{x}]$

Proposition (existence of (depth-3) universal circuits [Raz10])

Exists $P(\overline{x}, \overline{w})$ with a size $\mathrm{poly}(s)$*-size depth-3 circuit, over variables $\overline{x}, \overline{w}$ and coefficients from $\mathbb{Z}$ that is a* **universal** *depth-3 circuit. Any f with size-s depth-3 circuit has $f(\overline{x}) = P(\overline{x}, \overline{\gamma})$ for some $\overline{\gamma}$ from $\mathbb{F}$.*

Corollary

Rank method of LST implies that $P(\overline{x}, \overline{w})$ yields matrix M_P with low rank.

Proof.

- View P as polynomial in $\mathbb{Z}[\overline{w}][\overline{x}] \subseteq \mathbb{Q}(\overline{w})[\overline{x}]$.

Proposition (existence of (depth-3) universal circuits [Raz10])

Exists $P(\overline{x}, \overline{w})$ with a size poly(s)*-size depth-3 circuit, over variables $\overline{x}, \overline{w}$ and coefficients from $\mathbb{Z}$ that is a* **universal** *depth-3 circuit. Any f with size-s depth-3 circuit has $f(\overline{x}) = P(\overline{x}, \overline{\gamma})$ for some $\overline{\gamma}$ from $\mathbb{F}$.*

Corollary

Rank method of LST implies that $P(\overline{x}, \overline{w})$ yields matrix M_P with low rank.

Proof.

- View P as polynomial in $\mathbb{Z}[\overline{w}][\overline{x}] \subseteq \mathbb{Q}(\overline{w})[\overline{x}]$.
- P has a poly(s)-size depth-3 circuit

Proposition (existence of (depth-3) universal circuits [Raz10])

Exists $P(\overline{x}, \overline{w})$ with a size $\mathrm{poly}(s)$-size depth-3 circuit, over variables $\overline{x}, \overline{w}$ and coefficients from $\mathbb{Z}$ that is a **universal** *depth-3 circuit. Any f with size-s depth-3 circuit has $f(\overline{x}) = P(\overline{x}, \overline{\gamma})$ for some $\overline{\gamma}$ from $\mathbb{F}$.*

Corollary

Rank method of LST implies that $P(\overline{x}, \overline{w})$ yields matrix M_P with low rank.

Proof.

- View P as polynomial in $\mathbb{Z}[\overline{w}][\overline{x}] \subseteq \mathbb{Q}(\overline{w})[\overline{x}]$.
- P has a $\mathrm{poly}(s)$-size depth-3 circuit in variables $\overline{x}$,

Proposition (existence of (depth-3) universal circuits [Raz10])

Exists $P(\overline{x}, \overline{w})$ with a size poly(s)*-size depth-3 circuit, over variables $\overline{x}, \overline{w}$ and coefficients from $\mathbb{Z}$ that is a* **universal** *depth-3 circuit. Any f with size-s depth-3 circuit has $f(\overline{x}) = P(\overline{x}, \overline{\gamma})$ for some $\overline{\gamma}$ from $\mathbb{F}$.*

Corollary

Rank method of LST implies that $P(\overline{x}, \overline{w})$ yields matrix M_P with low rank.

Proof.

- View P as polynomial in $\mathbb{Z}[\overline{w}][\overline{x}] \subseteq \mathbb{Q}(\overline{w})[\overline{x}]$.
- P has a poly(s)-size depth-3 circuit in variables $\overline{x}$, with coefficients from $\mathbb{Z}[\overline{w}]$

Proposition (existence of (depth-3) universal circuits [Raz10])

Exists $P(\overline{x}, \overline{w})$ with a size $\mathrm{poly}(s)$*-size depth-3 circuit, over variables $\overline{x}, \overline{w}$ and coefficients from $\mathbb{Z}$ that is a* **universal** *depth-3 circuit. Any f with size-s depth-3 circuit has $f(\overline{x}) = P(\overline{x}, \overline{\gamma})$ for some $\overline{\gamma}$ from $\mathbb{F}$.*

Corollary

Rank method of LST implies that $P(\overline{x}, \overline{w})$ yields matrix M_P with low rank.

Proof.

- View P as polynomial in $\mathbb{Z}[\overline{w}][\overline{x}] \subseteq \mathbb{Q}(\overline{w})[\overline{x}]$.
- P has a $\mathrm{poly}(s)$-size depth-3 circuit in variables $\overline{x}$, with coefficients from $\mathbb{Z}[\overline{w}] \subseteq \mathbb{Q}(\overline{w})$,

Proposition (existence of (depth-3) universal circuits [Raz10])

Exists $P(\overline{x}, \overline{w})$ with a size $\mathrm{poly}(s)$*-size depth-3 circuit, over variables $\overline{x}, \overline{w}$ and coefficients from $\mathbb{Z}$ that is a* **universal** *depth-3 circuit. Any f with size-s depth-3 circuit has $f(\overline{x}) = P(\overline{x}, \overline{\gamma})$ for some $\overline{\gamma}$ from $\mathbb{F}$.*

Corollary

Rank method of LST implies that $P(\overline{x}, \overline{w})$ yields matrix M_P with low rank.

Proof.

- View P as polynomial in $\mathbb{Z}[\overline{w}][\overline{x}] \subseteq \mathbb{Q}(\overline{w})[\overline{x}]$.
- P has a $\mathrm{poly}(s)$-size depth-3 circuit in variables $\overline{x}$, with coefficients from $\mathbb{Z}[\overline{w}] \subseteq \mathbb{Q}(\overline{w})$, and $\mathrm{char}(\mathbb{Q}(\overline{w})) = 0$.

Proposition (existence of (depth-3) universal circuits [Raz10])

Exists $P(\overline{x}, \overline{w})$ with a size poly(s)*-size depth-3 circuit, over variables $\overline{x}, \overline{w}$ and coefficients from $\mathbb{Z}$ that is a* **universal** *depth-3 circuit. Any f with size-s depth-3 circuit has $f(\overline{x}) = P(\overline{x}, \overline{\gamma})$ for some $\overline{\gamma}$ from $\mathbb{F}$.*

Corollary

Rank method of LST implies that $P(\overline{x}, \overline{w})$ yields matrix M_P with low rank.

Proof.

- View P as polynomial in $\mathbb{Z}[\overline{w}][\overline{x}] \subseteq \mathbb{Q}(\overline{w})[\overline{x}]$.
- P has a poly(s)-size depth-3 circuit in variables $\overline{x}$, with coefficients from $\mathbb{Z}[\overline{w}] \subseteq \mathbb{Q}(\overline{w})$, and $\mathrm{char}(\mathbb{Q}(\overline{w})) = 0$.
- M_P is a matrix entries that are integer linear combinations of coefficients of P

Proposition (existence of (depth-3) universal circuits [Raz10])

Exists $P(\overline{x}, \overline{w})$ with a size $\mathrm{poly}(s)$*-size depth-3 circuit, over variables $\overline{x}, \overline{w}$ and coefficients from $\mathbb{Z}$ that is a* **universal** *depth-3 circuit. Any f with size-s depth-3 circuit has $f(\overline{x}) = P(\overline{x}, \overline{\gamma})$ for some $\overline{\gamma}$ from $\mathbb{F}$.*

Corollary

Rank method of LST implies that $P(\overline{x}, \overline{w})$ yields matrix M_P with low rank.

Proof.

- View P as polynomial in $\mathbb{Z}[\overline{w}][\overline{x}] \subseteq \mathbb{Q}(\overline{w})[\overline{x}]$.
- P has a $\mathrm{poly}(s)$-size depth-3 circuit in variables $\overline{x}$, with coefficients from $\mathbb{Z}[\overline{w}] \subseteq \mathbb{Q}(\overline{w})$, and $\mathrm{char}(\mathbb{Q}(\overline{w})) = 0$.
- M_P is a matrix entries that are integer linear combinations of coefficients of P $\implies$ M_P has entries from $\mathbb{Z}[\overline{w}]$.

Proposition (existence of (depth-3) universal circuits [Raz10])

Exists $P(\overline{x}, \overline{w})$ with a size $\mathrm{poly}(s)$-size depth-3 circuit, over variables $\overline{x}, \overline{w}$ and coefficients from $\mathbb{Z}$ that is a **universal** *depth-3 circuit. Any f with size-s depth-3 circuit has $f(\overline{x}) = P(\overline{x}, \overline{\gamma})$ for some $\overline{\gamma}$ from $\mathbb{F}$.*

Corollary

Rank method of LST implies that $P(\overline{x}, \overline{w})$ yields matrix M_P with low rank.

Proof.

- View P as polynomial in $\mathbb{Z}[\overline{w}][\overline{x}] \subseteq \mathbb{Q}(\overline{w})[\overline{x}]$.
- P has a $\mathrm{poly}(s)$-size depth-3 circuit in variables $\overline{x}$, with coefficients from $\mathbb{Z}[\overline{w}] \subseteq \mathbb{Q}(\overline{w})$, and $\mathrm{char}(\mathbb{Q}(\overline{w})) = 0$.
- M_P is a matrix entries that are integer linear combinations of coefficients of P $\implies$ M_P has entries from $\mathbb{Z}[\overline{w}]$.

$\implies$ $\mathrm{rank}_{\mathbb{Q}(\overline{w})} M_P(\overline{w})$

Proposition (existence of (depth-3) universal circuits [Raz10])

Exists $P(\overline{x}, \overline{w})$ with a size $\mathrm{poly}(s)$-size depth-3 circuit, over variables $\overline{x}, \overline{w}$ and coefficients from $\mathbb{Z}$ that is a **universal** *depth-3 circuit. Any f with size-s depth-3 circuit has $f(\overline{x}) = P(\overline{x}, \overline{\gamma})$ for some $\overline{\gamma}$ from $\mathbb{F}$.*

Corollary

Rank method of LST implies that $P(\overline{x}, \overline{w})$ yields matrix M_P with low rank.

Proof.

- View P as polynomial in $\mathbb{Z}[\overline{w}][\overline{x}] \subseteq \mathbb{Q}(\overline{w})[\overline{x}]$.
- P has a $\mathrm{poly}(s)$-size depth-3 circuit in variables $\overline{x}$, with coefficients from $\mathbb{Z}[\overline{w}] \subseteq \mathbb{Q}(\overline{w})$, and $\mathrm{char}(\mathbb{Q}(\overline{w})) = 0$.
- M_P is a matrix entries that are integer linear combinations of coefficients of P $\implies$ M_P has entries from $\mathbb{Z}[\overline{w}]$.

$\implies$ $\mathrm{rank}_{\mathbb{Q}(\overline{w})} M_P(\overline{w})$ is small $\square$

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-$\Theta(\log n)$ polynomial requiring size $n^{\Omega(\sqrt{\log n})}$ to be computed by depth-3 algebraic circuits over $\mathbb{F}$.

idea: <u>transfer</u> the result over characteristic zero to arbitrary fields, via "logic"

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-$\Theta(\log n)$ polynomial requiring size $n^{\Omega(\sqrt{\log n})}$ to be computed by depth-3 algebraic circuits over $\mathbb{F}$.

idea: transfer the result over characteristic zero to arbitrary fields, via "logic"

proof:

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-$\Theta(\log n)$ polynomial requiring size $n^{\Omega(\sqrt{\log n})}$ to be computed by depth-3 algebraic circuits over $\mathbb{F}$.

idea: transfer the result over characteristic zero to arbitrary fields, via "logic"

proof:

- **fact(universal depth-3 circuit):** exists $P(\overline{x}, \overline{w})$ with a size $\mathrm{poly}(s)$-size depth-3 circuit,

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-$\Theta(\log n)$ polynomial requiring size $n^{\Omega(\sqrt{\log n})}$ to be computed by depth-3 algebraic circuits over $\mathbb{F}$.

idea: transfer the result over characteristic zero to arbitrary fields, via "logic"

proof:

- **fact(universal depth-3 circuit):** exists $P(\overline{x}, \overline{w})$ with a size poly(s)-size depth-3 circuit, over variables $\overline{x}, \overline{w}$ and coefficients from $\mathbb{Z}$,

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-$\Theta(\log n)$ polynomial requiring size $n^{\Omega(\sqrt{\log n})}$ to be computed by depth-3 algebraic circuits over $\mathbb{F}$.

idea: transfer the result over characteristic zero to arbitrary fields, via "logic"

proof:

- **fact(universal depth-3 circuit):** exists $P(\overline{x}, \overline{w})$ with a size poly(s)-size depth-3 circuit, over variables $\overline{x}, \overline{w}$ and coefficients from $\mathbb{Z}$, any f with size-s depth-3 circuit

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-$\Theta(\log n)$ polynomial requiring size $n^{\Omega(\sqrt{\log n})}$ to be computed by depth-3 algebraic circuits over $\mathbb{F}$.

idea: transfer the result over characteristic zero to arbitrary fields, via "logic"

proof:

- **fact(universal depth-3 circuit):** exists $P(\overline{x}, \overline{w})$ with a size poly(s)-size depth-3 circuit, over variables $\overline{x}, \overline{w}$ and coefficients from $\mathbb{Z}$, any f with size-s depth-3 circuit has $f(\overline{x}) = P(\overline{x}, \overline{\gamma})$ for some $\overline{\gamma}$ from $\mathbb{F}$ [Raz10]

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-$\Theta(\log n)$ polynomial requiring size $n^{\Omega(\sqrt{\log n})}$ to be computed by depth-3 algebraic circuits over $\mathbb{F}$.

idea: transfer the result over characteristic zero to arbitrary fields, via "logic"

proof:

- **fact(universal depth-3 circuit):** exists $P(\overline{x}, \overline{w})$ with a size poly(s)-size depth-3 circuit, over variables $\overline{x}, \overline{w}$ and coefficients from $\mathbb{Z}$, any f with size-s depth-3 circuit has $f(\overline{x}) = P(\overline{x}, \overline{\gamma})$ for some $\overline{\gamma}$ from $\mathbb{F}$ [Raz10]
- interpret P as polynomial over $\overline{x}$ with coeffs from $\mathbb{Z}[\overline{w}]$

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-$\Theta(\log n)$ polynomial requiring size $n^{\Omega(\sqrt{\log n})}$ to be computed by depth-3 algebraic circuits over $\mathbb{F}$.

idea: transfer the result over characteristic zero to arbitrary fields, via "logic"

proof:

- **fact(universal depth-3 circuit):** exists $P(\overline{x}, \overline{w})$ with a size poly(s)-size depth-3 circuit, over variables $\overline{x}, \overline{w}$ and coefficients from $\mathbb{Z}$, any f with size-s depth-3 circuit has $f(\overline{x}) = P(\overline{x}, \overline{\gamma})$ for some $\overline{\gamma}$ from $\mathbb{F}$ [Raz10]
- interpret P as polynomial over $\overline{x}$ with coeffs from $\mathbb{Z}[\overline{w}] \subseteq \mathbb{Q}(\overline{w})$;

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-$\Theta(\log n)$ polynomial requiring size $n^{\Omega(\sqrt{\log n})}$ to be computed by depth-3 algebraic circuits over $\mathbb{F}$.

idea: transfer the result over characteristic zero to arbitrary fields, via "logic"

proof:

- **fact(universal depth-3 circuit):** exists $P(\overline{x}, \overline{w})$ with a size poly(s)-size depth-3 circuit, over variables $\overline{x}, \overline{w}$ and coefficients from $\mathbb{Z}$, any f with size-s depth-3 circuit has $f(\overline{x}) = P(\overline{x}, \overline{\gamma})$ for some $\overline{\gamma}$ from $\mathbb{F}$ [Raz10]
- interpret P as polynomial over $\overline{x}$ with coeffs from $\mathbb{Z}[\overline{w}] \subseteq \mathbb{Q}(\overline{w})$; $\operatorname{char} \mathbb{Q}(\overline{w}) = 0$.

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-$\Theta(\log n)$ polynomial requiring size $n^{\Omega(\sqrt{\log n})}$ to be computed by depth-3 algebraic circuits over $\mathbb{F}$.

idea: transfer the result over characteristic zero to arbitrary fields, via "logic"

proof:

- **fact(universal depth-3 circuit):** exists $P(\overline{x}, \overline{w})$ with a size poly(s)-size depth-3 circuit, over variables $\overline{x}, \overline{w}$ and coefficients from $\mathbb{Z}$, any f with size-s depth-3 circuit has $f(\overline{x}) = P(\overline{x}, \overline{\gamma})$ for some $\overline{\gamma}$ from $\mathbb{F}$ [Raz10]
- interpret P as polynomial over $\overline{x}$ with coeffs from $\mathbb{Z}[\overline{w}] \subseteq \mathbb{Q}(\overline{w})$; char $\mathbb{Q}(\overline{w}) = 0$.
- LST22:

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-$\Theta(\log n)$ polynomial requiring size $n^{\Omega(\sqrt{\log n})}$ to be computed by depth-3 algebraic circuits over $\mathbb{F}$.

idea: transfer the result over characteristic zero to arbitrary fields, via "logic"

proof:

- **fact(universal depth-3 circuit):** exists $P(\overline{x}, \overline{w})$ with a size poly(s)-size depth-3 circuit, over variables $\overline{x}, \overline{w}$ and coefficients from $\mathbb{Z}$, any f with size-s depth-3 circuit has $f(\overline{x}) = P(\overline{x}, \overline{\gamma})$ for some $\overline{\gamma}$ from $\mathbb{F}$ [Raz10]
- interpret P as polynomial over $\overline{x}$ with coeffs from $\mathbb{Z}[\overline{w}] \subseteq \mathbb{Q}(\overline{w})$; $\operatorname{char} \mathbb{Q}(\overline{w}) = 0$.
- LST22: P small depth-3 ckt

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-$\Theta(\log n)$ polynomial requiring size $n^{\Omega(\sqrt{\log n})}$ to be computed by depth-3 algebraic circuits over $\mathbb{F}$.

idea: transfer the result over characteristic zero to arbitrary fields, via "logic"

proof:

- **fact(universal depth-3 circuit):** exists $P(\overline{x}, \overline{w})$ with a size poly(s)-size depth-3 circuit, over variables $\overline{x}, \overline{w}$ and coefficients from $\mathbb{Z}$, any f with size-s depth-3 circuit has $f(\overline{x}) = P(\overline{x}, \overline{\gamma})$ for some $\overline{\gamma}$ from $\mathbb{F}$ [Raz10]
- interpret P as polynomial over $\overline{x}$ with coeffs from $\mathbb{Z}[\overline{w}] \subseteq \mathbb{Q}(\overline{w})$; $\operatorname{char} \mathbb{Q}(\overline{w}) = 0$.
- LST22: P small depth-3 ckt $\xRightarrow{\text{char } 0}$

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-$\Theta(\log n)$ polynomial requiring size $n^{\Omega(\sqrt{\log n})}$ to be computed by depth-3 algebraic circuits over $\mathbb{F}$.

idea: transfer the result over characteristic zero to arbitrary fields, via "logic"

proof:

- **fact(universal depth-3 circuit):** exists $P(\overline{x}, \overline{w})$ with a size poly(s)-size depth-3 circuit, over variables $\overline{x}, \overline{w}$ and coefficients from $\mathbb{Z}$, any f with size-s depth-3 circuit has $f(\overline{x}) = P(\overline{x}, \overline{\gamma})$ for some $\overline{\gamma}$ from $\mathbb{F}$ [Raz10]
- interpret P as polynomial over $\overline{x}$ with coeffs from $\mathbb{Z}[\overline{w}] \subseteq \mathbb{Q}(\overline{w})$; $\operatorname{char} \mathbb{Q}(\overline{w}) = 0$.
- LST22: P small depth-3 ckt $\overset{\text{char } 0}{\Longrightarrow}$ matrix M_P

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-$\Theta(\log n)$ polynomial requiring size $n^{\Omega(\sqrt{\log n})}$ to be computed by depth-3 algebraic circuits over $\mathbb{F}$.

idea: transfer the result over characteristic zero to arbitrary fields, via "logic"

proof:

- **fact(universal depth-3 circuit):** exists $P(\overline{x}, \overline{w})$ with a size poly(s)-size depth-3 circuit, over variables $\overline{x}, \overline{w}$ and coefficients from $\mathbb{Z}$, any f with size-s depth-3 circuit has $f(\overline{x}) = P(\overline{x}, \overline{\gamma})$ for some $\overline{\gamma}$ from $\mathbb{F}$ [Raz10]
- interpret P as polynomial over $\overline{x}$ with coeffs from $\mathbb{Z}[\overline{w}] \subseteq \mathbb{Q}(\overline{w})$; $\operatorname{char} \mathbb{Q}(\overline{w}) = 0$.
- LST22: P small depth-3 ckt $\overset{\text{char } 0}{\Longrightarrow}$ matrix M_P over $\mathbb{Z}[\overline{w}]$

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-$\Theta(\log n)$ polynomial requiring size $n^{\Omega(\sqrt{\log n})}$ to be computed by depth-3 algebraic circuits over $\mathbb{F}$.

idea: transfer the result over characteristic zero to arbitrary fields, via "logic"

proof:

- **fact(universal depth-3 circuit):** exists $P(\overline{x}, \overline{w})$ with a size poly(s)-size depth-3 circuit, over variables $\overline{x}, \overline{w}$ and coefficients from $\mathbb{Z}$, any f with size-s depth-3 circuit has $f(\overline{x}) = P(\overline{x}, \overline{\gamma})$ for some $\overline{\gamma}$ from $\mathbb{F}$ [Raz10]
- interpret P as polynomial over $\overline{x}$ with coeffs from $\mathbb{Z}[\overline{w}] \subseteq \mathbb{Q}(\overline{w})$; $\operatorname{char} \mathbb{Q}(\overline{w}) = 0$.
- LST22: P small depth-3 ckt $\overset{\text{char } 0}{\Longrightarrow}$ matrix M_P over $\mathbb{Z}[\overline{w}]$ has $\text{rank}_{\mathbb{Q}(\overline{w})} M_P$ small

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-$\Theta(\log n)$ polynomial requiring size $n^{\Omega(\sqrt{\log n})}$ to be computed by depth-3 algebraic circuits over $\mathbb{F}$.

idea: transfer the result over characteristic zero to arbitrary fields, via "logic"

proof:

- **fact(universal depth-3 circuit):** exists $P(\overline{x}, \overline{w})$ with a size poly(s)-size depth-3 circuit, over variables $\overline{x}, \overline{w}$ and coefficients from $\mathbb{Z}$, any f with size-s depth-3 circuit has $f(\overline{x}) = P(\overline{x}, \overline{\gamma})$ for some $\overline{\gamma}$ from $\mathbb{F}$ [Raz10]
- interpret P as polynomial over $\overline{x}$ with coeffs from $\mathbb{Z}[\overline{w}] \subseteq \mathbb{Q}(\overline{w})$; $\operatorname{char} \mathbb{Q}(\overline{w}) = 0$.
- LST22: P small depth-3 ckt $\overset{\text{char } 0}{\Longrightarrow}$ matrix M_P over $\mathbb{Z}[\overline{w}]$ has $\operatorname{rank}_{\mathbb{Q}(\overline{w})} M_P$ small
- $f(\overline{x}) = P(\overline{x}, \overline{\gamma})$

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-$\Theta(\log n)$ polynomial requiring size $n^{\Omega(\sqrt{\log n})}$ to be computed by depth-3 algebraic circuits over $\mathbb{F}$.

idea: transfer the result over characteristic zero to arbitrary fields, via "logic"

proof:

- **fact(universal depth-3 circuit):** exists $P(\overline{x}, \overline{w})$ with a size poly(s)-size depth-3 circuit, over variables $\overline{x}, \overline{w}$ and coefficients from $\mathbb{Z}$, any f with size-s depth-3 circuit has $f(\overline{x}) = P(\overline{x}, \overline{\gamma})$ for some $\overline{\gamma}$ from $\mathbb{F}$ [Raz10]
- interpret P as polynomial over $\overline{x}$ with coeffs from $\mathbb{Z}[\overline{w}] \subseteq \mathbb{Q}(\overline{w})$; char $\mathbb{Q}(\overline{w}) = 0$.
- LST22: P small depth-3 ckt $\overset{\text{char } 0}{\Longrightarrow}$ matrix M_P over $\mathbb{Z}[\overline{w}]$ has $\text{rank}_{\mathbb{Q}(\overline{w})} M_P$ small
- $f(\overline{x}) = P(\overline{x}, \overline{\gamma}) \implies M_f = M_P(\overline{\gamma})$

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-$\Theta(\log n)$ polynomial requiring size $n^{\Omega(\sqrt{\log n})}$ to be computed by depth-3 algebraic circuits over $\mathbb{F}$.

idea: transfer the result over characteristic zero to arbitrary fields, via "logic"

proof:

- **fact(universal depth-3 circuit):** exists $P(\overline{x}, \overline{w})$ with a size poly(s)-size depth-3 circuit, over variables $\overline{x}, \overline{w}$ and coefficients from $\mathbb{Z}$, any f with size-s depth-3 circuit has $f(\overline{x}) = P(\overline{x}, \overline{\gamma})$ for some $\overline{\gamma}$ from $\mathbb{F}$ [Raz10]
- interpret P as polynomial over $\overline{x}$ with coeffs from $\mathbb{Z}[\overline{w}] \subseteq \mathbb{Q}(\overline{w})$; $\operatorname{char} \mathbb{Q}(\overline{w}) = 0$.
- LST22: P small depth-3 ckt $\xRightarrow{\text{char } 0}$ matrix M_P over $\mathbb{Z}[\overline{w}]$ has $\operatorname{rank}_{\mathbb{Q}(\overline{w})} M_P$ small
- $f(\overline{x}) = P(\overline{x}, \overline{\gamma}) \implies M_f = M_P(\overline{\gamma})$
- $\operatorname{rank}_{\mathbb{F}} M_f$

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-$\Theta(\log n)$ polynomial requiring size $n^{\Omega(\sqrt{\log n})}$ to be computed by depth-3 algebraic circuits over $\mathbb{F}$.

idea: transfer the result over characteristic zero to arbitrary fields, via "logic"

proof:

- **fact(universal depth-3 circuit):** exists $P(\overline{x}, \overline{w})$ with a size poly(s)-size depth-3 circuit, over variables $\overline{x}, \overline{w}$ and coefficients from $\mathbb{Z}$, any f with size-s depth-3 circuit has $f(\overline{x}) = P(\overline{x}, \overline{\gamma})$ for some $\overline{\gamma}$ from $\mathbb{F}$ [Raz10]
- interpret P as polynomial over $\overline{x}$ with coeffs from $\mathbb{Z}[\overline{w}] \subseteq \mathbb{Q}(\overline{w})$; $\operatorname{char} \mathbb{Q}(\overline{w}) = 0$.
- LST22: P small depth-3 ckt $\overset{\text{char } 0}{\Longrightarrow}$ matrix M_P over $\mathbb{Z}[\overline{w}]$ has $\operatorname{rank}_{\mathbb{Q}(\overline{w})} M_P$ small
- $f(\overline{x}) = P(\overline{x}, \overline{\gamma}) \implies M_f = M_P(\overline{\gamma})$
- $\operatorname{rank}_{\mathbb{F}} M_f = \operatorname{rank}_{\mathbb{F}} M_P(\overline{\gamma})$

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-$\Theta(\log n)$ polynomial requiring size $n^{\Omega(\sqrt{\log n})}$ to be computed by depth-3 algebraic circuits over $\mathbb{F}$.

idea: transfer the result over characteristic zero to arbitrary fields, via "logic"

proof:

- **fact(universal depth-3 circuit):** exists $P(\overline{x}, \overline{w})$ with a size poly(s)-size depth-3 circuit, over variables $\overline{x}, \overline{w}$ and coefficients from $\mathbb{Z}$, any f with size-s depth-3 circuit has $f(\overline{x}) = P(\overline{x}, \overline{\gamma})$ for some $\overline{\gamma}$ from $\mathbb{F}$ [Raz10]
- interpret P as polynomial over $\overline{x}$ with coeffs from $\mathbb{Z}[\overline{w}] \subseteq \mathbb{Q}(\overline{w})$; $\operatorname{char} \mathbb{Q}(\overline{w}) = 0$.
- LST22: P small depth-3 ckt $\overset{\text{char } 0}{\Longrightarrow}$ matrix M_P over $\mathbb{Z}[\overline{w}]$ has $\operatorname{rank}_{\mathbb{Q}(\overline{w})} M_P$ small
- $f(\overline{x}) = P(\overline{x}, \overline{\gamma}) \implies M_f = M_P(\overline{\gamma})$
- $\operatorname{rank}_{\mathbb{F}} M_f = \operatorname{rank}_{\mathbb{F}} M_P(\overline{\gamma}) \leq \operatorname{rank}_{\mathbb{F}(\overline{w})} M_P(\overline{w})$

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-$\Theta(\log n)$ polynomial requiring size $n^{\Omega(\sqrt{\log n})}$ to be computed by depth-3 algebraic circuits over $\mathbb{F}$.

idea: transfer the result over characteristic zero to arbitrary fields, via "logic"

proof:

- **fact(universal depth-3 circuit):** exists $P(\overline{x}, \overline{w})$ with a size poly(s)-size depth-3 circuit, over variables $\overline{x}, \overline{w}$ and coefficients from $\mathbb{Z}$, any f with size-s depth-3 circuit has $f(\overline{x}) = P(\overline{x}, \overline{\gamma})$ for some $\overline{\gamma}$ from $\mathbb{F}$ [Raz10]
- interpret P as polynomial over $\overline{x}$ with coeffs from $\mathbb{Z}[\overline{w}] \subseteq \mathbb{Q}(\overline{w})$; $\operatorname{char} \mathbb{Q}(\overline{w}) = 0$.
- LST22: P small depth-3 ckt $\overset{\text{char } 0}{\Longrightarrow}$ matrix M_P over $\mathbb{Z}[\overline{w}]$ has $\operatorname{rank}_{\mathbb{Q}(\overline{w})} M_P$ small
- $f(\overline{x}) = P(\overline{x}, \overline{\gamma}) \implies M_f = M_P(\overline{\gamma})$
- $\operatorname{rank}_{\mathbb{F}} M_f = \operatorname{rank}_{\mathbb{F}} M_P(\overline{\gamma}) \leq \operatorname{rank}_{\mathbb{F}(\overline{w})} M_P(\overline{w}) \overset{\text{lem}}{\leq}$

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-$\Theta(\log n)$ polynomial requiring size $n^{\Omega(\sqrt{\log n})}$ to be computed by depth-3 algebraic circuits over $\mathbb{F}$.

idea: transfer the result over characteristic zero to arbitrary fields, via "logic"

proof:

- **fact(universal depth-3 circuit):** exists $P(\overline{x}, \overline{w})$ with a size poly(s)-size depth-3 circuit, over variables $\overline{x}, \overline{w}$ and coefficients from $\mathbb{Z}$, any f with size-s depth-3 circuit has $f(\overline{x}) = P(\overline{x}, \overline{\gamma})$ for some $\overline{\gamma}$ from $\mathbb{F}$ [Raz10]
- interpret P as polynomial over $\overline{x}$ with coeffs from $\mathbb{Z}[\overline{w}] \subseteq \mathbb{Q}(\overline{w})$; $\operatorname{char} \mathbb{Q}(\overline{w}) = 0$.
- LST22: P small depth-3 ckt $\overset{\text{char } 0}{\Longrightarrow}$ matrix M_P over $\mathbb{Z}[\overline{w}]$ has $\operatorname{rank}_{\mathbb{Q}(\overline{w})} M_P$ small
- $f(\overline{x}) = P(\overline{x}, \overline{\gamma}) \implies M_f = M_P(\overline{\gamma})$
- $\operatorname{rank}_{\mathbb{F}} M_f = \operatorname{rank}_{\mathbb{F}} M_P(\overline{\gamma}) \leq \operatorname{rank}_{\mathbb{F}(\overline{w})} M_P(\overline{w}) \overset{\text{lem}}{\leq} \operatorname{rank}_{\mathbb{Q}(\overline{w})} M_P(\overline{w})$

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-$\Theta(\log n)$ polynomial requiring size $n^{\Omega(\sqrt{\log n})}$ to be computed by depth-3 algebraic circuits over $\mathbb{F}$.

idea: transfer the result over characteristic zero to arbitrary fields, via "logic"

proof:

- **fact(universal depth-3 circuit):** exists $P(\overline{x}, \overline{w})$ with a size poly(s)-size depth-3 circuit, over variables $\overline{x}, \overline{w}$ and coefficients from $\mathbb{Z}$, any f with size-s depth-3 circuit has $f(\overline{x}) = P(\overline{x}, \overline{\gamma})$ for some $\overline{\gamma}$ from $\mathbb{F}$ [Raz10]
- interpret P as polynomial over $\overline{x}$ with coeffs from $\mathbb{Z}[\overline{w}] \subseteq \mathbb{Q}(\overline{w})$; $\operatorname{char} \mathbb{Q}(\overline{w}) = 0$.
- LST22: P small depth-3 ckt $\overset{\text{char } 0}{\Longrightarrow}$ matrix M_P over $\mathbb{Z}[\overline{w}]$ has $\operatorname{rank}_{\mathbb{Q}(\overline{w})} M_P$ small
- $f(\overline{x}) = P(\overline{x}, \overline{\gamma}) \implies M_f = M_P(\overline{\gamma})$
- $\operatorname{rank}_{\mathbb{F}} M_f = \operatorname{rank}_{\mathbb{F}} M_P(\overline{\gamma}) \le \operatorname{rank}_{\mathbb{F}(\overline{w})} M_P(\overline{w}) \overset{\text{lem}}{\le} \operatorname{rank}_{\mathbb{Q}(\overline{w})} M_P(\overline{w}) \le$ small

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-$\Theta(\log n)$ polynomial requiring size $n^{\Omega(\sqrt{\log n})}$ to be computed by depth-3 algebraic circuits over $\mathbb{F}$.

idea: transfer the result over characteristic zero to arbitrary fields, via "logic"

proof:

- **fact(universal depth-3 circuit):** exists $P(\overline{x}, \overline{w})$ with a size poly(s)-size depth-3 circuit, over variables $\overline{x}, \overline{w}$ and coefficients from $\mathbb{Z}$, any f with size-s depth-3 circuit has $f(\overline{x}) = P(\overline{x}, \overline{\gamma})$ for some $\overline{\gamma}$ from $\mathbb{F}$ [Raz10]
- interpret P as polynomial over $\overline{x}$ with coeffs from $\mathbb{Z}[\overline{w}] \subseteq \mathbb{Q}(\overline{w})$; $\operatorname{char} \mathbb{Q}(\overline{w}) = 0$.
- LST22: P small depth-3 ckt $\overset{\text{char } 0}{\Longrightarrow}$ matrix M_P over $\mathbb{Z}[\overline{w}]$ has $\operatorname{rank}_{\mathbb{Q}(\overline{w})} M_P$ small
- $f(\overline{x}) = P(\overline{x}, \overline{\gamma}) \implies M_f = M_P(\overline{\gamma})$
- $\operatorname{rank}_{\mathbb{F}} M_f = \operatorname{rank}_{\mathbb{F}} M_P(\overline{\gamma}) \leq \operatorname{rank}_{\mathbb{F}(\overline{w})} M_P(\overline{w}) \overset{\text{lem}}{\leq} \operatorname{rank}_{\mathbb{Q}(\overline{w})} M_P(\overline{w}) \leq \text{small}$
- LST22 exhibits f with $\operatorname{rank}_{\mathbb{F}} M_f$ large for **any** $\mathbb{F}$

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-$\Theta(\log n)$ polynomial requiring size $n^{\Omega(\sqrt{\log n})}$ to be computed by depth-3 algebraic circuits over $\mathbb{F}$.

idea: <u>transfer</u> the result over characteristic zero to arbitrary fields, via "logic"

proof:

- **fact(universal depth-3 circuit):** exists $P(\overline{x}, \overline{w})$ with a size poly(s)-size depth-3 circuit, over variables $\overline{x}, \overline{w}$ and coefficients from $\mathbb{Z}$, any f with size-s depth-3 circuit has $f(\overline{x}) = P(\overline{x}, \overline{\gamma})$ for some $\overline{\gamma}$ from $\mathbb{F}$ [Raz10]
- interpret P as polynomial over $\overline{x}$ with coeffs from $\mathbb{Z}[\overline{w}] \subseteq \mathbb{Q}(\overline{w})$; $\operatorname{char} \mathbb{Q}(\overline{w}) = 0$.
- LST22: P small depth-3 ckt $\overset{\text{char } 0}{\Longrightarrow}$ matrix M_P over $\mathbb{Z}[\overline{w}]$ has $\operatorname{rank}_{\mathbb{Q}(\overline{w})} M_P$ small
- $f(\overline{x}) = P(\overline{x}, \overline{\gamma}) \implies M_f = M_P(\overline{\gamma})$
- $\operatorname{rank}_{\mathbb{F}} M_f = \operatorname{rank}_{\mathbb{F}} M_P(\overline{\gamma}) \leq \operatorname{rank}_{\mathbb{F}(\overline{w})} M_P(\overline{w}) \overset{\text{lem}}{\leq} \operatorname{rank}_{\mathbb{Q}(\overline{w})} M_P(\overline{w}) \leq \text{small}$
- LST22 exhibits f with $\operatorname{rank}_{\mathbb{F}} M_f$ large for **any** $\mathbb{F}$

$\Longrightarrow$ this f cannot have a small depth-3 ckt over any $\mathbb{F}$ $\square$

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-$\Theta(\log n)$ polynomial requiring size $n^{\Omega(\sqrt{\log n})}$ to be computed by depth-3 algebraic circuits over $\mathbb{F}$.

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-$\Theta(\log n)$ polynomial requiring size $n^{\Omega(\sqrt{\log n})}$ to be computed by depth-3 algebraic circuits over $\mathbb{F}$.

idea:

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-$\Theta(\log n)$ polynomial requiring size $n^{\Omega(\sqrt{\log n})}$ to be computed by depth-3 algebraic circuits over $\mathbb{F}$.

idea: combine efficient homogenization and set-multilinearization steps

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-$\Theta(\log n)$ polynomial requiring size $n^{\Omega(\sqrt{\log n})}$ to be computed by depth-3 algebraic circuits over $\mathbb{F}$.

idea: combine efficient homogenization and set-multilinearization steps

proof 2 (constructive):

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-$\Theta(\log n)$ polynomial requiring size $n^{\Omega(\sqrt{\log n})}$ to be computed by depth-3 algebraic circuits over $\mathbb{F}$.

idea: combine efficient homogenization and set-multilinearization steps

proof 2 (constructive):

depth-3 ckt

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-$\Theta(\log n)$ polynomial requiring size $n^{\Omega(\sqrt{\log n})}$ to be computed by depth-3 algebraic circuits over $\mathbb{F}$.

idea: combine efficient homogenization and set-multilinearization steps

proof 2 (constructive):

homog depth-5 ckt

depth-3 ckt

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-$\Theta(\log n)$ polynomial requiring size $n^{\Omega(\sqrt{\log n})}$ to be computed by depth-3 algebraic circuits over $\mathbb{F}$.

idea: combine efficient homogenization and set-multilinearization steps

proof 2 (constructive):

homog depth-5 ckt

depth-3 ckt

set-mult depth-5 ckt

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-$\Theta(\log n)$ polynomial requiring size $n^{\Omega(\sqrt{\log n})}$ to be computed by depth-3 algebraic circuits over $\mathbb{F}$.

idea: <u>combine</u> efficient homogenization and set-multilinearization steps

proof 2 (constructive):

depth-3 ckt $\xrightarrow{\text{Newton Identities}}$ homog depth-5 ckt

set-mult depth-5 ckt

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-$\Theta(\log n)$ polynomial requiring size $n^{\Omega(\sqrt{\log n})}$ to be computed by depth-3 algebraic circuits over $\mathbb{F}$.

idea: <u>combine</u> efficient homogenization and set-multilinearization steps

proof 2 (constructive):

$$\begin{tikzcd} & \text{homog depth-5 ckt} \arrow[dr, bend left, "\text{gate simulation}"] & \\ \text{depth-3 ckt} \arrow[ur, bend left, "\text{Newton Identities}"] & & \text{set-mult depth-5 ckt} \end{tikzcd}$$

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-$\Theta(\log n)$ polynomial requiring size $n^{\Omega(\sqrt{\log n})}$ to be computed by depth-3 algebraic circuits over $\mathbb{F}$.

idea: <u>combine</u> efficient homogenization and set-multilinearization steps

proof 2 (constructive):

$$\begin{tikzcd} \text{depth-3 ckt} \arrow[r, bend left, "\text{Newton Identities}", "\mathrm{char}(\mathbb{F}) \ggg 0"'] & \text{homog depth-5 ckt} \arrow[r, bend left, "\text{gate simulation}"] & \text{set-mult depth-5 ckt} \end{tikzcd}$$

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-$\Theta(\log n)$ polynomial requiring size $n^{\Omega(\sqrt{\log n})}$ to be computed by depth-3 algebraic circuits over $\mathbb{F}$.

idea: combine efficient homogenization and set-multilinearization steps

proof 2 (constructive):

$$\begin{tikzcd}
& \text{homog depth-5 ckt} \arrow[dr, bend left, "\text{gate simulation}", "\text{any } \mathbb{F}"'] & \\
\text{depth-3 ckt} \arrow[ur, bend left, "\text{Newton Identities}", "\text{char}(\mathbb{F}) \gg 0"'] & & \text{set-mult depth-5 ckt}
\end{tikzcd}$$

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-$\Theta(\log n)$ polynomial requiring size $n^{\Omega(\sqrt{\log n})}$ to be computed by depth-3 algebraic circuits over $\mathbb{F}$.

idea: combine efficient homogenization and set-multilinearization steps

proof 2 (constructive):

$$
\begin{tikzcd}
& \text{homog depth-5 ckt} \arrow[dr, "\text{gate simulation}", "\text{any } \mathbb{F}"'] & \\
\text{depth-3 ckt} \arrow[ur, "\text{Newton Identities}", "\mathrm{char}(\mathbb{F}) \gg 0"'] \arrow[rr] & & \text{set-mult depth-5 ckt}
\end{tikzcd}
$$

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-$\Theta(\log n)$ polynomial requiring size $n^{\Omega(\sqrt{\log n})}$ to be computed by depth-3 algebraic circuits over $\mathbb{F}$.

idea: <u>combine</u> efficient homogenization and set-multilinearization steps

proof 2 (constructive):

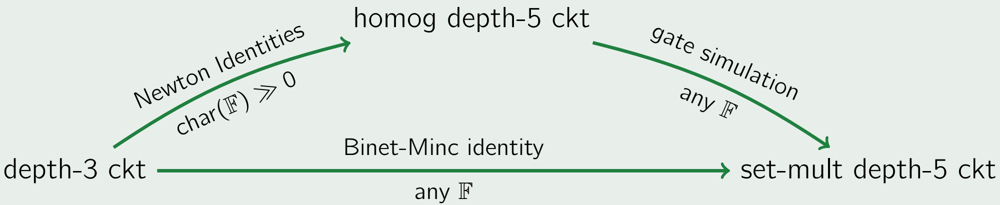
$$\begin{tikzcd}
 & \text{homog depth-5 ckt} \arrow[dr, bend left, "\text{gate simulation}", "\text{any } \mathbb{F}"'] & \\
\text{depth-3 ckt} \arrow[ur, bend left, "\text{Newton Identities}", "\mathrm{char}(\mathbb{F}) \ggg 0"'] \arrow[rr, "\text{Binet-Minc identity}"] & & \text{set-mult depth-5 ckt}
\end{tikzcd}$$

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-$\Theta(\log n)$ polynomial requiring size $n^{\Omega(\sqrt{\log n})}$ to be computed by depth-3 algebraic circuits over $\mathbb{F}$.

idea: combine efficient homogenization and set-multilinearization steps

proof 2 (constructive):



Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-$\Theta(\log n)$ polynomial requiring size $n^{\Omega(\sqrt{\log n})}$ to be computed by depth-3 algebraic circuits over $\mathbb{F}$.

idea: combine efficient homogenization and set-multilinearization steps

proof 2 (constructive):

$$\begin{tikzcd}
& \text{homog depth-5 ckt} \arrow[dr, bend left, "\text{gate simulation}", "\text{any } \mathbb{F}"'] & \\
\text{depth-3 ckt} \arrow[ur, bend left, "\text{Newton Identities}", "\mathrm{char}(\mathbb{F}) \gg 0"'] \arrow[rr, "\text{Binet-Minc identity}", "\text{any } \mathbb{F}"'] & & \text{set-mult depth-5 ckt}
\end{tikzcd}$$

- LST22 gives explicit polynomial without small set-mult depth-5 circuit, any $\mathbb{F}$.

Theorem

Let $\mathbb{F}$ be a field. There is an explicit n-variate degree-$\Theta(\log n)$ polynomial requiring size $n^{\Omega(\sqrt{\log n})}$ to be computed by depth-3 algebraic circuits over $\mathbb{F}$.

idea: combine efficient homogenization and set-multilinearization steps

proof 2 (constructive):

$$
\begin{tikzcd}
& \text{homog depth-5 ckt} \arrow[dr, bend left, "\text{gate simulation}", "\text{any } \mathbb{F}"'] & \\
\text{depth-3 ckt} \arrow[ur, bend left, "\text{Newton Identities}", "\mathrm{char}(\mathbb{F}) \gg 0"'] \arrow[rr, "\text{Binet-Minc identity}", "\text{any } \mathbb{F}"'] & & \text{set-mult depth-5 ckt}
\end{tikzcd}
$$

- LST22 gives explicit polynomial without small set-mult depth-5 circuit, any $\mathbb{F}$.

$\implies$ same polynomial has no small depth-3 circuit $\square$

Definition

Let the variables be partitioned into $\overline{x} = \overline{x}_1, \cdots, \overline{x}_d$. A monomial is **set-multilinear** if is a product of one variable per $\overline{x}_i$, e.g. $\prod_{i=1}^{d} x_{i,j_i}$. A polynomial is **set-multilinear** if all monomials are set-multilinear. A circuit is **set-multilinear** if all gates compute set-multilinear polynomials.

Definition

Let the variables be partitioned into $\overline{x} = \overline{x}_1, \cdots, \overline{x}_d$. A monomial is **set-multilinear** if is a product of one variable per $\overline{x}_i$, e.g. $\prod_{i=1}^{d} x_{i,j_i}$. A polynomial is **set-multilinear** if all monomials are set-multilinear. A circuit is **set-multilinear** if all gates compute set-multilinear polynomials.

Theorem (Binet-Minc)

Definition

Let the variables be partitioned into $\overline{x} = \overline{x}_1, \cdots, \overline{x}_d$. A monomial is **set-multilinear** if is a product of one variable per $\overline{x}_i$, e.g. $\prod_{i=1}^{d} x_{i,j_i}$. A polynomial is **set-multilinear** if all monomials are set-multilinear. A circuit is **set-multilinear** if all gates compute set-multilinear polynomials.

Theorem (Binet-Minc)

The rectangular permanent $\mathrm{perm}_{n,d} = \sum_{\sigma:[d]\hookrightarrow[n]} \prod_{i=1}^{d} x_{i,\sigma(i)}$

Definition

Let the variables be partitioned into $\overline{x} = \overline{x}_1, \cdots, \overline{x}_d$. A monomial is **set-multilinear** if is a product of one variable per $\overline{x}_i$, e.g. $\prod_{i=1}^{d} x_{i,j_i}$. A polynomial is **set-multilinear** if all monomials are set-multilinear. A circuit is **set-multilinear** if all gates compute set-multilinear polynomials.

Theorem (Binet-Minc)

The rectangular permanent $\mathrm{perm}_{n,d} = \sum_{\sigma:[d]\hookrightarrow[n]} \prod_{i=1}^{d} x_{i,\sigma(i)}$ *has* $\mathrm{poly}(n, d^d)$*-size*

Definition

Let the variables be partitioned into $\overline{x} = \overline{x}_1, \cdots, \overline{x}_d$. A monomial is **set-multilinear** if is a product of one variable per $\overline{x}_i$, e.g. $\prod_{i=1}^{d} x_{i,j_i}$. A polynomial is **set-multilinear** if all monomials are set-multilinear. A circuit is **set-multilinear** if all gates compute set-multilinear polynomials.

Theorem (Binet-Minc)

The rectangular permanent $\mathrm{perm}_{n,d} = \sum_{\sigma:[d]\hookrightarrow[n]} \prod_{i=1}^{d} x_{i,\sigma(i)}$ *has* $\mathrm{poly}(n, d^d)$*-size depth-4*

Definition

Let the variables be partitioned into $\overline{x} = \overline{x}_1, \cdots, \overline{x}_d$. A monomial is **set-multilinear** if is a product of one variable per $\overline{x}_i$, e.g. $\prod_{i=1}^{d} x_{i,j_i}$. A polynomial is **set-multilinear** if all monomials are set-multilinear. A circuit is **set-multilinear** if all gates compute set-multilinear polynomials.

Theorem (Binet-Minc)

The rectangular permanent $\mathrm{perm}_{n,d} = \sum_{\sigma:[d]\hookrightarrow[n]} \prod_{i=1}^{d} x_{i,\sigma(i)}$ *has* $\mathrm{poly}(n, d^d)$*-size depth-4 set-multilinear circuit,*

Definition

Let the variables be partitioned into $\overline{x} = \overline{x}_1, \cdots, \overline{x}_d$. A monomial is **set-multilinear** if is a product of one variable per $\overline{x}_i$, e.g. $\prod_{i=1}^{d} x_{i,j_i}$. A polynomial is **set-multilinear** if all monomials are set-multilinear. A circuit is **set-multilinear** if all gates compute set-multilinear polynomials.

Theorem (Binet-Minc)

The rectangular permanent $\mathrm{perm}_{n,d} = \sum_{\sigma:[d]\hookrightarrow[n]} \prod_{i=1}^{d} x_{i,\sigma(i)}$ *has* $\mathrm{poly}(n, d^d)$*-size depth-4 set-multilinear circuit, over any* $\mathbb{F}$*.*

Definition

Let the variables be partitioned into $\overline{x} = \overline{x}_1, \cdots, \overline{x}_d$. A monomial is **set-multilinear** if is a product of one variable per $\overline{x}_i$, e.g. $\prod_{i=1}^{d} x_{i,j_i}$. A polynomial is **set-multilinear** if all monomials are set-multilinear. A circuit is **set-multilinear** if all gates compute set-multilinear polynomials.

Theorem (Binet-Minc)

The rectangular permanent $\mathrm{perm}_{n,d} = \sum_{\sigma:[d]\hookrightarrow[n]} \prod_{i=1}^{d} x_{i,\sigma(i)}$ *has* $\mathrm{poly}(n, d^d)$*-size depth-4 set-multilinear circuit, over any* $\mathbb{F}$*.*

Example

$\mathrm{perm}_{n,2}(\overline{x}, \overline{y})$

Definition

Let the variables be partitioned into $\overline{x} = \overline{x}_1, \cdots, \overline{x}_d$. A monomial is **set-multilinear** if is a product of one variable per $\overline{x}_i$, e.g. $\prod_{i=1}^{d} x_{i,j_i}$. A polynomial is **set-multilinear** if all monomials are set-multilinear. A circuit is **set-multilinear** if all gates compute set-multilinear polynomials.

Theorem (Binet-Minc)

The rectangular permanent $\mathrm{perm}_{n,d} = \sum_{\sigma:[d]\hookrightarrow[n]} \prod_{i=1}^{d} x_{i,\sigma(i)}$ *has* $\mathrm{poly}(n, d^d)$*-size depth-4 set-multilinear circuit, over any* $\mathbb{F}$*.*

Example

$\mathrm{perm}_{n,2}(\overline{x}, \overline{y}) = \sum_{i \neq j} x_i y_j$

Definition

Let the variables be partitioned into $\overline{x} = \overline{x}_1, \cdots, \overline{x}_d$. A monomial is **set-multilinear** if is a product of one variable per $\overline{x}_i$, e.g. $\prod_{i=1}^{d} x_{i,j_i}$. A polynomial is **set-multilinear** if all monomials are set-multilinear. A circuit is **set-multilinear** if all gates compute set-multilinear polynomials.

Theorem (Binet-Minc)

The rectangular permanent $\mathrm{perm}_{n,d} = \sum_{\sigma:[d]\hookrightarrow[n]} \prod_{i=1}^{d} x_{i,\sigma(i)}$ *has* $\mathrm{poly}(n, d^d)$*-size depth-4 set-multilinear circuit, over any* $\mathbb{F}$*.*

Example

$\mathrm{perm}_{n,2}(\overline{x}, \overline{y}) = \sum_{i\neq j} x_i y_j = (\sum_{i=1}^{n} x_i)(\sum_{j=1}^{n} y_j)$

Definition

Let the variables be partitioned into $\overline{x} = \overline{x}_1, \cdots, \overline{x}_d$. A monomial is **set-multilinear** if is a product of one variable per $\overline{x}_i$, e.g. $\prod_{i=1}^{d} x_{i,j_i}$. A polynomial is **set-multilinear** if all monomials are set-multilinear. A circuit is **set-multilinear** if all gates compute set-multilinear polynomials.

Theorem (Binet-Minc)

The rectangular permanent $\mathrm{perm}_{n,d} = \sum_{\sigma:[d]\hookrightarrow[n]} \prod_{i=1}^{d} x_{i,\sigma(i)}$ *has* $\mathrm{poly}(n, d^d)$*-size depth-4 set-multilinear circuit, over any* $\mathbb{F}$.

Example

$\mathrm{perm}_{n,2}(\overline{x}, \overline{y}) = \sum_{i \neq j} x_i y_j = (\sum_{i=1}^{n} x_i)(\sum_{j=1}^{n} y_j) - \sum_i x_i y_i$

Definition

Let the variables be partitioned into $\overline{x} = \overline{x}_1, \cdots, \overline{x}_d$. A monomial is **set-multilinear** if is a product of one variable per $\overline{x}_i$, e.g. $\prod_{i=1}^{d} x_{i,j_i}$. A polynomial is **set-multilinear** if all monomials are set-multilinear. A circuit is **set-multilinear** if all gates compute set-multilinear polynomials.

Theorem (Binet-Minc)

The rectangular permanent $\mathrm{perm}_{n,d} = \sum_{\sigma:[d]\hookrightarrow[n]} \prod_{i=1}^{d} x_{i,\sigma(i)}$ *has* $\mathrm{poly}(n, d^d)$*-size depth-4 set-multilinear circuit, over any* $\mathbb{F}$*.*

Example

$\mathrm{perm}_{n,2}(\overline{x}, \overline{y}) = \sum_{i \neq j} x_i y_j = (\sum_{i=1}^{n} x_i)(\sum_{j=1}^{n} y_j) - \sum_i x_i y_i$

$\mathrm{perm}_{n,3}(\overline{x}, \overline{y}, \overline{z})$

Definition

Let the variables be partitioned into $\overline{x} = \overline{x}_1, \cdots, \overline{x}_d$. A monomial is **set-multilinear** if is a product of one variable per $\overline{x}_i$, e.g. $\prod_{i=1}^{d} x_{i,j_i}$. A polynomial is **set-multilinear** if all monomials are set-multilinear. A circuit is **set-multilinear** if all gates compute set-multilinear polynomials.

Theorem (Binet-Minc)

The rectangular permanent $\mathrm{perm}_{n,d} = \sum_{\sigma:[d]\hookrightarrow[n]} \prod_{i=1}^{d} x_{i,\sigma(i)}$ *has* $\mathrm{poly}(n, d^d)$*-size depth-4 set-multilinear circuit, over any* $\mathbb{F}$.

Example

$\mathrm{perm}_{n,2}(\overline{x}, \overline{y}) = \sum_{i \neq j} x_i y_j = (\sum_{i=1}^{n} x_i)(\sum_{j=1}^{n} y_j) - \sum_i x_i y_i$
$\mathrm{perm}_{n,3}(\overline{x}, \overline{y}, \overline{z}) = \sum_{|\{i,j,k\}|=3} x_i y_j z_k$

Definition

Let the variables be partitioned into $\overline{x} = \overline{x}_1, \cdots, \overline{x}_d$. A monomial is **set-multilinear** if is a product of one variable per $\overline{x}_i$, e.g. $\prod_{i=1}^d x_{i,j_i}$. A polynomial is **set-multilinear** if all monomials are set-multilinear. A circuit is **set-multilinear** if all gates compute set-multilinear polynomials.

Theorem (Binet-Minc)

The rectangular permanent $\mathrm{perm}_{n,d} = \sum_{\sigma:[d]\hookrightarrow[n]} \prod_{i=1}^d x_{i,\sigma(i)}$ *has* $\mathrm{poly}(n, d^d)$*-size depth-4 set-multilinear circuit, over any* $\mathbb{F}$*.*

Example

$$\mathrm{perm}_{n,2}(\overline{x}, \overline{y}) = \sum_{i\neq j} x_i y_j = \left(\sum_{i=1}^n x_i\right)\left(\sum_{j=1}^n y_j\right) - \sum_i x_i y_i$$

$$\begin{aligned}\mathrm{perm}_{n,3}(\overline{x}, \overline{y}, \overline{z}) &= \sum_{|\{i,j,k\}|=3} x_i y_j z_k \\ &= \left(\sum_i x_i\right)\left(\sum_j y_j\right)\left(\sum_k z_k\right)\end{aligned}$$

Definition

Let the variables be partitioned into $\overline{x} = \overline{x}_1, \cdots, \overline{x}_d$. A monomial is **set-multilinear** if is a product of one variable per $\overline{x}_i$, e.g. $\prod_{i=1}^d x_{i,j_i}$. A polynomial is **set-multilinear** if all monomials are set-multilinear. A circuit is **set-multilinear** if all gates compute set-multilinear polynomials.

Theorem (Binet-Minc)

The rectangular permanent $\mathrm{perm}_{n,d} = \sum_{\sigma:[d]\hookrightarrow[n]} \prod_{i=1}^d x_{i,\sigma(i)}$ *has* $\mathrm{poly}(n, d^d)$*-size depth-4 set-multilinear circuit, over any* $\mathbb{F}$.

Example

$$\mathrm{perm}_{n,2}(\overline{x}, \overline{y}) = \sum_{i \neq j} x_i y_j = (\sum_{i=1}^n x_i)(\sum_{j=1}^n y_j) - \sum_i x_i y_i$$

$$\begin{aligned}\mathrm{perm}_{n,3}(\overline{x}, \overline{y}, \overline{z}) &= \sum_{|\{i,j,k\}|=3} x_i y_j z_k \\ &= (\sum_i x_i)(\sum_j y_j)(\sum_k z_k) - (\sum_i x_i y_i)(\sum_k z_k)\end{aligned}$$

Definition

Let the variables be partitioned into $\overline{x} = \overline{x}_1, \cdots, \overline{x}_d$. A monomial is **set-multilinear** if is a product of one variable per $\overline{x}_i$, e.g. $\prod_{i=1}^{d} x_{i,j_i}$. A polynomial is **set-multilinear** if all monomials are set-multilinear. A circuit is **set-multilinear** if all gates compute set-multilinear polynomials.

Theorem (Binet-Minc)

The rectangular permanent $\mathrm{perm}_{n,d} = \sum_{\sigma:[d]\hookrightarrow[n]} \prod_{i=1}^{d} x_{i,\sigma(i)}$ *has* $\mathrm{poly}(n, d^d)$*-size depth-4 set-multilinear circuit, over any* $\mathbb{F}$*.*

Example

$$\mathrm{perm}_{n,2}(\overline{x}, \overline{y}) = \sum_{i \neq j} x_i y_j = \left(\sum_{i=1}^{n} x_i\right)\left(\sum_{j=1}^{n} y_j\right) - \sum_i x_i y_i$$

$$\begin{aligned}\mathrm{perm}_{n,3}(\overline{x}, \overline{y}, \overline{z}) &= \sum_{|\{i,j,k\}|=3} x_i y_j z_k \\ &= \left(\sum_i x_i\right)\left(\sum_j y_j\right)\left(\sum_k z_k\right) - \left(\sum_i x_i y_i\right)\left(\sum_k z_k\right) - \cdots\end{aligned}$$

Definition

Let the variables be partitioned into $\overline{x} = \overline{x}_1, \cdots, \overline{x}_d$. A monomial is **set-multilinear** if is a product of one variable per $\overline{x}_i$, e.g. $\prod_{i=1}^d x_{i,j_i}$. A polynomial is **set-multilinear** if all monomials are set-multilinear. A circuit is **set-multilinear** if all gates compute set-multilinear polynomials.

Theorem (Binet-Minc)

The rectangular permanent $\mathrm{perm}_{n,d} = \sum_{\sigma:[d]\hookrightarrow[n]} \prod_{i=1}^d x_{i,\sigma(i)}$ *has* $\mathrm{poly}(n, d^d)$*-size depth-4 set-multilinear circuit, over any* $\mathbb{F}$*.*

Example

$$\mathrm{perm}_{n,2}(\overline{x},\overline{y}) = \sum_{i\neq j} x_i y_j = \left(\sum_{i=1}^n x_i\right)\left(\sum_{j=1}^n y_j\right) - \sum_i x_i y_i$$

$$\begin{aligned}\mathrm{perm}_{n,3}(\overline{x},\overline{y},\overline{z}) &= \sum_{|\{i,j,k\}|=3} x_i y_j z_k \\ &= \left(\sum_i x_i\right)\left(\sum_j y_j\right)\left(\sum_k z_k\right) - \left(\sum_i x_i y_i\right)\left(\sum_k z_k\right) - \cdots \\ &\qquad + 3\sum_i x_i y_i z_i\end{aligned}$$

Proposition (**F**24)

Proposition (**F**24)

The rectangular permanent is "complete" for set-multilinearization.

Proposition (**F**24)

The rectangular permanent is "complete" for set-multilinearization.

Proof.

Proposition (**F**24)

The rectangular permanent is "complete" for set-multilinearization.

Proof.

for depth-3 circuits,

Proposition ($\mathbf{F}$24)

The rectangular permanent is "complete" for set-multilinearization.

Proof.

for depth-3 circuits, with two sets of variables $\overline{x}, \overline{y}$.

Proposition (**F**24)

The rectangular permanent is "complete" for set-multilinearization.

Proof.

for depth-3 circuits, with two sets of variables $\overline{x}, \overline{y}$.

- suffices to extract set-multilinear each product gate individually

Proposition (**F**24)

The rectangular permanent is "complete" for set-multilinearization.

Proof.

for depth-3 circuits, with two sets of variables $\overline{x}, \overline{y}$.

- suffices to extract set-multilinear each product gate individually

  $\prod_{k=1}^{D}(\gamma_k + \sum_i \alpha_{k,i} x_i + \sum_j \beta_{k,j} y_j)$

Proposition (**F**24)

The rectangular permanent is "complete" for set-multilinearization.

Proof.

for depth-3 circuits, with two sets of variables $\overline{x}, \overline{y}$.

- suffices to extract set-multilinear each product gate individually

$$\prod_{k=1}^{D}(\gamma_k + \sum_i \alpha_{k,i} x_i + \sum_j \beta_{k,j} y_j) \approx \prod_k (1 + X_k + Y_k)$$

Proposition (**F**24)

The rectangular permanent is "complete" for set-multilinearization.

Proof.

for depth-3 circuits, with two sets of variables $\overline{x}, \overline{y}$.

- suffices to extract set-multilinear each product gate individually

$$\begin{aligned}\textstyle\prod_{k=1}^{D}(\gamma_k + \sum_i \alpha_{k,i}x_i + \sum_j \beta_{k,j}y_j) &\approx \textstyle\prod_k(1 + X_k + Y_k)\\ &= (1 + X_1 + Y_1)\cdots(1 + X_D + Y_D)\end{aligned}$$

Proposition (**F**24)

The rectangular permanent is "complete" for set-multilinearization.

Proof.

for depth-3 circuits, with two sets of variables $\overline{x}, \overline{y}$.

- suffices to extract set-multilinear each product gate individually

$$\begin{aligned}\prod_{k=1}^{D}(\gamma_k + \textstyle\sum_i \alpha_{k,i}x_i + \sum_j \beta_{k,j}y_j) &\approx \textstyle\prod_k (1 + X_k + Y_k)\\ &= (1 + X_1 + Y_1)\cdots(1 + X_D + Y_D)\\ &=\end{aligned}$$

Proposition (**F**24)

The rectangular permanent is "complete" for set-multilinearization.

Proof.

for depth-3 circuits, with two sets of variables $\overline{x}, \overline{y}$.

- suffices to extract set-multilinear each product gate individually

$$
\begin{aligned}
\textstyle\prod_{k=1}^{D}(\gamma_k + \sum_i \alpha_{k,i}x_i + \sum_j \beta_{k,j}y_j) &\approx \textstyle\prod_k (1 + X_k + Y_k) \\
&= (1 + X_1 + Y_1)\cdots(1 + X_D + Y_D) \\
&= \ \mathrm{perm}_{D,2}(\overline{X}, \overline{Y})
\end{aligned}
$$

Proposition (**F**24)

The rectangular permanent is "complete" for set-multilinearization.

Proof.

for depth-3 circuits, with two sets of variables $\overline{x}, \overline{y}$.

- suffices to extract set-multilinear each product gate individually

$$\begin{aligned}
\prod_{k=1}^{D}(\gamma_k + \textstyle\sum_i \alpha_{k,i} x_i + \sum_j \beta_{k,j} y_j) &\approx \prod_k (1 + X_k + Y_k) \\
&= (1 + X_1 + Y_1) \cdots (1 + X_D + Y_D) \\
&= \operatorname{perm}_{D,2}(\overline{X}, \overline{Y}) + (\text{non-set-mult terms})
\end{aligned}$$

Proposition (**F**24)

The rectangular permanent is "complete" for set-multilinearization.

Proof.

for depth-3 circuits, with two sets of variables $\overline{x}, \overline{y}$.

- suffices to extract set-multilinear each product gate individually

$$\begin{aligned}\prod_{k=1}^{D}(\gamma_k + \sum_i \alpha_{k,i}x_i + \sum_j \beta_{k,j}y_j) &\approx \prod_k(1 + X_k + Y_k)\\ &= (1 + X_1 + Y_1)\cdots(1 + X_D + Y_D)\\ &= \mathrm{perm}_{D,2}(\overline{X}, \overline{Y}) + (\text{non-set-mult terms})\end{aligned}$$

- apply depth-4 set-mult circuit for $\mathrm{perm}_{D,2}$

Proposition (**F**24)

The rectangular permanent is "complete" for set-multilinearization.

Proof.

for depth-3 circuits, with two sets of variables $\overline{x}, \overline{y}$.

- suffices to extract set-multilinear each product gate individually

$$\begin{aligned}\prod_{k=1}^{D}(\gamma_k + \sum_i \alpha_{k,i} x_i + \sum_j \beta_{k,j} y_j) &\approx \prod_k (1 + X_k + Y_k) \\ &= (1 + X_1 + Y_1) \cdots (1 + X_D + Y_D) \\ &= \ \mathrm{perm}_{D,2}(\overline{X}, \overline{Y}) + (\text{non-set-mult terms})\end{aligned}$$

- apply depth-4 set-mult circuit for $\mathrm{perm}_{D,2}$ to set-mult $X_i \leftarrow \sum_k \beta_{k,\ell} x_\ell,\ Y_j$ $\square$

Proposition (**F**24)

The rectangular permanent is "complete" for set-multilinearization.

Proof.

for depth-3 circuits, with two sets of variables $\overline{x}, \overline{y}$.

- suffices to extract set-multilinear each product gate individually

$$\begin{aligned}\prod_{k=1}^{D}(\gamma_k + \textstyle\sum_i \alpha_{k,i}x_i + \sum_j \beta_{k,j}y_j) &\approx \textstyle\prod_k(1 + X_k + Y_k)\\ &= (1 + X_1 + Y_1)\cdots(1 + X_D + Y_D)\\ &= \mathrm{perm}_{D,2}(\overline{X}, \overline{Y}) + (\text{non-set-mult terms})\end{aligned}$$

- apply depth-4 set-mult circuit for $\mathrm{perm}_{D,2}$ to set-mult $X_i \leftarrow \sum_k \beta_{k,\ell}x_\ell,\ Y_j$ □

Corollary

size s depth-3 circuit

Proposition (**F**24)

The rectangular permanent is "complete" for set-multilinearization.

Proof.

for depth-3 circuits, with two sets of variables $\overline{x}, \overline{y}$.

- suffices to extract set-multilinear each product gate individually

$$\begin{aligned}\prod_{k=1}^{D}(\gamma_k + \textstyle\sum_i \alpha_{k,i}x_i + \sum_j \beta_{k,j}y_j) &\approx \textstyle\prod_k(1 + X_k + Y_k) \\ &= (1 + X_1 + Y_1)\cdots(1 + X_D + Y_D) \\ &= \mathrm{perm}_{D,2}(\overline{X}, \overline{Y}) + (\text{non-set-mult terms})\end{aligned}$$

- apply depth-4 set-mult circuit for $\mathrm{perm}_{D,2}$ to set-mult $X_i \leftarrow \sum_k \beta_{k,\ell}x_\ell,\ Y_j$ □

Corollary

size s depth-3 circuit $\xRightarrow{\text{any } \mathbb{F}}$ *depth-5 set-multilinear circuit of size* $\mathrm{poly}(s, d^d)$.

This talk:

- LST22 gave super-polynomial lower bounds against constant-depth algebraic circuits, in *large* characteristic fields
  - low-depth homogenization via the Newton identities, in *large* characteristic fields
  - low-depth set-multilinearization (of homogeneous circuits), over *any* field
  - strong lower bounds against constant-depth set-multilinear circuits, over *any* field
- **this work:** LST22 over *any* field
  - proof 1 (logical): proof LST22 is sufficiently "algebraic" so a proof in characteristic zero implies a proof over any field
  - proof 2 (constructive): low-depth set-multilinearization (of general circuits), via the Binet-Minc identity, over *any* field

Open Questions:

- low-depth homogenization over any field?

Thanks!

TOC