Diagonal Circuit Identity Testing and Lower Bounds

Nitin Saxena

Hausdorff Center for Mathematics
Bonn, Germany

ICALP 2008
Reykjavik

Outline

The Problem

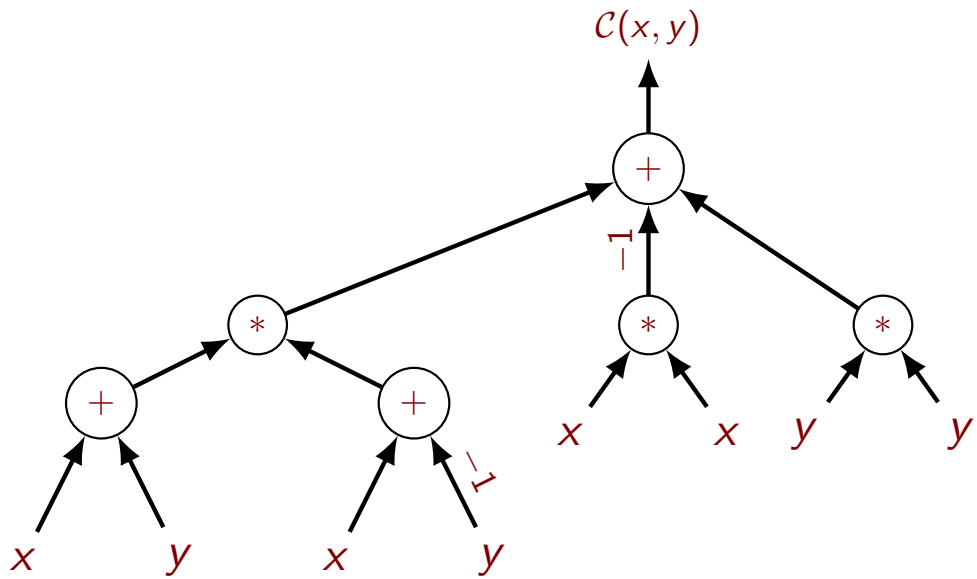
- Arithmetic circuits, over a field $\mathbb{F}$, compute a polynomial.

- Identity testing is the problem of checking whether a given circuit is zero or not.

The Problem

- Arithmetic circuits, over a field $\mathbb{F}$, compute a polynomial.

$\mathcal{C}$:

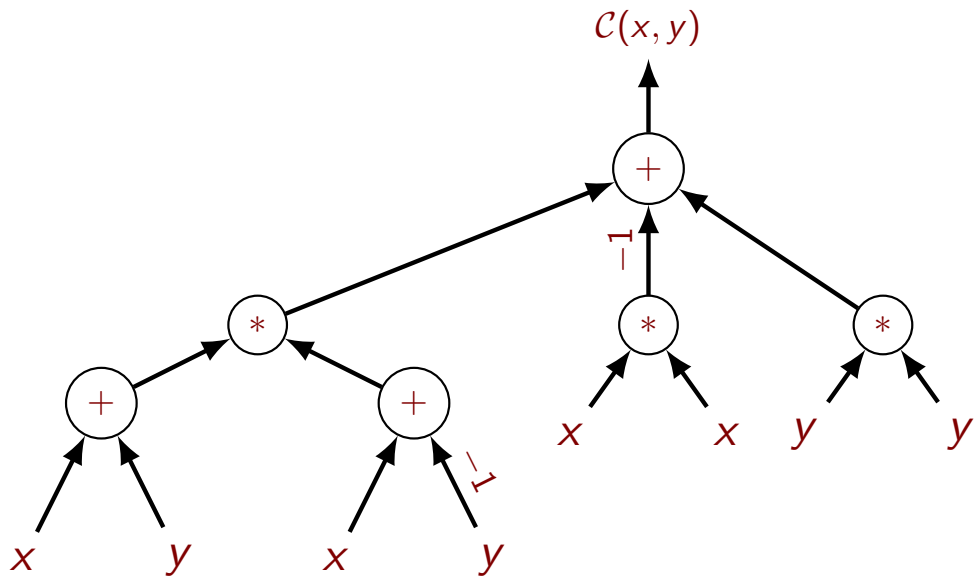


- Identity testing is the problem of checking whether a given circuit is zero or not.

The Problem

- Arithmetic circuits, over a field $\mathbb{F}$, compute a polynomial.

$\mathcal{C}$:



- Identity testing is the problem of checking whether a given circuit is zero or not.

Motivation

- It is a natural algebraic problem but no efficient algorithm is known.
- Identity testing is instrumental in many results: Parallel algorithms for matching problems (Lovasz '79), PSPACE=IP (Shamir '92), PCP theorem (Arora-Safra '97) and primality testing (AKS '02).
- (Schwartz '80, Zippel '79) gave a randomized algorithm for identity testing.
- (Impagliazzo-Kabanets '03) showed that derandomizing identity testing would mean proving lower bounds for either NEXP or Permanent.

Motivation

- It is a natural algebraic problem but no efficient algorithm is known.
- Identity testing is instrumental in many results: Parallel algorithms for matching problems (Lovasz '79), PSPACE=IP (Shamir '92), PCP theorem (Arora-Safra '97) and primality testing (AKS '02).
- (Schwartz '80, Zippel '79) gave a randomized algorithm for identity testing.
- (Impagliazzo-Kabanets '03) showed that derandomizing identity testing would mean proving lower bounds for either NEXP or Permanent.

Motivation

- It is a natural algebraic problem but no efficient algorithm is known.
- Identity testing is instrumental in many results: Parallel algorithms for matching problems (Lovasz '79), PSPACE=IP (Shamir '92), PCP theorem (Arora-Safra '97) and primality testing (AKS '02).
- (Schwartz '80, Zippel '79) gave a randomized algorithm for identity testing.
- (Impagliazzo-Kabanets '03) showed that derandomizing identity testing would mean proving lower bounds for either NEXP or Permanent.

Motivation

- It is a natural algebraic problem but no efficient algorithm is known.
- Identity testing is instrumental in many results: Parallel algorithms for matching problems (Lovasz '79), PSPACE=IP (Shamir '92), PCP theorem (Arora-Safra '97) and primality testing (AKS '02).
- (Schwartz '80, Zippel '79) gave a randomized algorithm for identity testing.
- (Impagliazzo-Kabanets '03) showed that derandomizing identity testing would mean proving lower bounds for either NEXP or Permanent.

Outline

Special Cases of Identity Testing

- Non-commutative formulas: (Raz & Shpilka '04) gave a deterministic polynomial time identity test.
- Circuits of depth 3 with bounded top fanin: (Kayal & Saxena '06) gave a deterministic polynomial time identity test.

Special Cases of Identity Testing

- Non-commutative formulas: (Raz & Shpilka '04) gave a deterministic polynomial time identity test.
- Circuits of depth 3 with bounded top fanin: (Kayal & Saxena '06) gave a deterministic polynomial time identity test.

Outline

The Notation

- For identity testing, wlog we can assume that a depth 4 circuit has a $+$ gate at the top.
- Thus, a depth 4 circuit is a "sum of product of sparse polynomials" ($\Sigma\Pi\Sigma\Pi$ *circuit*).
- Explicitly, a depth-4 circuit C over a field $\mathbb{F}$ will look like:

$$C(x_1, \ldots, x_n) = T_1 + \cdots + T_k$$

where, T_i is a product of polynomials $L_{i,1}, \ldots, L_{i,d}$

where, $L_{i,j}(\bar{x}) = \sum_{\bar{\ell}} a_{i,j,\bar{\ell}} \bar{x}^{\bar{\ell}}$, a's $\in \mathbb{F}$.

The Notation

- For identity testing, wlog we can assume that a depth 4 circuit has a $+$ gate at the top.
- Thus, a depth 4 circuit is a "sum of product of sparse polynomials" ($\Sigma\Pi\Sigma\Pi$ *circuit*).
- Explicitly, a depth-4 circuit C over a field $\mathbb{F}$ will look like:

$$C(x_1, \ldots, x_n) = T_1 + \cdots + T_k$$

where, T_i is a product of polynomials $L_{i,1}, \ldots, L_{i,d}$

where, $L_{i,j}(\bar{x}) = \sum_{\bar{\ell}} a_{i,j,\bar{\ell}} \bar{x}^{\bar{\ell}}$, a's $\in \mathbb{F}$.

The Notation

- For identity testing, wlog we can assume that a depth 4 circuit has a $+$ gate at the top.
- Thus, a depth 4 circuit is a "sum of product of sparse polynomials" ($\Sigma\Pi\Sigma\Pi$ *circuit*).
- Explicitly, a depth-4 circuit $\mathcal{C}$ over a field $\mathbb{F}$ will look like:

$$\mathcal{C}(x_1, \ldots, x_n) = T_1 + \cdots + T_k$$

where, T_i is a product of polynomials $L_{i,1}, \ldots, L_{i,d}$

where, $L_{i,j}(\overline{x}) = \sum_{\overline{\ell}} a_{i,j,\overline{\ell}} \overline{x}^{\overline{\ell}}$, a's $\in \mathbb{F}$.

The Notation

- For identity testing, wlog we can assume that a depth 4 circuit has a $+$ gate at the top.
- Thus, a depth 4 circuit is a "sum of product of sparse polynomials" ($\Sigma\Pi\Sigma\Pi$ *circuit*).
- Explicitly, a depth-4 circuit $\mathcal{C}$ over a field $\mathbb{F}$ will look like:

$$\mathcal{C}(x_1, \ldots, x_n) = T_1 + \cdots + T_k$$

where, T_i is a product of polynomials $L_{i,1}, \ldots, L_{i,d}$

where, $L_{i,j}(\overline{x}) = \sum_{\overline{\ell}} a_{i,j,\overline{\ell}} \overline{x}^{\overline{\ell}}$, a's $\in \mathbb{F}$.

The Notation

- For identity testing, wlog we can assume that a depth 4 circuit has a $+$ gate at the top.
- Thus, a depth 4 circuit is a "sum of product of sparse polynomials" ($\Sigma\Pi\Sigma\Pi$ *circuit*).
- Explicitly, a depth-4 circuit $\mathcal{C}$ over a field $\mathbb{F}$ will look like:

$$\mathcal{C}(x_1, \ldots, x_n) = T_1 + \cdots + T_k$$

where, T_i is a product of polynomials $L_{i,1}, \ldots, L_{i,d}$

where, $L_{i,j}(\overline{x}) = \sum_{\overline{\ell}} a_{i,j,\overline{\ell}} \overline{x}^{\overline{\ell}}$, a's $\in \mathbb{F}$.

The Notation

- For identity testing, wlog we can assume that a depth 4 circuit has a $+$ gate at the top.
- Thus, a depth 4 circuit is a "sum of product of sparse polynomials" ($\Sigma\Pi\Sigma\Pi$ *circuit*).
- Explicitly, a depth-4 circuit $\mathcal{C}$ over a field $\mathbb{F}$ will look like:

$$\mathcal{C}(x_1, \ldots, x_n) = T_1 + \cdots + T_k$$

where, T_i is a product of polynomials $L_{i,1}, \ldots, L_{i,d}$

where, $L_{i,j}(\overline{x}) = \sum_{\overline{\ell}} a_{i,j,\overline{\ell}} \overline{x}^{\overline{\ell}}$, a's $\in \mathbb{F}$.

Peculiarity of Depth-4

- Depth-4 is not just another circuit restriction!
- Agrawal & Vinay (FOCS 2008) show that proving exponential lower bounds for depth-4 circuits imply exponential lower bounds for unrestricted depth circuits.
- Also, a black-box derandomization of identity testing for depth-4 circuits implies a *nearly* complete derandomization of general identity testing.

Peculiarity of Depth-4

- Depth-4 is not just another circuit restriction!
- Agrawal & Vinay (FOCS 2008) show that proving exponential lower bounds for depth-4 circuits imply exponential lower bounds for unrestricted depth circuits.
- Also, a black-box derandomization of identity testing for depth-4 circuits implies a *nearly* complete derandomization of general identity testing.

Peculiarity of Depth-4

- Depth-4 is not just another circuit restriction!
- Agrawal & Vinay (FOCS 2008) show that proving exponential lower bounds for depth-4 circuits imply exponential lower bounds for unrestricted depth circuits.
- Also, a black-box derandomization of identity testing for depth-4 circuits implies a *nearly* complete derandomization of general identity testing.

Diagonal Depth-4 Circuits

- Here we look at the case of depth-4 when the inputs to the multiplication gates are just sums of univariates.
- A *diagonal* depth-4 circuit $\mathcal{C}$ over a field $\mathbb{F}$ looks like:

$$\mathcal{C}(x_1, \ldots, x_n) = T_1 + \cdots + T_k$$

where, T_i is a product of polynomials $L_{i,1}, \ldots, L_{i,d}$

where, $L_{i,j}(\overline{x}) = \sum_{\ell=1}^{n} g_{i,j,\ell}(x_\ell)$

- Newton's identities are of this form:

$$(x_1 + x_2 + x_3)^3 + 2(x_1^3 + x_2^3 + x_3^3) - 3(x_1 + x_2 + x_3)(x_1^2 + x_2^2 + x_3^2) - 6x_1x_2x_3 = 0$$

Diagonal Depth-4 Circuits

- Here we look at the case of depth-4 when the inputs to the multiplication gates are just sums of univariates.
- A *diagonal* depth-4 circuit $\mathcal{C}$ over a field $\mathbb{F}$ looks like:

$$\mathcal{C}(x_1, \ldots, x_n) = T_1 + \cdots + T_k$$

where, T_i is a product of polynomials $L_{i,1}, \ldots, L_{i,d}$

where, $L_{i,j}(\overline{x}) = \sum_{\ell=1}^{n} g_{i,j,\ell}(x_\ell)$

- Newton's identities are of this form:

$$(x_1 + x_2 + x_3)^3 + 2(x_1^3 + x_2^3 + x_3^3) - 3(x_1 + x_2 + x_3)(x_1^2 + x_2^2 + x_3^2) - 6x_1x_2x_3 = 0$$

Diagonal Depth-4 Circuits

- Here we look at the case of depth-4 when the inputs to the multiplication gates are just sums of univariates.
- A *diagonal* depth-4 circuit $\mathcal{C}$ over a field $\mathbb{F}$ looks like:

$$\mathcal{C}(x_1, \ldots, x_n) = T_1 + \cdots + T_k$$

where, T_i is a product of polynomials $L_{i,1}, \ldots, L_{i,d}$

where, $L_{i,j}(\overline{x}) = \sum_{\ell=1}^{n} g_{i,j,\ell}(x_\ell)$

- Newton's identities are of this form:

$$(x_1 + x_2 + x_3)^3 + 2(x_1^3 + x_2^3 + x_3^3) - 3(x_1 + x_2 + x_3)(x_1^2 + x_2^2 + x_3^2) - 6x_1x_2x_3 = 0$$

Diagonal Depth-4 Circuits

- Here we look at the case of depth-4 when the inputs to the multiplication gates are just sums of univariates.
- A *diagonal* depth-4 circuit $\mathcal{C}$ over a field $\mathbb{F}$ looks like:

$$\mathcal{C}(x_1, \ldots, x_n) = T_1 + \cdots + T_k$$

where, T_i is a product of polynomials $L_{i,1}, \ldots, L_{i,d}$

where, $L_{i,j}(\overline{x}) = \sum_{\ell=1}^{n} g_{i,j,\ell}(x_\ell)$

- Newton's identities are of this form:

$$(x_1 + x_2 + x_3)^3 + 2(x_1^3 + x_2^3 + x_3^3) - 3(x_1 + x_2 + x_3)(x_1^2 + x_2^2 + x_3^2) - 6x_1x_2x_3 = 0$$

Diagonal Depth-4 Circuits

- Here we look at the case of depth-4 when the inputs to the multiplication gates are just sums of univariates.
- A *diagonal* depth-4 circuit $\mathcal{C}$ over a field $\mathbb{F}$ looks like:

$$\mathcal{C}(x_1, \ldots, x_n) = T_1 + \cdots + T_k$$

where, T_i is a product of polynomials $L_{i,1}, \ldots, L_{i,d}$

where, $L_{i,j}(\overline{x}) = \sum_{\ell=1}^{n} g_{i,j,\ell}(x_\ell)$

- Newton's identities are of this form:

$$(x_1 + x_2 + x_3)^3 + 2(x_1^3 + x_2^3 + x_3^3) - 3(x_1 + x_2 + x_3)(x_1^2 + x_2^2 + x_3^2) - 6x_1x_2x_3 = 0$$

Diagonal Depth-4 Circuits

- Here we look at the case of depth-4 when the inputs to the multiplication gates are just sums of univariates.
- A *diagonal* depth-4 circuit $\mathcal{C}$ over a field $\mathbb{F}$ looks like:

$$\mathcal{C}(x_1, \ldots, x_n) = T_1 + \cdots + T_k$$

where, T_i is a product of polynomials $L_{i,1}, \ldots, L_{i,d}$

where, $L_{i,j}(\overline{x}) = \sum_{\ell=1}^{n} g_{i,j,\ell}(x_\ell)$

- Newton's identities are of this form:

$$(x_1 + x_2 + x_3)^3 + 2(x_1^3 + x_2^3 + x_3^3) - 3(x_1 + x_2 + x_3)(x_1^2 + x_2^2 + x_3^2) - 6x_1x_2x_3 = 0$$

Outline

The Four Ideas

We transform a diagonal circuit $\mathcal{C}$ to a form that is easier to handle. The main ideas are:

(1) We note that the multiplication gate $L_1^{e_1} \dots L_s^{e_s}$ appears in the power series of $exp(zz_1L_1 + \dots + zz_sL_s)$.

(2) We evaluate $exp(zz_1L_1 + \dots + zz_sL_s)$ for various values of z and extract $L_1^{e_1} \dots L_s^{e_s}$ by interpolation.

(3) We transform each multiplication gate to the form above and then stitch them to get a dual form of $\mathcal{C}$: a sum of product of univariates over an algebra.

(4) The above transformation needs a slight modification in the case when the field is of prime characteristic.

The Four Ideas

We transform a diagonal circuit $\mathcal{C}$ to a form that is easier to handle. The main ideas are:

(1) We note that the multiplication gate $L_1^{e_1} \dots L_s^{e_s}$ appears in the power series of $exp(zz_1L_1 + \cdots + zz_sL_s)$.

(2) We evaluate $exp(zz_1L_1 + \cdots + zz_sL_s)$ for various values of z and extract $L_1^{e_1} \dots L_s^{e_s}$ by interpolation.

(3) We transform each multiplication gate to the form above and then stitch them to get a dual form of $\mathcal{C}$: a sum of product of univariates over an algebra.

(4) The above transformation needs a slight modification in the case when the field is of prime characteristic.

The Four Ideas

We transform a diagonal circuit $\mathcal{C}$ to a form that is easier to handle. The main ideas are:

(1) We note that the multiplication gate $L_1^{e_1} \dots L_s^{e_s}$ appears in the power series of $exp(zz_1L_1 + \cdots + zz_sL_s)$.

(2) We evaluate $exp(zz_1L_1 + \cdots + zz_sL_s)$ for various values of z and extract $L_1^{e_1} \dots L_s^{e_s}$ by interpolation.

(3) We transform each multiplication gate to the form above and then stitch them to get a dual form of $\mathcal{C}$: a sum of product of univariates over an algebra.

(4) The above transformation needs a slight modification in the case when the field is of prime characteristic.

The Four Ideas

We transform a diagonal circuit $\mathcal{C}$ to a form that is easier to handle. The main ideas are:

(1) We note that the multiplication gate $L_1^{e_1} \dots L_s^{e_s}$ appears in the power series of $exp(zz_1L_1 + \dots + zz_sL_s)$.

(2) We evaluate $exp(zz_1L_1 + \dots + zz_sL_s)$ for various values of z and extract $L_1^{e_1} \dots L_s^{e_s}$ by interpolation.

(3) We transform each multiplication gate to the form above and then stitch them to get a dual form of $\mathcal{C}$: a sum of product of univariates over an algebra.

(4) The above transformation needs a slight modification in the case when the field is of prime characteristic.

The Four Ideas

We transform a diagonal circuit $\mathcal{C}$ to a form that is easier to handle. The main ideas are:

(1) We note that the multiplication gate $L_1^{e_1} \dots L_s^{e_s}$ appears in the power series of $exp(zz_1L_1 + \cdots + zz_sL_s)$.

(2) We evaluate $exp(zz_1L_1 + \cdots + zz_sL_s)$ for various values of z and extract $L_1^{e_1} \dots L_s^{e_s}$ by interpolation.

(3) We transform each multiplication gate to the form above and then stitch them to get a dual form of $\mathcal{C}$: a sum of product of univariates over an algebra.

(4) The above transformation needs a slight modification in the case when the field is of prime characteristic.

The Four Ideas

We transform a diagonal circuit $\mathcal{C}$ to a form that is easier to handle. The main ideas are:

(1) We note that the multiplication gate $L_1^{e_1} \dots L_s^{e_s}$ appears in the power series of $exp(zz_1L_1 + \cdots + zz_sL_s)$.

(2) We evaluate $exp(zz_1L_1 + \cdots + zz_sL_s)$ for various values of z and extract $L_1^{e_1} \dots L_s^{e_s}$ by interpolation.

(3) We transform each multiplication gate to the form above and then stitch them to get a dual form of $\mathcal{C}$: a sum of product of univariates over an algebra.

(4) The above transformation needs a slight modification in the case when the field is of prime characteristic.

The Four Ideas

We transform a diagonal circuit $\mathcal{C}$ to a form that is easier to handle. The main ideas are:

(1) We note that the multiplication gate $L_1^{e_1} \dots L_s^{e_s}$ appears in the power series of $exp(zz_1L_1 + \cdots + zz_sL_s)$.

(2) We evaluate $exp(zz_1L_1 + \cdots + zz_sL_s)$ for various values of z and extract $L_1^{e_1} \dots L_s^{e_s}$ by interpolation.

(3) We transform each multiplication gate to the form above and then stitch them to get a dual form of $\mathcal{C}$: a sum of product of univariates over an algebra.

(4) The above transformation needs a slight modification in the case when the field is of prime characteristic.

The Four Ideas

We transform a diagonal circuit $\mathcal{C}$ to a form that is easier to handle. The main ideas are:

(1) We note that the multiplication gate $L_1^{e_1} \dots L_s^{e_s}$ appears in the power series of $exp(zz_1L_1 + \cdots + zz_sL_s)$.

(2) We evaluate $exp(zz_1L_1 + \cdots + zz_sL_s)$ for various values of z and extract $L_1^{e_1} \dots L_s^{e_s}$ by interpolation.

(3) We transform each multiplication gate to the form above and then stitch them to get a dual form of $\mathcal{C}$: a sum of product of univariates over an algebra.

(4) The above transformation needs a slight modification in the case when the field is of prime characteristic.

The Four Ideas

We transform a diagonal circuit $\mathcal{C}$ to a form that is easier to handle. The main ideas are:

(1) We note that the multiplication gate $L_1^{e_1} \dots L_s^{e_s}$ appears in the power series of $exp(zz_1L_1 + \cdots + zz_sL_s)$.

(2) We evaluate $exp(zz_1L_1 + \cdots + zz_sL_s)$ for various values of z and extract $L_1^{e_1} \dots L_s^{e_s}$ by interpolation.

(3) We transform each multiplication gate to the form above and then stitch them to get a dual form of $\mathcal{C}$: a sum of product of univariates over an algebra.

(4) The above transformation needs a slight modification in the case when the field is of prime characteristic.

Idea 1: Power Series

- We embed a multiplication gate $L_1^{e_1} \cdots L_s^{e_s}$, where $L_i = \sum_{j=1}^{n} g_{i,j}(x_j)$, in a power series:
- where, $e = (e_1 + \cdots + e_s)$ and E_e is the truncated $\exp(x)$: $1 + x + \cdots + \frac{x^e}{e!}$.

Idea 1: Power Series

- We embed a multiplication gate $L_1^{e_1} \cdots L_s^{e_s}$, where $L_i = \sum_{j=1}^{n} g_{i,j}(x_j)$, in a power series:

$$(e_1! \cdots e_s!)^{-1} \cdot L_1^{e_1} \cdots L_s^{e_s} = [z^e z_1^{e_1} \cdots z_s^{e_s}] \exp(z z_1 L_1) \cdots \exp(z z_s L_s)$$

- where, $e = (e_1 + \cdots + e_s)$ and E_e is the truncated $\exp(x)$: $1 + x + \cdots + \frac{x^e}{e!}$.

Idea 1: Power Series

- We embed a multiplication gate $L_1^{e_1} \cdots L_s^{e_s}$, where $L_i = \sum_{j=1}^{n} g_{i,j}(x_j)$, in a power series:

$$(e_1! \cdots e_s!)^{-1} \cdot L_1^{e_1} \cdots L_s^{e_s} = [z^e z_1^{e_1} \cdots z_s^{e_s}] \exp(z z_1 L_1) \cdots \exp(z z_s L_s)$$
$$= [z^e z_1^{e_1} \cdots z_s^{e_s}] \exp(\textstyle\sum_{i=1}^{s} z z_i L_i)$$

- where, $e = (e_1 + \cdots + e_s)$ and E_e is the truncated $\exp(x)$: $1 + x + \cdots + \frac{x^e}{e!}$.

Idea 1: Power Series

- We embed a multiplication gate $L_1^{e_1} \cdots L_s^{e_s}$, where $L_i = \sum_{j=1}^{n} g_{i,j}(x_j)$, in a power series:

$$\begin{aligned}(e_1! \cdots e_s!)^{-1} \cdot L_1^{e_1} \cdots L_s^{e_s} &= [z^e z_1^{e_1} \cdots z_s^{e_s}] \exp(zz_1 L_1) \cdots \exp(zz_s L_s) \\ &= [z^e z_1^{e_1} \cdots z_s^{e_s}] \exp(\textstyle\sum_{i=1}^{s} zz_i L_i) \\ &= [z^e z_1^{e_1} \cdots z_s^{e_s}] \prod_{j=1}^{n} \exp\left((z_1 g_{1,j} + \cdots + z_s g_{s,j})z\right)\end{aligned}$$

- where, $e = (e_1 + \cdots + e_s)$ and E_e is the truncated $\exp(x)$: $1 + x + \cdots + \frac{x^e}{e!}$.

Idea 1: Power Series

- We embed a multiplication gate $L_1^{e_1} \cdots L_s^{e_s}$, where $L_i = \sum_{j=1}^{n} g_{i,j}(x_j)$, in a power series:

$$\begin{aligned}(e_1! \cdots e_s!)^{-1} \cdot L_1^{e_1} \cdots L_s^{e_s} &= [z^e z_1^{e_1} \cdots z_s^{e_s}] \exp(z z_1 L_1) \cdots \exp(z z_s L_s) \\ &= [z^e z_1^{e_1} \cdots z_s^{e_s}] \exp(\textstyle\sum_{i=1}^{s} z z_i L_i) \\ &= [z^e z_1^{e_1} \cdots z_s^{e_s}] \prod_{j=1}^{n} \exp\left((z_1 g_{1,j} + \cdots + z_s g_{s,j}) z\right) \\ &= [z^e z_1^{e_1} \cdots z_s^{e_s}] \prod_{j=1}^{n} E_e\left((z_1 g_{1,j} + \cdots + z_s g_{s,j}) z\right)\end{aligned}$$

- where, $e = (e_1 + \cdots + e_s)$ and E_e is the truncated $\exp(x)$: $1 + x + \cdots + \frac{x^e}{e!}$.

Idea 1: Power Series

- We embed a multiplication gate $L_1^{e_1} \cdots L_s^{e_s}$, where $L_i = \sum_{j=1}^{n} g_{i,j}(x_j)$, in a power series:

$$\begin{aligned}(e_1! \cdots e_s!)^{-1} \cdot L_1^{e_1} \cdots L_s^{e_s} &= [z^e z_1^{e_1} \cdots z_s^{e_s}] \exp(z z_1 L_1) \cdots \exp(z z_s L_s) \\ &= [z^e z_1^{e_1} \cdots z_s^{e_s}] \exp(\textstyle\sum_{i=1}^{s} z z_i L_i) \\ &= [z^e z_1^{e_1} \cdots z_s^{e_s}] \prod_{j=1}^{n} \exp\left((z_1 g_{1,j} + \cdots + z_s g_{s,j}) z\right) \\ &= [z^e z_1^{e_1} \cdots z_s^{e_s}] \prod_{j=1}^{n} E_e\left((z_1 g_{1,j} + \cdots + z_s g_{s,j}) z\right)\end{aligned}$$

- where, $e = (e_1 + \cdots + e_s)$ and E_e is the truncated $\exp(x)$: $1 + x + \cdots + \frac{x^e}{e!}$.

Idea 1: Power Series

- We embed a multiplication gate $L_1^{e_1} \cdots L_s^{e_s}$, where $L_i = \sum_{j=1}^{n} g_{i,j}(x_j)$, in a power series:

$$\begin{aligned}(e_1! \cdots e_s!)^{-1} \cdot L_1^{e_1} \cdots L_s^{e_s} &= [z^e z_1^{e_1} \cdots z_s^{e_s}] \exp(z z_1 L_1) \cdots \exp(z z_s L_s) \\ &= [z^e z_1^{e_1} \cdots z_s^{e_s}] \exp(\textstyle\sum_{i=1}^{s} z z_i L_i) \\ &= [z^e z_1^{e_1} \cdots z_s^{e_s}] \prod_{j=1}^{n} \exp\left((z_1 g_{1,j} + \cdots + z_s g_{s,j}) z\right) \\ &= [z^e z_1^{e_1} \cdots z_s^{e_s}] \prod_{j=1}^{n} E_e\left((z_1 g_{1,j} + \cdots + z_s g_{s,j}) z\right)\end{aligned}$$

- where, $e = (e_1 + \cdots + e_s)$ and E_e is the truncated $\exp(x)$: $1 + x + \cdots + \frac{x^e}{e!}$.

Idea 2: Interpolation

- We will now extract the degree e part from the above expression.
- If we look at the above sum modulo the ideal $(z_1^{e_1+1}, \ldots, z_s^{e_s+1})$ then the surviving monomial in $\overline{z}$ is exactly $z_1^{e_1} \cdots z_s^{e_s}$.
- Thus, over the algebra $R := \mathbb{F}[z_1, \ldots, z_s]/(z_1^{e_1+1}, \ldots, z_s^{e_s+1})$:
- Thus, we expressed the diagonal depth-4 multiplication gate as a sum-of-product-of-univariates.

Idea 2: Interpolation

- We will now extract the degree e part from the above expression.

$$(e_1! \cdots e_s!)^{-1} \cdot L_1^{e_1} \cdots L_s^{e_s} = [z^e z_1^{e_1} \cdots z_s^{e_s}] \prod_{i=1}^{n} E_e\left((z_1 g_{1,i} + \cdots + z_s g_{s,i})z\right)$$

- If we look at the above sum modulo the ideal $(z_1^{e_1+1}, \ldots, z_s^{e_s+1})$ then the surviving monomial in $\overline{z}$ is exactly $z_1^{e_1} \cdots z_s^{e_s}$.
- Thus, over the algebra $R := \mathbb{F}[z_1, \ldots, z_s]/(z_1^{e_1+1}, \ldots, z_s^{e_s+1})$:
- Thus, we expressed the diagonal depth-4 multiplication gate as a sum-of-product-of-univariates.

Idea 2: Interpolation

- We will now extract the degree e part from the above expression.

$$(e_1! \cdots e_s!)^{-1} \cdot L_1^{e_1} \cdots L_s^{e_s} = [z^e z_1^{e_1} \cdots z_s^{e_s}] \prod_{i=1}^{n} E_e\left((z_1 g_{1,i} + \cdots + z_s g_{s,i}) z\right)$$
$$= [z_1^{e_1} \cdots z_s^{e_s}] \sum_{j=1}^{ne+1} \beta_j \cdot \prod_{i=1}^{n} E_e\left((z_1 g_{1,i} + \cdots + z_s g_{s,i}) \alpha_j\right)$$

- If we look at the above sum modulo the ideal $(z_1^{e_1+1}, \ldots, z_s^{e_s+1})$ then the surviving monomial in $\overline{z}$ is exactly $z_1^{e_1} \cdots z_s^{e_s}$.
- Thus, over the algebra $R := \mathbb{F}[z_1, \ldots, z_s]/(z_1^{e_1+1}, \ldots, z_s^{e_s+1})$:
- Thus, we expressed the diagonal depth-4 multiplication gate as a sum-of-product-of-univariates.

Idea 2: Interpolation

- We will now extract the degree e part from the above expression.

$$(e_1! \cdots e_s!)^{-1} \cdot L_1^{e_1} \cdots L_s^{e_s} = [z^e z_1^{e_1} \cdots z_s^{e_s}] \prod_{i=1}^{n} E_e\left((z_1 g_{1,i} + \cdots + z_s g_{s,i}) z\right)$$
$$= [z_1^{e_1} \cdots z_s^{e_s}] \sum_{j=1}^{ne+1} \beta_j \cdot \prod_{i=1}^{n} E_e\left((z_1 g_{1,i} + \cdots + z_s g_{s,i}) \alpha_j\right)$$

- If we look at the above sum modulo the ideal $(z_1^{e_1+1}, \ldots, z_s^{e_s+1})$ then the surviving monomial in $\overline{z}$ is exactly $z_1^{e_1} \cdots z_s^{e_s}$.
- Thus, over the algebra $R := \mathbb{F}[z_1, \ldots, z_s]/(z_1^{e_1+1}, \ldots, z_s^{e_s+1})$:
- Thus, we expressed the diagonal depth-4 multiplication gate as a sum-of-product-of-univariates.

Idea 2: Interpolation

- We will now extract the degree e part from the above expression.

$$(e_1! \cdots e_s!)^{-1} \cdot L_1^{e_1} \cdots L_s^{e_s} = [z^e z_1^{e_1} \cdots z_s^{e_s}] \prod_{i=1}^{n} E_e((z_1 g_{1,i} + \cdots + z_s g_{s,i})z)$$
$$= [z_1^{e_1} \cdots z_s^{e_s}] \sum_{j=1}^{ne+1} \beta_j \cdot \prod_{i=1}^{n} E_e((z_1 g_{1,i} + \cdots + z_s g_{s,i})\alpha_j)$$

- If we look at the above sum modulo the ideal $(z_1^{e_1+1}, \ldots, z_s^{e_s+1})$ then the surviving monomial in $\overline{z}$ is exactly $z_1^{e_1} \cdots z_s^{e_s}$.
- Thus, over the algebra $R := \mathbb{F}[z_1, \ldots, z_s]/(z_1^{e_1+1}, \ldots, z_s^{e_s+1})$:
- Thus, we expressed the diagonal depth-4 multiplication gate as a sum-of-product-of-univariates.

Idea 2: Interpolation

- We will now extract the degree e part from the above expression.

$$(e_1! \cdots e_s!)^{-1} \cdot L_1^{e_1} \cdots L_s^{e_s} = [z^e z_1^{e_1} \cdots z_s^{e_s}] \prod_{i=1}^{n} E_e\left((z_1 g_{1,i} + \cdots + z_s g_{s,i})z\right)$$
$$= [z_1^{e_1} \cdots z_s^{e_s}] \sum_{j=1}^{ne+1} \beta_j \cdot \prod_{i=1}^{n} E_e\left((z_1 g_{1,i} + \cdots + z_s g_{s,i})\alpha_j\right)$$

- If we look at the above sum modulo the ideal $(z_1^{e_1+1}, \ldots, z_s^{e_s+1})$ then the surviving monomial in $\overline{z}$ is exactly $z_1^{e_1} \cdots z_s^{e_s}$.
- Thus, over the algebra $R := \mathbb{F}[z_1, \ldots, z_s]/(z_1^{e_1+1}, \ldots, z_s^{e_s+1})$:

$$\sum_{j=1}^{ne+1} \beta_j \cdot \prod_{i=1}^{n} E_e\left((z_1 g_{1,i} + \cdots + z_s g_{s,i})\alpha_j\right)$$

- Thus, we expressed the diagonal depth-4 multiplication gate as a sum-of-product-of-univariates.

Idea 2: Interpolation

- We will now extract the degree e part from the above expression.

$$(e_1! \cdots e_s!)^{-1} \cdot L_1^{e_1} \cdots L_s^{e_s} = [z^e z_1^{e_1} \cdots z_s^{e_s}] \prod_{i=1}^{n} E_e((z_1 g_{1,i} + \cdots + z_s g_{s,i})z)$$
$$= [z_1^{e_1} \cdots z_s^{e_s}] \sum_{j=1}^{ne+1} \beta_j \cdot \prod_{i=1}^{n} E_e((z_1 g_{1,i} + \cdots + z_s g_{s,i})\alpha_j)$$

- If we look at the above sum modulo the ideal $(z_1^{e_1+1}, \ldots, z_s^{e_s+1})$ then the surviving monomial in $\overline{z}$ is exactly $z_1^{e_1} \cdots z_s^{e_s}$.
- Thus, over the algebra $R := \mathbb{F}[z_1, \ldots, z_s]/(z_1^{e_1+1}, \ldots, z_s^{e_s+1})$:

$$\sum_{j=1}^{ne+1} \beta_j \cdot \prod_{i=1}^{n} E_e((z_1 g_{1,i} + \cdots + z_s g_{s,i})\alpha_j)$$
$$= (e_1! \cdots e_s!)^{-1} \cdot L_1^{e_1} \cdots L_s^{e_s} \cdot z_1^{e_1} \cdots z_s^{e_s}$$

- Thus, we expressed the diagonal depth-4 multiplication gate as a sum-of-product-of-univariates.

Idea 2: Interpolation

- We will now extract the degree e part from the above expression.

$$(e_1! \cdots e_s!)^{-1} \cdot L_1^{e_1} \cdots L_s^{e_s} = [z^e z_1^{e_1} \cdots z_s^{e_s}] \prod_{i=1}^{n} E_e\left((z_1 g_{1,i} + \cdots + z_s g_{s,i}) z\right)$$
$$= [z_1^{e_1} \cdots z_s^{e_s}] \sum_{j=1}^{ne+1} \beta_j \cdot \prod_{i=1}^{n} E_e\left((z_1 g_{1,i} + \cdots + z_s g_{s,i}) \alpha_j\right)$$

- If we look at the above sum modulo the ideal $(z_1^{e_1+1}, \ldots, z_s^{e_s+1})$ then the surviving monomial in $\overline{z}$ is exactly $z_1^{e_1} \cdots z_s^{e_s}$.
- Thus, over the algebra $R := \mathbb{F}[z_1, \ldots, z_s]/(z_1^{e_1+1}, \ldots, z_s^{e_s+1})$:

$$\sum_{j=1}^{ne+1} \beta_j \cdot \prod_{i=1}^{n} E_e\left((z_1 g_{1,i} + \cdots + z_s g_{s,i}) \alpha_j\right)$$
$$= (e_1! \cdots e_s!)^{-1} \cdot L_1^{e_1} \cdots L_s^{e_s} \cdot z_1^{e_1} \cdots z_s^{e_s}$$

- Thus, we expressed the diagonal depth-4 multiplication gate as a sum-of-product-of-univariates.

Idea 3: Dual Form

- Given a diagonal depth-4 circuit $C(\overline{x}) = T_1 + \cdots + T_k$, where $T_i = \prod_{j=1}^{s} L_{i,j}^{e_{i,j}}$.
- The last two ideas allow us to write T_i as a sum-of-product-of-univariates:
- The third idea is to *stitch* these k algebras R_i to an algebra R of dimension $\sum_{i=1}^{k}(1+e_{i,1})\cdots(1+e_{i,s})$.
- Such that over R, C is a sum-of-product-of-univariates:

Idea 3: Dual Form

- Given a diagonal depth-4 circuit $C(\overline{x}) = T_1 + \cdots + T_k$, where $T_i = \prod_{j=1}^{s} L_{i,j}^{e_{i,j}}$.
- The last two ideas allow us to write T_i as a sum-of-product-of-univariates:
- The third idea is to *stitch* these k algebras R_i to an algebra R of dimension $\sum_{i=1}^{k}(1+e_{i,1})\cdots(1+e_{i,s})$.
- Such that over R, C is a sum-of-product-of-univariates:

Idea 3: Dual Form

- Given a diagonal depth-4 circuit $C(\bar{x}) = T_1 + \cdots + T_k$, where $T_i = \prod_{j=1}^{s} L_{i,j}^{e_{i,j}}$.
- The last two ideas allow us to write T_i as a sum-of-product-of-univariates:

$$T_i \cdot z_{i,1}^{e_{i,1}} \cdots z_{i,s}^{e_{i,s}} = \sum_{j_1=1}^{t_i} f_{i,j_1,1}(x_1) \cdots f_{i,j_1,n}(x_n) \text{ over } R_i$$

- The third idea is to *stitch* these k algebras R_i to an algebra R of dimension $\sum_{i=1}^{k}(1+e_{i,1}) \cdots (1+e_{i,s})$.
- Such that over R, C is a sum-of-product-of-univariates:

Idea 3: Dual Form

- Given a diagonal depth-4 circuit $C(\bar{x}) = T_1 + \cdots + T_k$, where $T_i = \prod_{j=1}^{s} L_{i,j}^{e_{i,j}}$.
- The last two ideas allow us to write T_i as a sum-of-product-of-univariates:

$$T_i \cdot z_{i,1}^{e_{i,1}} \cdots z_{i,s}^{e_{i,s}} = \sum_{j_1=1}^{t_i} f_{i,j_1,1}(x_1) \cdots f_{i,j_1,n}(x_n) \text{ over } R_i$$

where, $t_i = n(e_{i,1} + \cdots + e_{i,s}) + 1$ and $R_i := \mathbb{F}[z_{i,1}, \ldots, z_{i,s}]/(z_{i,1}^{e_{i,1}+1}, \ldots, z_{i,s}^{e_{i,s}+1})$

- The third idea is to *stitch* these k algebras R_i to an algebra R of dimension $\sum_{i=1}^{k}(1 + e_{i,1}) \cdots (1 + e_{i,s})$.
- Such that over R, C is a sum-of-product-of-univariates:

Idea 3: Dual Form

- Given a diagonal depth-4 circuit $C(\overline{x}) = T_1 + \cdots + T_k$, where $T_i = \prod_{j=1}^{s} L_{i,j}^{e_{i,j}}$.
- The last two ideas allow us to write T_i as a sum-of-product-of-univariates:

$$T_i \cdot z_{i,1}^{e_{i,1}} \cdots z_{i,s}^{e_{i,s}} = \sum_{j_1=1}^{t_i} f_{i,j_1,1}(x_1) \cdots f_{i,j_1,n}(x_n) \text{ over } R_i$$

where, $t_i = n(e_{i,1} + \cdots + e_{i,s}) + 1$ and $R_i := \mathbb{F}[z_{i,1}, \ldots, z_{i,s}]/(z_{i,1}^{e_{i,1}+1}, \ldots, z_{i,s}^{e_{i,s}+1})$

- The third idea is to *stitch* these k algebras R_i to an algebra R of dimension $\sum_{i=1}^{k}(1 + e_{i,1}) \cdots (1 + e_{i,s})$.
- Such that over R, C is a sum-of-product-of-univariates:

Idea 3: Dual Form

- Given a diagonal depth-4 circuit $C(\overline{x}) = T_1 + \cdots + T_k$, where $T_i = \prod_{j=1}^{s} L_{i,j}^{e_{i,j}}$.
- The last two ideas allow us to write T_i as a sum-of-product-of-univariates:

$$T_i \cdot z_{i,1}^{e_{i,1}} \cdots z_{i,s}^{e_{i,s}} = \sum_{j_1=1}^{t_i} f_{i,j_1,1}(x_1) \cdots f_{i,j_1,n}(x_n) \text{ over } R_i$$

where, $t_i = n(e_{i,1} + \cdots + e_{i,s}) + 1$ and $R_i := \mathbb{F}[z_{i,1}, \ldots, z_{i,s}]/(z_{i,1}^{e_{i,1}+1}, \ldots, z_{i,s}^{e_{i,s}+1})$

- The third idea is to *stitch* these k algebras R_i to an algebra R of dimension $\sum_{i=1}^{k}(1 + e_{i,1}) \cdots (1 + e_{i,s})$.
- Such that over R, C is a sum-of-product-of-univariates:

Idea 3: Dual Form

- Given a diagonal depth-4 circuit $C(\overline{x}) = T_1 + \cdots + T_k$, where $T_i = \prod_{j=1}^{s} L_{i,j}^{e_{i,j}}$.
- The last two ideas allow us to write T_i as a sum-of-product-of-univariates:

$$T_i \cdot z_{i,1}^{e_{i,1}} \cdots z_{i,s}^{e_{i,s}} = \sum_{j_1=1}^{t_i} f_{i,j_1,1}(x_1) \cdots f_{i,j_1,n}(x_n) \text{ over } R_i$$

where, $t_i = n(e_{i,1} + \cdots + e_{i,s}) + 1$ and $R_i := \mathbb{F}[z_{i,1}, \ldots, z_{i,s}]/(z_{i,1}^{e_{i,1}+1}, \ldots, z_{i,s}^{e_{i,s}+1})$

- The third idea is to *stitch* these k algebras R_i to an algebra R of dimension $\sum_{i=1}^{k}(1 + e_{i,1}) \cdots (1 + e_{i,s})$.
- Such that over R, C is a sum-of-product-of-univariates:

$$C(x_1, \ldots, x_n) \cdot z_{1,1}^{e_{1,1}} \cdots z_{1,s}^{e_{1,s}} = \sum_{i=1}^{k} \sum_{j_1=1}^{t_i} f_{i,j_1,1}(x_1) \cdots f_{i,j_1,n}(x_n)$$

A Generalization of the Known Results

- This sum-of-product-of-univariates circuit is vulnerable!
- We attack it by generalizing the results of Raz & Shpilka (CCC '04) to general commutative algebras.

Thm 1: Let R be an algebra over a field $\mathbb{F}$. Given a sum-of-product-of-univariates circuit $C(x_1, \ldots, x_n)$ over R we can verify deterministically in $poly(size(C), dim(R))$ field operations whether C is zero.

Thm 2: Let R be an algebra over a field $\mathbb{F}$, $r \in R \setminus \{0\}$ and $r' \in R$. If $det((x_{i,j})) \cdot r - r'$ can be expressed as a sum-of-k-products-of-univariates circuit, then $k \cdot dim(R) = 2^{\Omega(n)}$.

A Generalization of the Known Results

- This sum-of-product-of-univariates circuit is vulnerable!
- We attack it by generalizing the results of Raz & Shpilka (CCC '04) to general commutative algebras.

Thm 1: Let R be an algebra over a field $\mathbb{F}$. Given a sum-of-product-of-univariates circuit $C(x_1, \ldots, x_n)$ over R we can verify deterministically in $poly(size(C), dim(R))$ field operations whether C is zero.

Thm 2: Let R be an algebra over a field $\mathbb{F}$, $r \in R \setminus \{0\}$ and $r' \in R$. If $det((x_{i,j})) \cdot r - r'$ can be expressed as a sum-of-k-products-of-univariates circuit, then $k \cdot dim(R) = 2^{\Omega(n)}$.

A Generalization of the Known Results

- This sum-of-product-of-univariates circuit is vulnerable!
- We attack it by generalizing the results of Raz & Shpilka (CCC '04) to general commutative algebras.

Thm 1: Let R be an algebra over a field $\mathbb{F}$. Given a sum-of-product-of-univariates circuit $C(x_1, \ldots, x_n)$ over R we can verify deterministically in $poly(size(C), dim(R))$ field operations whether C is zero.

Thm 2: Let R be an algebra over a field $\mathbb{F}$, $r \in R \setminus \{0\}$ and $r' \in R$. If $det((x_{i,j})) \cdot r - r'$ can be expressed as a sum-of-k-products-of-univariates circuit, then $k \cdot dim(R) = 2^{\Omega(n)}$.

A Generalization of the Known Results

- This sum-of-product-of-univariates circuit is vulnerable!
- We attack it by generalizing the results of Raz & Shpilka (CCC '04) to general commutative algebras.

Thm 1: Let R be an algebra over a field $\mathbb{F}$. Given a sum-of-product-of-univariates circuit $C(x_1, \ldots, x_n)$ over R we can verify deterministically in $poly(size(C), dim(R))$ field operations whether C is zero.

Thm 2: Let R be an algebra over a field $\mathbb{F}$, $r \in R \setminus \{0\}$ and $r' \in R$. If $det((x_{i,j})) \cdot r - r'$ can be expressed as a sum-of-k-products-of-univariates circuit, then $k \cdot dim(R) = 2^{\Omega(n)}$.

Final Calculation

- Let the given diagonal depth-4 circuit be $C(x_1, \ldots, x_n) = \sum_{i=1}^{k} \prod_{j=1}^{s} L_{i,j}^{e_{i,j}}$.
- Our transformation is over a base algebra R with dimension $\sum_{i=1}^{k}(1+e_{i,1})\cdots(1+e_{i,s})$.
- This gives us the following results:

Thm 1: We can deterministically test C for zeroness in $poly(size(C), max_i\{(1+e_{i,1})\cdots(1+e_{i,s})\})$ field operations.

Thm 2: If C expresses the determinant (or permanent) of a formal $m \times m$ matrix then either $s = \Omega\left(\frac{m}{\log m}\right)$ or $k = 2^{\Omega(m)}$.

Final Calculation

- Let the given diagonal depth-4 circuit be $C(x_1, \ldots, x_n) = \sum_{i=1}^{k} \prod_{j=1}^{s} L_{i,j}^{e_{i,j}}$.
- Our transformation is over a base algebra R with dimension $\sum_{i=1}^{k}(1 + e_{i,1}) \cdots (1 + e_{i,s})$.
- This gives us the following results:

Thm 1: We can deterministically test C for zeroness in $poly(size(C), max_i\{(1 + e_{i,1}) \cdots (1 + e_{i,s})\})$ field operations.

Thm 2: If C expresses the determinant (or permanent) of a formal $m \times m$ matrix then either $s = \Omega\left(\frac{m}{\log m}\right)$ or $k = 2^{\Omega(m)}$.

Final Calculation

- Let the given diagonal depth-4 circuit be $C(x_1, \ldots, x_n) = \sum_{i=1}^{k} \prod_{j=1}^{s} L_{i,j}^{e_{i,j}}$.
- Our transformation is over a base algebra R with dimension $\sum_{i=1}^{k}(1 + e_{i,1}) \cdots (1 + e_{i,s})$.
- This gives us the following results:

Thm 1: We can deterministically test C for zeroness in $poly(size(C), max_i\{(1 + e_{i,1}) \cdots (1 + e_{i,s})\})$ field operations.

Thm 2: If C expresses the determinant (or permanent) of a formal $m \times m$ matrix then either $s = \Omega\left(\frac{m}{\log m}\right)$ or $k = 2^{\Omega(m)}$.

Final Calculation

- Let the given diagonal depth-4 circuit be $C(x_1, \ldots, x_n) = \sum_{i=1}^{k} \prod_{j=1}^{s} L_{i,j}^{e_{i,j}}$.
- Our transformation is over a base algebra R with dimension $\sum_{i=1}^{k}(1+e_{i,1}) \cdots (1+e_{i,s})$.
- This gives us the following results:

Thm 1: We can deterministically test C for zeroness in $poly(size(C), max_i\{(1+e_{i,1}) \cdots (1+e_{i,s})\})$ field operations.

Thm 2: If C expresses the determinant (or permanent) of a formal $m \times m$ matrix then either $s = \Omega\left(\frac{m}{\log m}\right)$ or $k = 2^{\Omega(m)}$.

Final Calculation

- Let the given diagonal depth-4 circuit be $C(x_1, \ldots, x_n) = \sum_{i=1}^{k} \prod_{j=1}^{s} L_{i,j}^{e_{i,j}}$.
- Our transformation is over a base algebra R with dimension $\sum_{i=1}^{k}(1+e_{i,1})\cdots(1+e_{i,s})$.
- This gives us the following results:

Thm 1: We can deterministically test C for zeroness in $poly(size(C), max_i\{(1+e_{i,1})\cdots(1+e_{i,s})\})$ field operations.

Thm 2: If C expresses the determinant (or permanent) of a formal $m \times m$ matrix then either $s = \Omega\left(\frac{m}{\log m}\right)$ or $k = 2^{\Omega(m)}$.

Idea 4: Prime Characteristic

- The circuit transformation we showed had terms like $\frac{1}{e_1}$, so we need to be careful when the field is of a prime characteristic $p \geq 2$.
- The basic idea is to do the transformation treating the constants as rationals and then clear away p from the denominators.
- This gives us a dual form of C in the form: $p^b \cdot C(x_1, \ldots, x_n) \cdot z_{1,1}^{e_{1,1}} \cdots z_{1,s}^{e_{1,s}}$ is a sum-of-product-of-univariates over a ring R of characteristic p^{b+1}.
- All our results carry over to even rings above $\mathbb{Z}/(p^{b+1}\mathbb{Z})$.

Idea 4: Prime Characteristic

- The circuit transformation we showed had terms like $\frac{1}{e_1}$, so we need to be careful when the field is of a prime characteristic $p \geq 2$.
- The basic idea is to do the transformation treating the constants as rationals and then clear away p from the denominators.
- This gives us a dual form of C in the form: $p^b \cdot C(x_1, \ldots, x_n) \cdot z_{1,1}^{e_{1,1}} \cdots z_{1,s}^{e_{1,s}}$ is a sum-of-product-of-univariates over a ring R of characteristic p^{b+1}.
- All our results carry over to even rings above $\mathbb{Z}/(p^{b+1}\mathbb{Z})$.

Idea 4: Prime Characteristic

- The circuit transformation we showed had terms like $\frac{1}{e_1}$, so we need to be careful when the field is of a prime characteristic $p \geq 2$.
- The basic idea is to do the transformation treating the constants as rationals and then clear away p from the denominators.
- This gives us a dual form of C in the form: $p^b \cdot C(x_1, \ldots, x_n) \cdot z_{1,1}^{e_{1,1}} \cdots z_{1,s}^{e_{1,s}}$ is a sum-of-product-of-univariates over a ring R of characteristic p^{b+1}.
- All our results carry over to even rings above $\mathbb{Z}/(p^{b+1}\mathbb{Z})$.

Idea 4: Prime Characteristic

- The circuit transformation we showed had terms like $\frac{1}{e_1}$, so we need to be careful when the field is of a prime characteristic $p \geq 2$.
- The basic idea is to do the transformation treating the constants as rationals and then clear away p from the denominators.
- This gives us a dual form of C in the form: $p^b \cdot C(x_1, \ldots, x_n) \cdot z_{1,1}^{e_{1,1}} \cdots z_{1,s}^{e_{1,s}}$ is a sum-of-product-of-univariates over a ring R of characteristic p^{b+1}.
- All our results carry over to even rings above $\mathbb{Z}/(p^{b+1}\mathbb{Z})$.

Over any commutative ring

- Suppose we are given a diagonal depth-4 circuit over any commutative ring. Say, the ring is specified in the input in basis form.
- Our identity test and lower bounds also hold for such circuits.

Over any commutative ring

- Suppose we are given a diagonal depth-4 circuit over any commutative ring. Say, the ring is specified in the input in basis form.
- Our identity test and lower bounds also hold for such circuits.

In Conclusion

- For a diagonal depth-4 circuit C of the form $\sum_{i=1}^{k} L_{i,1}^{e_{i,1}} \cdots L_{i,s}^{e_{i,s}}$ having *small* s, we gave an identity test and proved lower bounds.
- The main idea was to define a dual form of such circuits.
- Is the dual form useful even when s is variable?

Questions?

In Conclusion

- For a diagonal depth-4 circuit C of the form $\sum_{i=1}^{k} L_{i,1}^{e_{i,1}} \cdots L_{i,s}^{e_{i,s}}$ having *small* s, we gave an identity test and proved lower bounds.
- The main idea was to define a dual form of such circuits.
- Is the dual form useful even when s is variable?

Questions?

In Conclusion

- For a diagonal depth-4 circuit C of the form $\sum_{i=1}^{k} L_{i,1}^{e_{i,1}} \cdots L_{i,s}^{e_{i,s}}$ having *small* s, we gave an identity test and proved lower bounds.
- The main idea was to define a dual form of such circuits.
- Is the dual form useful even when s is variable?

Questions?

In Conclusion

- For a diagonal depth-4 circuit C of the form $\sum_{i=1}^{k} L_{i,1}^{e_{i,1}} \cdots L_{i,s}^{e_{i,s}}$ having *small* s, we gave an identity test and proved lower bounds.
- The main idea was to define a dual form of such circuits.
- Is the dual form useful even when s is variable?

Questions?