Blackbox PIT for Bounded Fan-in Depth 3 Circuits: the field doesn't matter

N. Saxena and C. Seshadri

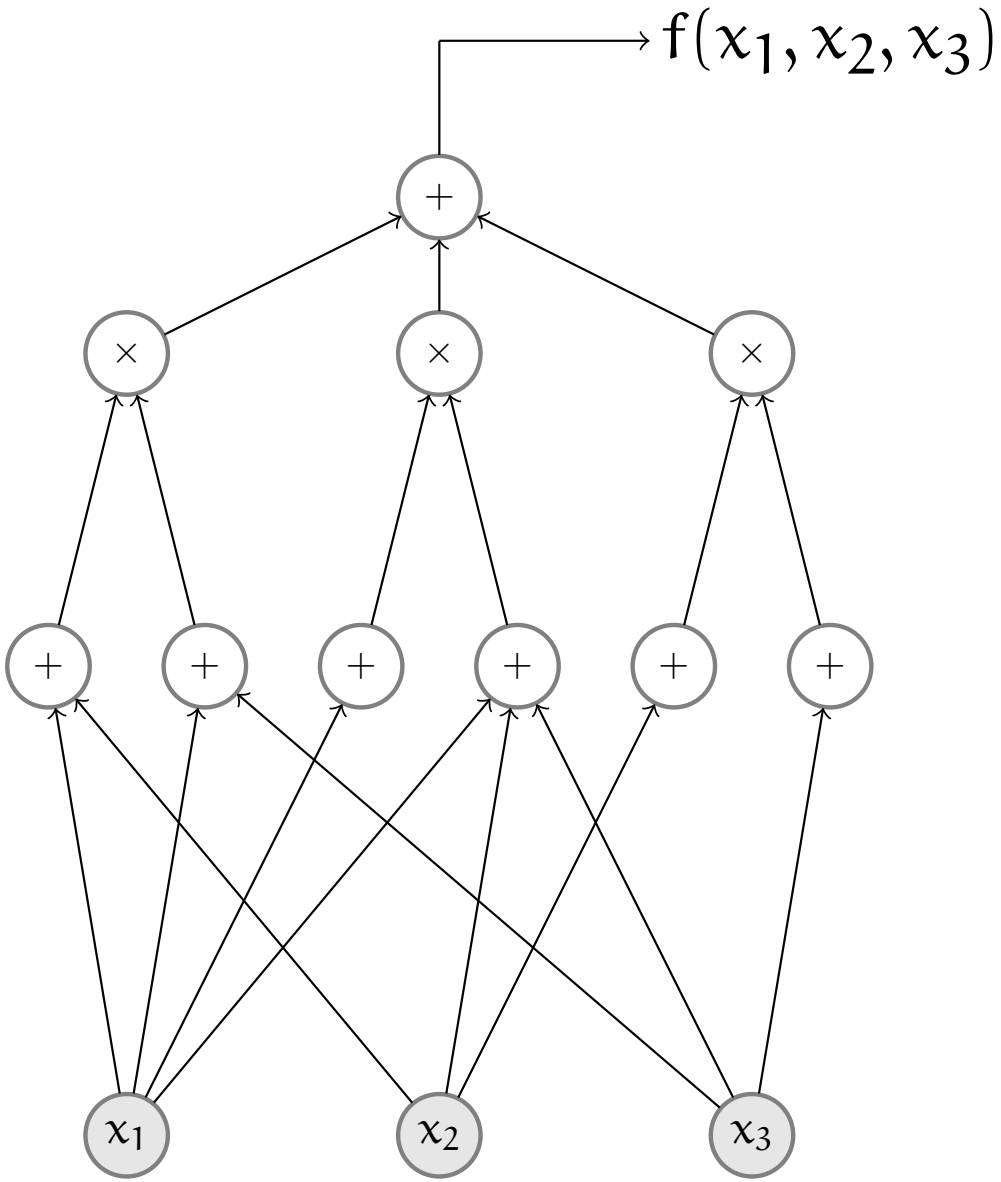
Presented by Ramprasad Saptharishi

Second Mysore Park Workshop in Theoretical Computer Science:
Algorithms and Complexity
6th May, 2011

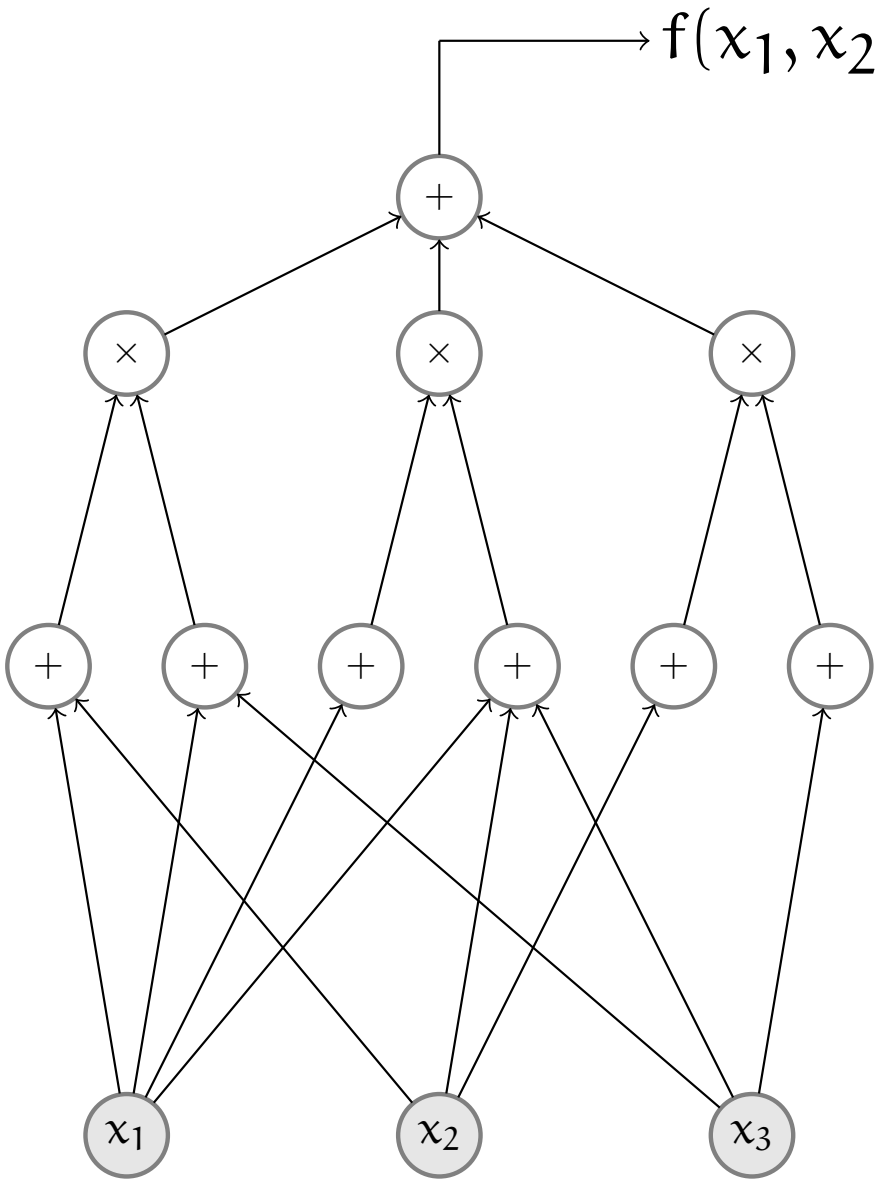
Outline

Outline

Arithmetic Circuits

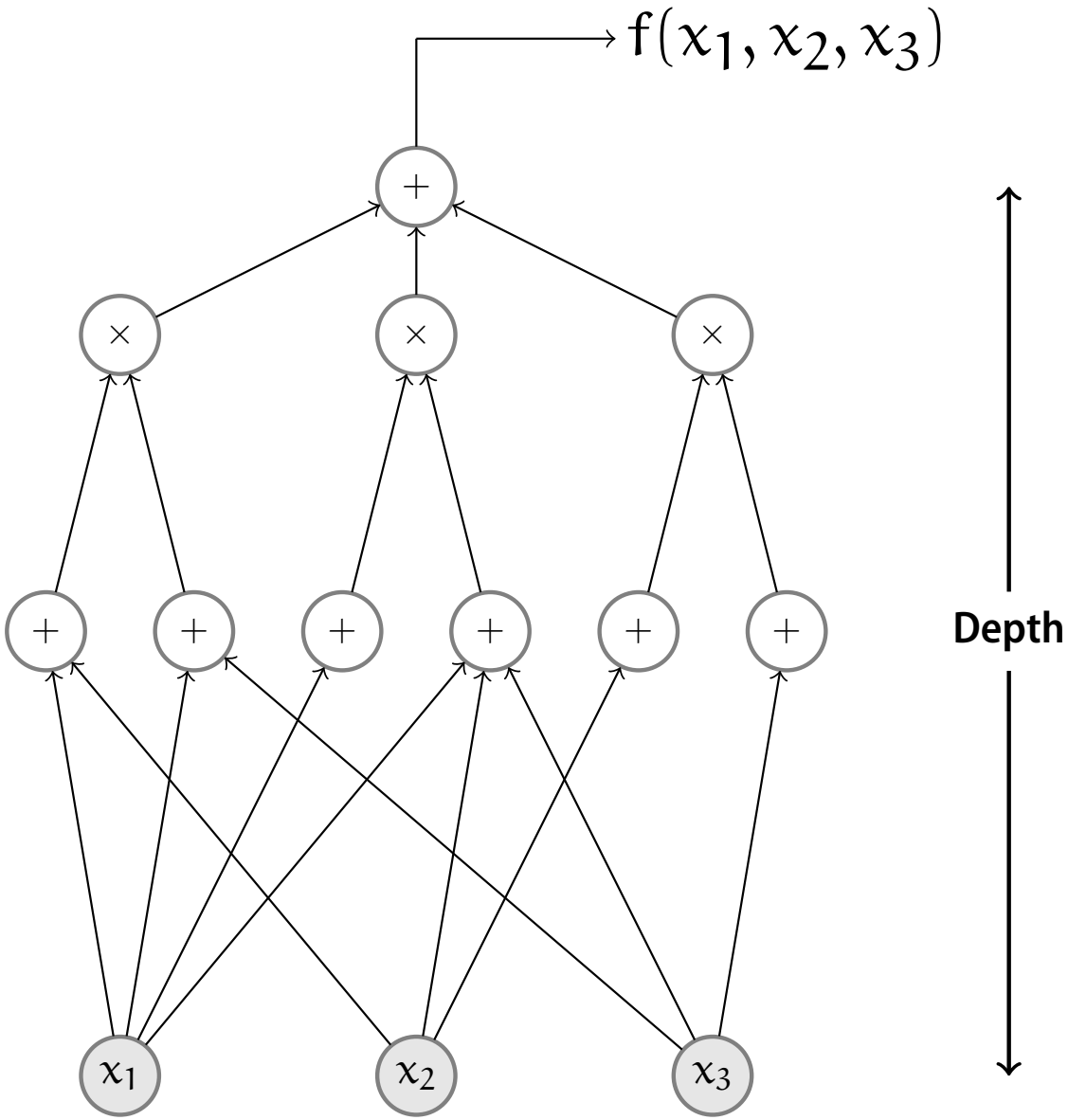


Arithmetic Circuits

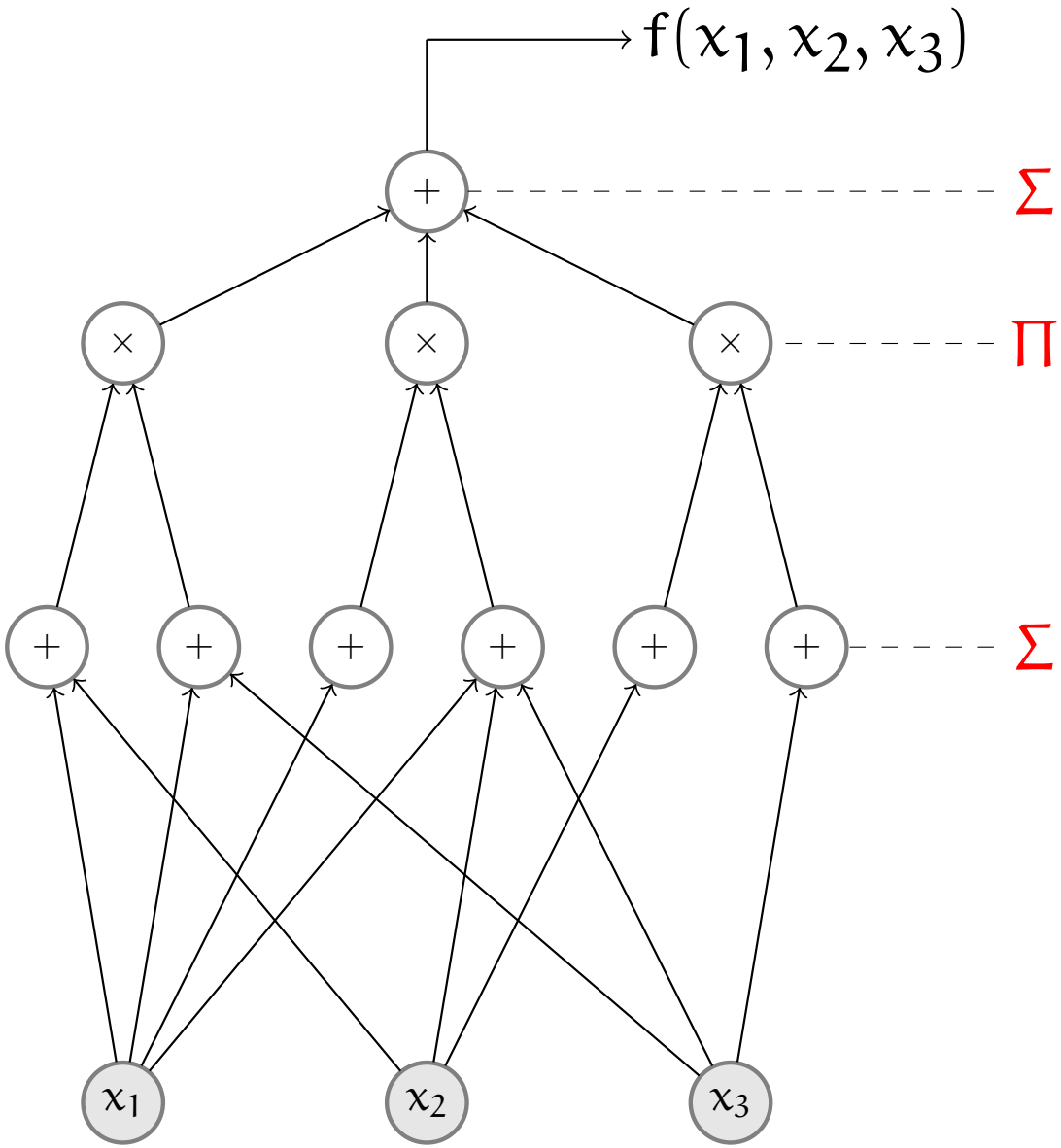


Size = number of gates

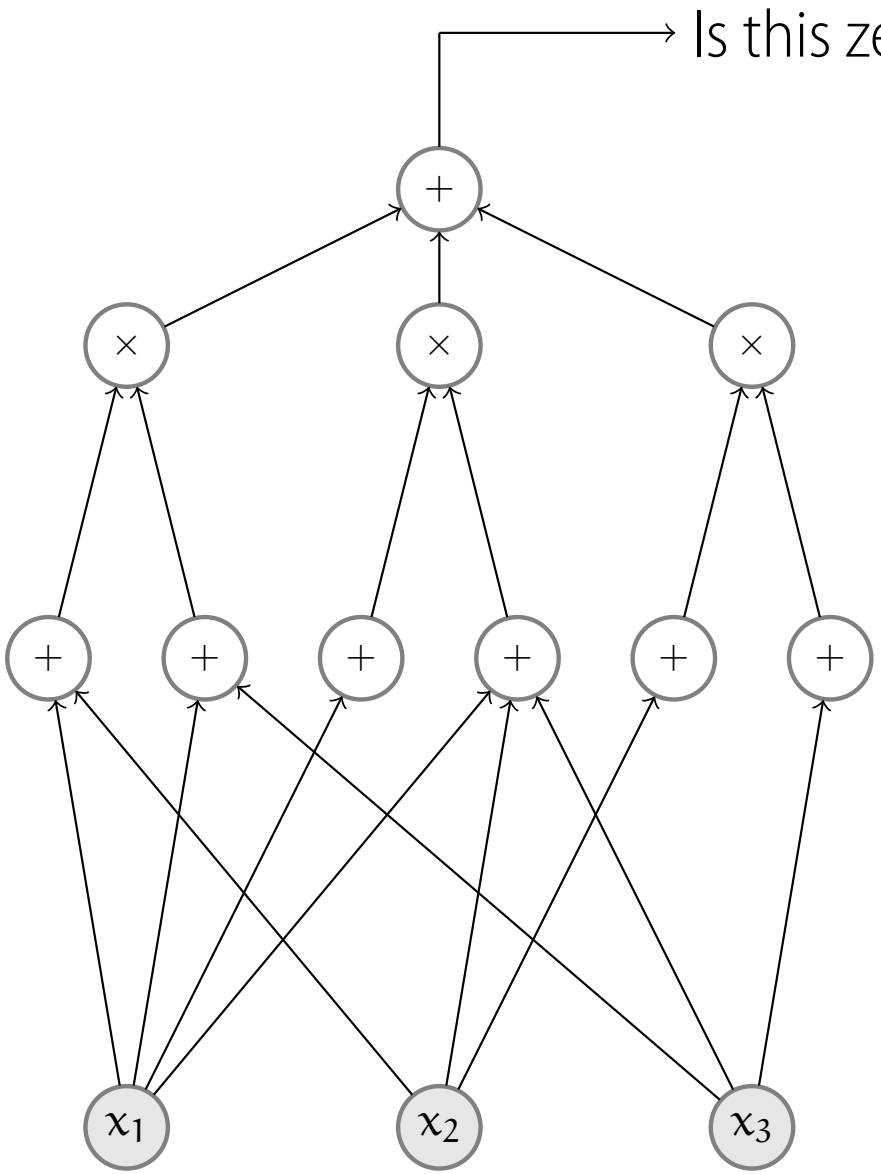
Arithmetic Circuits



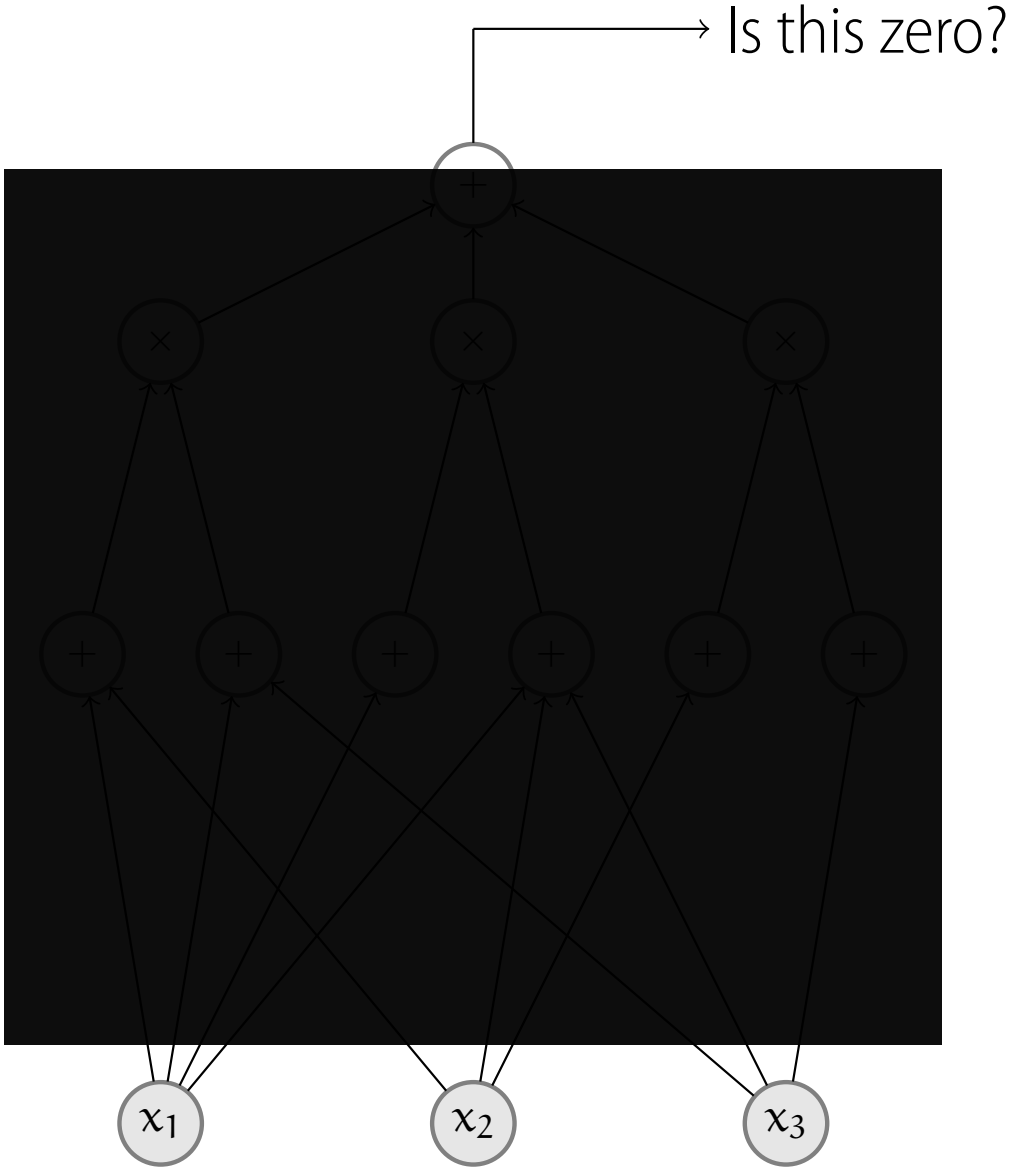
Arithmetic Circuits



Identity Testing of Arithmetic Circuits



Blackbox Identity Testing of Arithmetic Circuits



Why do we care?

Part of many important results like IP $=$ PSPACE, the PCP theorem, AKS primality test etc.

Connections with lower bounds. [Kabanets-Impagliazzo03], [Agrawal05]: "Efficient PIT algorithms imply lower bounds"

Why do we care?

Part of many important results like IP = PSPACE, the PCP theorem, AKS primality test etc.

Connections with lower bounds. [Kabanets-Impagliazzo03], [Agrawal05]: "Efficient PIT algorithms imply lower bounds"

> *"For the pessimist, this indicates that derandomizing identity testing is a hopeless problem. For the optimist, this means on the contrary that to obtain an arithmetic circuit lower bound, we 'simply' have to prove a good upper bound on identity testing."*
>
> - *[Kayal-Saraf09]*

Why do we care?

Part of many important results like IP = PSPACE, the PCP theorem, AKS primality test etc.

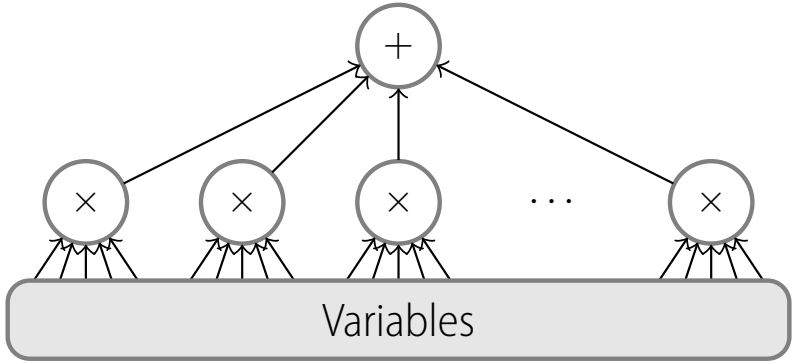
Connections with lower bounds. [Kabanets-Impagliazzo03], [Agrawal05]: "Efficient PIT algorithms imply lower bounds"

> *"For the pessimist, this indicates that derandomizing identity testing is a hopeless problem. For the optimist, this means on the contrary that to obtain an arithmetic circuit lower bound, we 'simply' have to prove a good upper bound on identity testing."*
>
> - *[Kayal-Saraf09]*

Of course, it is a natural problem!

Outline

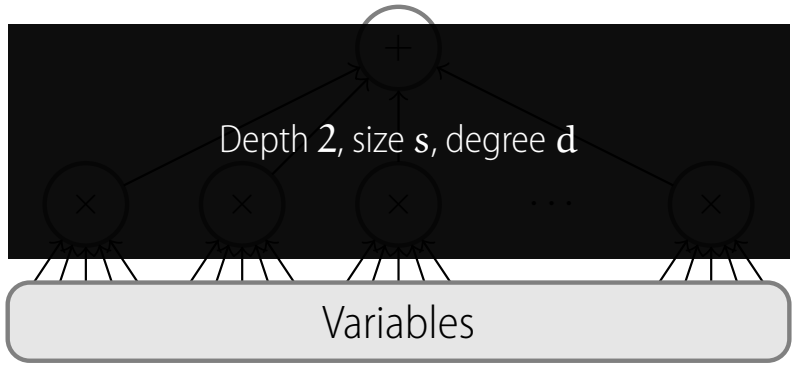
State of affairs: Depth 2



$$f = \sum_{i=1}^{\text{poly}} \text{monomial}_i$$

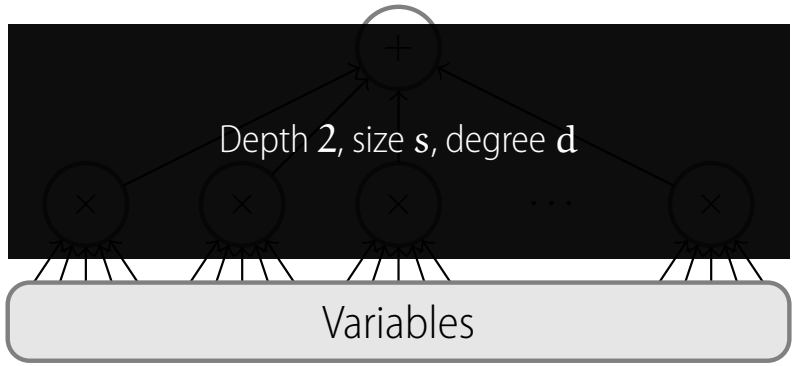
Depth 2 is easy (sparse polynomials)

State of affairs: Depth 2



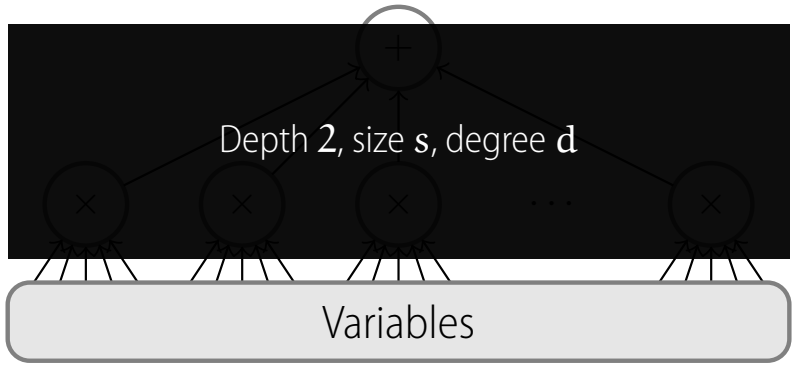
Blackbox easy as well.

State of affairs: Depth 2



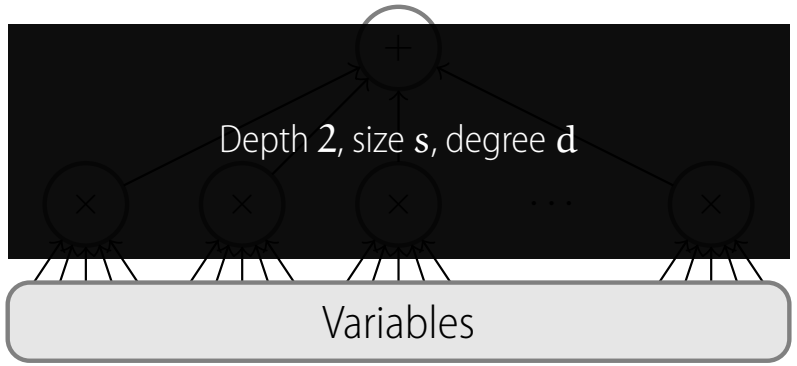
$$\Phi : \quad x_i \mapsto t^{(d+1)^i}$$

State of affairs: Depth 2



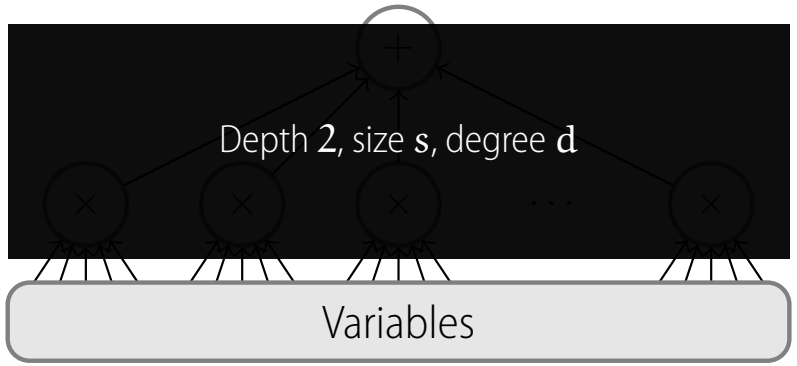
$$\Phi : \quad x_1^{a_1} \cdots x_n^{a_n} \quad \mapsto \quad t^A$$

State of affairs: Depth 2



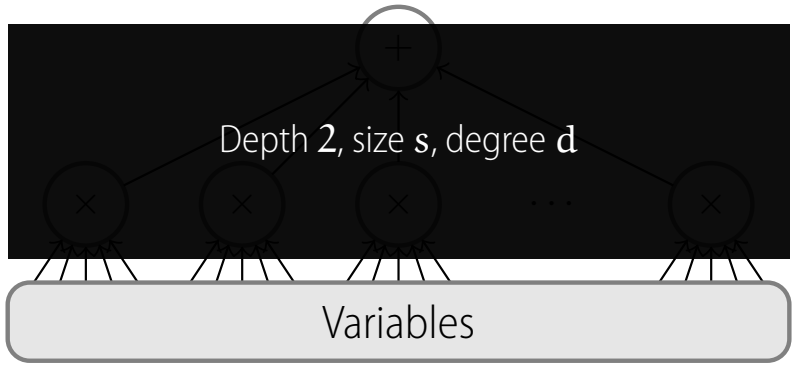
$$\Phi_r : \quad x_i \mapsto t^{(d+1)^i \bmod r}$$

State of affairs: Depth 2



$$\Phi_r : \quad x_1^{a_1} \cdots x_n^{a_n} \quad \mapsto \quad t^{A \bmod r}$$

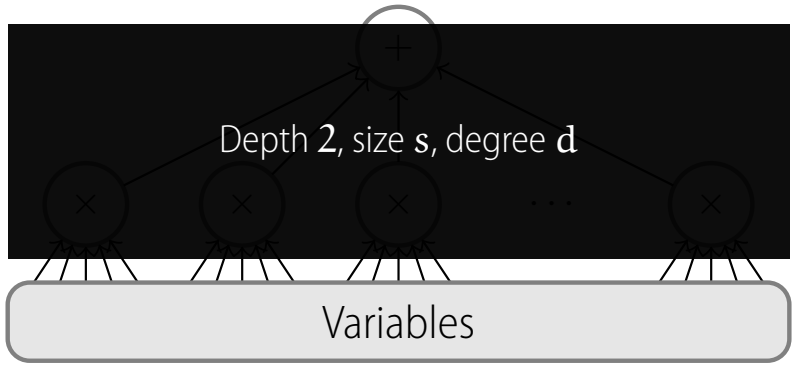
State of affairs: Depth 2



$$\Phi_r : \quad x_1^{a_1} \cdots x_n^{a_n} \quad \mapsto \quad t^{A \bmod r}$$

$$\Phi_r(m_A) = \Phi_r(m_B) \quad \Longrightarrow \quad r \mid B - A$$

State of affairs: Depth 2

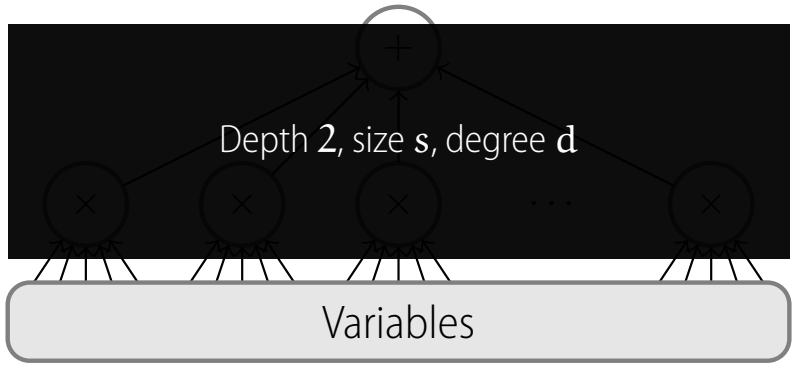


$$\Phi_r : \quad x_1^{a_1} \cdots x_n^{a_n} \quad \mapsto \quad t^{A \bmod r}$$

$$\Phi_r(m_A) = \Phi_r(m_B) \quad \Longrightarrow \quad r \mid B - A$$

At most $(n \log d)$ bad r's for a pair A, B.

State of affairs: Depth 2

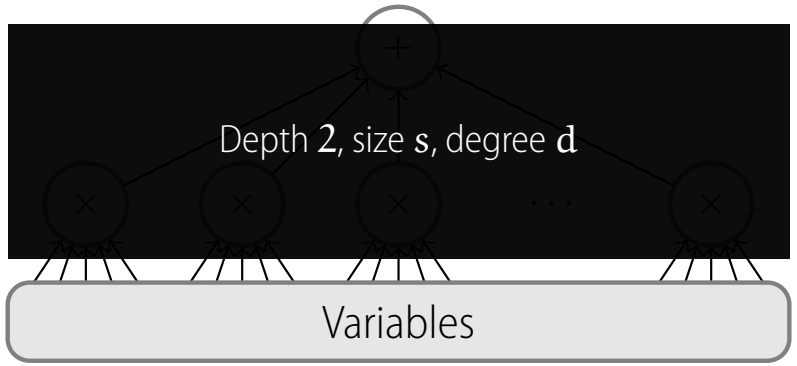


$$\Phi_r : \quad x_1^{a_1} \cdots x_n^{a_n} \quad \mapsto \quad t^{A \bmod r}$$

$$\Phi_r(m_A) = \Phi_r(m_B) \quad \Longrightarrow \quad r \mid B - A$$

At most $s^2(n \log d)$ bad r's overall.

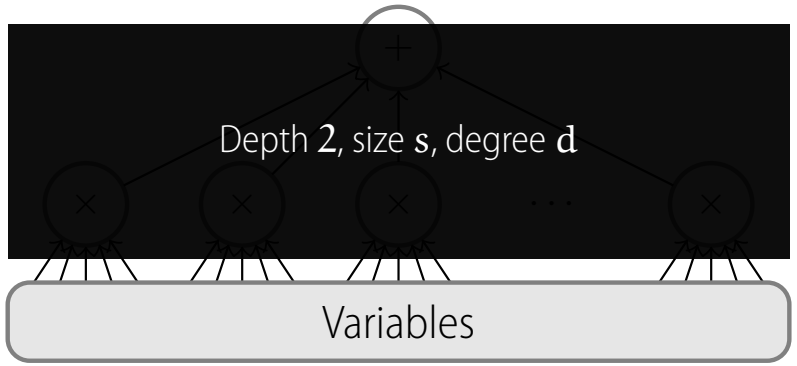
State of affairs: Depth 2



Hitting set:

$$\mathcal{H}_t = \left\{ (t^{(d+1) \bmod r}, \cdots, t^{(d+1)^n \bmod r}) \ : \ r \in [(s^2 n \log d)^2] \right\}$$

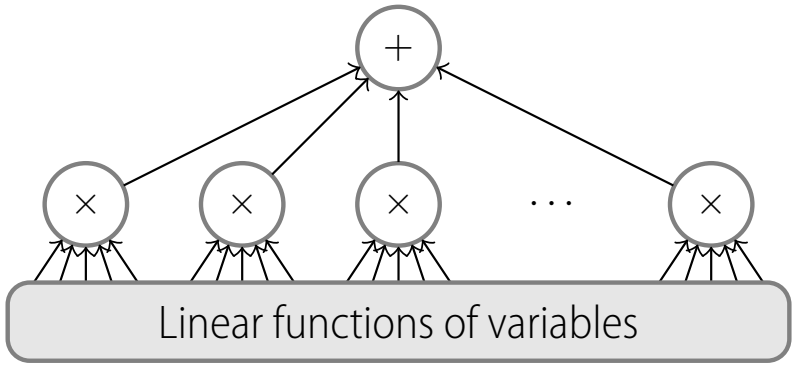
State of affairs: Depth 2



Hitting set:

$$\mathcal{H} = \left\{ (t^{(d+1) \bmod r}, \cdots, t^{(d+1)^n \bmod r}) \; : \; \begin{array}{c} r \in [(s^2 n \log d)^2] \\ t \in [ndr + 1] \end{array} \right\}$$

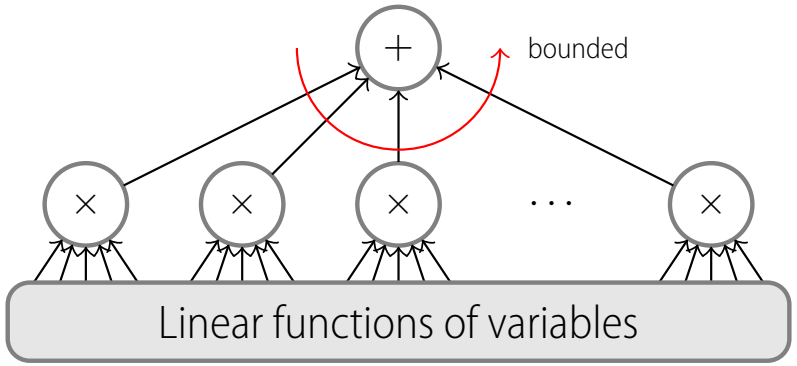
State of affairs: Depth 3



$$f = \sum_{i=1}^{k} \ell_{i1} \cdots \ell_{id}$$

PIT for even depth 3 circuits is open.

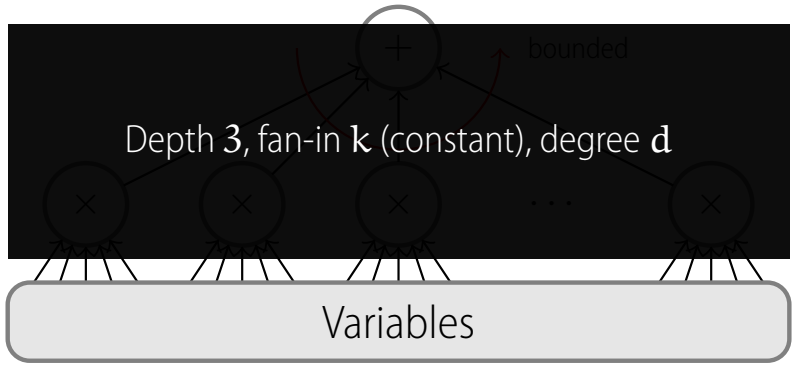
State of affairs: Depth 3



$$f = \sum_{i=1}^{k} \ell_{i1} \cdots \ell_{id}$$

[KayalSaxena07] : polynomial time algorithm when k is a constant

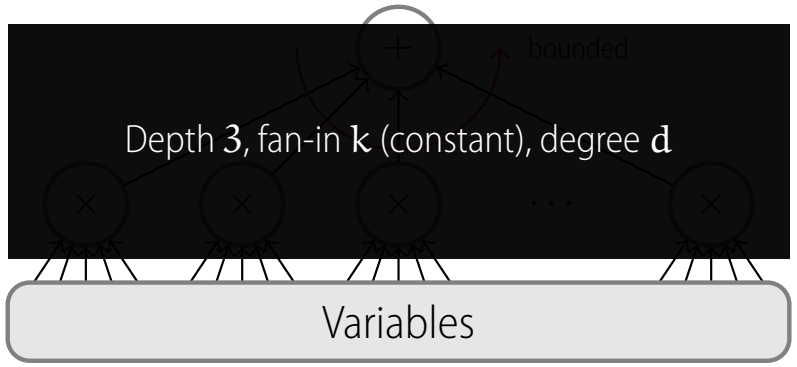
State of affairs: Depth 3



$$f = \sum_{i=1}^{k} \ell_{i1} \cdots \ell_{id}$$

[KayalSaraf08] : Blackbox algorithm over the field $\mathbb{Q}$

State of affairs: Depth 3

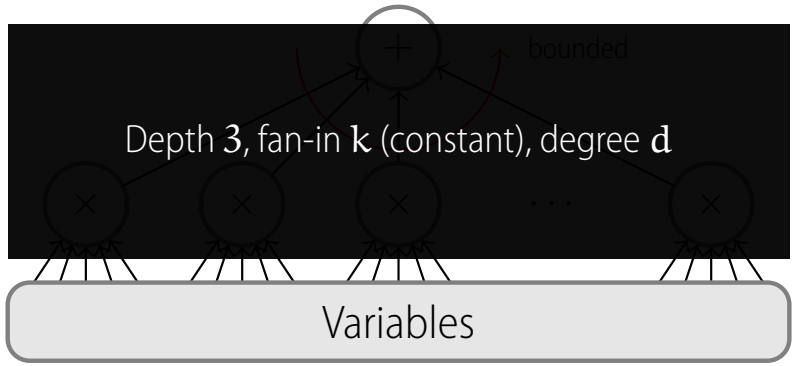


$$f = \sum_{i=1}^{k} \ell_{i1} \cdots \ell_{id}$$

[KayalSaraf08] : Blackbox algorithm over the field $\mathbb{Q}$

This talk [SaxenaSeshadri11]: Blackbox algorithm over any field

State of affairs: Depth 3



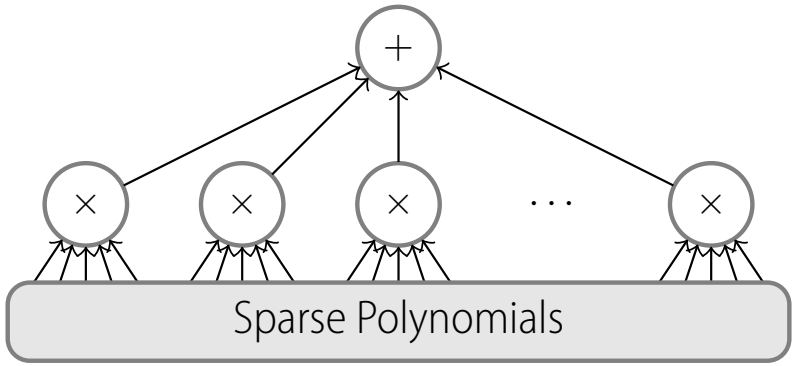
$$f = \sum_{i=1}^{k} \ell_{i1} \cdots \ell_{id}$$

[KayalSaraf08] : Blackbox algorithm over the field $\mathbb{Q}$

This talk [SaxenaSeshadri11]: Blackbox algorithm over any field

Main Ingredient: Rank bounds

State of affairs: Depth 4



$$f = \sum_{i=1}^{\text{poly}} g_{i1} \cdots g_{id}$$

[AgrawalVinay08] : Blackbox PIT for depth 4 implies $n^{O(\log n)}$ blackbox PIT for any depth!

Depth 4 is (almost) as hard as the general case.

Outline

Outline

The Schwartz-Zippel Lemma

Lemma

Let $f(x_1, \cdots, x_n)$ *be a non-zero polynomial with total degree bounded by* d. *Then,*

$$\Pr_{a_1,\cdots,a_n}[f(\bar{a}) = 0] \quad \leq \quad \frac{d}{|\mathbb{F}|}$$

The Schwartz-Zippel Lemma

Lemma

Let $f(x_1, \cdots, x_n)$ *be a non-zero polynomial with total degree bounded by* d. *Then,*

$$\Pr_{a_1, \cdots, a_n}[f(\bar{a}) = 0] \quad \leq \quad \frac{d}{|\mathbb{F}|}$$

Proof.

$$f(x_1, \cdots, x_n) \quad = \quad \sum_{i=0}^{k} f_i(x_2, \cdots, x_n) \cdot x_1^i$$

□

The Schwartz-Zippel Lemma

Lemma

Let $f(x_1, \cdots, x_n)$ *be a non-zero polynomial with total degree bounded by* d. *Then,*

$$\Pr_{a_1, \cdots, a_n}[f(\bar{a}) = 0] \quad \leq \quad \frac{d}{|\mathbb{F}|}$$

Proof.

$$f(x_1, \cdots, x_n) \quad = \quad \sum_{i=0}^{k} f_i(x_2, \cdots, x_n) \cdot x_1^i$$

$$\begin{aligned} \Pr[f(\bar{a}) = 0] \quad &\leq \quad \Pr[f(x_1, a_2, \cdots, a_n) = 0] \\ &\quad + \Pr[f(a_1, \cdots, a_n) = 0 \mid f(x_1, a_2, \cdots, a_n) \neq 0] \end{aligned}$$

□

The Schwartz-Zippel Lemma

Lemma

Let $f(x_1, \cdots, x_n)$ *be a non-zero polynomial with total degree bounded by* d. *Then,*

$$\Pr_{a_1,\cdots,a_n}[f(\bar{a}) = 0] \quad \leq \quad \frac{d}{|\mathbb{F}|}$$

Proof.

$$\begin{aligned} f(x_1, \cdots, x_n) &= \sum_{i=0}^{k} f_i(x_2, \cdots, x_n) \cdot x_1^i \\ \Pr[f(\bar{a}) = 0] &\leq \Pr[f(x_1, a_2, \cdots, a_n) = 0] \\ &\quad + \Pr[f(a_1, \cdots, a_n) = 0 \mid f(x_1, a_2, \cdots, a_n) \neq 0] \\ &\leq \frac{d-k}{|\mathbb{F}|} + \frac{k}{|\mathbb{F}|} \end{aligned}$$

□

The Schwartz-Zippel Lemma

Lemma

Let $f(x_1, \cdots, x_n)$ *be a non-zero polynomial with total degree bounded by* d. *Then,*

$$\Pr_{a_1,\cdots,a_n}[f(\bar{a}) = 0] \quad \leq \quad \frac{d}{|\mathbb{F}|}$$

Proof.

$$\begin{aligned} f(x_1, \cdots, x_n) &= \sum_{i=0}^{k} f_i(x_2, \cdots, x_n) \cdot x_1^i \\ \Pr[f(\bar{a}) = 0] &\leq \Pr[f(x_1, a_2, \cdots, a_n) = 0] \\ &\quad + \Pr[f(a_1, \cdots, a_n) = 0 \mid f(x_1, a_2, \cdots, a_n) \neq 0] \\ &\leq \frac{d-k}{|\mathbb{F}|} + \frac{k}{|\mathbb{F}|} = \frac{d}{|\mathbb{F}|} \quad \square \end{aligned}$$

The Schwartz-Zippel Lemma

Lemma

Let $f(x_1, \cdots, x_n)$ *be a non-zero polynomial with total degree bounded by* d. *Then, for any* $S \subseteq \mathbb{F}$,

$$\Pr_{a_1, \cdots, a_n}[f(\bar{a}) = 0] \quad \leq \quad \frac{d}{|S|}$$

The Schwartz-Zippel Lemma

Lemma

Let $f(x_1, \cdots, x_n)$ *be a non-zero polynomial with total degree bounded by* d. *Then, for any* $S \subseteq \mathbb{F}$,

$$\Pr_{a_1, \cdots, a_n}[f(\bar{a}) = 0] \quad \leq \quad \frac{d}{|S|}$$

Hitting set of size $(d+1)^n$.

The Schwartz-Zippel Lemma

Lemma

Let $f(x_1, \cdots, x_n)$ *be a non-zero polynomial with total degree bounded by* d. *Then, for any* $S \subseteq \mathbb{F}$,

$$\Pr_{a_1,\cdots,a_n}[f(\bar{a}) = 0] \quad \leq \quad \frac{d}{|S|}$$

Hitting set of size $(d+1)^n$.

Question: Can we get reduce the number of variables?

The "rank" of a circuit is...

... essentially the number of variables the circuit truly depends on.

The "rank" of a circuit is...

... essentially the number of variables the circuit truly depends on.

- For $\Sigma\Pi\Sigma$ circuits:

$$C \quad = \quad \sum_{i=1}^{k} \ell_{i1} \cdots \ell_{id}$$

[DvirShpilka05]: $\operatorname{rank}(C) \quad = \quad \operatorname{rank}\{\ell_{ij}\}$

The "rank" of a circuit is...

... essentially the number of variables the circuit truly depends on.

- For $\Sigma\Pi\Sigma$ circuits:

$$C = \sum_{i=1}^{k} \ell_{i1} \cdots \ell_{id}$$

[DvirShpilka05]: $\text{rank}(C) = \text{rank}\{\ell_{ij}\}$

... thus C "essentially" computes a $\text{rank}(C)$-variate polynomial

The "rank" of a circuit is...

... essentially the number of variables the circuit truly depends on.

- For $\Sigma\Pi\Sigma$ circuits:

$$C = \sum_{i=1}^{k} \ell_{i1} \cdots \ell_{id}$$

[DvirShpilka05]: $\text{rank}(C) = \text{rank}\{\ell_{ij}\}$

... thus C "essentially" computes a $\text{rank}(C)$-variate polynomial

- For $\Sigma\Pi\Sigma\Pi$ circuits:

$$C = \sum_{i=1}^{k} f_{i1} \cdots f_{id}$$

[BeeckenMittmannSaxena11]: $\text{rank}(C) = \text{TrDeg}\{f_{ij}\}$

General Road map

Whitebox:

- Compute the rank r of the circuit C.
- (if the rank was small) Construct a map

$$\Phi : \mathbb{F}[x_1, \cdots, x_n] \longrightarrow \mathbb{F}[y_1, \cdots, y_r]$$

  that *preserves the rank*. That is, $\text{rank}(C) = \text{rank}(\Phi(C))$. And use Schwartz-Zippel to get a $O(d^r)$-sized hitting set.
- For large rank, ...

General Road map

Whitebox:

- Compute the rank r of the circuit C.
- (if the rank was small) Construct a map

$$\Phi : \mathbb{F}[x_1, \cdots, x_n] \longrightarrow \mathbb{F}[y_1, \cdots, y_r]$$

  that *preserves the rank*. That is, $\text{rank}(C) = \text{rank}(\Phi(C))$. And use Schwartz-Zippel to get a $O(d^r)$-sized hitting set.
- For large rank, ... prove the following:

Meta-theorem for rank bounds

If the given circuit C has rank more than R, then C cannot be identically zero.*

* Conditions apply

Outline

Meta-theorem for $\Sigma\Pi\Sigma$ circuits

Meta theorem for rank bounds

Any $\Sigma\Pi\Sigma(n, k, d)$ circuit that has rank more than $R(n, k, d)$ cannot be identically zero.

Ways to cheat:

$$(x + y)^2 - x^2 - y^2 - 2xy$$

Meta-theorem for $\Sigma\Pi\Sigma$ circuits

Meta theorem for rank bounds

Any $\Sigma\Pi\Sigma(n, k, d)$ circuit that has rank more than $R(n, k, d)$ cannot be identically zero.

Ways to cheat:

$$z_1 z_2 \cdots z_n (x+y)^2 - z_1 z_2 \cdots z_n x^2 - z_1 z_2 \cdots z_n y^2 - 2 z_1 z_2 \cdots z_n xy$$

Meta-theorem for $\Sigma\Pi\Sigma$ circuits

Meta theorem for rank bounds

Any simple $\Sigma\Pi\Sigma(n, k, d)$ circuit that has rank more than $R(n, k, d)$ cannot be identically zero.

Ways to cheat:

$$z_1 z_2 \cdots z_n (x + y)^2 - z_1 z_2 \cdots z_n x^2 - z_1 z_2 \cdots z_n y^2 - 2 z_1 z_2 \cdots z_n xy$$

- Circuit must be *simple*.

Meta-theorem for $\Sigma\Pi\Sigma$ circuits

Meta theorem for rank bounds

Any simple $\Sigma\Pi\Sigma(n, k, d)$ circuit that has rank more than $R(n, k, d)$ cannot be identically zero.

Ways to cheat:

$$x_1 \cdots x_n - x_1 \cdots x_n \quad + \quad y_1 \cdots y_n - y_1 \cdots y_n$$

- Circuit must be *simple*.

Meta-theorem for $\Sigma\Pi\Sigma$ circuits

Meta theorem for rank bounds

Any simple $\Sigma\Pi\Sigma(n, k, d)$ circuit that has rank more than $R(n, k, d)$ cannot be identically zero.

Ways to cheat:

$$x_1 \cdots x_n - x_1 \cdots x_n \quad + \quad y_1 \cdots y_n - y_1 \cdots y_n$$

- Circuit must be *simple*.

Meta-theorem for $\Sigma\Pi\Sigma$ circuits

Meta theorem for rank bounds

Any simple, minimal $\Sigma\Pi\Sigma(n, k, d)$ circuit that has rank more than $R(n, k, d)$ cannot be identically zero.

Ways to cheat:

$$x_1 \cdots x_n - x_1 \cdots x_n \quad + \quad y_1 \cdots y_n - y_1 \cdots y_n$$

- Circuit must be *simple*.
- Circuit must be *minimal*.

Rank bounds for $\Sigma\Pi\Sigma$ circuits

Theorem

Any simple and minimal $\Sigma\Pi\Sigma(n, k, d)$ circuit that has rank more than $R(n, k, d)$ cannot be identically zero.

Rank bounds for $\Sigma\Pi\Sigma$ circuits

Theorem

Any simple and minimal $\Sigma\Pi\Sigma(n, k, d)$ circuit that has rank more than $R(n, k, d)$ cannot be identically zero.

[DvirShpilka05] $\quad R(n, k, d) = 2^{O(k^2)}(\log d)^{k-2}$

Rank bounds for $\Sigma\Pi\Sigma$ circuits

Theorem

Any simple and minimal $\Sigma\Pi\Sigma(n, k, d)$ circuit that has rank more than $R(n, k, d)$ cannot be identically zero.

[DvirShpilka05]	$R(n, k, d) = 2^{O(k^2)}(\log d)^{k-2}$
[KayalSaxena07]	$R(n, k, d) = \Omega(k \log d)$ over finite fields

Rank bounds for $\Sigma\Pi\Sigma$ circuits

Theorem

Any simple and minimal $\Sigma\Pi\Sigma(n, k, d)$ circuit that has rank more than $R(n, k, d)$ cannot be identically zero.

[DvirShpilka05]	$R(n, k, d) = 2^{O(k^2)}(\log d)^{k-2}$
[KayalSaxena07]	$R(n, k, d) = \Omega(k \log d)$ over finite fields
[SaxenaSeshadri09]	$R(n, k, d) = O(k^3 \log d)$

Rank bounds for $\Sigma\Pi\Sigma$ circuits

Theorem

Any simple and minimal $\Sigma\Pi\Sigma(n, k, d)$ circuit that has rank more than $R(n, k, d)$ cannot be identically zero.

[DvirShpilka05]	$R(n, k, d) = 2^{O(k^2)}(\log d)^{k-2}$
[KayalSaxena07]	$R(n, k, d) = \Omega(k \log d)$ over finite fields
[SaxenaSeshadri09]	$R(n, k, d) = O(k^3 \log d)$
[KayalSaraf09]	$R(n, k, d) = 2^{O(k \log k)}$ over the field $\mathbb{R}$

Rank bounds for $\Sigma\Pi\Sigma$ circuits

Theorem

Any simple and minimal $\Sigma\Pi\Sigma(n, k, d)$ circuit that has rank more than $R(n, k, d)$ cannot be identically zero.

[DvirShpilka05]	$R(n, k, d) = 2^{O(k^2)}(\log d)^{k-2}$
[KayalSaxena07]	$R(n, k, d) = \Omega(k \log d)$ over finite fields
[SaxenaSeshadri09]	$R(n, k, d) = O(k^3 \log d)$
[KayalSaraf09]	$R(n, k, d) = 2^{O(k \log k)}$ over the field $\mathbb{R}$
[SaxenaSeshadri10]	$R(n, k, d) = O(k^2 \log d)$
	$R(n, k, d) = O(k^2)$ over the field $\mathbb{R}$

Rank bounds for $\Sigma\Pi\Sigma$ circuits

Theorem

Any simple and minimal $\Sigma\Pi\Sigma(n, k, d)$ circuit that has rank more than $R(n, k, d)$ cannot be identically zero.

[DvirShpilka05]	$R(n, k, d) = 2^{O(k^2)}(\log d)^{k-2}$
[KayalSaxena07]	$R(n, k, d) = \Omega(k \log d)$ over finite fields
[SaxenaSeshadri09]	$R(n, k, d) = O(k^3 \log d)$
[KayalSaraf09]	$R(n, k, d) = 2^{O(k \log k)}$ over the field $\mathbb{R}$
[SaxenaSeshadri10]	$R(n, k, d) = O(k^2 \log d)$
	$R(n, k, d) = O(k^2)$ over the field $\mathbb{R}$

Translates to a poly$(d^{R(n,k,d)}, n)$ whitebox PIT.

Rank bounds for $\Sigma\Pi\Sigma$ circuits

Theorem

Any simple and minimal $\Sigma\Pi\Sigma(n, k, d)$ circuit that has rank more than $R(n, k, d)$ cannot be identically zero.

[DvirShpilka05]	$R(n, k, d) = 2^{O(k^2)}(\log d)^{k-2}$
[KayalSaxena07]	$R(n, k, d) = \Omega(k \log d)$ over finite fields
[SaxenaSeshadri09]	$R(n, k, d) = O(k^3 \log d)$
[KayalSaraf09]	$R(n, k, d) = 2^{O(k \log k)}$ over the field $\mathbb{R}$
[SaxenaSeshadri10]	$R(n, k, d) = O(k^2 \log d)$
	$R(n, k, d) = O(k^2)$ over the field $\mathbb{R}$

Translates to a poly$(d^{R(n,k,d)}, n)$ whitebox PIT.

Rank bounds for $\Sigma\Pi\Sigma$ circuits

Theorem

Any simple and minimal $\Sigma\Pi\Sigma(n, k, d)$ circuit that has rank more than $R(n, k, d)$ cannot be identically zero.

[DvirShpilka05]	$R(n, k, d) = 2^{O(k^2)}(\log d)^{k-2}$
[KayalSaxena07]	$R(n, k, d) = \Omega(k \log d)$ over finite fields
[SaxenaSeshadri09]	$R(n, k, d) = O(k^3 \log d)$
[KayalSaraf09]	$R(n, k, d) = 2^{O(k \log k)}$ over the field $\mathbb{R}$
[SaxenaSeshadri10]	$R(n, k, d) = O(k^2 \log d)$
	$R(n, k, d) = O(k^2)$ over the field $\mathbb{R}$

Translates to a poly$(d^{R(n,k,d)}, n)$ whitebox PIT.

What about blackbox?

Outline

Rank bounds to blackbox algorithms

Theorem (KarninShpilka08)

If R *is an upper bound on the rank of a simple minimal* $\Sigma\Pi\Sigma(n, k, d)$ *identity, then there is a blackbox polynomial identity test running in time* $\mathrm{poly}(d^R, n)$.

Rank bounds to blackbox algorithms

Theorem (KarninShpilka08)

If R *is an upper bound on the rank of a simple minimal* $\Sigma\Pi\Sigma(n, k, d)$ *identity, then there is a blackbox polynomial identity test running in time* $\text{poly}(d^R, n)$.

General Idea:

- Find a linear map $\Phi : \mathbb{F}[x_1, \cdots, x_n] \to \mathbb{F}[y_1, \cdots, y_{R+1}]$ that preserves a *subspace* of dimension $R + 1$ (if it exists).
- Apply Schwartz-Zippel on this $(R + 1)$-variate circuit.

Rank bounds to blackbox algorithms

Theorem (KarninShpilka08)

If R *is an upper bound on the rank of a simple minimal* $\Sigma\Pi\Sigma(n, k, d)$ *identity, then there is a blackbox polynomial identity test running in time* $\text{poly}(d^R, n)$.

General Idea:

- Find a linear map $\Phi : \mathbb{F}[x_1, \cdots, x_n] \to \mathbb{F}[y_1, \cdots, y_{R+1}]$ that preserves a *subspace* of dimension $R + 1$ (if it exists).
- Apply Schwartz-Zippel on this $(R + 1)$-variate circuit.
- $\text{rank}(\Phi(C)) = \min(\text{rank}(C), R + 1)$. Can also preserve simplicity and minimality.

Rank bounds to blackbox algorithms

Theorem (KarninShpilka08)

If R *is an upper bound on the rank of a simple minimal* $\Sigma\Pi\Sigma(n, k, d)$ *identity, then there is a blackbox polynomial identity test running in time* $\text{poly}(d^R, n)$.

General Idea:

- Find a linear map $\Phi : \mathbb{F}[x_1, \cdots, x_n] \to \mathbb{F}[y_1, \cdots, y_{R+1}]$ that preserves a *subspace* of dimension $R + 1$ (if it exists).
- Apply Schwartz-Zippel on this $(R + 1)$-variate circuit.
- $\text{rank}(\Phi(C)) = \min(\text{rank}(C), R + 1)$. Can also preserve simplicity and minimality.
- Large rank circuits stay non-identities
  Smaller rank circuits are transformed "isomorphically".

Rank preserving maps

Lemma (GabizonRaz05)

Given n, k*, there is a set of* $nk^2 + 1$ *of linear transformations* $\{\Phi_t\} : \mathbb{F}^n \to \mathbb{F}^k$ *such that for any subspace* $V \subset \mathbb{F}^n$ *of dimension* k*, there is at least one* Φ_t *that is an isomorphism between* V *and* $\mathbb{F}^k$*.*

Rank preserving maps

Lemma (GabizonRaz05)

Given n, k*, there is a set of* $nk^2 + 1$ *of linear transformations* $\{\Phi_t\} : \mathbb{F}^n \to \mathbb{F}^k$ *such that for any subspace* $V \subset \mathbb{F}^n$ *of dimension* k*, there is at least one* Φ_t *that is an isomorphism between* V *and* $\mathbb{F}^k$*.*

$$\Phi_t = \begin{bmatrix} t & t^2 & \cdots & t^n \\ t^2 & t^4 & \cdots & t^{2n} \\ \vdots & \vdots & \ddots & \vdots \\ t^k & t^{2k} & \cdots & t^{nk} \end{bmatrix}_{n \times k}$$

Rank preserving maps

Lemma (GabizonRaz05)

Given n, k*, there is a set of* $nk^2 + 1$ *of linear transformations* $\{\Phi_t\} : \mathbb{F}^n \to \mathbb{F}^k$ *such that for any subspace* $V \subset \mathbb{F}^n$ *of dimension* k*, there is at least one* Φ_t *that is an isomorphism between* V *and* $\mathbb{F}^k$*.*

Proof.

$$\begin{bmatrix} t & t^2 & \cdots & t^n \\ t^2 & t^4 & \cdots & t^{2n} \\ \vdots & \vdots & \ddots & \vdots \\ t^k & t^{2k} & \cdots & t^{nk} \end{bmatrix} \begin{bmatrix} \uparrow & \uparrow & & \uparrow \\ f_1 & f_2 & \cdots & f_k \\ \downarrow & \downarrow & & \downarrow \end{bmatrix} = \begin{bmatrix} f_1(t) & \cdots & f_k(t) \\ f_1(t^2) & \cdots & f_k(t^2) \\ \vdots & \ddots & \vdots \\ f_1(t^k) & \cdots & f_k(t^k) \end{bmatrix}$$

Rank preserving maps

Lemma (GabizonRaz05)

Given n, k*, there is a set of* $nk^2 + 1$ *of linear transformations* $\{\Phi_t\} : \mathbb{F}^n \to \mathbb{F}^k$ *such that for any subspace* $V \subset \mathbb{F}^n$ *of dimension* k*, there is at least one* Φ_t *that is an isomorphism between* V *and* $\mathbb{F}^k$*.*

Proof.

$$\begin{bmatrix} t & t^2 & \cdots & t^n \\ t^2 & t^4 & \cdots & t^{2n} \\ \vdots & \vdots & \ddots & \vdots \\ t^k & t^{2k} & \cdots & t^{nk} \end{bmatrix} \begin{bmatrix} \uparrow & \uparrow & & \uparrow \\ f_1 & f_2 & \cdots & f_k \\ \downarrow & \downarrow & & \downarrow \end{bmatrix} = \begin{bmatrix} f_1(t) & \cdots & f_k(t) \\ f_1(t^2) & \cdots & f_k(t^2) \\ \vdots & \ddots & \vdots \\ f_1(t^k) & \cdots & f_k(t^k) \end{bmatrix}$$

Rank preserving maps

Lemma (GabizonRaz05)

Given n, k*, there is a set of* $nk^2 + 1$ *of linear transformations* $\{\Phi_t\} : \mathbb{F}^n \to \mathbb{F}^k$ *such that for any subspace* $V \subset \mathbb{F}^n$ *of dimension* k*, there is at least one* Φ_t *that is an isomorphism between* V *and* $\mathbb{F}^k$*.*

Proof.

$$\begin{bmatrix} t & t^2 & \cdots & t^n \\ t^2 & t^4 & \cdots & t^{2n} \\ \vdots & \vdots & \ddots & \vdots \\ t^k & t^{2k} & \cdots & t^{nk} \end{bmatrix} \begin{bmatrix} \uparrow & \uparrow & & \uparrow \\ f_1 & f_2 & \cdots & f_k \\ \downarrow & \downarrow & & \downarrow \end{bmatrix} = \begin{bmatrix} f_1(t) & \cdots & f_k(t) \\ f_1(t^2) & \cdots & f_k(t^2) \\ \vdots & \ddots & \vdots \\ f_1(t^k) & \cdots & f_k(t^k) \end{bmatrix}$$

□

Rank preserving maps

Lemma (GabizonRaz05)

Given n, k, s*, there is a set of* $snk^2 + 1$ *of linear transformations* $\{\Phi_t\} : \mathbb{F}^n \to \mathbb{F}^k$ *such that for any* s *subspaces* $V_1, \cdots, V_s \subset \mathbb{F}^n$ *of dimension* k *each , there is at least one* Φ_t *that is an isomorphism between* V_i *and* $\mathbb{F}^k$ *for each* $1 \leq i \leq s$*.*

Proof.

$$\begin{bmatrix} t & t^2 & \cdots & t^n \\ t^2 & t^4 & \cdots & t^{2n} \\ \vdots & \vdots & \ddots & \vdots \\ t^k & t^{2k} & \cdots & t^{nk} \end{bmatrix} \begin{bmatrix} \uparrow & \uparrow & & \uparrow \\ f_1 & f_2 & \cdots & f_k \\ \downarrow & \downarrow & & \downarrow \\ & \ddots & & \\ & & & \end{bmatrix} = \begin{bmatrix} f_1(t) & \cdots & f_k(t) \\ f_1(t^2) & \cdots & f_k(t^2) \\ \vdots & \ddots & \vdots \\ f_1(t^k) & \cdots & f_k(t^k) \end{bmatrix}$$

□

Main issue with rank bound approaches

- [KayalSaxena07]: $R(n, k, d) = \Omega(k \log d)$ over finite fields.
- Best case: poly$(n, d^{k \log d})$
- Φ_t converts C to an "isomorphic circuit".

Main issue with rank bound approaches

- [KayalSaxena07]: $R(n, k, d) = \Omega(k \log d)$ over finite fields.
- Best case: poly$(n, d^{k \log d})$
- Φ_t converts C to an "isomorphic circuit".

- [SaxenaSeshadri11]: Φ only needs to preserve non-zeroness. Find a certificate for non-zeroness and preserve that instead.

Main issue with rank bound approaches

- [KayalSaxena07]: $R(n, k, d) = \Omega(k \log d)$ over finite fields.
- Best case: poly$(n, d^{k \log d})$
- Φ_t converts C to an "isomorphic circuit".

- [SaxenaSeshadri11]: Φ only needs to preserve non-zeroness. Find a certificate for non-zeroness and preserve that instead.

*** SPOILER ***
Certificate is an ideal of small rank

Outline

$$\begin{aligned} C &= T_1 + \cdots + T_k \\ \text{where} \quad T_i &= \ell_{i1} \cdots \ell_{id} \end{aligned}$$

Reviewing the Kayal-Saxena test

$$\begin{aligned} C &= T_1 + \cdots + T_k \\ \text{where} \quad T_i &= \ell_{i1} \cdots \ell_{id} \end{aligned}$$

- Can assume $\mathrm{LM}(T_1) \succeq \mathrm{LM}(C)$.

Reviewing the Kayal-Saxena test

$$\begin{aligned} C &= T_1 + \cdots + T_k \\ \text{where} \quad T_i &= \ell_{i1} \cdots \ell_{id} \end{aligned}$$

- Can assume $\mathrm{LM}(T_1) \succeq \mathrm{LM}(C)$.
- Check if $C = 0 \bmod T_1$.

Reviewing the Kayal-Saxena test

$$\begin{aligned} C &= T_1 + \cdots + T_k \\ \text{where} \quad T_i &= \ell_{i1} \cdots \ell_{id} \end{aligned}$$

- Can assume $\mathrm{LM}(T_1) \succeq \mathrm{LM}(C)$.
- Check if $C = 0 \bmod T_1$.

- Then $C = \alpha T_1$. Check if $\alpha = 0$.

Reviewing the Kayal-Saxena test

$$\begin{aligned} C &= T_1 + \cdots + T_k \\ \text{where} \quad T_i &= \ell_{i1} \cdots \ell_{id} \end{aligned}$$

- Can assume $\mathrm{LM}(T_1) \succeq \mathrm{LM}(C)$.
- Check if $C = 0 \bmod T_1$.
  - Use Chinese Remaindering:
  - Recursively check $C = 0 \bmod \ell_{1j}$ for all j.
- Then $C = \alpha T_1$. Check if $\alpha = 0$.

Reviewing the Kayal-Saxena test

$$\begin{aligned} C &= T_1 + \cdots + T_k \\ \text{where} \quad T_i &= \ell_{i1} \cdots \ell_{id} \end{aligned}$$

- Can assume $\mathrm{LM}(T_1) \succeq \mathrm{LM}(C)$.
- Check if $C = 0 \bmod T_1$.
  - Use Chinese Remaindering:
  - Recursively check $C = 0 \bmod \ell_{1j}$ for all j. (works only for distinct ℓ_{1j}'s)
- Then $C = \alpha T_1$. Check if $\alpha = 0$.

Reviewing the Kayal-Saxena test

$$\begin{aligned} C &= T_1 + \cdots + T_k \\ \text{where} \quad T_i &= \ell_{i1} \cdots \ell_{id} \end{aligned}$$

- Can assume $\mathrm{LM}(T_1) \succeq \mathrm{LM}(C)$.
- Check if $C = 0 \bmod T_1$.
  - Use Chinese Remaindering, over local rings:
  - Recursively check $C = 0 \bmod \ell_{1j}^{e_j}$ for all j.
- Then $C = \alpha T_1$. Check if $\alpha = 0$.

Reviewing the Kayal-Saxena test

$$\begin{aligned} C &= T_1 + \cdots + T_k \\ \text{where} \quad T_i &= \ell_{i1} \cdots \ell_{id} \end{aligned}$$

- Can assume $\mathrm{LM}(T_1) \succeq \mathrm{LM}(C)$.
- Check if $C = 0 \bmod T_1$.
  - Use Chinese Remaindering, over local rings: (For e.g. $\frac{\mathbb{F}[x]}{x^5}$)
  - Recursively check $C = 0 \bmod \ell_{1j}^{e_j}$ for all j.
- Then $C = \alpha T_1$. Check if $\alpha = 0$.

Outline

Some notation

$$
\begin{aligned}
T &= (x+y+z)(2y+3u+z)^2(3x+2y+2z)(3x+6u+2z) \\
I &= \left\langle x^2, (x+y)^3 \right\rangle
\end{aligned}
$$

Some notation

$$\begin{aligned} T &= (x+y+z)(2y+3u+z)^2(3x+2y+2z)(3x+6u+2z) \\ I &= \left\langle x^2, (x+y)^3 \right\rangle \end{aligned}$$

- $L(T) = \{x+y+z, 2y+3u+z, 3x+2y+2z, 3x+6u+2z\}$

Some notation

$$\begin{aligned} T &= (x+y+z)(2y+3u+z)^2(3x+2y+2z)(3x+6u+2z) \\ I &= \left\langle x^2, (x+y)^3 \right\rangle \end{aligned}$$

- $L(T) = \{x+y+z, 2y+3u+z, 3x+2y+2z, 3x+6u+2z\}$
- $\mathsf{radSpan}(I) = \mathsf{span}(x, x+y)$.

Some notation

$$\begin{aligned} T &= (x+y+z)(2y+3u+z)^2(3x+2y+2z)(3x+6u+2z) \\ I &= \left\langle x^2, (x+y)^3 \right\rangle \end{aligned}$$

- $L(T) = \{x+y+z, 2y+3u+z, 3x+2y+2z, 3x+6u+2z\}$
- $\mathrm{radSpan}(I) = \mathrm{span}(x, x+y)$.
- $\ell_1 \equiv_I \ell_2 \quad$ if $\quad \ell_1 - c\ell_2 \in \mathrm{radSpan}(I)$ for some $c \in \mathbb{F}^*$.

Some notation

$$\begin{aligned} T &= (x+y+z)(2y+3u+z)^2(3x+2y+2z)(3x+6u+2z) \\ I &= \left\langle x^2, (x+y)^3 \right\rangle \end{aligned}$$

- $L(T) = \{x+y+z, 2y+3u+z, 3x+2y+2z, 3x+6u+2z\}$
- $\mathrm{radSpan}(I) = \mathrm{span}(x, x+y)$.
- $\ell_1 \equiv_I \ell_2 \quad$ if $\quad \ell_1 - c\ell_2 \in \mathrm{radSpan}(I)$ for some $c \in \mathbb{F}^*$.
- $\mathrm{nodes}(T) = \left\{ \begin{array}{c} (x+y+z)(3x+2y+2z), \\ (2y+3u+z)^2(3x+6u+2z) \end{array} \right\}$

Cancellation Lemma

Lemma

Let I *be an ideal generated by multiplication terms, and let* $\ell \notin \mathit{radSpan}(\mathrm{I})$. *Then for any polynomial* $\mathfrak{g}$,

$$\ell\mathfrak{g} \in \mathrm{I} \quad \textit{if and only if} \quad \mathfrak{g} \in \mathrm{I}$$

Cancellation Lemma

Lemma

Let I *be an ideal generated by multiplication terms, and let* $\ell \notin \mathit{radSpan}(\mathrm{I})$. *Then for any polynomial* g,

$$\ell \mathrm{g} \in \mathrm{I} \quad \textit{if and only if} \quad \mathrm{g} \in \mathrm{I}$$

Proof.

WLOG, $\ell = \mathrm{x}_1$ and radSpan(I) is x_1-free.

Cancellation Lemma

Lemma

Let I *be an ideal generated by multiplication terms, and let* $\ell \notin$ *radSpan*(I). *Then for any polynomial* g,

$$\ell g \in I \quad \textit{if and only if} \quad g \in I$$

Proof.

WLOG, $\ell = x_1$ and radSpan(I) is x_1-free.

$$\sum g_i x_1^i \in I \quad \text{if and only if} \quad g_i \in I \text{ for each } i \qquad \square$$

Chinese Remainder Theorem

Theorem

Let I *be an ideal generated by multiplication terms. Let* f *and* g *be two multiplication terms such that*

$$\begin{aligned} \mathrm{L}(\mathrm{f}) \cap \mathit{radSpan}(\mathrm{I}) &= \emptyset \\ \mathrm{L}(\mathrm{g}) \cap \mathit{radSpan}(\mathrm{I}, \mathrm{f}) &= \emptyset \end{aligned}$$

Then, $\langle \mathrm{I}, \mathrm{f} \rangle \cap \langle \mathrm{I}, \mathrm{g} \rangle = \langle \mathrm{I}, \mathrm{fg} \rangle$.

Theorem

Let I *be an ideal generated by multiplication terms. Let* f *and* g *be two multiplication terms such that*

$$\begin{aligned} L(f) \cap \mathit{radSpan}(I) &= \emptyset \\ L(g) \cap \mathit{radSpan}(I, f) &= \emptyset \end{aligned}$$

Then, $\langle I, f\rangle \cap \langle I, g\rangle = \langle I, fg\rangle$.

Proof.

$$h = i_1 + af = i_2 + bg$$

Theorem

Let I *be an ideal generated by multiplication terms. Let* f *and* g *be two multiplication terms such that*

$$\begin{aligned} L(f) \cap \mathit{radSpan}(I) &= \emptyset \\ L(g) \cap \mathit{radSpan}(I, f) &= \emptyset \end{aligned}$$

Then, $\langle I, f\rangle \cap \langle I, g\rangle = \langle I, fg\rangle$.

Proof.

$$\begin{aligned} h \quad = \quad i_1 + af \quad &= \quad i_2 + bg \\ \Longrightarrow \qquad i_2 + bg &\in \langle I, f\rangle \end{aligned}$$

□

Theorem

Let I *be an ideal generated by multiplication terms. Let* f *and* g *be two multiplication terms such that*

$$\begin{aligned} L(f) \cap \mathit{radSpan}(I) &= \emptyset \\ L(g) \cap \mathit{radSpan}(I, f) &= \emptyset \end{aligned}$$

Then, $\langle I, f\rangle \cap \langle I, g\rangle = \langle I, fg\rangle$.

Proof.

$$\begin{aligned} h &= i_1 + af = i_2 + bg \\ &\Longrightarrow \quad bg \in \langle I, f\rangle \end{aligned}$$

□

Theorem

Let I *be an ideal generated by multiplication terms. Let* f *and* g *be two multiplication terms such that*

$$\begin{aligned} L(f) \cap \mathit{radSpan}(I) &= \emptyset \\ L(g) \cap \mathit{radSpan}(I, f) &= \emptyset \end{aligned}$$

Then, $\langle I, f\rangle \cap \langle I, g\rangle = \langle I, fg\rangle$.

Proof.

$$\begin{aligned} h \quad = \quad i_1 + af \quad &= \quad i_2 + bg \\ \Longrightarrow \qquad b &\in \langle I, f\rangle \end{aligned}$$

□

Theorem

Let I *be an ideal generated by multiplication terms. Let* f *and* g *be two multiplication terms such that*

$$\begin{aligned} L(f) \cap \mathit{radSpan}(I) &= \emptyset \\ L(g) \cap \mathit{radSpan}(I, f) &= \emptyset \end{aligned}$$

Then, $\langle I, f\rangle \cap \langle I, g\rangle = \langle I, fg\rangle$.

Proof.

$$h = i_1 + af = i_2 + bg$$

$$\therefore \quad b = i' + cf$$

□

Theorem

Let I *be an ideal generated by multiplication terms. Let* f *and* g *be two multiplication terms such that*

$$\begin{aligned} \mathrm{L}(\mathrm{f}) \cap \mathit{radSpan}(\mathrm{I}) &= \emptyset \\ \mathrm{L}(\mathrm{g}) \cap \mathit{radSpan}(\mathrm{I}, \mathrm{f}) &= \emptyset \end{aligned}$$

Then, $\langle \mathrm{I}, \mathrm{f} \rangle \cap \langle \mathrm{I}, \mathrm{g} \rangle = \langle \mathrm{I}, \mathrm{fg} \rangle$.

Proof.

$$\Longrightarrow \qquad \mathrm{h} = \mathrm{i}_2 + (\mathrm{i}' + \mathrm{cf})\mathrm{g}$$

□

Theorem

Let I *be an ideal generated by multiplication terms. Let* f *and* g *be two multiplication terms such that*

$$\begin{aligned} \mathrm{L}(\mathrm{f}) \cap \mathit{radSpan}(\mathrm{I}) &= \emptyset \\ \mathrm{L}(\mathrm{g}) \cap \mathit{radSpan}(\mathrm{I}, \mathrm{f}) &= \emptyset \end{aligned}$$

Then, $\langle \mathrm{I}, \mathrm{f} \rangle \cap \langle \mathrm{I}, \mathrm{g} \rangle = \langle \mathrm{I}, \mathrm{fg} \rangle$.

Proof.

$$\Longrightarrow \qquad \mathrm{h} = \mathrm{i}_2 + (\mathrm{i}' + \mathrm{cf})\mathrm{g} = \mathrm{i} + \mathrm{cfg}$$

□

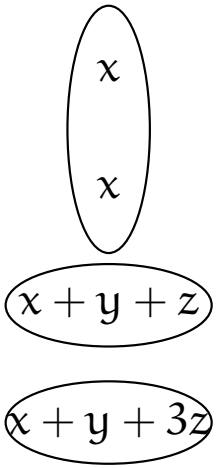
In search of a certificate

x	y	x	$3x+y$	x
x	$x+y$	y	$5x+y$	y
$x+y+z$	$x+z$	y	$x+y+z$	$x+y+z$
$x+y+3z$	$x+y+z$	$x+y+4z$	$x+y+z$	$x+y+z$
$\mathbf{T_1}$	$\mathbf{T_2}$	$\mathbf{T_3}$	$\mathbf{T_4}$	$\mathbf{T_5}$

$$I = \langle 0 \rangle$$

$$\mathsf{radSpan}(I) = \mathsf{span}(0)$$

In search of a certificate

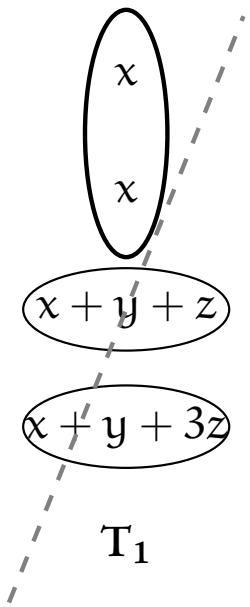


T_1	T_2	T_3	T_4	T_5
x	y	x	$3x + y$	x
x	$x + y$	y	$5x + y$	y
$x + y + z$	$x + z$	y	$x + y + z$	$x + y + z$
$x + y + 3z$	$x + y + z$	$x + y + 4z$	$x + y + z$	$x + y + z$

$$I = \langle 0 \rangle$$

$$\mathsf{radSpan}(I) = \mathsf{span}(0)$$

In search of a certificate

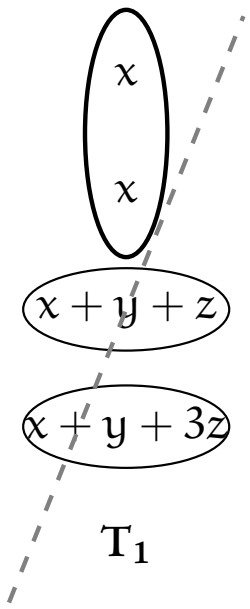


T_1	T_2	T_3	T_4	T_5
x	y	x	$3x + y$	x
x	$x + y$	y	$5x + y$	y
$x + y + z$	$x + z$	y	$x + y + z$	$x + y + z$
$x + y + 3z$	$x + y + z$	$x + y + 4z$	$x + y + z$	$x + y + z$

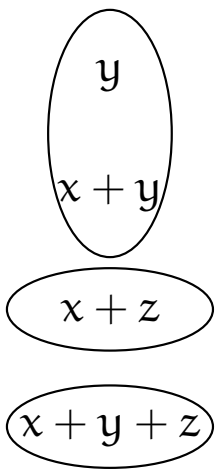
$$I = \langle x^2 \rangle$$

$$\mathsf{radSpan}(I) = \mathsf{span}(x)$$

In search of a certificate



T_1



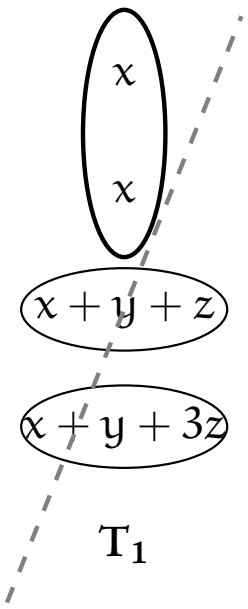
T_2

T_3	T_4	T_5
x	$3x + y$	x
y	$5x + y$	y
y	$x + y + z$	$x + y + z$
$x + y + 4z$	$x + y + z$	$x + y + z$

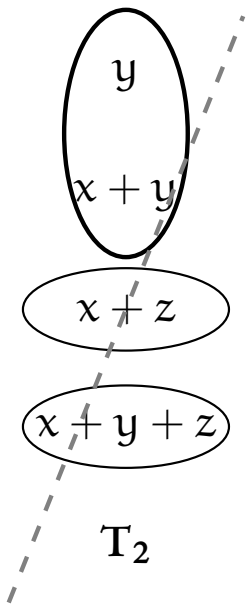
$$I = \langle x^2 \rangle$$

$$\mathsf{radSpan}(I) = \mathsf{span}(x)$$

In search of a certificate



T_1



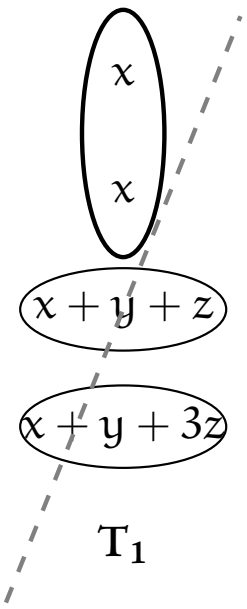
T_2

T_3	T_4	T_5
x	$3x + y$	x
y	$5x + y$	y
y	$x + y + z$	$x + y + z$
$x + y + 4z$	$x + y + z$	$x + y + z$

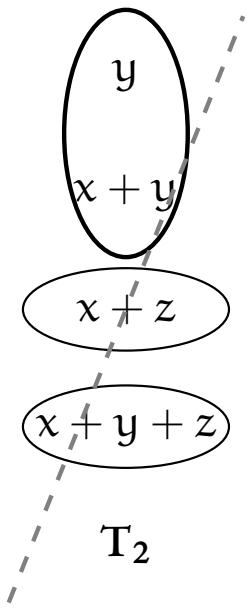
$$I = \langle x^2, y(x + y) \rangle$$

$$\mathsf{radSpan}(I) = \mathsf{span}(y, x + y)$$

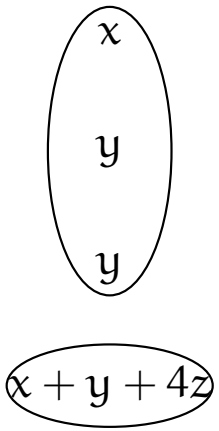
In search of a certificate



T_1



T_2



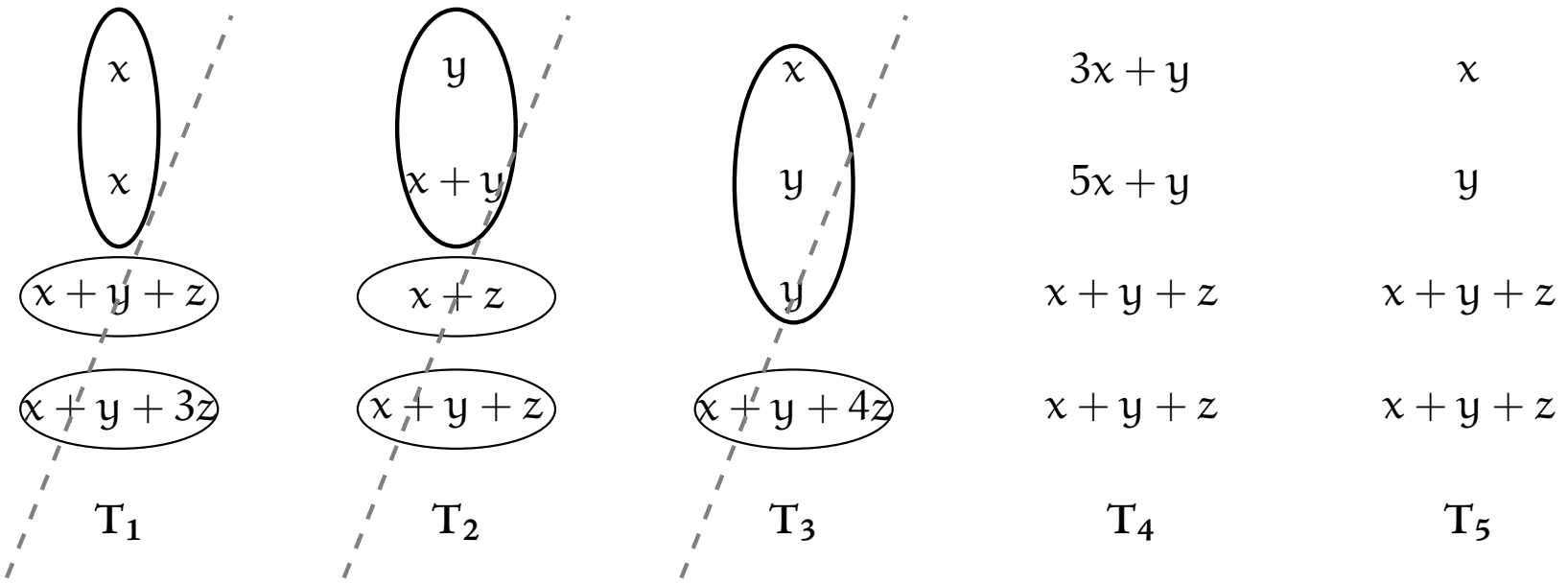
T_3

T_4	T_5
$3x + y$	x
$5x + y$	y
$x + y + z$	$x + y + z$
$x + y + z$	$x + y + z$

$$I = \langle x^2, y(x + y) \rangle$$

$$\mathsf{radSpan}(I) = \mathsf{span}(y, x + y)$$

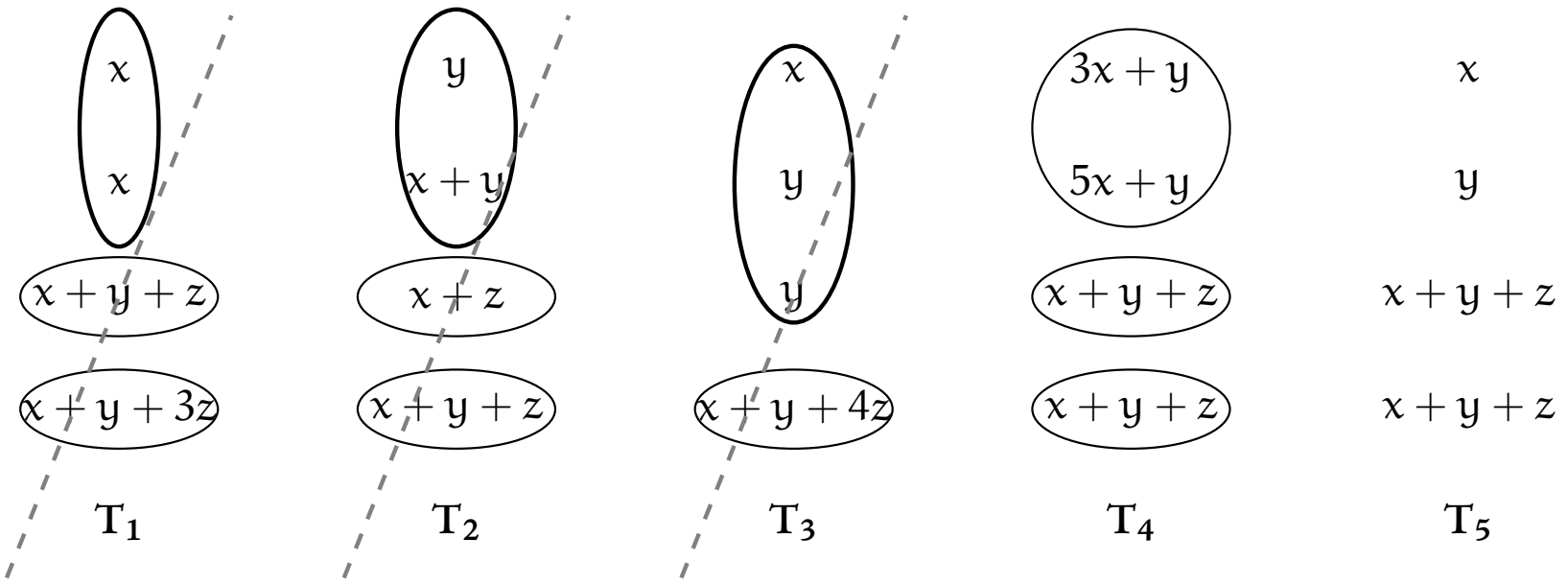
In search of a certificate



$$I = \langle x^2, y(x+y) \rangle$$

$$\mathsf{radSpan}(I) = \mathsf{span}(y, x+y)$$

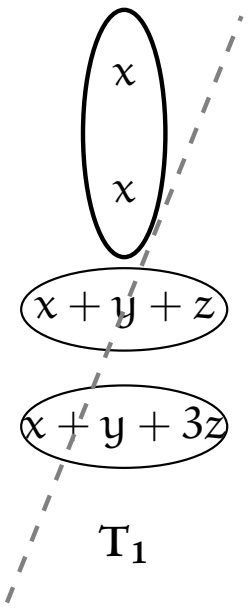
In search of a certificate



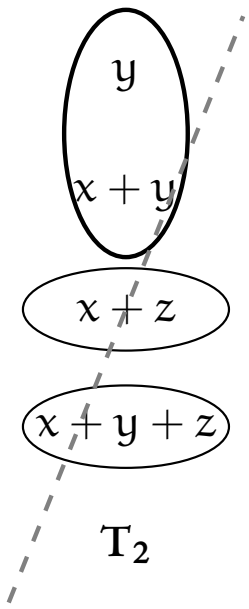
$$I = \langle x^2, y(x+y) \rangle$$

$$\mathsf{radSpan}(I) = \mathsf{span}(y, x+y)$$

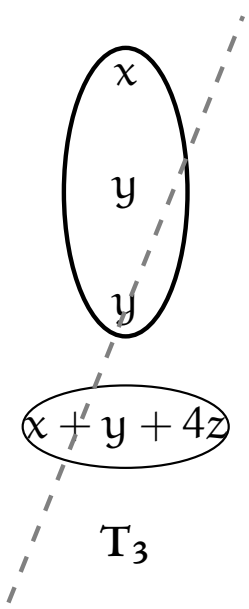
In search of a certificate



T_1



T_2



T_3

$3x + y$	x
$5x + y$	y
$x + y + z$	$x + y + z$
$x + y + z$	$x + y + z$

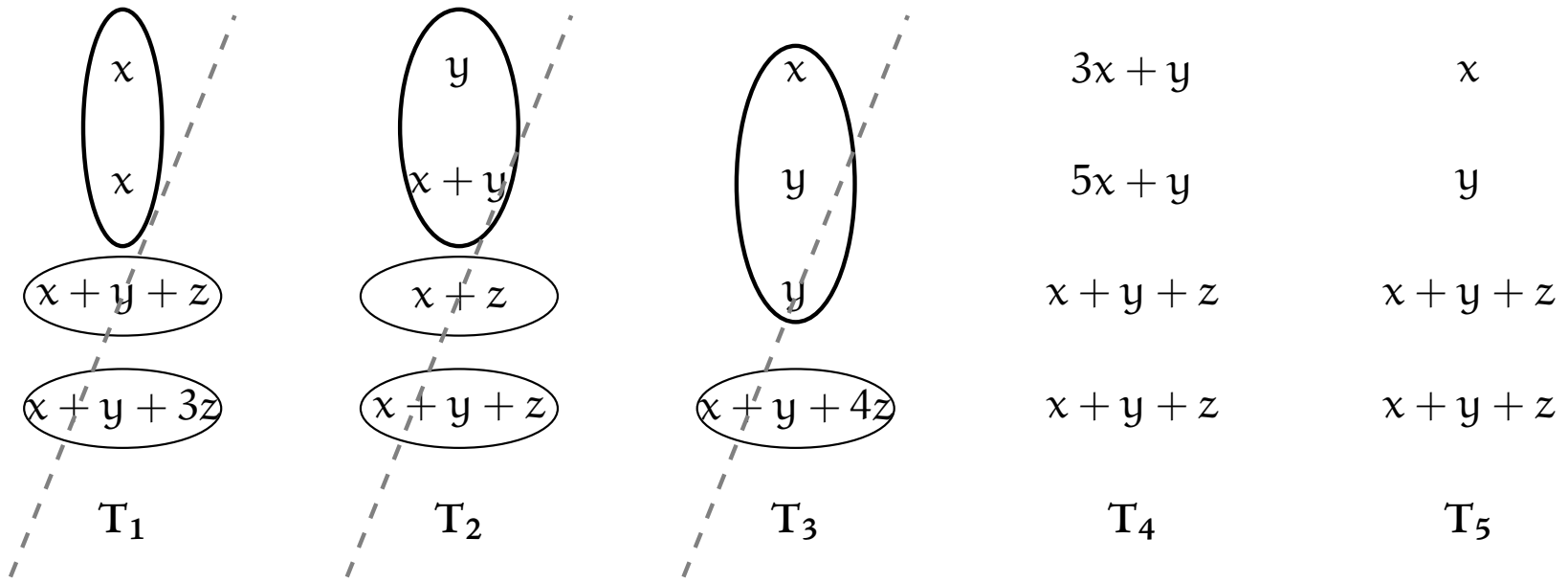
T_4 T_5

$$I = \langle x^2, y(x+y) \rangle$$

$$\mathsf{radSpan}(I) = \mathsf{span}(y, x+y)$$

$$C = \alpha T_4 \mod I$$

In search of a certificate



Theorem ([KayalSaxena07] rephrased)

For any non-zero $\Sigma\Pi\Sigma(n, k, d)$ *circuit* C*, then there is a path certificate* $p = \langle v_1, \cdots, v_{k'} \rangle$ *and a* T_i *such that*

$$C = \alpha T_i \bmod p \quad \textit{(for } \alpha \in \mathbb{F}^*\textit{)}$$

Outline

$$0 \neq C \quad = \quad T \bmod \langle v_1, \cdots, v_{k'} \rangle$$

$$0 \neq C \quad = \quad T \bmod \langle v_1, \cdots, v_{k'} \rangle$$

We know $T \notin I$

Preserving the certificate

$$0 \neq C \quad = \quad T \bmod \langle v_1, \cdots, v_{k'} \rangle$$

We know $T \notin I$

We want $\Phi(T) \notin \Phi(I)$

Preserving the certificate

$$0 \neq C \quad = \quad T \bmod \langle v_1, \cdots, v_{k'} \rangle$$

We know $T \notin I$

We want $\Phi(T) \notin \Phi(I)$

Properties that Φ must satisfy:

Preserving the certificate

$$0 \neq C \quad = \quad T \bmod \langle v_1, \cdots, v_{k'} \rangle$$

We know $T \notin I$ $\Leftrightarrow$ $v_T \notin I$

We want $\Phi(T) \notin \Phi(I)$

Properties that Φ must satisfy:

Preserving the certificate

$$0 \neq C \quad = \quad T \bmod \langle v_1, \cdots, v_{k'} \rangle$$

We know $T \notin I$ $\Leftrightarrow$ $v_T \notin I$

$\Updownarrow$

We want $\Phi(T) \notin \Phi(I)$ $\Phi(v_T) \notin \Phi(I)$

Properties that Φ must satisfy:

Preserving the certificate

$$0 \neq C \quad = \quad T \bmod \langle v_1, \cdots, v_{k'} \rangle$$

We know $T \notin I$ $\Leftrightarrow$ $v_T \notin I$

$\Updownarrow$

We want $\Phi(T) \notin \Phi(I)$ $\Phi(v_T) \notin \Phi(I)$

Properties that Φ must satisfy:

- $v_T \in I \Leftrightarrow \Phi(v_T) \in \Phi(I)$

Preserving the certificate

$$0 \neq C \quad = \quad T \bmod \langle v_1, \cdots, v_{k'} \rangle$$

$$\begin{array}{lcl} \text{We know } T \notin I & \Leftrightarrow & v_T \notin I \\ & & \Updownarrow \\ \text{We want } \Phi(T) \notin \Phi(I) & \Leftrightarrow & \Phi(v_T) \notin \Phi(I) \end{array}$$

Properties that Φ must satisfy:

- $v_T \in I \Leftrightarrow \Phi(v_T) \in \Phi(I)$

Preserving the certificate

$$0 \neq C \quad = \quad T \bmod \langle v_1, \cdots, v_{k'} \rangle$$

$$\begin{array}{lcl} \text{We know } T \notin I & \Leftrightarrow & v_T \notin I \\ & & \Updownarrow \\ \text{We want } \Phi(T) \notin \Phi(I) & \Leftrightarrow & \Phi(v_T) \notin \Phi(I) \end{array}$$

Properties that Φ must satisfy:

- $v_T \in I \Leftrightarrow \Phi(v_T) \in \Phi(I)$
- $\ell \in \text{radSpan}(I)$ if and only if $\Phi(\ell) \in \text{radSpan}(\Phi(I))$ for each $\ell \in L(T)$.

Preserving the certificate

$$0 \neq C \quad = \quad T \bmod \langle v_1, \cdots, v_{k'} \rangle$$

$$\begin{array}{ccc} \text{We know } T \notin I & \Leftrightarrow & v_T \notin I \\ \Updownarrow & & \Updownarrow \\ \text{We want } \Phi(T) \notin \Phi(I) & \Leftrightarrow & \Phi(v_T) \notin \Phi(I) \end{array}$$

Properties that Φ must satisfy:

- $v_T \in I \Leftrightarrow \Phi(v_T) \in \Phi(I)$
- $\ell \in \text{radSpan}(I)$ if and only if $\Phi(\ell) \in \text{radSpan}(\Phi(I))$ for each $\ell \in L(T)$.

Preserving the certificate

$$0 \neq C \quad = \quad T \bmod \langle v_1, \cdots, v_{k'} \rangle$$

$$\begin{array}{ccc} \text{We know } T \notin I & \Leftrightarrow & v_T \notin I \\ \Updownarrow & & \Updownarrow \\ \text{We want } \Phi(T) \notin \Phi(I) & \Leftrightarrow & \Phi(v_T) \notin \Phi(I) \end{array}$$

Properties that Φ must satisfy:

- $v_T \in I \Leftrightarrow \Phi(v_T) \in \Phi(I)$
- $\ell \in \text{radSpan}(I)$ if and only if $\Phi(\ell) \in \text{radSpan}(\Phi(I))$ for each $\ell \in L(T)$.

Question: Do we know of such a Φ?

Preserving the certificate

$$0 \neq C \quad = \quad T \bmod \langle v_1, \cdots, v_{k'} \rangle$$

$$\begin{array}{ccc} \text{We know } T \notin I & \Leftrightarrow & v_T \notin I \\ \Updownarrow & & \Updownarrow \\ \text{We want } \Phi(T) \notin \Phi(I) & \Leftrightarrow & \Phi(v_T) \notin \Phi(I) \end{array}$$

Properties that Φ must satisfy:

- $v_T \in I \Leftrightarrow \Phi(v_T) \in \Phi(I)$
- $\ell \in \text{radSpan}(I)$ if and only if $\Phi(\ell) \in \text{radSpan}(\Phi(I))$ for each $\ell \in L(T)$.

Question: Do we know of such a Φ?

[SaxenaSeshadri11]: The same [GabizonRaz05] map preserves low rank ideals!

Vandermonde works

Lemma

Let $f_0, f_1, \cdots, f_m$ *be multiplication terms with span* $\{\bigcup L(f_i)\}$ *has rank at most* k. *Let* Φ *be a linear map the preserves the space* V *generated by* $\bigcup L(f_i)$. *Then,*

$$f_0 \in \langle f_1, \cdots, f_m \rangle \quad \Longleftrightarrow \quad \Phi(f_0) \in \langle \Phi(f_1), \cdots, \Phi(f_m) \rangle$$

Vandermonde works

Lemma

Let $f_0, f_1, \cdots, f_m$ *be multiplication terms with span* $\{\bigcup L(f_i)\}$ *has rank at most* k. *Let* Φ *be a linear map the preserves the space* V *generated by* $\bigcup L(f_i)$. *Then,*

$$f_0 \in \langle f_1, \cdots, f_m \rangle \iff \Phi(f_0) \in \langle \Phi(f_1), \cdots, \Phi(f_m) \rangle$$

Proof overview.

Since Φ preserves V, it can be shown that Φ induces an isomorphism between the two algebras $\mathbb{F}[\ell_1, \cdots, \ell_k]$ and $\mathbb{F}[y_1, \cdots, y_k]$... □

... and we are nearly done

$$0 \neq C \quad = \quad T \bmod \langle v_1, \cdots, v_{k'} \rangle$$

Properties that Φ must satisfy:

- $v_T \in I \Leftrightarrow \Phi(v_T) \in \Phi(I)$
- $\ell \in \text{radSpan}(I)$ if and only if $\Phi(\ell) \in \text{radSpan}(\Phi(I))$ for each $\ell \in L(T)$.

... and we are nearly done

$$0 \neq C \quad = \quad T \bmod \langle v_1, \cdots, v_{k'} \rangle$$

Properties that Φ must satisfy:

- $v_T \in I \Leftrightarrow \Phi(v_T) \in \Phi(I)$ — need to preserve a dimension k space
- $\ell \in \text{radSpan}(I)$ if and only if $\Phi(\ell) \in \text{radSpan}(\Phi(I))$ for each $\ell \in L(T)$.

... and we are nearly done

$$0 \neq C \quad = \quad T \bmod \langle v_1, \cdots, v_{k'} \rangle$$

Properties that Φ must satisfy:

- $v_T \in I \Leftrightarrow \Phi(v_T) \in \Phi(I)$ — need to preserve a dimension k space
- $\ell \in \text{radSpan}(I)$ if and only if $\Phi(\ell) \in \text{radSpan}(\Phi(I))$ for each $\ell \in L(T)$. — need to preserve the space generated by ℓ and radSpan(I); need to preserve d spaces of dimension k

... and we are nearly done

$$0 \neq C \quad = \quad T \bmod \langle v_1, \cdots, v_{k'} \rangle$$

Properties that Φ must satisfy:

- $v_T \in I \Leftrightarrow \Phi(v_T) \in \Phi(I)$ — need to preserve a dimension k space
- $\ell \in \text{radSpan}(I)$ if and only if $\Phi(\ell) \in \text{radSpan}(\Phi(I))$ for each $\ell \in L(T)$. — need to preserve the space generated by ℓ and $\text{radSpan}(I)$; need to preserve d spaces of dimension k

Besides possibly nk^2d bad α's, the map Φ_α ensures that

$$T \in \langle v_1, \cdots, v_{k'} \rangle \quad \text{if and only if} \quad \Phi_\alpha(T) \in \Phi_\alpha(\langle v_1, \cdots, v_{k'} \rangle)$$

... and we are nearly done

$$0 \neq C \quad = \quad T \bmod \langle v_1, \cdots, v_{k'} \rangle$$

Properties that Φ must satisfy:

- $v_T \in I \Leftrightarrow \Phi(v_T) \in \Phi(I)$ — need to preserve a dimension k space
- $\ell \in \text{radSpan}(I)$ if and only if $\Phi(\ell) \in \text{radSpan}(\Phi(I))$ for each $\ell \in L(T)$. — need to preserve the space generated by ℓ and radSpan(I); need to preserve d spaces of dimension k

Besides possibly nk^2d bad α's, the map Φ_α ensures that

$$T \in \langle v_1, \cdots, v_{k'} \rangle \quad \text{if and only if} \quad \Phi_\alpha(T) \in \Phi_\alpha(\langle v_1, \cdots, v_{k'} \rangle)$$
$$\implies C = 0 \quad \text{if and only if} \quad \Phi_\alpha(C) = 0$$

... and we are nearly done

$$0 \neq C \quad = \quad T \bmod \langle v_1, \cdots, v_{k'} \rangle$$

Properties that Φ must satisfy:

- $v_T \in I \Leftrightarrow \Phi(v_T) \in \Phi(I)$ — need to preserve a dimension k space
- $\ell \in \text{radSpan}(I)$ if and only if $\Phi(\ell) \in \text{radSpan}(\Phi(I))$ for each $\ell \in L(T)$. — need to preserve the space generated by ℓ and radSpan(I); need to preserve d spaces of dimension k

Besides possibly nk^2d bad α's, the map Φ_α ensures that

$$T \in \langle v_1, \cdots, v_{k'} \rangle \quad \text{if and only if} \quad \Phi_\alpha(T) \in \Phi_\alpha(\langle v_1, \cdots, v_{k'} \rangle)$$
$$\implies C = 0 \quad \text{if and only if} \quad \Phi_\alpha(C) = 0$$

Schwartz-Zippel on the k-variate $\Phi_\alpha(C)$ finishes the job.

... and we are done

$$0 \neq C \quad = \quad T \bmod \langle v_1, \cdots, v_{k'} \rangle$$

Properties that Φ must satisfy:

- $v_T \in I \Leftrightarrow \Phi(v_T) \in \Phi(I)$ — need to preserve a dimension k space
- $\ell \in \text{radSpan}(I)$ if and only if $\Phi(\ell) \in \text{radSpan}(\Phi(I))$ for each $\ell \in L(T)$. — need to preserve the space generated by ℓ and radSpan(I); need to preserve d spaces of dimension k

Besides possibly nk^2d bad α's, the map Φ_α ensures that

$$T \in \langle v_1, \cdots, v_{k'} \rangle \quad \text{if and only if} \quad \Phi_\alpha(T) \in \Phi_\alpha(\langle v_1, \cdots, v_{k'} \rangle)$$
$$\implies C = 0 \quad \text{if and only if} \quad \Phi_\alpha(C) = 0$$

Schwartz-Zippel on the k-variate $\Phi_\alpha(C)$ finishes the job. □

Conclusions and open questions

- Studying the original [KayalSaxena07] test carefully, we obtained a low-rank path certificate for non-zeroness.
- The Vandermonde preserves ideals with small radical span.
- Certificate can be preserved by mapping (via the Vandermonde) to just a $\mathbf{k}$-variate polynomial ring.
- [BeeckenMittmannSaxena11] defined a "rank" for $\Sigma\Pi\Sigma\Pi$ circuits, and gave blackbox PITs for bounded rank circuits.

Conclusions and open questions

- Studying the original [KayalSaxena07] test carefully, we obtained a low-rank path certificate for non-zeroness.
- The Vandermonde preserves ideals with small radical span.
- Certificate can be preserved by mapping (via the Vandermonde) to just a $\mathbf{k}$-variate polynomial ring.
- [BeeckenMittmannSaxena11] defined a "rank" for $\Sigma\Pi\Sigma\Pi$ circuits, and gave blackbox PITs for bounded rank circuits. Vandermonde used again.

Conclusions and open questions

- Studying the original [KayalSaxena07] test carefully, we obtained a low-rank path certificate for non-zeroness.
- The Vandermonde preserves ideals with small radical span.
- Certificate can be preserved by mapping (via the Vandermonde) to just a k-variate polynomial ring.
- [BeeckenMittmannSaxena11] defined a "rank" for $\Sigma\Pi\Sigma\Pi$ circuits, and gave blackbox PITs for bounded rank circuits. Vandermonde used again.

Question: Can these ideas be used for Σ-Pow-Σ?

$$C = \sum_{i=1}^{m} \ell_i^d$$

Conclusions and open questions

- Studying the original [KayalSaxena07] test carefully, we obtained a low-rank path certificate for non-zeroness.
- The Vandermonde preserves ideals with small radical span.
- Certificate can be preserved by mapping (via the Vandermonde) to just a k-variate polynomial ring.
- [BeeckenMittmannSaxena11] defined a "rank" for $\Sigma\Pi\Sigma\Pi$ circuits, and gave blackbox PITs for bounded rank circuits. Vandermonde used again.

Question: Can these ideas be used for Σ-Pow-Σ?

$$C = \sum_{i=1}^{m} \ell_i^d$$

Whitebox PITs are known. [Saxena08], [Kayal10]

Thank you!

Questions?