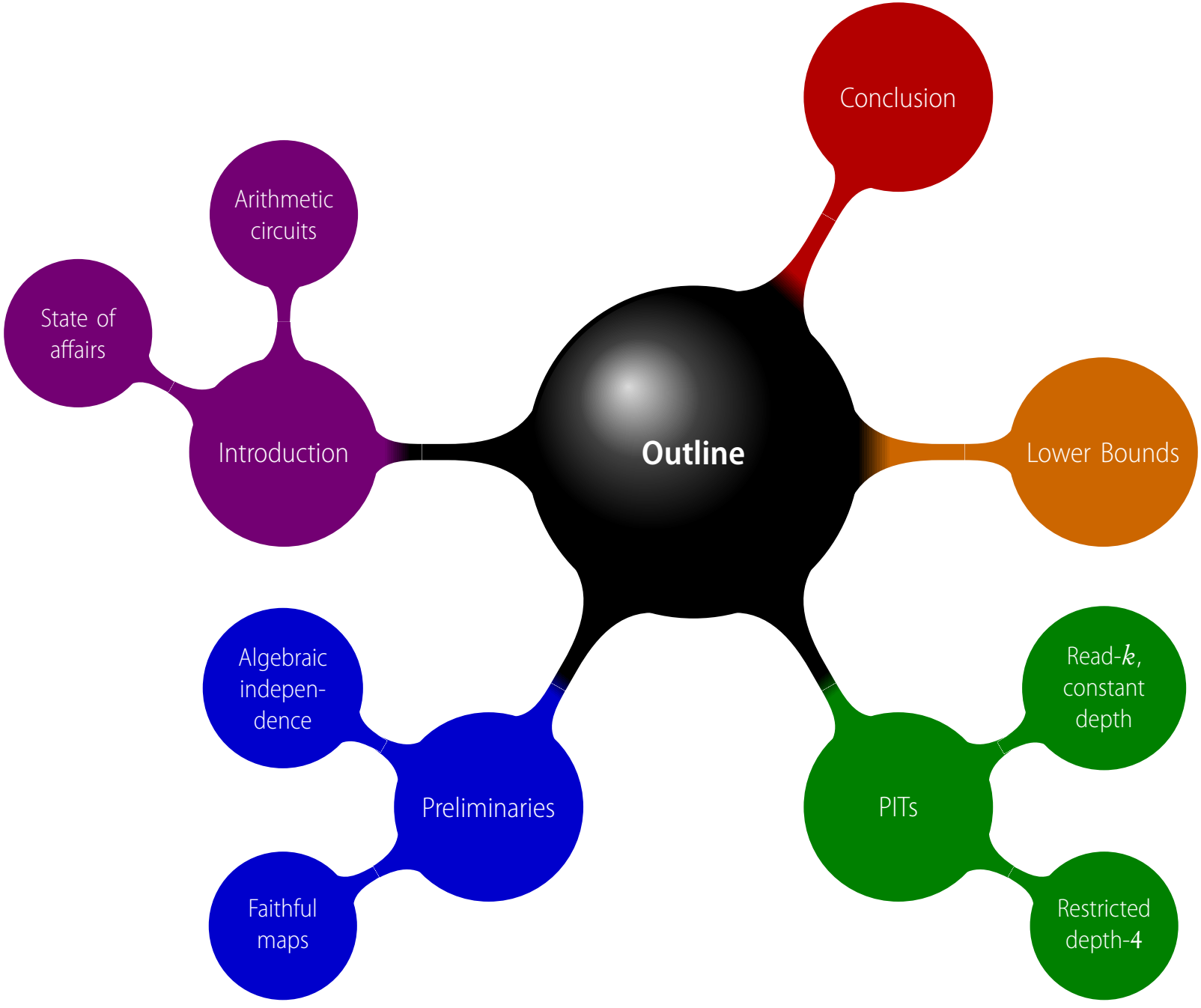
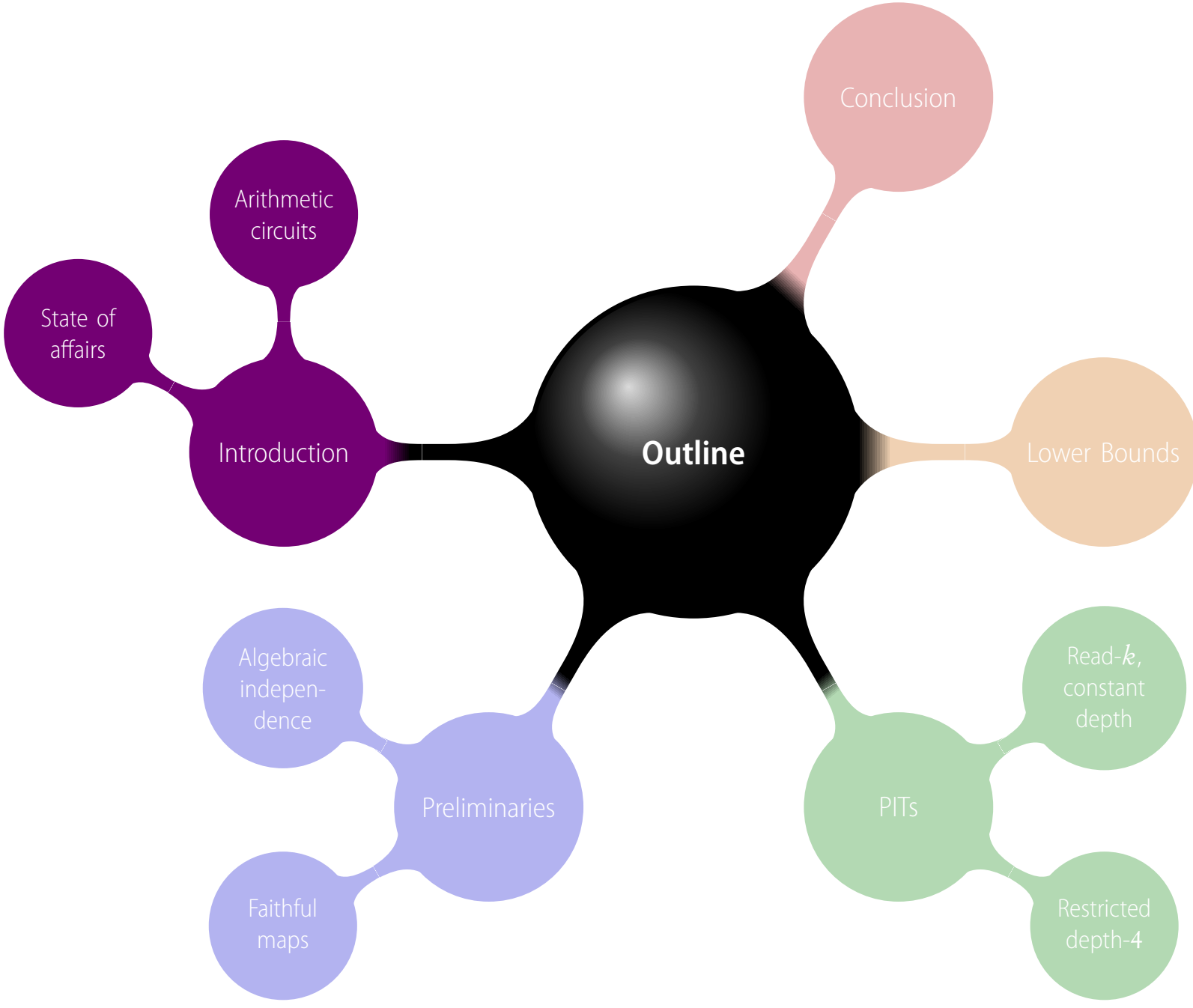
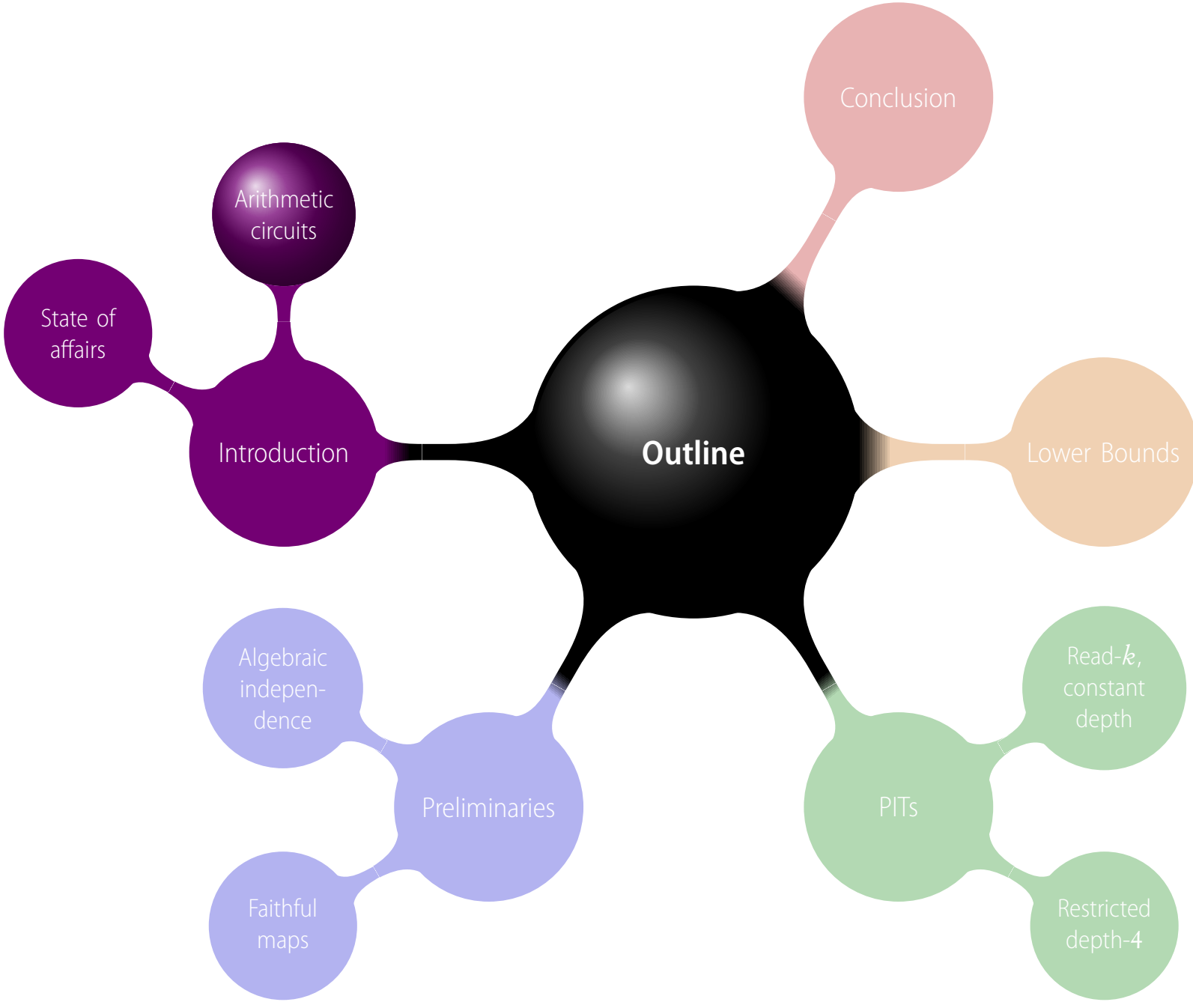
Jacobian hits the circuits

Manindra Agrawal Chandan Saha *Ramprasad Saptharishi*
Nitin Saxena

China Theory Week 2011
Århus, Denmark
October, 2011


Outline
Introduction
Arithmetic circuits
State of affairs
Preliminaries
Algebraic indepen-dence
Faithful maps
Lower Bounds
PITs
Read-k, constant depth
Restricted depth-4
Conclusion


Outline
Introduction
State of affairs
Arithmetic circuits
Preliminaries
Algebraic indepen-dence
Faithful maps
Lower Bounds
PITs
Read-k, constant depth
Restricted depth-4
Conclusion

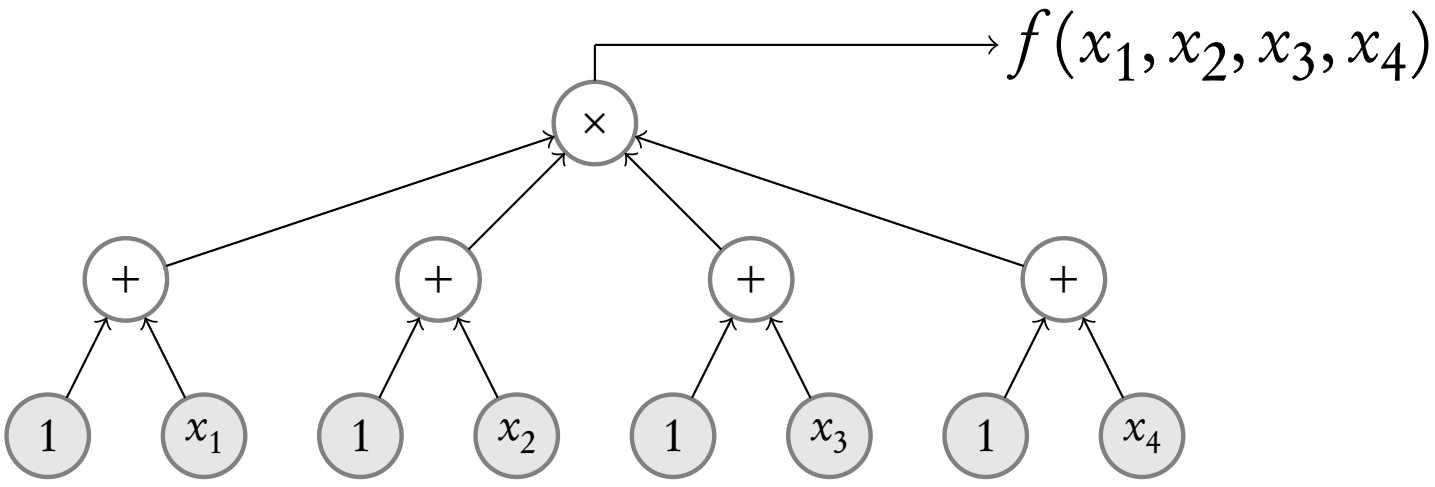

Outline
Introduction
Arithmetic circuits
State of affairs
Preliminaries
Algebraic independence
Faithful maps
Lower Bounds
PITs
Read-k, constant depth
Restricted depth-4
Conclusion

$$
\begin{aligned}
f(x_1, x_2, x_3, x_4) \quad = \quad & 1 + x_1 + x_2 + x_3 + x_4 \\
& + x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4 \\
& + x_2x_3x_4 + x_1x_3x_4 + x_1x_2x_4 + x_1x_2x_3 \\
& + x_1x_2x_3x_4
\end{aligned}
$$

$$
\begin{aligned}
f(x_1, x_2, x_3, x_4) &= 1 + x_1 + x_2 + x_3 + x_4 \\
&\quad + x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4 \\
&\quad + x_2x_3x_4 + x_1x_3x_4 + x_1x_2x_4 + x_1x_2x_3 \\
&\quad + x_1x_2x_3x_4 \\
&= (1 + x_1)(1 + x_2)(1 + x_3)(1 + x_4)
\end{aligned}
$$

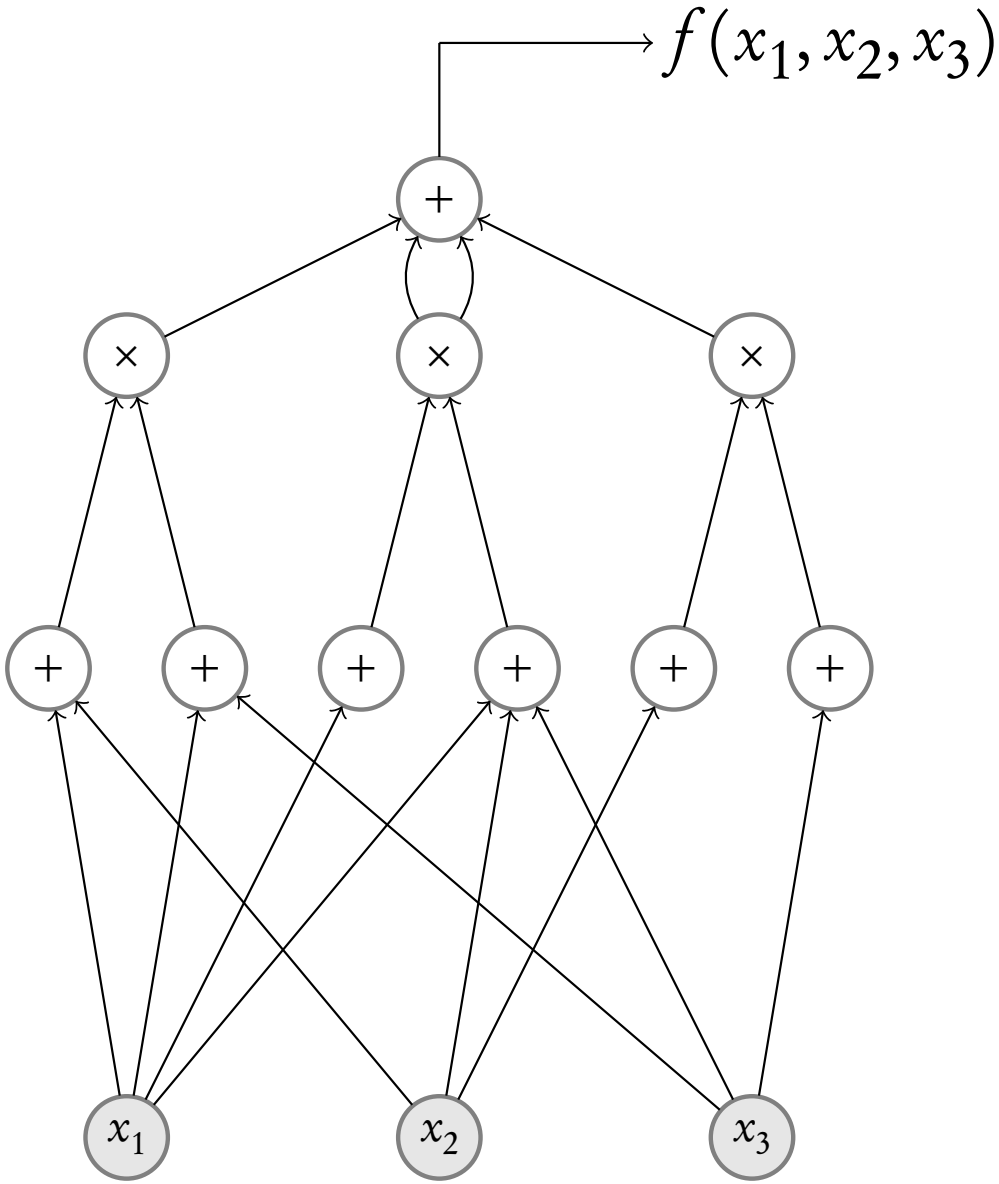
... certainly a more compact representation.

Arithmetic Formulae

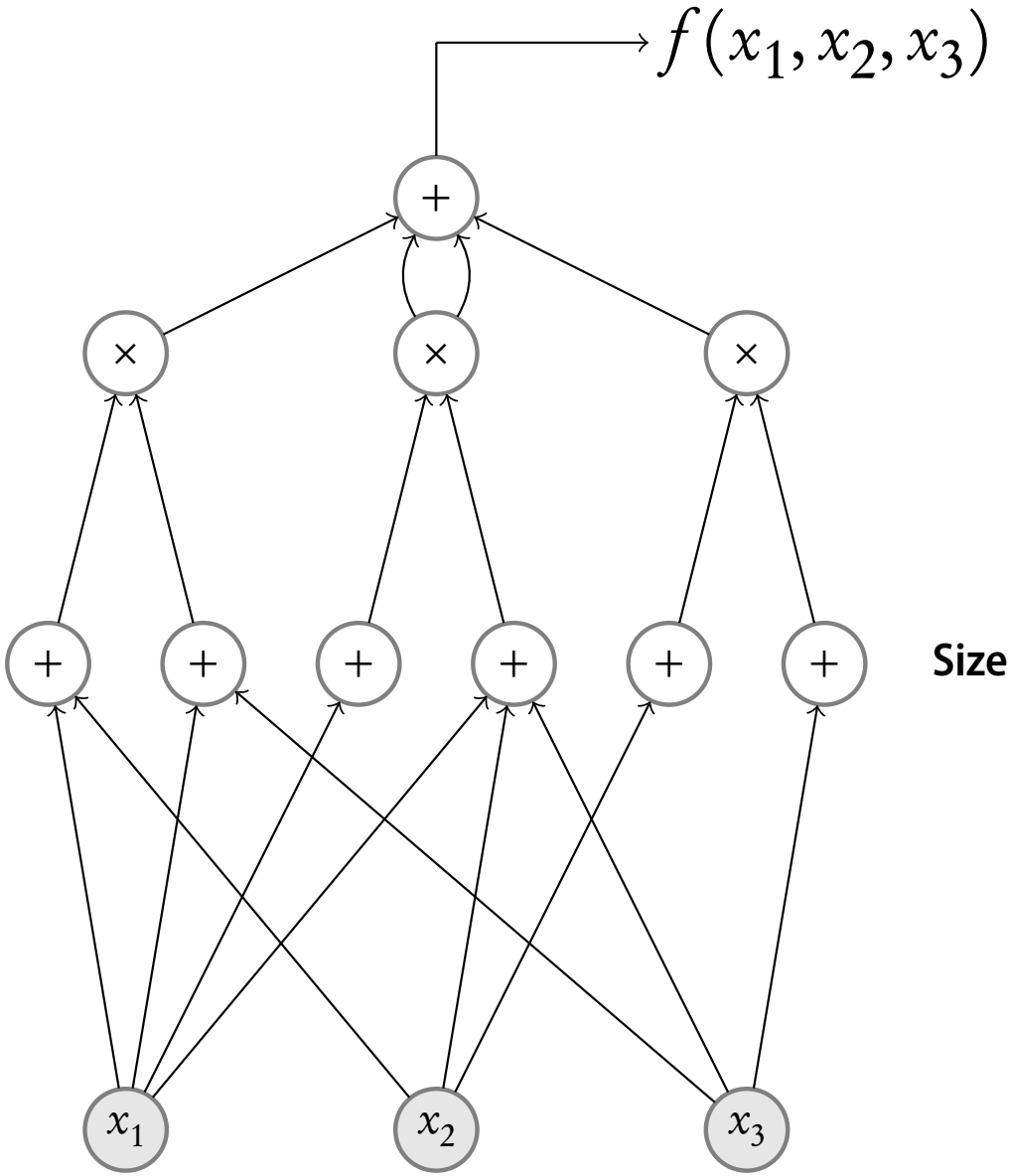


- Tree
- Leaves containing variables or constants

Arithmetic Circuits

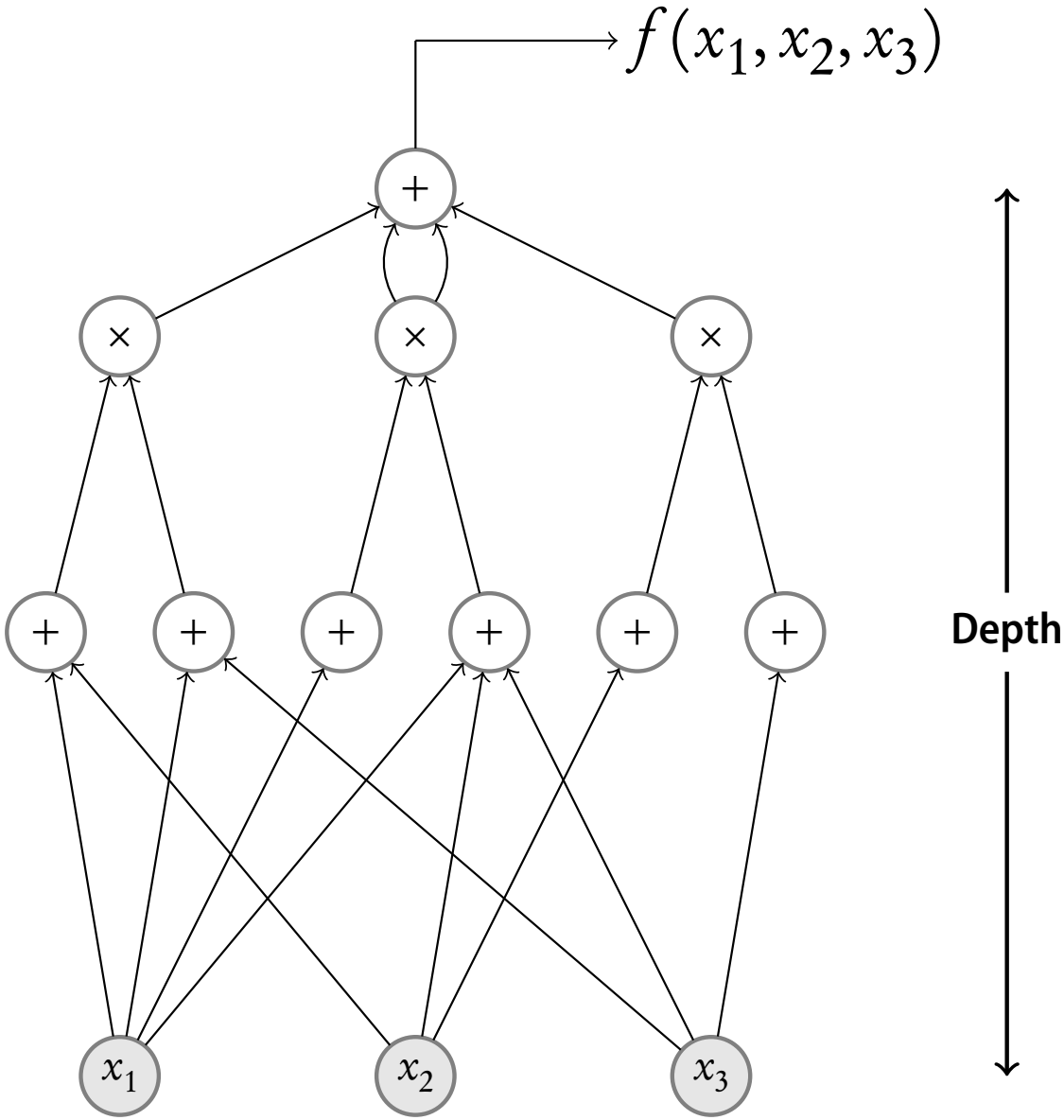


Arithmetic Circuits

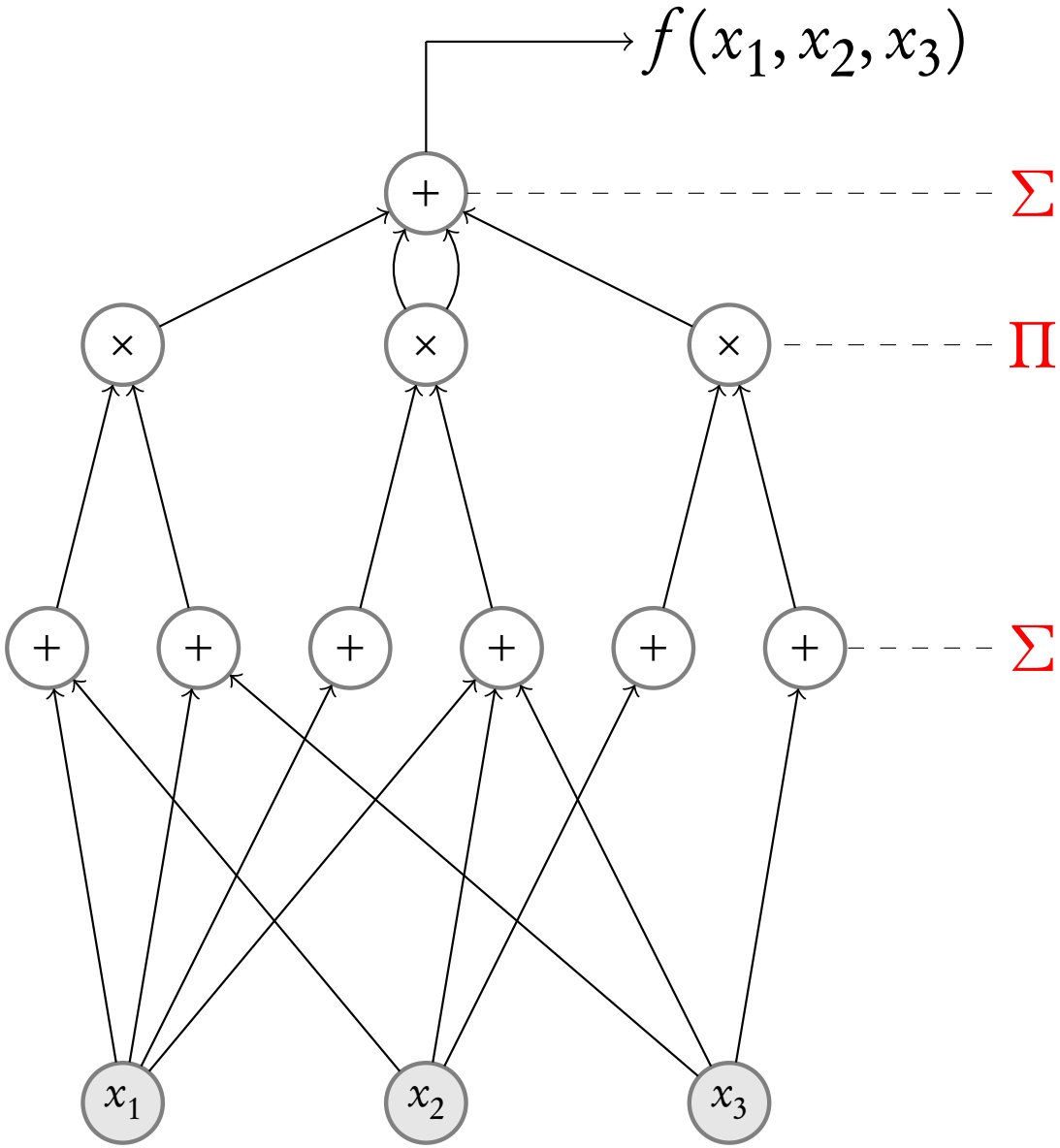


Size = number of gates

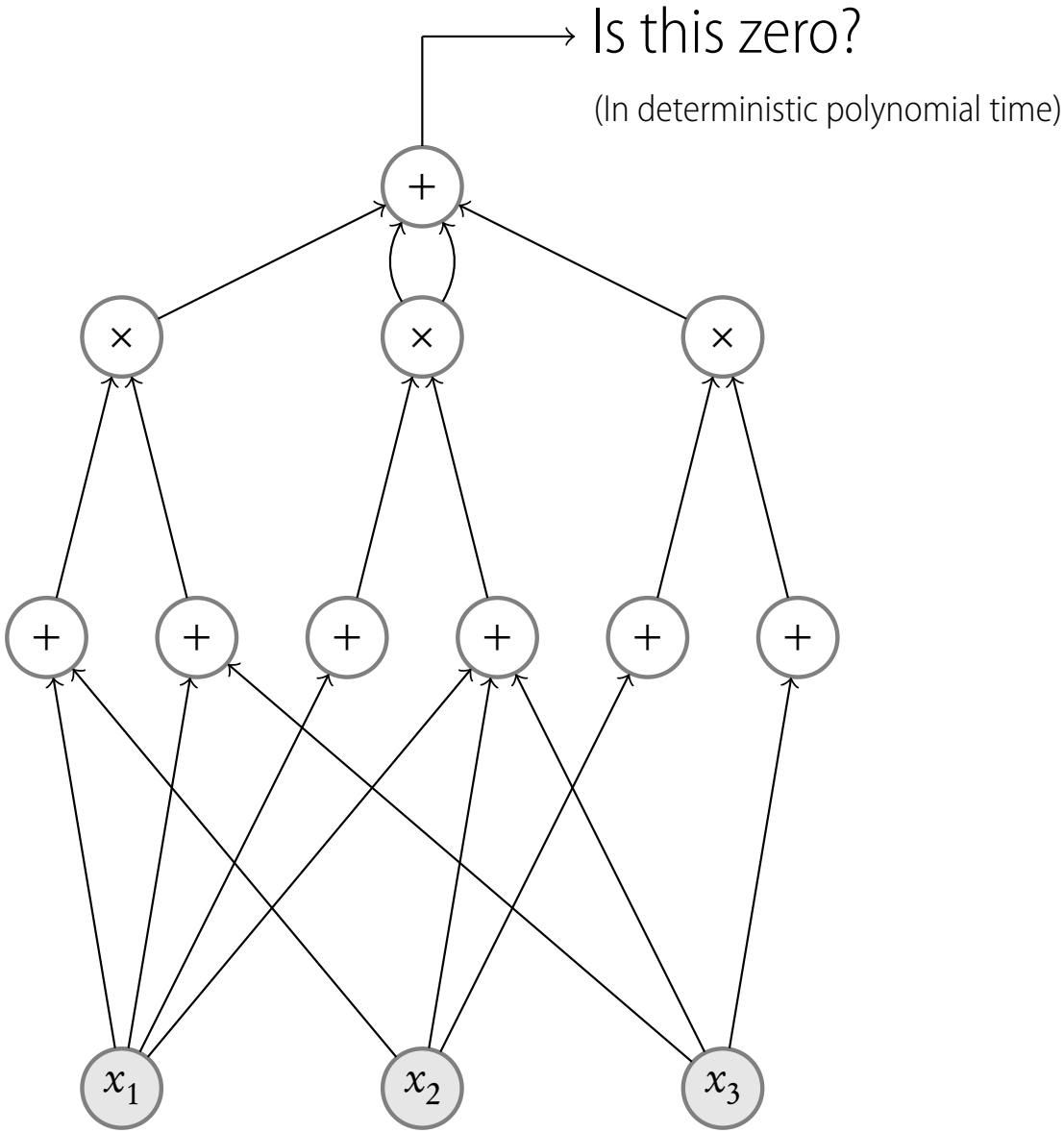
Arithmetic Circuits



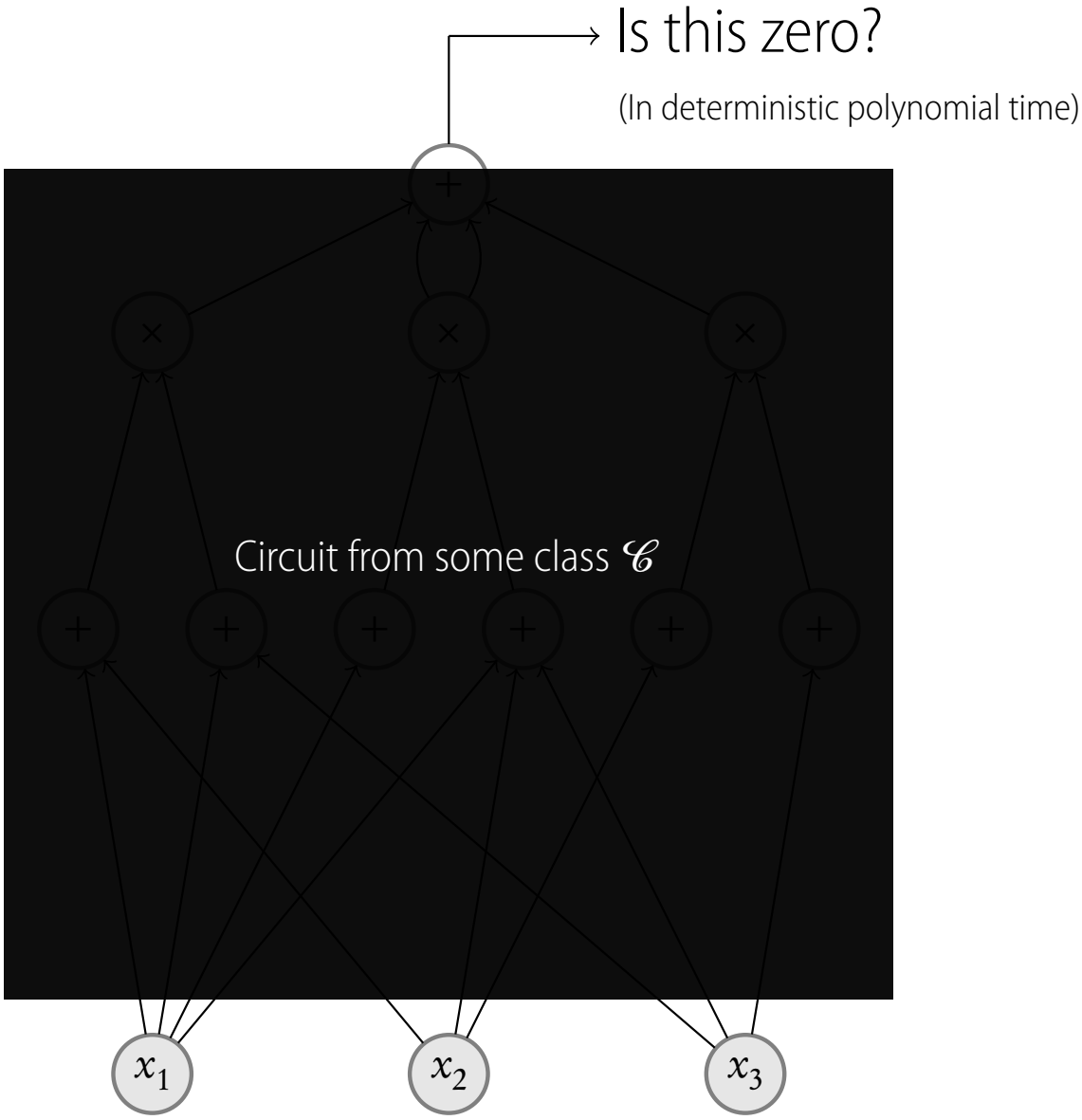
Arithmetic Circuits



Identity Testing of Arithmetic Circuits



Black-box Identity Testing of Arithmetic Circuits



Why do we care?

Part of many important results like $\mathbf{IP} = \mathbf{PSPACE}$, the $\mathbf{PCP}$ 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 $\mathbf{IP} = \mathbf{PSPACE}$, the $\mathbf{PCP}$ 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]*

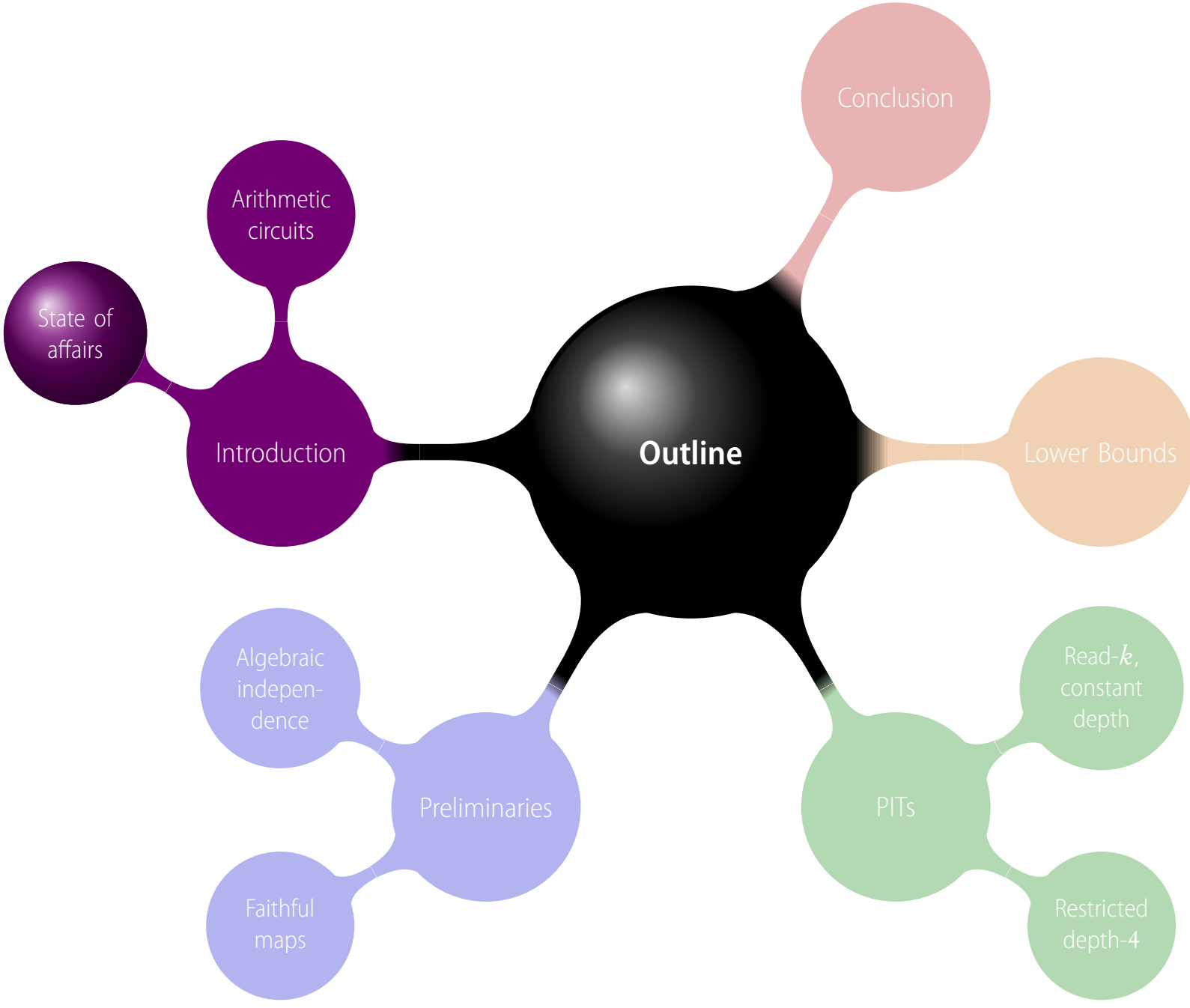
Why do we care?

Part of many important results like $\mathbf{IP} = \mathbf{PSPACE}$, the $\mathbf{PCP}$ 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
Introduction
State of affairs
Arithmetic circuits
Preliminaries
Algebraic independence
Faithful maps
Lower Bounds
PITs
Read-k, constant depth
Restricted depth-4
Conclusion

State of affairs

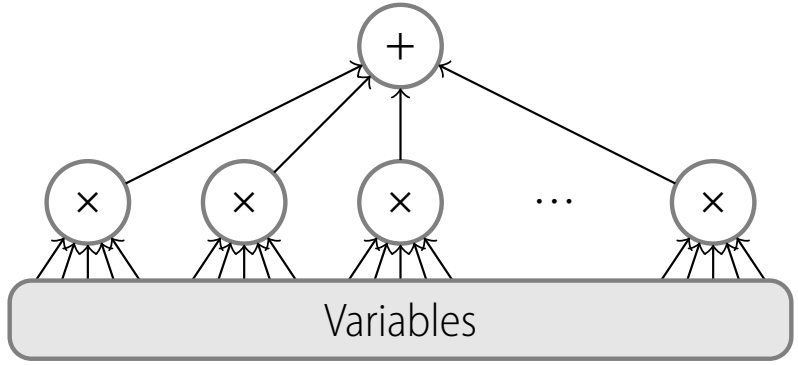
"If you can't solve a problem, then there is an easier problem you can solve: find it."

- George Pólya

Identity tests of restricted types of circuits:

- Formulae:
  1. Bounded depth formulae
  2. Bounded read formulae

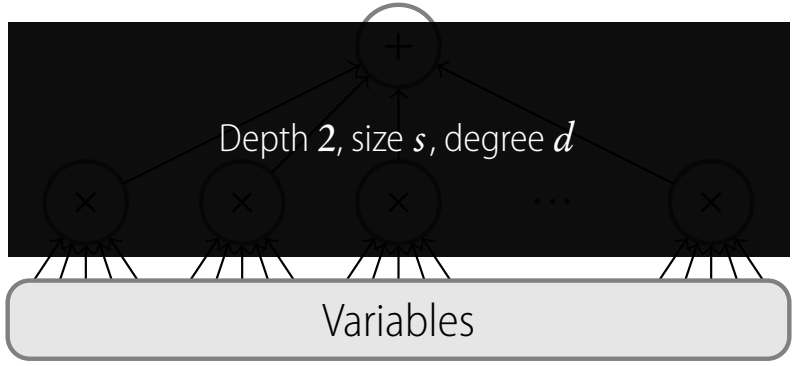
State of affairs for Depth 2 Circuits



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

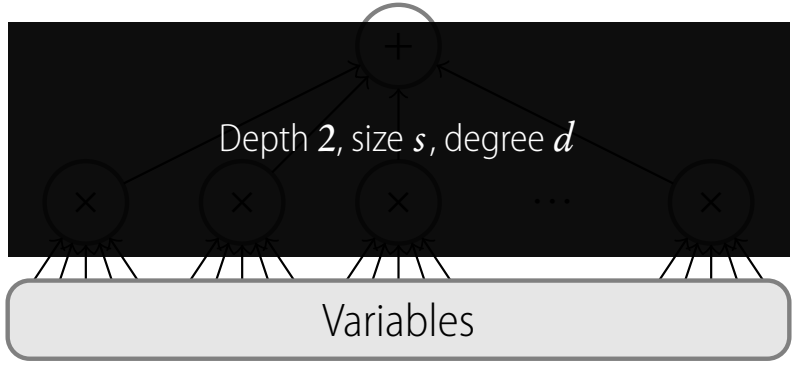
Depth **2** is easy (sparse polynomials)

State of affairs for Depth **2** *Circuits*



Black-box not-too-hard as well.

State of affairs for Depth 2 Circuits

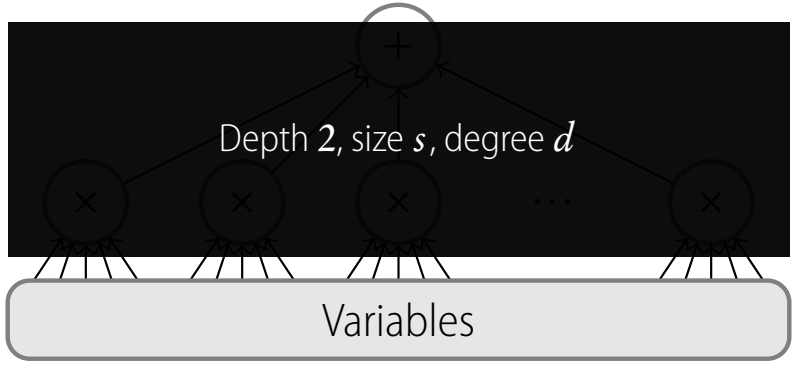


Black-box not-too-hard as well.

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

Works, but exponential degree

State of affairs for Depth 2 Circuits

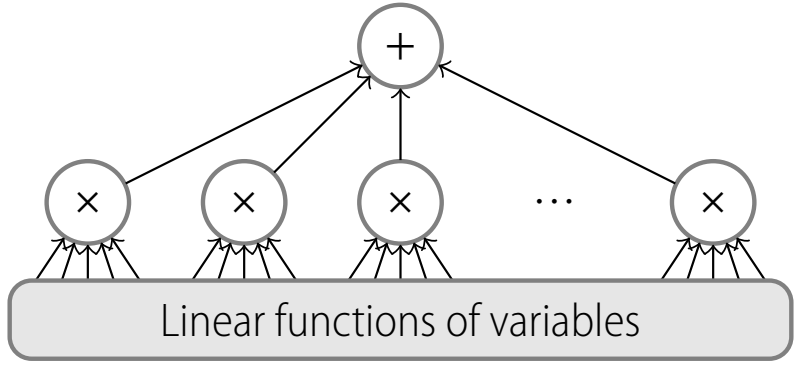


Black-box not-too-hard as well.

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

Works for most r's

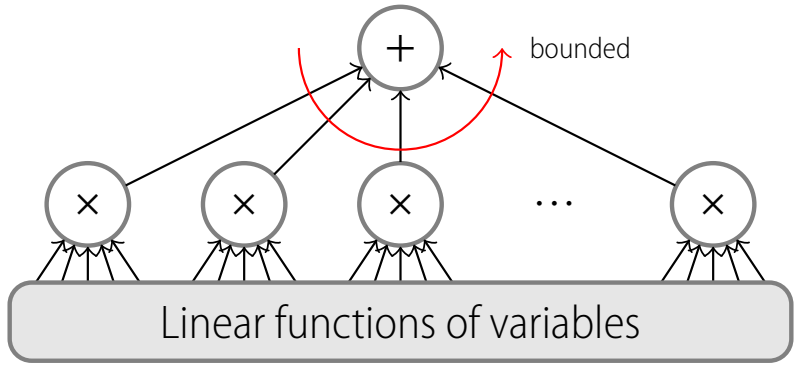
State of affairs for Depth 3 Circuits



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

PIT for even depth **3** circuits is open.

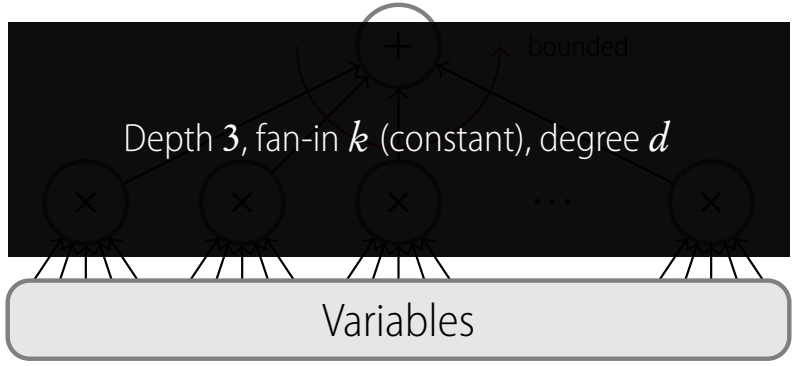
State of affairs for Depth 3 Circuits



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

[KayalSaxena07] : PIT in time $\mathbf{poly}(s^k)$

State of affairs for Depth 3 Circuits

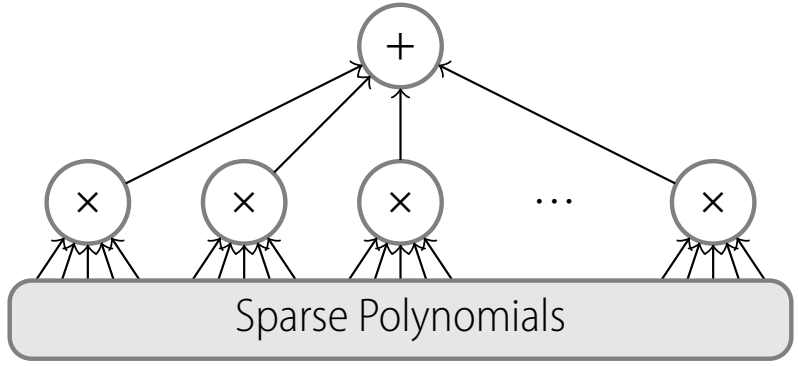


$$f \quad = \quad \sum_{i=1}^{k} \ell_{i1} \cdots \ell_{id}$$

[KayalSaxena07] : PIT in time $\mathbf{poly}(s^k)$

[SaxenaSeshadri11]: Black-box PIT in time $\mathbf{poly}(s^k)$

State of affairs for Depth 4 Circuits

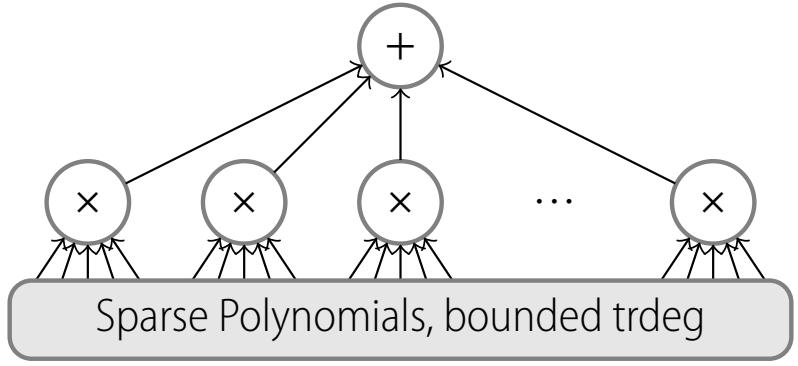


$$f \quad = \quad \sum_{i=1}^{\text{poly}} g_{i1} \cdots g_{id}$$

[AgrawalVinay08] : Black-box PIT for depth **4** implies $n^{O(\log n)}$ black-box PIT for any depth!

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

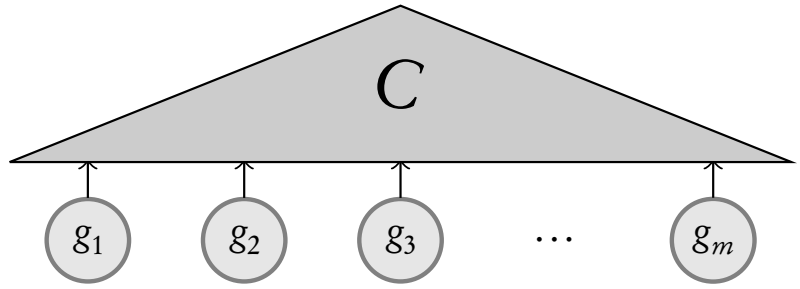
State of affairs for Depth **4** *Circuits*



$$f \quad = \quad \sum_{i=1}^{\text{poly}} g_{i1} \cdots g_{id} \quad \text{with } \mathbf{trdeg}\left\{ g_{ij} \right\} \leq k$$

[BeeckenMittmannSaxena11]: Polynomial time black-box PIT

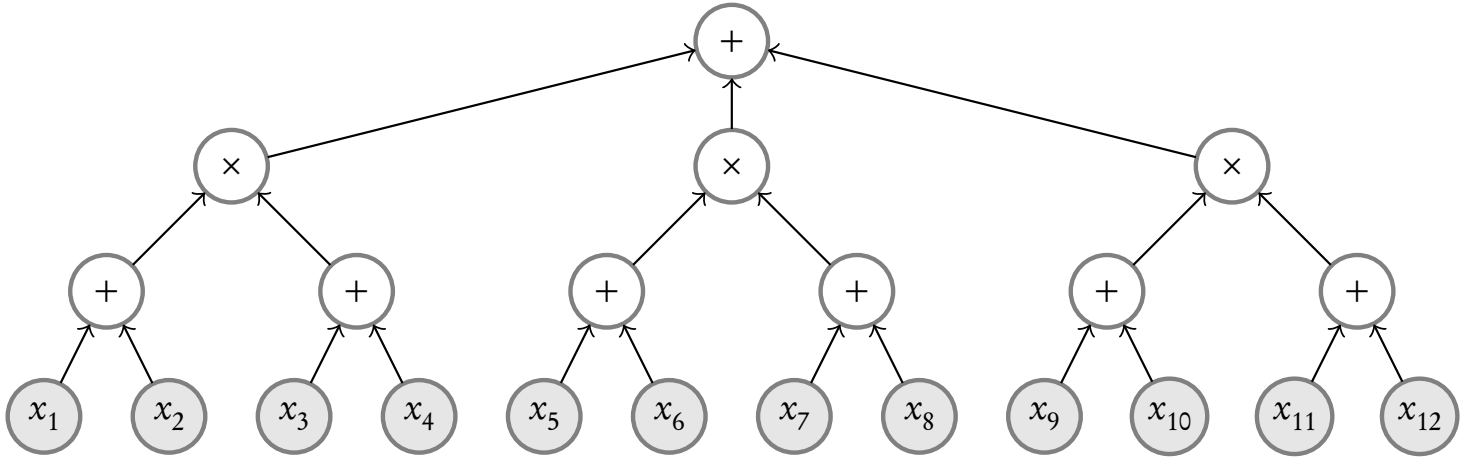
State of affairs for Depth **4** *Circuits*



$$f \quad = \quad C(g_1, \cdots, g_m) \quad \text{with } \mathbf{trdeg}\{g_i\} \leq k$$

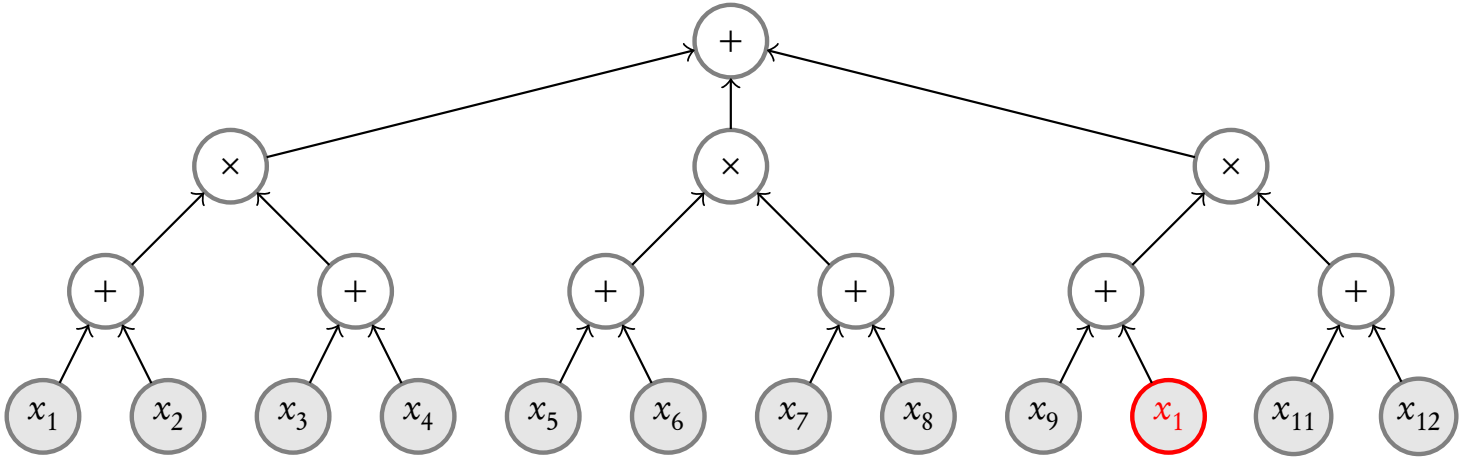
[BeeckenMittmannSaxena11]: Polynomial time black-box PIT

State of affairs for bounded read formulae



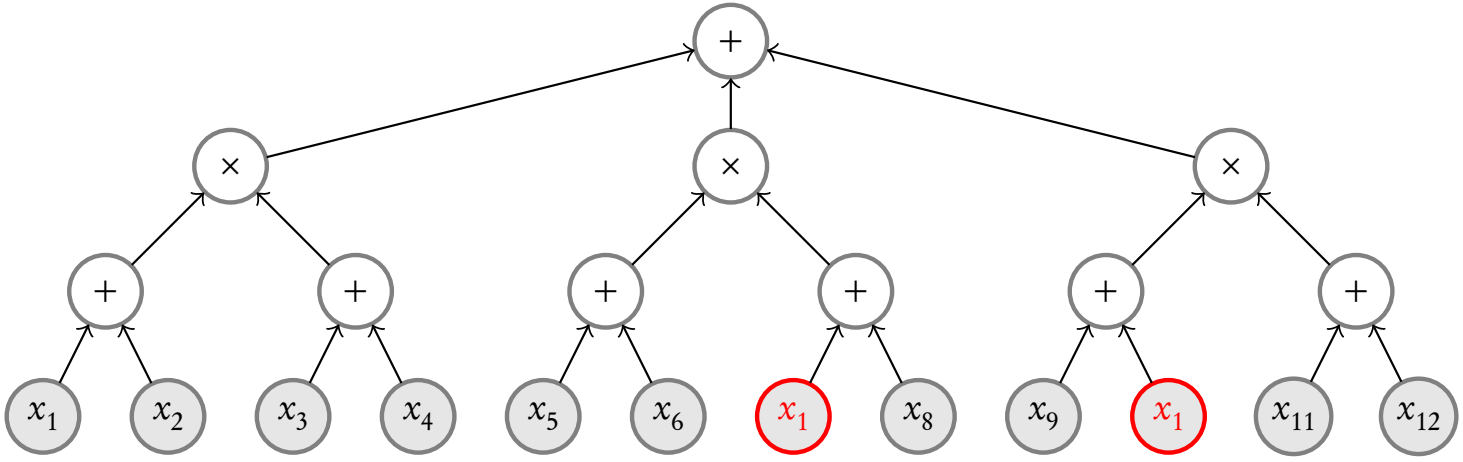
Read-**1** formula

State of affairs for bounded read formulae



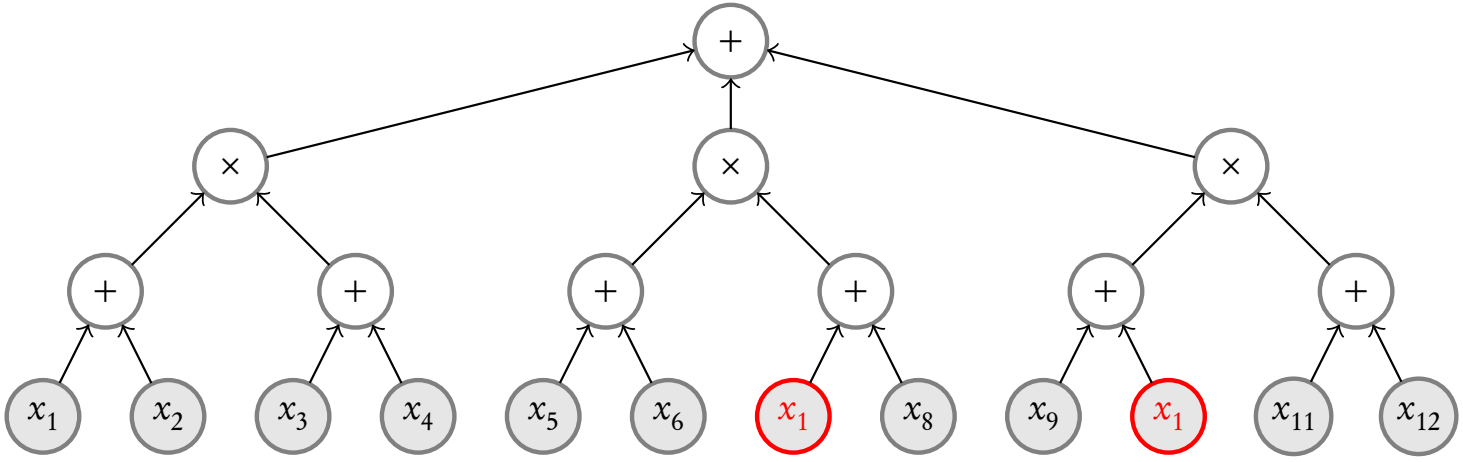
Read-**2** formula

State of affairs for bounded read formulae



Read-**3** formula

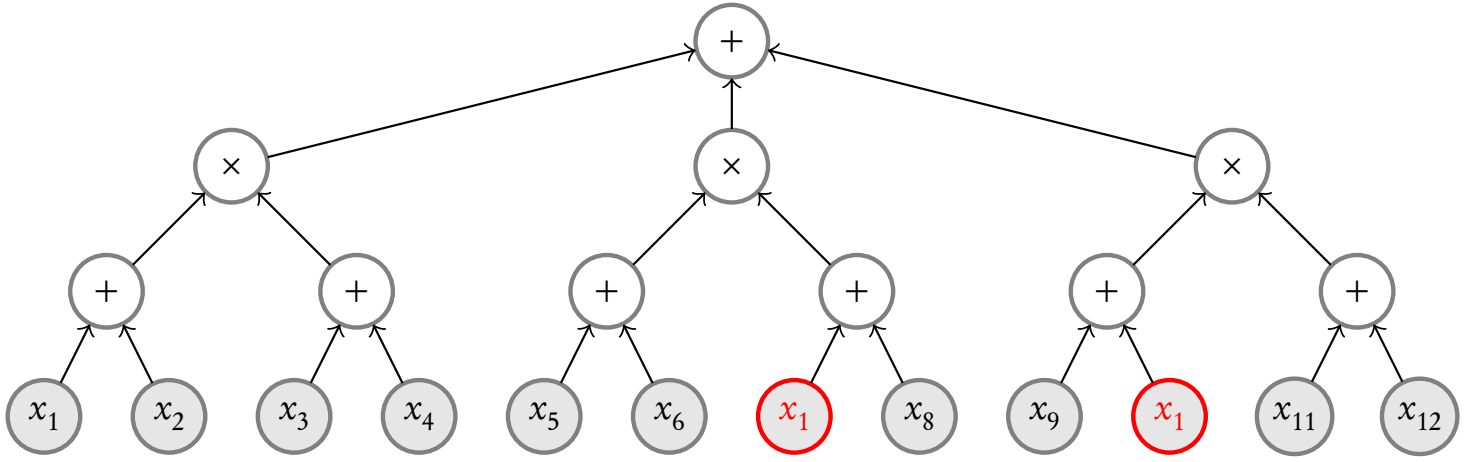
State of affairs for bounded read formulae



Read-k formula

Status of PIT:

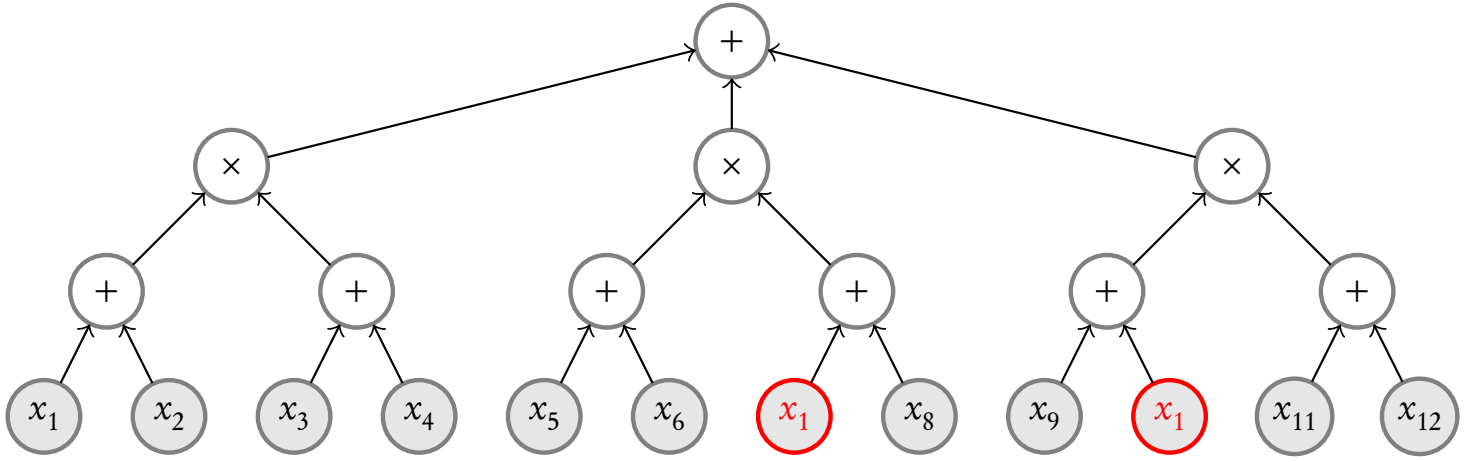
State of affairs for bounded read formulae



Read-k formula

Status of PIT: Open!

State of affairs for bounded read formulae



Read-k multilinear formula

Status of PIT:

- [SarafVolkovich11]: Polytime black-box PIT for depth-4 multilinear read-k.
- [Anderson-vanMelkebeek-Volkovich11]: Polytime black-box PIT for constant depth, multilinear, read-k formulae.
  Quasi-poly black-box PIT for arbitrary depth, multilinear read-k formulae, and polynomial time non-blackbox PIT.

Summary of results

Model	**Best known PIT**	**Idea**
fan-in k, depth-3	s^k black-box	CRT over local rings
depth-4, bounded $\mathbf{trdeg}$	Polytime black-box	Jacobian
multilinear depth-4 read-k	s^{k^3} black-box	sparsity bounds
multilinear read-k	Quasi-poly black-box	shattering, fragmentation under partial derivatives

Summary of results

Model	**Best known PIT**	**Idea**
$T_1 + \cdots + T_k \stackrel{?}{=} 0$	s^k black-box	CRT over local rings
depth-4, bounded $\mathbf{trdeg}$	Polytime black-box	Jacobian
multilinear depth-4 read-k	s^{k^3} black-box	sparsity bounds
multilinear read-k	Quasi-poly black-box	shattering, fragmentation under partial derivatives

Summary of our results

Model*	**Best known PIT**	**Idea**
$C(T_1, \cdots, T_m) \stackrel{?}{=} 0$ $\mathrm{trdeg}\{T_1, \cdots, T_m\} \leq k$	s^k black-box	CRT over local rings
depth-4, bounded $\mathbf{trdeg}$	Polytime black-box	Jacobian
multilinear depth-4 read-k	s^{k^3} black-box	sparsity bounds
multilinear read-k	Quasi-poly black-box	shattering, fragmentation under partial derivatives

Summary of our results

Model*	**Best known PIT**	**Idea**
$C(T_1, \cdots, T_m) \stackrel{?}{=} 0$ $\mathrm{trdeg}\{T_1, \cdots, T_m\} \leq k$	s^k black-box	CRT over local rings
depth-4, bounded $\mathbf{trdeg}$	Polytime black-box	Jacobian
~~multilinear~~ depth-4 read-k	s^{k^2} black-box	sparsity bounds
multilinear read-k	Quasi-poly black-box	shattering, fragmentation under partial derivatives

Summary of our results

Model*	**Best known PIT**	**Idea**
$C(T_1, \cdots, T_m) \stackrel{?}{=} 0$ $\mathrm{trdeg}\{T_1, \cdots, T_m\} \leq k$	s^k black-box	CRT over local rings
depth-4, bounded $\mathbf{trdeg}$	Polytime black-box	Jacobian
~~multilinear~~ depth-4 read-k	s^{k^2} black-box	sparsity bounds
~~multilinear~~ read-k constant depth	Polytime black-box	shattering, fragmentation under partial derivatives

Summary of our results

Model*	**Best known PIT**	**Idea**
$C(T_1, \cdots, T_m) \stackrel{?}{=} 0$ $\mathrm{trdeg}\{T_1, \cdots, T_m\} \leq k$	s^k black-box	Jacobian
depth-4, bounded $\mathbf{trdeg}$	Polytime black-box	Jacobian
~~multilinear~~ depth-4 read-k	s^{k^2} black-box	Jacobian
~~multilinear~~ read-k constant depth	Polytime black-box	Jacobian

Summary of our results

Model*	**Best known PIT**	**Idea**
$C(T_1, \cdots, T_m) \stackrel{?}{=} 0$ $\mathrm{trdeg}\{T_1, \cdots, T_m\} \leq k$	s^k black-box	Jacobian
depth-4, bounded $\mathbf{trdeg}$	Polytime black-box	Jacobian
~~multilinear~~ depth-4 read-k	s^{k^2} black-box	Jacobian
~~multilinear~~ read-k constant depth	Polytime black-box	Jacobian

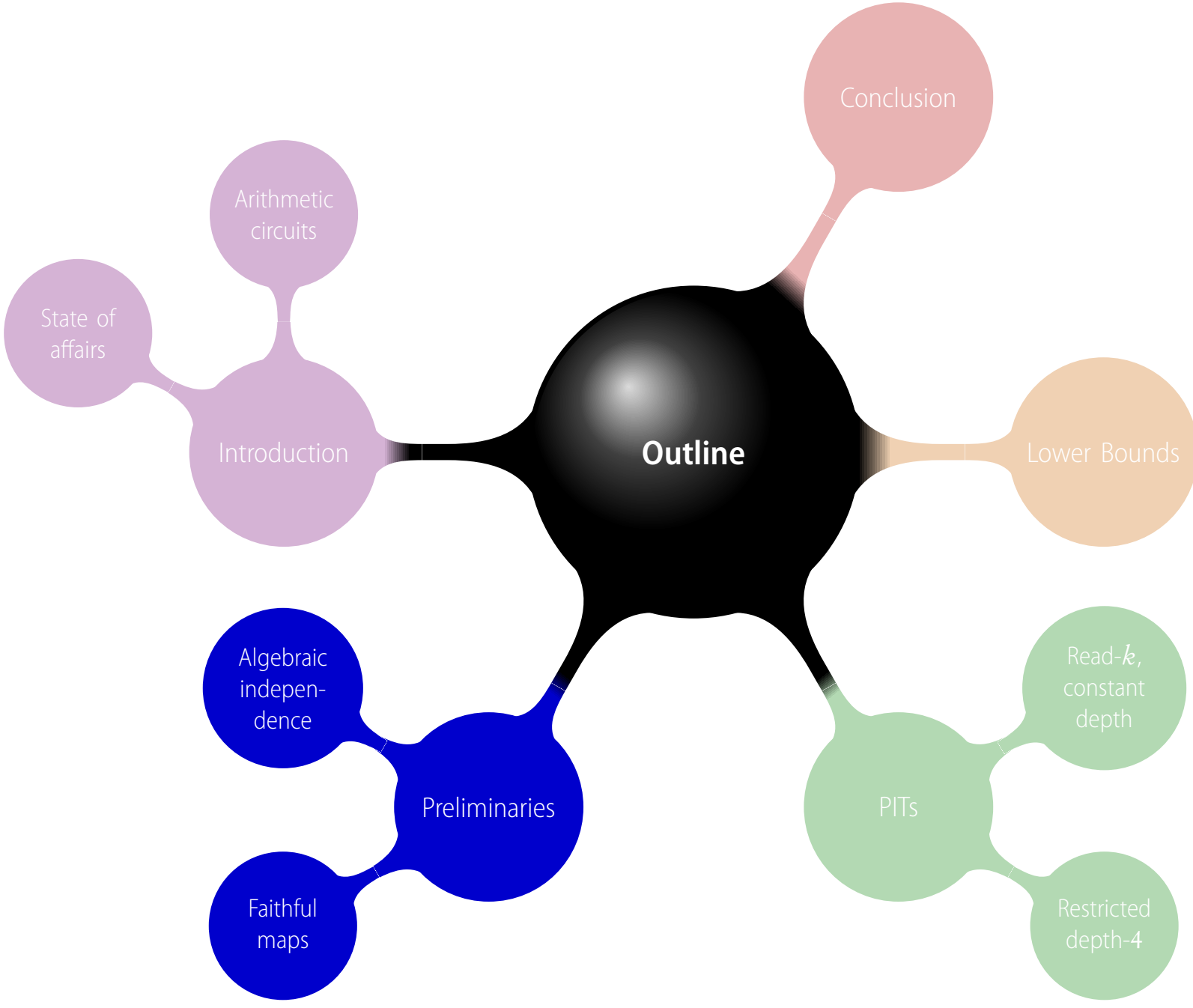
... and lower bounds

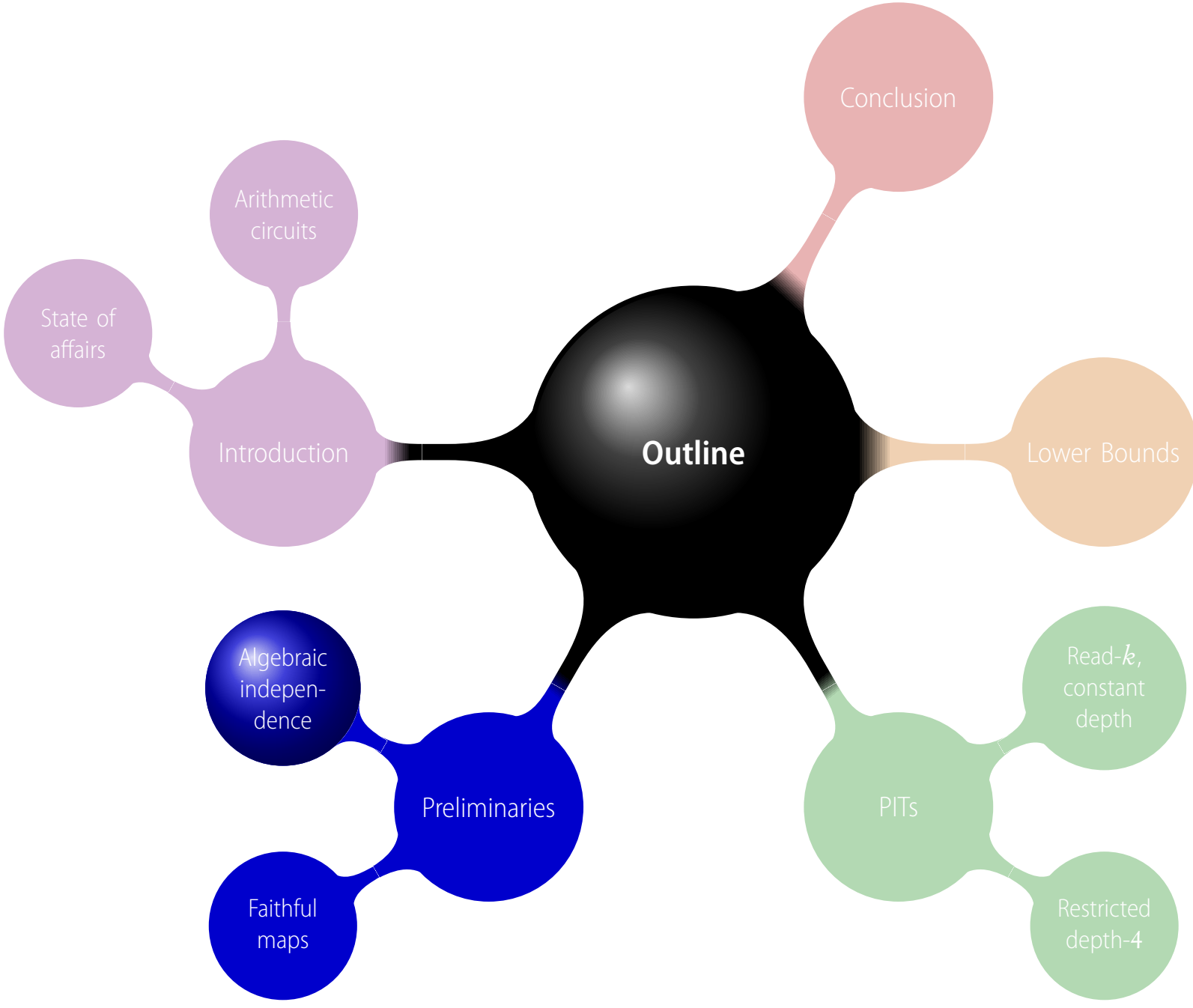
Summary of our results

Model*	**Best known PIT**	**Idea**
$C(T_1, \cdots, T_m) \stackrel{?}{=} 0$ $\mathrm{trdeg}\{T_1, \cdots, T_m\} \leq k$	s^k black-box	Jacobian
depth-4, bounded $\mathbf{trdeg}$	Polytime black-box	Jacobian
~~multilinear~~ depth-4 read-k	s^{k^2} black-box	Jacobian
~~multilinear~~ read-k constant depth	Polytime black-box	Jacobian

... and lower bounds

*: $\mathrm{char}(\mathbb{F}) = 0$ or large


Outline
Introduction
State of affairs
Arithmetic circuits
Preliminaries
Algebraic indepen-dence
Faithful maps
Lower Bounds
PITs
Read-k, constant depth
Restricted depth-4
Conclusion


Outline
Introduction
Arithmetic circuits
State of affairs
Preliminaries
Algebraic indepen-dence
Faithful maps
Lower Bounds
PITs
Read-k, constant depth
Restricted depth-4
Conclusion

Algebraic independence

Definition

$\{f_1, \cdots, f_m\}$ are algebraically independent if there is no non-trivial polynomial relation between them. That is,

$$H(f_1, \cdots, f_m) = 0 \quad \Longleftrightarrow \quad H = 0$$

Algebraic independence

Definition

$\{f_1, \cdots, f_m\}$ are algebraically independent if there is no non-trivial polynomial relation between them. That is,

$$H(f_1, \cdots, f_m) = 0 \quad \Longleftrightarrow \quad H = 0$$

Definition

The transcendence degree (**trdeg**) of $\{f_1, \cdots, f_m\}$ is the size of the largest algebraically independent subset.

The Jacobian

$$\mathscr{J}_{x_1,\cdots,x_n}(f_1,\cdots,f_m)=\begin{bmatrix} \frac{\partial f_1}{\partial x_1} & \cdots & \frac{\partial f_1}{\partial x_n} \\ \vdots & \ddots & \vdots \\ \frac{\partial f_m}{\partial x_1} & \cdots & \frac{\partial f_m}{\partial x_n} \end{bmatrix}_{m\times n}$$

The Jacobian

$$\mathscr{J}_{x_1,\cdots,x_n}(f_1,\cdots,f_m) = \begin{bmatrix} \frac{\partial f_1}{\partial x_1} & \cdots & \frac{\partial f_1}{\partial x_n} \\ \vdots & \ddots & \vdots \\ \frac{\partial f_m}{\partial x_1} & \cdots & \frac{\partial f_m}{\partial x_n} \end{bmatrix}_{m \times n}$$

Theorem (Jacobi Criterion)

If $\mathrm{char}(\mathbb{F}) = 0$ *or "large enough",*

$$\mathrm{trdeg}\{f_1,\cdots,f_m\} \quad = \quad \mathrm{rank}(\mathscr{J}(f_1,\cdots,f_m))$$

The Jacobian

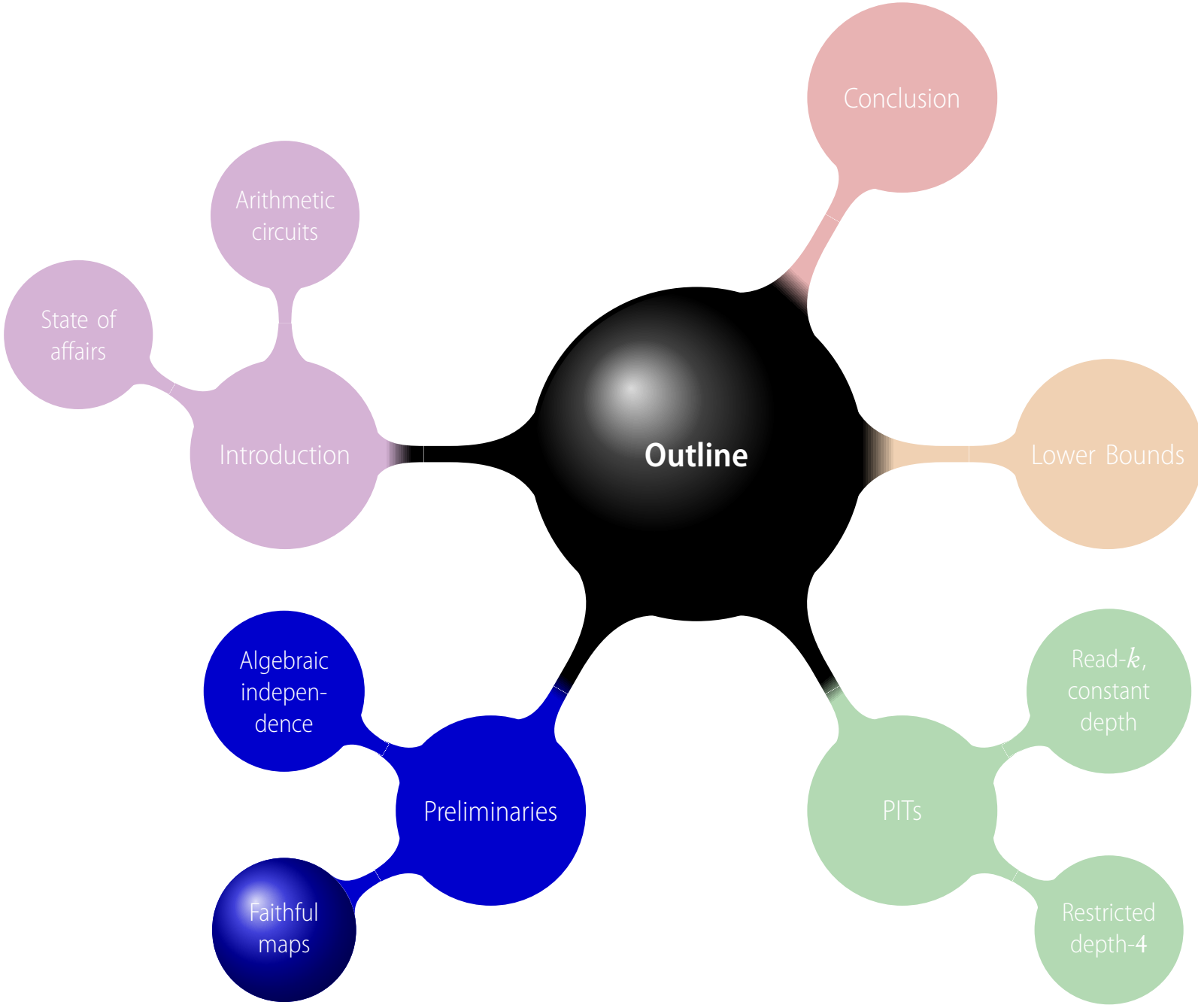
$$\mathscr{J}_{x_1,\cdots,x_n}(f_1,\cdots,f_m) = \begin{bmatrix} \frac{\partial f_1}{\partial x_1} & \cdots & \frac{\partial f_1}{\partial x_n} \\ \vdots & \ddots & \vdots \\ \frac{\partial f_m}{\partial x_1} & \cdots & \frac{\partial f_m}{\partial x_n} \end{bmatrix}_{m \times n}$$

Theorem (Jacobi Criterion)

If $\mathrm{char}(\mathbb{F}) = 0$ *or "large enough",*

$$\mathrm{trdeg}\{f_1,\cdots,f_m\} \quad = \quad \mathrm{rank}(\mathscr{J}(f_1,\cdots,f_m))$$

Aside: trdeg can be computed in randomized polynomial time.


Outline
Introduction
State of affairs
Arithmetic circuits
Preliminaries
Algebraic indepen-dence
Faithful maps
Lower Bounds
PITs
Read-k, constant depth
Restricted depth-4
Conclusion

Faithful maps

Definition

A map $\Phi : \mathbb{F}[x_1, \cdots, x_n] \to \mathbb{F}[y_1, \cdots, y_k]$ is faithful for $\{f_1, \cdots, f_m\}$ if

$$\text{trdeg}\{f_1, \cdots, f_m\} \quad = \quad \text{trdeg}\{\Phi(f_1), \cdots, \Phi(f_m)\}$$

Faithful maps

Definition

A map $\Phi : \mathbb{F}[x_1, \cdots, x_n] \to \mathbb{F}[y_1, \cdots, y_k]$ is faithful for $\{f_1, \cdots, f_m\}$ if

$$\operatorname{trdeg}\{f_1, \cdots, f_m\} \quad = \quad \operatorname{trdeg}\{\Phi(f_1), \cdots, \Phi(f_m)\}$$

Goal: Construct such a Φ where $k \approx \operatorname{trdeg}\{f_1, \cdots, f_m\}$.

Faithful maps

Definition

A map $\Phi : \mathbb{F}[x_1, \cdots, x_n] \to \mathbb{F}[y_1, \cdots, y_k]$ is faithful for $\{f_1, \cdots, f_m\}$ if

$$\operatorname{trdeg}\{f_1, \cdots, f_m\} \quad = \quad \operatorname{trdeg}\{\Phi(f_1), \cdots, \Phi(f_m)\}$$

Goal: Construct such a Φ where $k \approx \operatorname{trdeg}\{f_1, \cdots, f_m\}$.

... but what's this got to do with PIT?

Faithful maps preserve identities

Theorem (Beecken-Mittmann-Saxena)

If $\Phi : \mathbb{F}[x_1, \cdots, x_n] \to \mathbb{F}[y_1, \cdots, y_k]$ *is faithful for* $\{f_1, \cdots, f_m\}$*, then for any* C

$$C(f_1, \cdots, f_m) = 0 \quad \textit{if and only if} \quad C(\Phi(f_1), \cdots, \Phi(f_m)) = 0$$

Faithful maps preserve identities

Theorem (Beecken-Mittmann-Saxena)

If $\Phi : \mathbb{F}[x_1, \cdots, x_n] \to \mathbb{F}[y_1, \cdots, y_k]$ *is faithful for* $\{f_1, \cdots, f_m\}$*, then for any* C

$$C(f_1, \cdots, f_m) = 0 \quad \textit{if and only if} \quad C(\Phi(f_1), \cdots, \Phi(f_m)) = 0$$

$$\in \qquad\qquad\qquad\qquad \in$$

$$\mathbb{F}[x_1, \cdots, x_n] \qquad\qquad \mathbb{F}[y_1, \cdots, y_k]$$

Faithful maps preserve identities

Theorem (Beecken-Mittmann-Saxena)

If $\Phi : \mathbb{F}[x_1, \cdots, x_n] \to \mathbb{F}[y_1, \cdots, y_k]$ *is faithful for* $\{f_1, \cdots, f_m\}$*, then for any* C

$$C(f_1, \cdots, f_m) = 0 \quad \textit{if and only if} \quad C(\Phi(f_1), \cdots, \Phi(f_m)) = 0$$

$$\in \qquad\qquad\qquad\qquad \in$$

$$\mathbb{F}[x_1, \cdots, x_n] \qquad\qquad \mathbb{F}[y_1, \cdots, y_k]$$

Lemma (Schwartz-Zippel)

Let $f(y_1, \cdots, y_k)$ *is a non-zero polynomial over a field* $\mathbb{F}$ *of degree* d*. Then, for any* $S \subseteq \mathbb{F}$*, it has at most* $d|S|^{k-1}$ *roots in* S^k*.*

Faithful maps preserve identities

Theorem (Beecken-Mittmann-Saxena)

If $\Phi : \mathbb{F}[x_1, \cdots, x_n] \to \mathbb{F}[y_1, \cdots, y_k]$ *is faithful for* $\{f_1, \cdots, f_m\}$*, then for any* C

$$C(f_1, \cdots, f_m) = 0 \quad \textit{if and only if} \quad C(\Phi(f_1), \cdots, \Phi(f_m)) = 0$$

$$\in \qquad\qquad\qquad\qquad \in$$

$$\mathbb{F}[x_1, \cdots, x_n] \qquad\qquad \mathbb{F}[y_1, \cdots, y_k]$$

Lemma (Schwartz-Zippel)

Let $f(y_1, \cdots, y_k)$ *is a non-zero polynomial over a field* $\mathbb{F}$ *of degree* d*. Then, for any* $S \subseteq \mathbb{F}$*, it has at most* $d|S|^{k-1}$ *roots in* S^k*.*

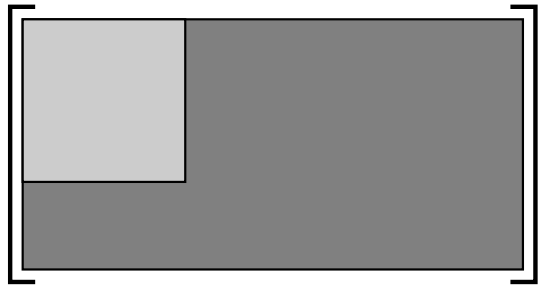
Hence, if we can construct Φ with $k = O(1)$, we are done!

Recipe for constructing faithful maps

$$\mathscr{J}(f_1,\cdots,f_m)=$$

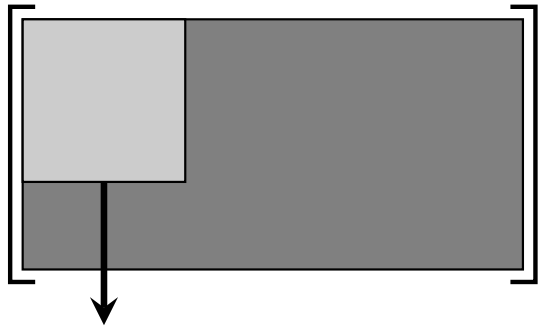
Recipe for constructing faithful maps

$$\mathscr{J}(f_1,\cdots,f_m)=$$



Recipe for constructing faithful maps

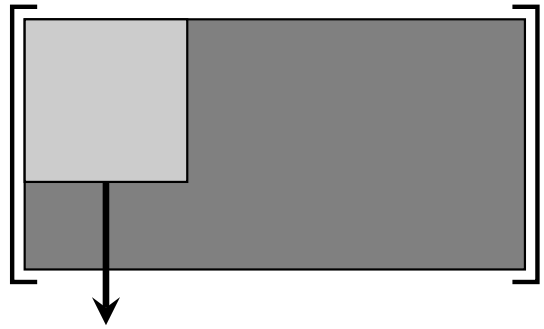
$$\mathcal{J}(f_1,\cdots,f_m)=$$



$$J=\begin{vmatrix} \partial_{x_1} f_1 & \cdots & \partial_{x_k} f_1 \\ \vdots & \ddots & \vdots \\ \partial_{x_1} f_k & \cdots & \partial_{x_k} f_k \end{vmatrix}$$

Recipe for constructing faithful maps

$$\mathcal{J}(f_1, \cdots, f_m) =$$



$$J = \begin{vmatrix} \partial_{x_1} f_1 & \cdots & \partial_{x_k} f_1 \\ \vdots & \ddots & \vdots \\ \partial_{x_1} f_k & \cdots & \partial_{x_k} f_k \end{vmatrix} \longleftarrow \text{Preserve this determinant}$$

Lemma (Composition Lemma)

Let Ψ *be a map such that* $\Psi(J) \neq 0$. *Then the map* Φ *is faithful to* $\{f_1, \cdots, f_m\}$:

$$\Phi : x_i \quad \mapsto \quad \sum_{j=1}^{k} y_j t^{ij} \quad + \quad \Psi(x_i)$$

Proof of Composition Lemma

$$\begin{aligned}\frac{\partial \Phi(f)}{\partial y_1} &= \frac{\partial f(\overline{\Phi(x)})}{\partial y_1} \\ &= \sum_{i=1}^{n} \frac{\partial f}{\partial x_i}\left[\overline{\Phi(x)}\right] \cdot \frac{\partial \Phi(x_i)}{\partial y_1}\end{aligned}$$

Proof of Composition Lemma

$$\begin{bmatrix} \partial_{y_1}\Phi(f_1) & \cdots & \partial_{y_k}\Phi(f_1) \\ \vdots & \ddots & \vdots \\ \partial_{y_1}\Phi(f_m) & \cdots & \partial_{y_k}\Phi(f_m) \end{bmatrix} =$$

$$\Phi \circ \begin{bmatrix} \partial_{x_1} f_1 & \cdots & \partial_{x_n} f_1 \\ \vdots & \ddots & \vdots \\ \partial_{x_1} f_m & \cdots & \partial_{x_n} f_m \end{bmatrix} \cdot \begin{bmatrix} \partial_{y_1}\Phi(x_1) & \cdots & \partial_{y_k}\Phi(x_1) \\ \vdots & \ddots & \vdots \\ \partial_{y_1}\Phi(x_n) & \cdots & \partial_{y_k}\Phi(x_n) \end{bmatrix}$$

Proof of Composition Lemma

$$\begin{bmatrix} \partial_{y_1}\Phi(f_1) & \cdots & \partial_{y_k}\Phi(f_1) \\ \vdots & \ddots & \vdots \\ \partial_{y_1}\Phi(f_m) & \cdots & \partial_{y_k}\Phi(f_m) \end{bmatrix} =$$

$$\Phi \circ \begin{bmatrix} \partial_{x_1} f_1 & \cdots & \partial_{x_n} f_1 \\ \vdots & \ddots & \vdots \\ \partial_{x_1} f_m & \cdots & \partial_{x_n} f_m \end{bmatrix} \cdot \begin{bmatrix} \partial_{y_1}\Phi(x_1) & \cdots & \partial_{y_k}\Phi(x_1) \\ \vdots & \ddots & \vdots \\ \partial_{y_1}\Phi(x_n) & \cdots & \partial_{y_k}\Phi(x_n) \end{bmatrix}$$

$$\Phi : x_i \quad \mapsto \quad \sum_{j=1}^{k} y_j t^{ij} \quad + \Psi(x_i)$$

Proof of Composition Lemma

$$\begin{bmatrix} \partial_{y_1}\Phi(f_1) & \cdots & \partial_{y_k}\Phi(f_1) \\ \vdots & \ddots & \vdots \\ \partial_{y_1}\Phi(f_m) & \cdots & \partial_{y_k}\Phi(f_m) \end{bmatrix} =$$

$$\Phi \circ \begin{bmatrix} \partial_{x_1} f_1 & \cdots & \partial_{x_n} f_1 \\ \vdots & \ddots & \vdots \\ \partial_{x_1} f_m & \cdots & \partial_{x_n} f_m \end{bmatrix} \cdot \begin{bmatrix} t & t^2 & \cdots & t^k \\ \vdots & \vdots & \ddots & \vdots \\ t^n & t^{2n} & \cdots & t^{nk} \end{bmatrix}$$

$$\Phi : x_i \quad \mapsto \quad \sum_{j=1}^{k} y_j t^{ij} \quad + \Psi(x_i)$$

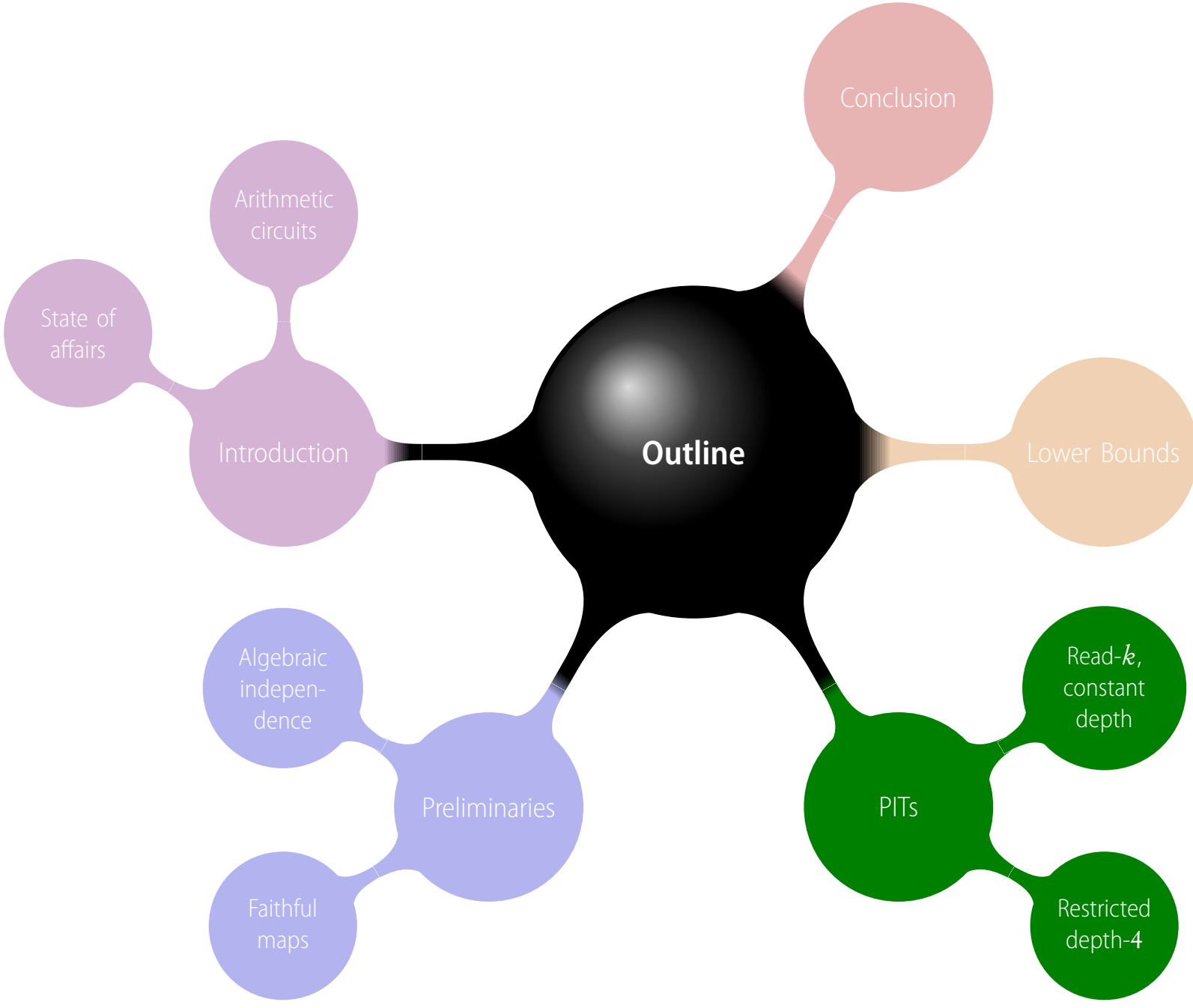
Proof of Composition Lemma

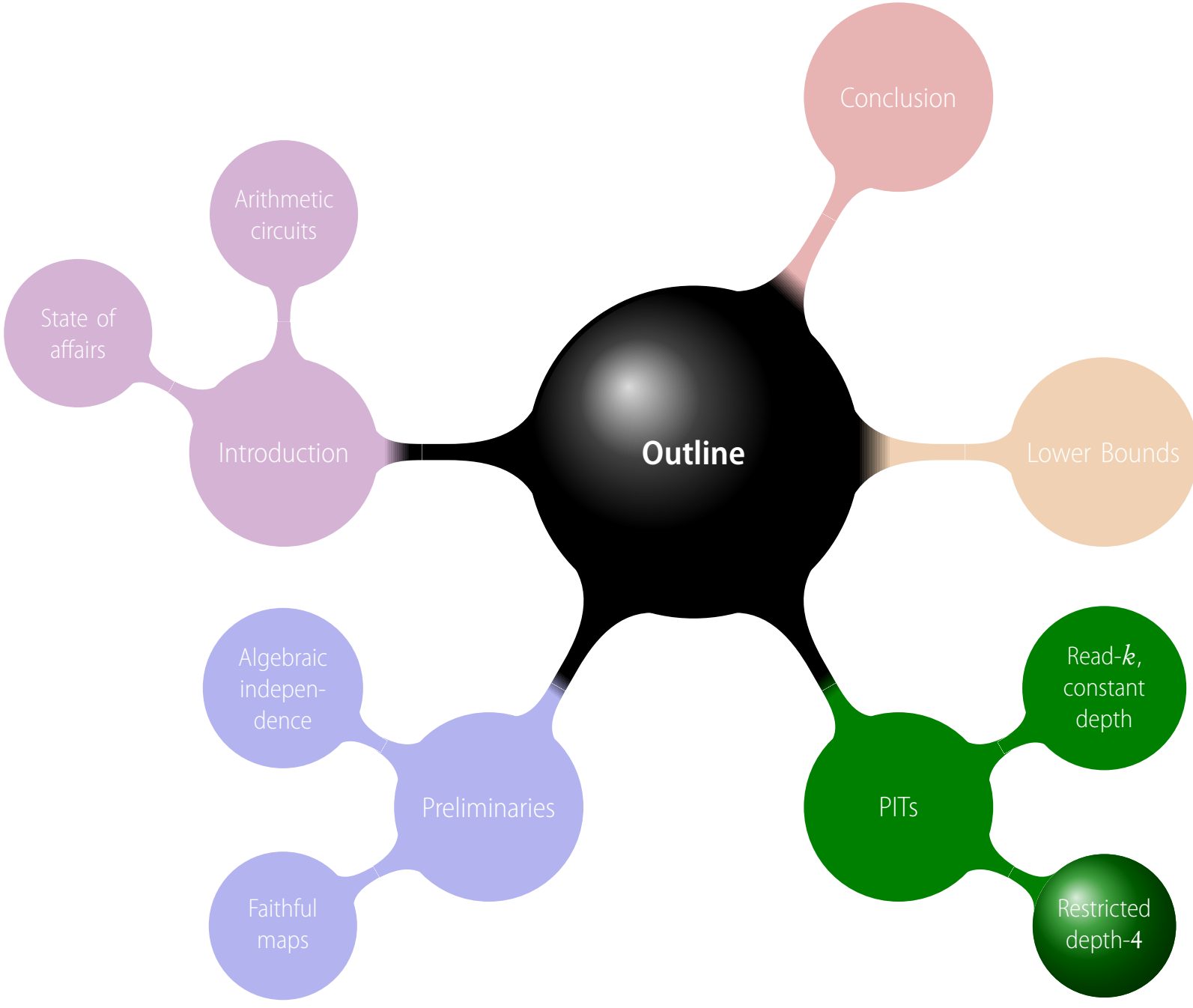
$$\begin{bmatrix} \partial_{y_1}\Phi(f_1) & \cdots & \partial_{y_k}\Phi(f_1) \\ \vdots & \ddots & \vdots \\ \partial_{y_1}\Phi(f_m) & \cdots & \partial_{y_k}\Phi(f_m) \end{bmatrix} =$$

$$\Phi \circ \begin{bmatrix} \partial_{x_1} f_1 & \cdots & \partial_{x_n} f_1 \\ \vdots & \ddots & \vdots \\ \partial_{x_1} f_m & \cdots & \partial_{x_n} f_m \end{bmatrix} \cdot \begin{bmatrix} t & t^2 & \cdots & t^k \\ \vdots & \vdots & \ddots & \vdots \\ t^n & t^{2n} & \cdots & t^{nk} \end{bmatrix}$$

$$\Phi : x_i \quad \mapsto \quad \sum_{j=1}^{k} y_j t^{ij} \quad + \Psi(x_i)$$

[GabizonRaz08]: Vandermonde maintains rank □


Outline
Introduction
State of affairs
Arithmetic circuits
Preliminaries
Algebraic independence
Faithful maps
Lower Bounds
PITs
Read-k, constant depth
Restricted depth-4
Conclusion


Outline
Introduction
State of affairs
Arithmetic circuits
Preliminaries
Algebraic independence
Faithful maps
Lower Bounds
PITs
Read-k, constant depth
Restricted depth-4
Conclusion

[BeeckenMittmannSaxena]'s PIT

Theorem

There is a black-box PIT for circuits of the form $C(f_1, \cdots, f_m)$ *where each* f_i *is "sparse" and* $\mathbf{trdeg}\{f_1, \cdots, f_m\} = k$.

Proof.

[BeeckenMittmannSaxena]'s PIT

Theorem

There is a black-box PIT for circuits of the form $C(f_1, \cdots, f_m)$ *where each* f_i *is "sparse" and* $\mathrm{trdeg}\{f_1, \cdots, f_m\} = k$.

Proof.

$$\mathcal{J}(f_1, \cdots, f_m) = \left[\begin{array}{c} \\ \\ \\ \end{array}\right]$$

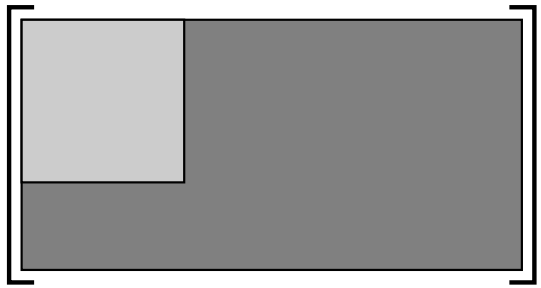
□

[BeeckenMittmannSaxena]'s PIT

Theorem

There is a black-box PIT for circuits of the form $C(f_1, \cdots, f_m)$ *where each* f_i *is "sparse" and* $\mathrm{trdeg}\{f_1, \cdots, f_m\} = k$.

Proof.

$\mathcal{J}(f_1, \cdots, f_m) =$ 

□

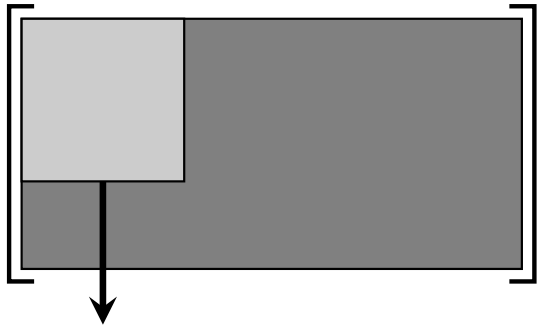
[BeeckenMittmannSaxena]'s PIT

Theorem

There is a black-box PIT for circuits of the form $C(f_1, \cdots, f_m)$ *where each* f_i *is "sparse" and* $\mathrm{trdeg}\{f_1, \cdots, f_m\} = k$.

Proof.

$$\mathcal{J}(f_1, \cdots, f_m) =$$



$$J = \begin{vmatrix} \partial_{x_1} f_1 & \cdots & \partial_{x_k} f_1 \\ \vdots & \ddots & \vdots \\ \partial_{x_1} f_k & \cdots & \partial_{x_k} f_k \end{vmatrix}$$

□

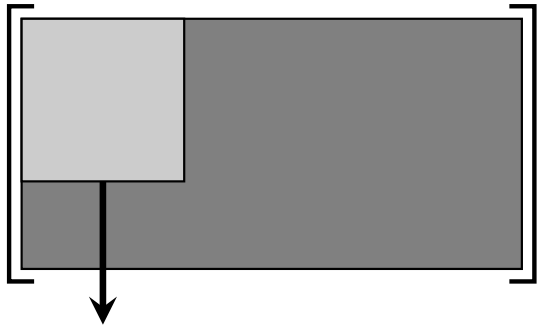
[BeeckenMittmannSaxena]'s PIT

Theorem

There is a black-box PIT for circuits of the form $C(f_1, \cdots, f_m)$ *where each* f_i *is "sparse" and* $\mathrm{trdeg}\{f_1, \cdots, f_m\} = k$.

Proof.

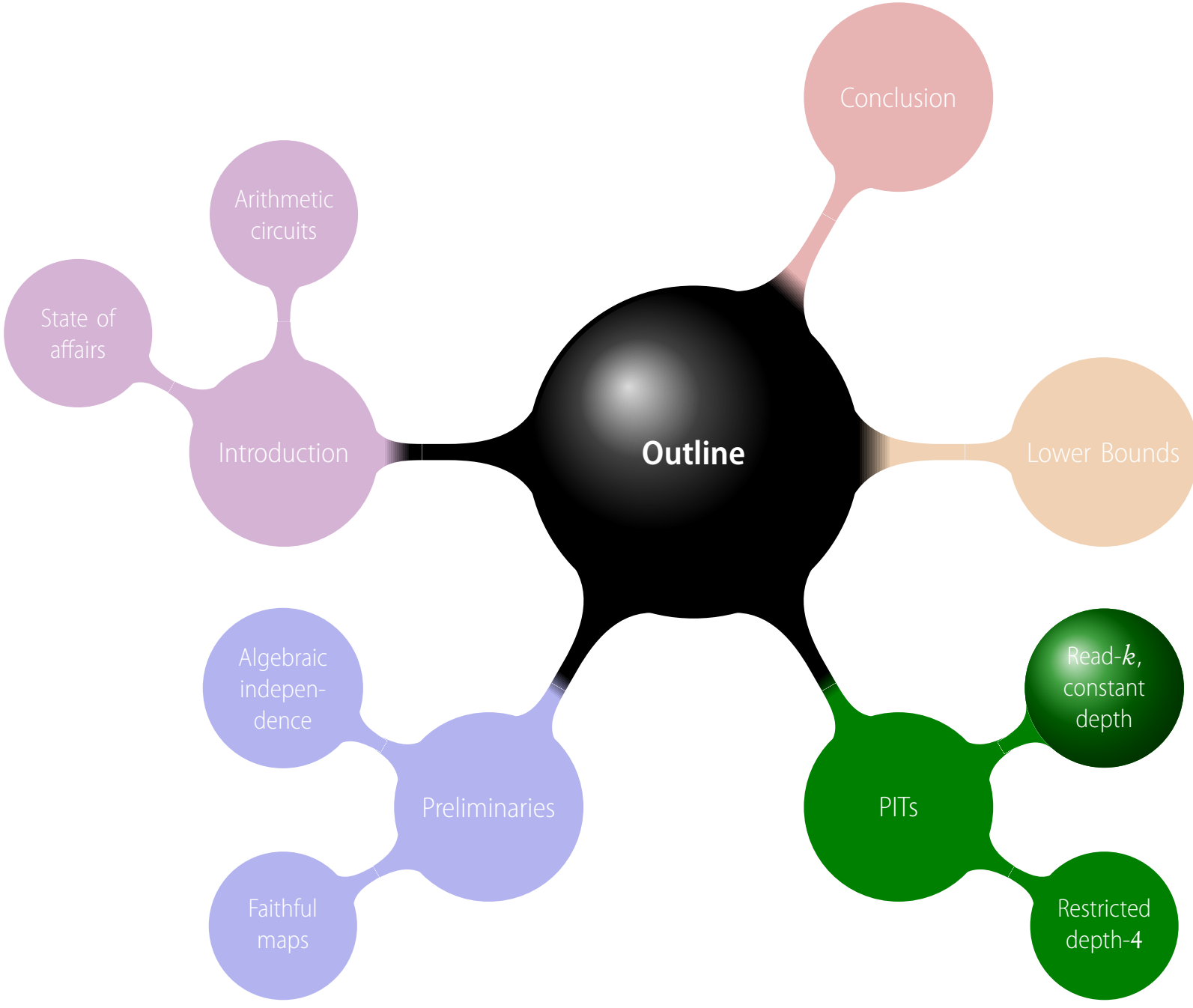
$$\mathcal{J}(f_1, \cdots, f_m) =$$



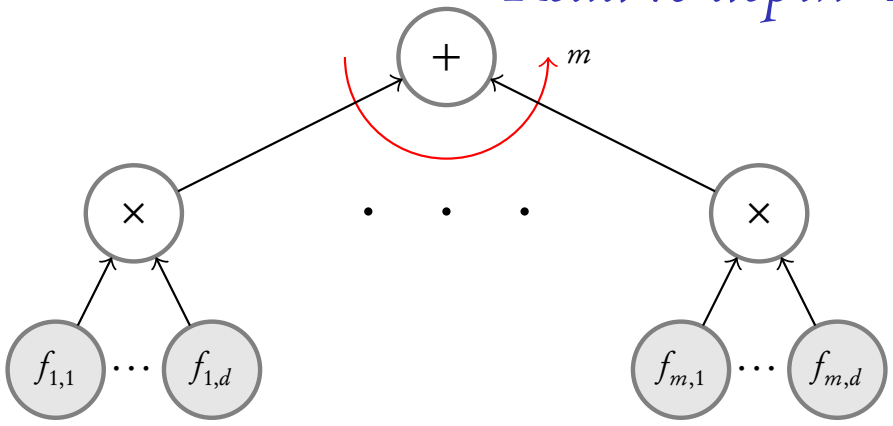
$$J = \begin{vmatrix} \partial_{x_1} f_1 & \cdots & \partial_{x_k} f_1 \\ \vdots & \ddots & \vdots \\ \partial_{x_1} f_k & \cdots & \partial_{x_k} f_k \end{vmatrix}$$

which is a sparse poly!

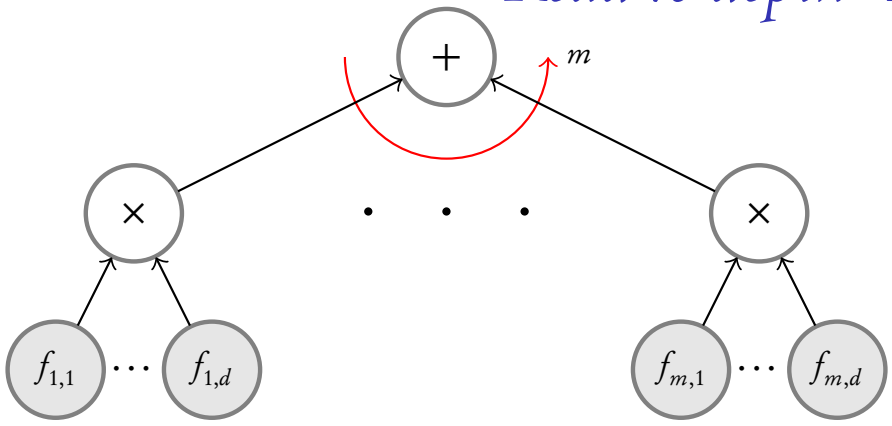
□


Outline
Introduction
State of affairs
Arithmetic circuits
Preliminaries
Algebraic independence
Faithful maps
Lower Bounds
PITs
Read-k, constant depth
Restricted depth-4
Conclusion

Read-k depth-4 formulae



Read-k depth-4 formulae



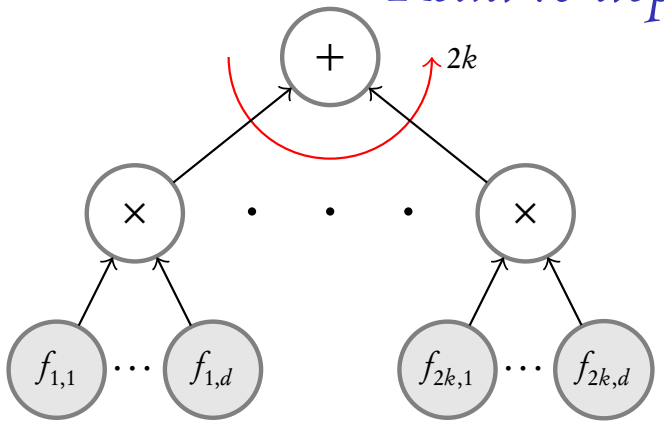
Observation

If $C(x_1, \cdots, x_n) \neq 0$, *then there exists an* i *such that*

$$C(x_1, \cdots, x_i + 1, \cdots, x_n) - C(x_1, \cdots, x_i, \cdots, x_n) \neq 0$$

In fact, any x_i that C non-trivially depends on.

Read-k depth-4 formulae



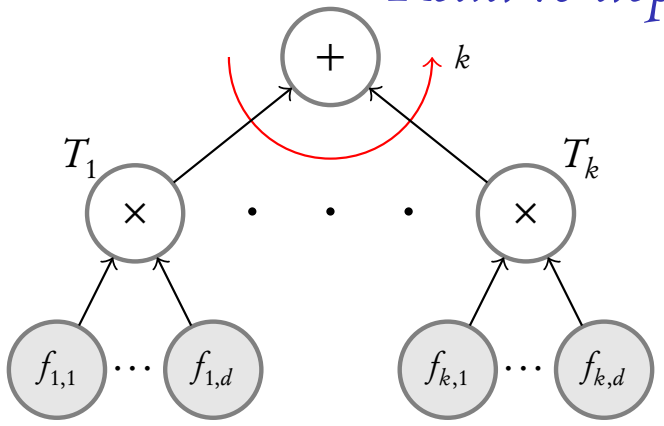
Observation

If $C(x_1, \cdots, x_n) \neq 0$, *then there exists an* i *such that*

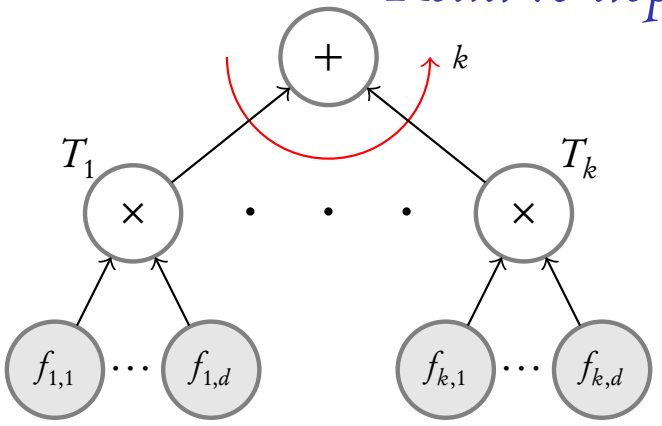
$$C(x_1, \cdots, x_i + 1, \cdots, x_n) - C(x_1, \cdots, x_i, \cdots, x_n) \neq 0$$

In fact, any x_i that C non-trivially depends on.

Read-k depth-4 formulae



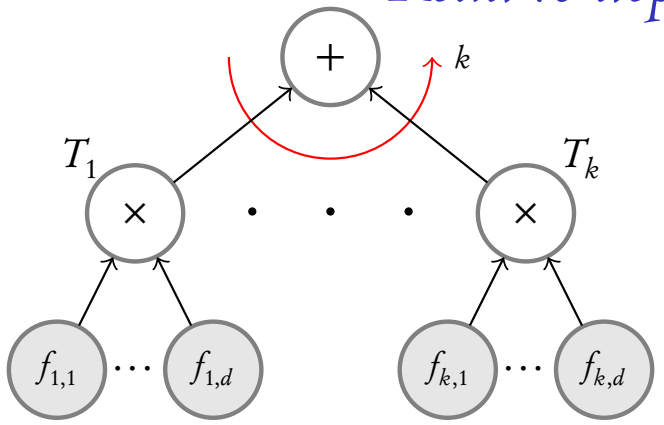
Read-k depth-4 formulae



$$\mathcal{J}(T_1,\cdots,T_k) = \left[\begin{array}{c} \\ \\ \\ \\ \\ \\ \\ \\ \\ \end{array}\right]$$

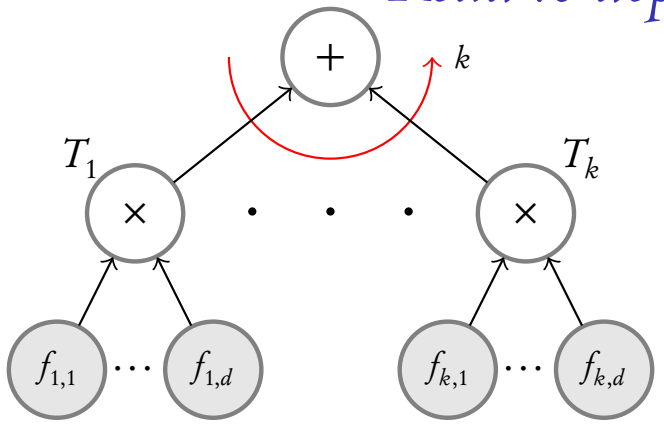
$$J = \begin{vmatrix} \partial_{x_1} T_1 & \cdots & \partial_{x_r} T_1 \\ \vdots & \ddots & \vdots \\ \partial_{x_r} T_r & \cdots & \partial_{x_r} T_r \end{vmatrix}$$

Read-k depth-4 formulae



$$J = \begin{vmatrix} \partial_{x_1} T_1 & \cdots & \partial_{x_r} T_1 \\ \vdots & \ddots & \vdots \\ \partial_{x_r} T_r & \cdots & \partial_{x_r} T_r \end{vmatrix}$$

Read-k depth-4 formulae

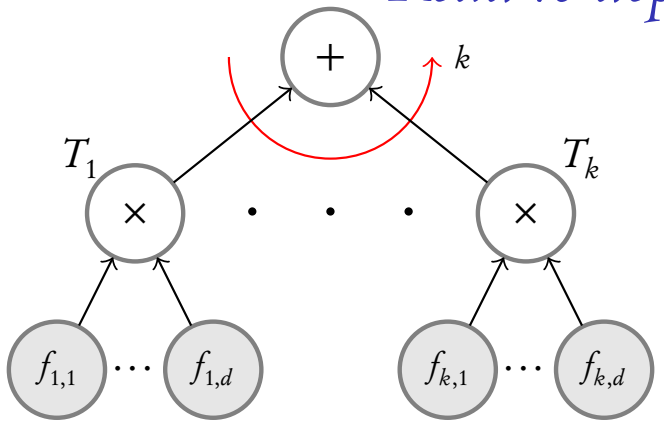


$$J = \begin{vmatrix} \partial_{x_1} T_1 & \cdots & \partial_{x_r} T_1 \\ \vdots & \ddots & \vdots \\ \partial_{x_r} T_r & \cdots & \partial_{x_r} T_r \end{vmatrix}$$

Observation

At most rk of the f_{ij}'s depend on $x_1, \cdots, x_r$.

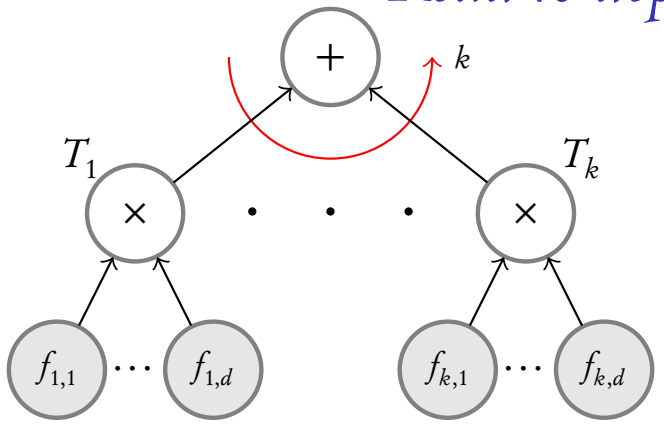
Read-k depth-4 formulae



$$J = \begin{vmatrix} \partial_{x_1} T_1 & \cdots & \partial_{x_r} T_1 \\ \vdots & \ddots & \vdots \\ \partial_{x_r} T_r & \cdots & \partial_{x_r} T_r \end{vmatrix} = \left(\prod f_{ij}\right) \cdot \begin{vmatrix} \partial_{x_1} T'_1 & \cdots & \partial_{x_r} T'_1 \\ \vdots & \ddots & \vdots \\ \partial_{x_r} T'_r & \cdots & \partial_{x_r} T'_r \end{vmatrix}$$

... a product of sparse polys!

Read-k depth-4 formulae

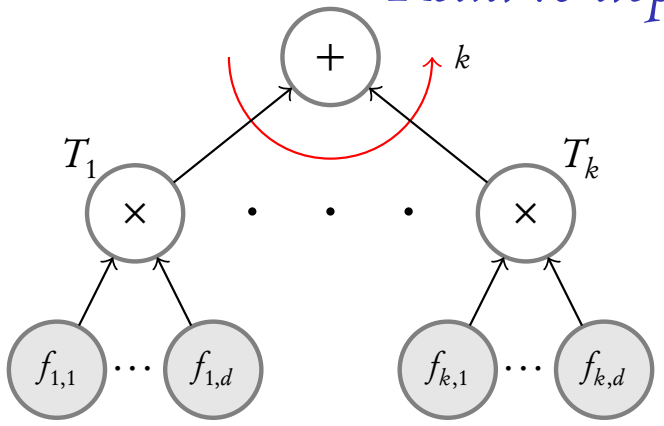


$$J = \begin{vmatrix} \partial_{x_1} T_1 & \cdots & \partial_{x_r} T_1 \\ \vdots & \ddots & \vdots \\ \partial_{x_r} T_r & \cdots & \partial_{x_r} T_r \end{vmatrix} = \left(\prod f_{ij}\right) \cdot \begin{vmatrix} \partial_{x_1} T_1' & \cdots & \partial_{x_r} T_1' \\ \vdots & \ddots & \vdots \\ \partial_{x_r} T_r' & \cdots & \partial_{x_r} T_r' \end{vmatrix}$$

... a product of sparse polys!

$$\Psi_r : x_i \mapsto u^{d^i \bmod r} \quad \text{preserves } J$$

Read-k depth-4 formulae



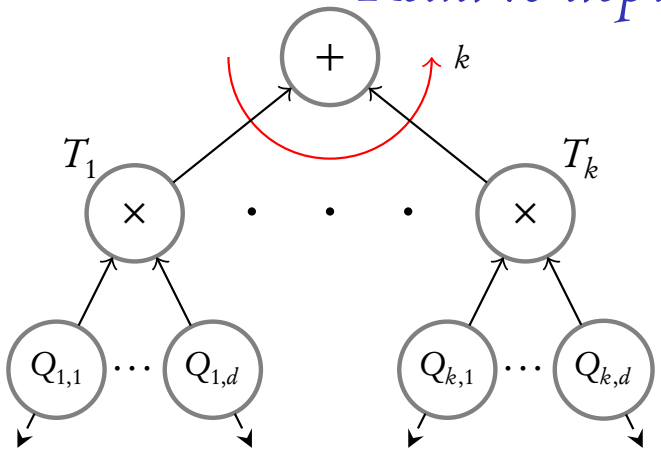
$$J = \begin{vmatrix} \partial_{x_1} T_1 & \cdots & \partial_{x_r} T_1 \\ \vdots & \ddots & \vdots \\ \partial_{x_r} T_r & \cdots & \partial_{x_r} T_r \end{vmatrix} = \left(\prod f_{ij}\right) \cdot \begin{vmatrix} \partial_{x_1} T'_1 & \cdots & \partial_{x_r} T'_1 \\ \vdots & \ddots & \vdots \\ \partial_{x_r} T'_r & \cdots & \partial_{x_r} T'_r \end{vmatrix}$$

... a product of sparse polys!

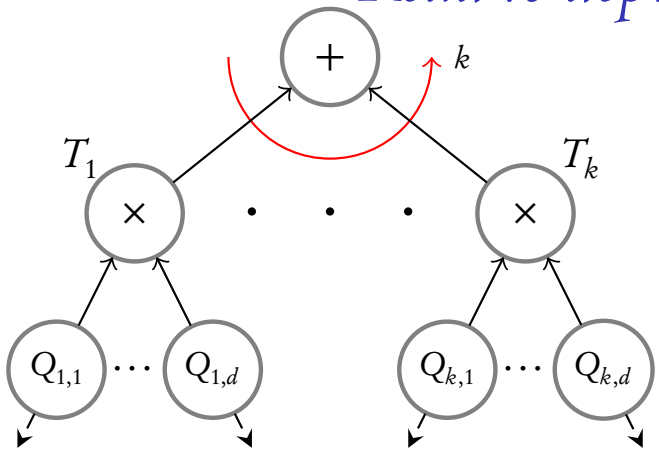
$\Psi_r : x_i \mapsto u^{d^i \bmod r}$ preserves J

$\Phi_r : x_i \mapsto \sum_{j=1}^{k} y_j t^{ij} + u^{d^i \bmod r}$ is a black-box PIT

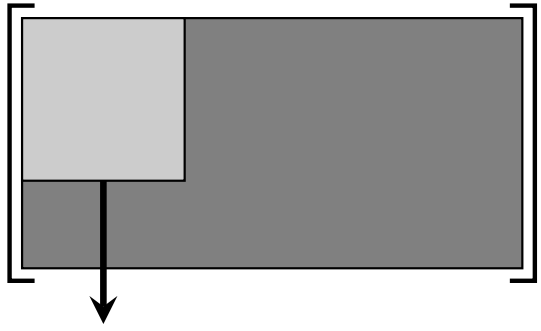
Read-k depth-D formulae



Read-k depth-D formulae

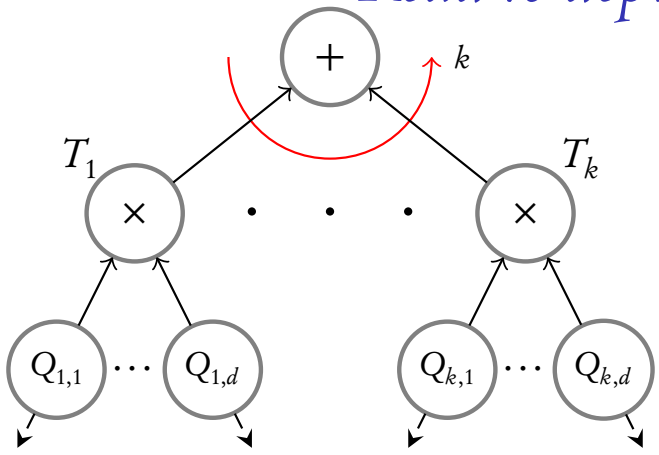


$$\mathscr{J}(T_1,\cdots,T_k)=$$



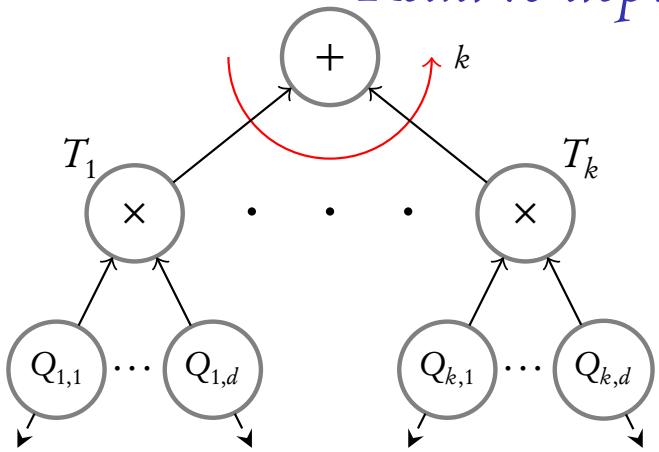
$$J \quad = \quad \begin{vmatrix} \partial_{x_1} T_1 & \cdots & \partial_{x_r} T_1 \\ \vdots & \ddots & \vdots \\ \partial_{x_r} T_r & \cdots & \partial_{x_r} T_r \end{vmatrix}$$

Read-k depth-D formulae



$$J = \begin{vmatrix} \partial_{x_1} T_1 & \cdots & \partial_{x_r} T_1 \\ \vdots & \ddots & \vdots \\ \partial_{x_r} T_r & \cdots & \partial_{x_r} T_r \end{vmatrix}$$

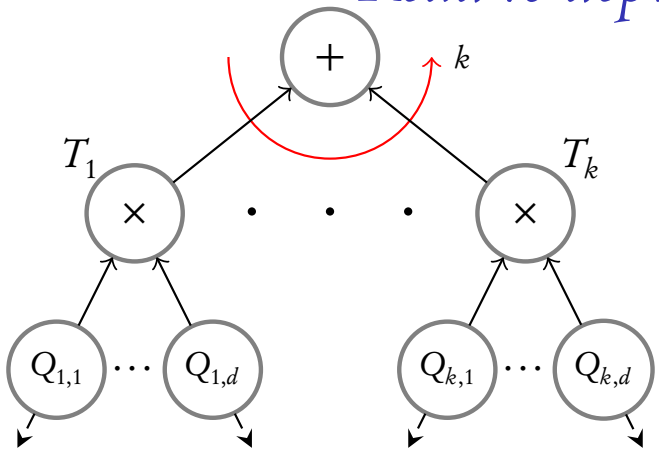
Read-k depth-D formulae



$$J = \begin{vmatrix} \partial_{x_1} T_1 & \cdots & \partial_{x_r} T_1 \\ \vdots & \ddots & \vdots \\ \partial_{x_r} T_r & \cdots & \partial_{x_r} T_r \end{vmatrix} = \left(\prod Q_{ij}\right) \cdot \begin{vmatrix} \partial_{x_1} T_1' & \cdots & \partial_{x_r} T_1' \\ \vdots & \ddots & \vdots \\ \partial_{x_r} T_r' & \cdots & \partial_{x_r} T_r' \end{vmatrix}$$

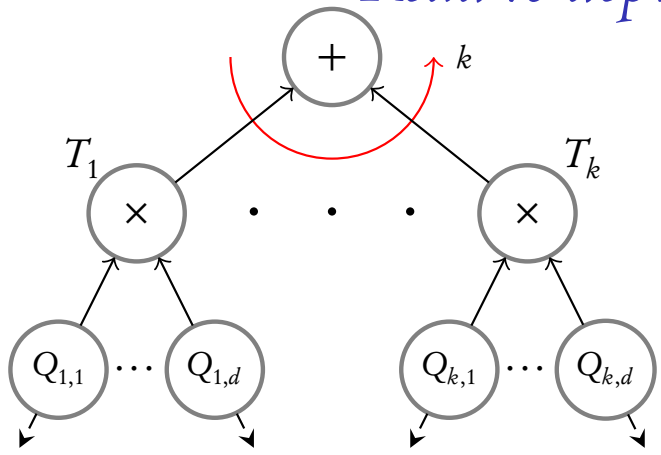
Function of "few" Q_{ij}'s

Read-k depth-D formulae



$$J = \begin{vmatrix} \partial_{x_1} T_1 & \cdots & \partial_{x_r} T_1 \\ \vdots & \ddots & \vdots \\ \partial_{x_r} T_r & \cdots & \partial_{x_r} T_r \end{vmatrix} = \underbrace{\left(\prod Q_{ij}\right) \cdot \begin{vmatrix} \partial_{x_1} T'_1 & \cdots & \partial_{x_r} T'_1 \\ \vdots & \ddots & \vdots \\ \partial_{x_r} T'_r & \cdots & \partial_{x_r} T'_r \end{vmatrix}}_{\text{Product of functions of “few” } Q_{ij}\text{'s}}$$

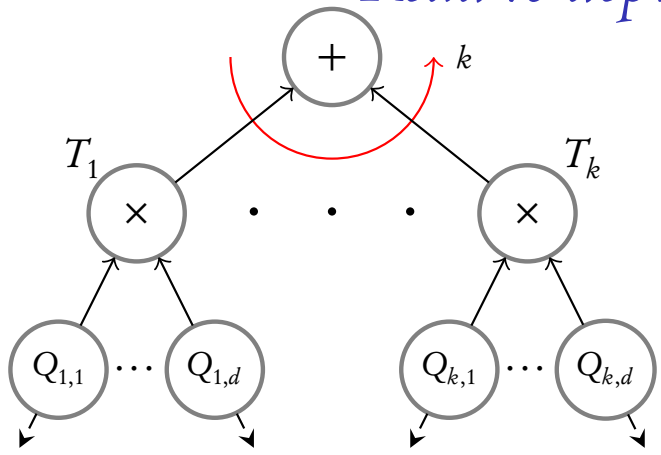
Read-k depth-D formulae



$$J = \begin{vmatrix} \partial_{x_1} T_1 & \cdots & \partial_{x_r} T_1 \\ \vdots & \ddots & \vdots \\ \partial_{x_r} T_r & \cdots & \partial_{x_r} T_r \end{vmatrix} = \underbrace{\left(\prod Q_{ij}\right) \cdot \begin{vmatrix} \partial_{x_1} T'_1 & \cdots & \partial_{x_r} T'_1 \\ \vdots & \ddots & \vdots \\ \partial_{x_r} T'_r & \cdots & \partial_{x_r} T'_r \end{vmatrix}}_{\text{Product of functions of "few" } Q_{ij}\text{'s}}$$

To preserve non-zeroness of C it suffices to preserve non-zeroness of J.

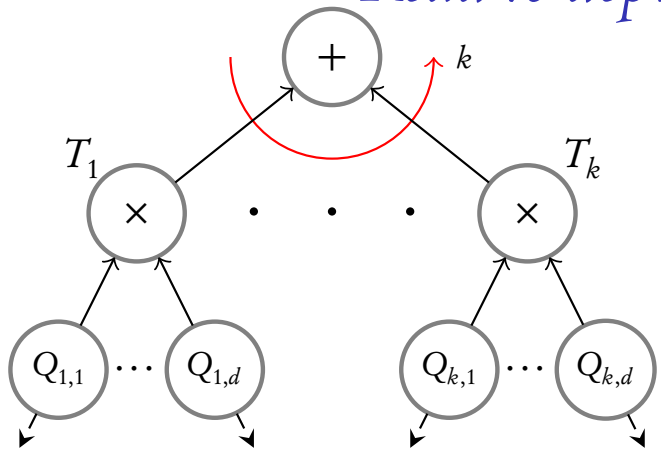
Read-k depth-D formulae



$$J = \begin{vmatrix} \partial_{x_1} T_1 & \cdots & \partial_{x_r} T_1 \\ \vdots & \ddots & \vdots \\ \partial_{x_r} T_r & \cdots & \partial_{x_r} T_r \end{vmatrix} = \underbrace{\left(\prod Q_{ij}\right) \cdot \begin{vmatrix} \partial_{x_1} T'_1 & \cdots & \partial_{x_r} T'_1 \\ \vdots & \ddots & \vdots \\ \partial_{x_r} T'_r & \cdots & \partial_{x_r} T'_r \end{vmatrix}}_{\text{Product of functions of "few" } Q_{ij}\text{'s}}$$

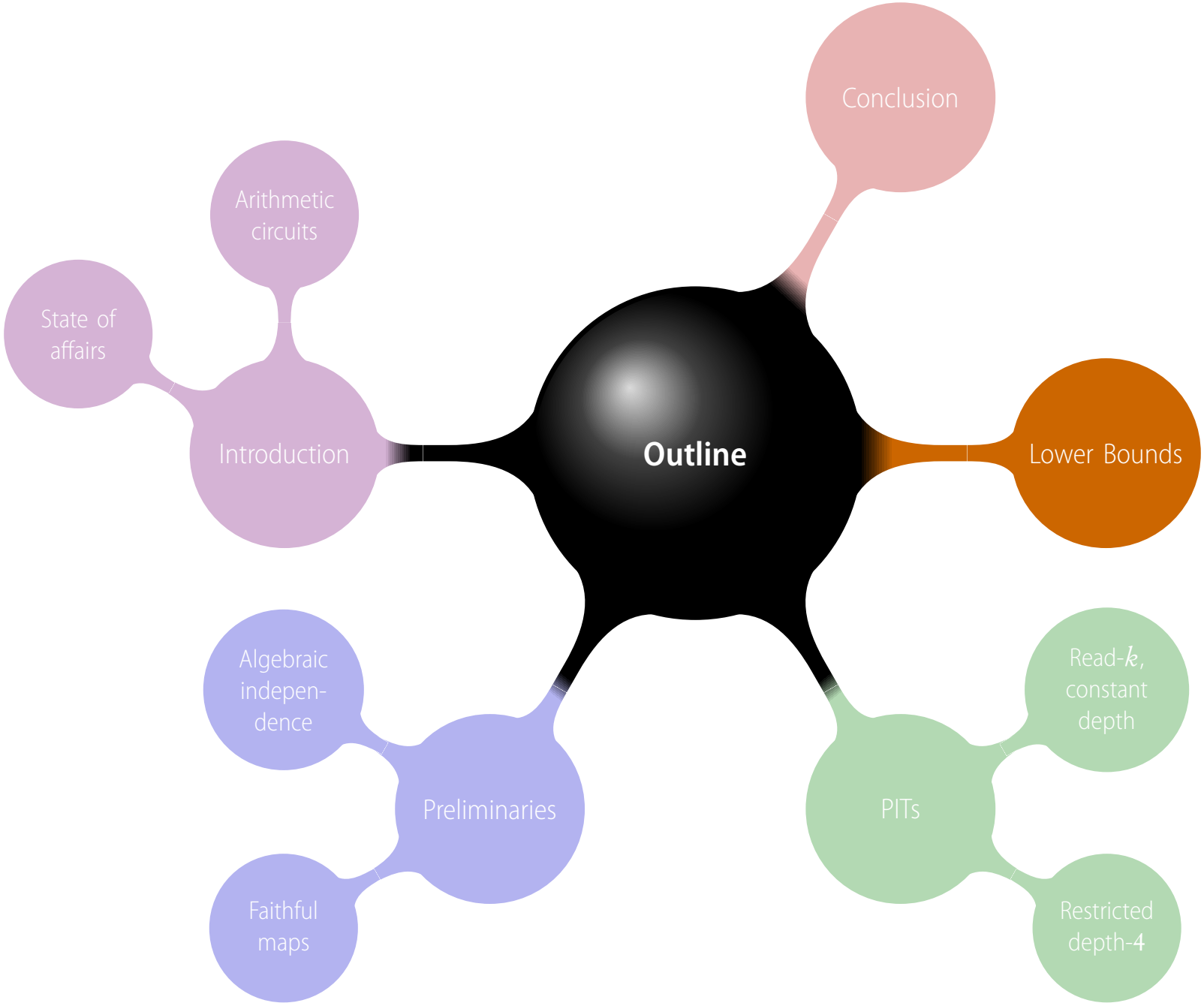
To preserve non-zeroness of C it suffices to preserve non-zeroness of J.
Hence, suffices to preserve the Jacobian of the Q_{ij}'s.

Read-k depth-D formulae



$$J = \begin{vmatrix} \partial_{x_1} T_1 & \cdots & \partial_{x_r} T_1 \\ \vdots & \ddots & \vdots \\ \partial_{x_r} T_r & \cdots & \partial_{x_r} T_r \end{vmatrix} = \underbrace{\left(\prod Q_{ij}\right) \cdot \begin{vmatrix} \partial_{x_1} T'_1 & \cdots & \partial_{x_r} T'_1 \\ \vdots & \ddots & \vdots \\ \partial_{x_r} T'_r & \cdots & \partial_{x_r} T'_r \end{vmatrix}}_{\text{Product of functions of "few" } Q_{ij}\text{'s}}$$

To preserve non-zeroness of C it suffices to preserve non-zeroness of J.
Hence, suffices to preserve the Jacobian of the Q_{ij}'s. Recurse! □


Outline
Introduction
Arithmetic circuits
State of affairs
Preliminaries
Algebraic independence
Faithful maps
Lower Bounds
PITs
Read-k, constant depth
Restricted depth-4
Conclusion

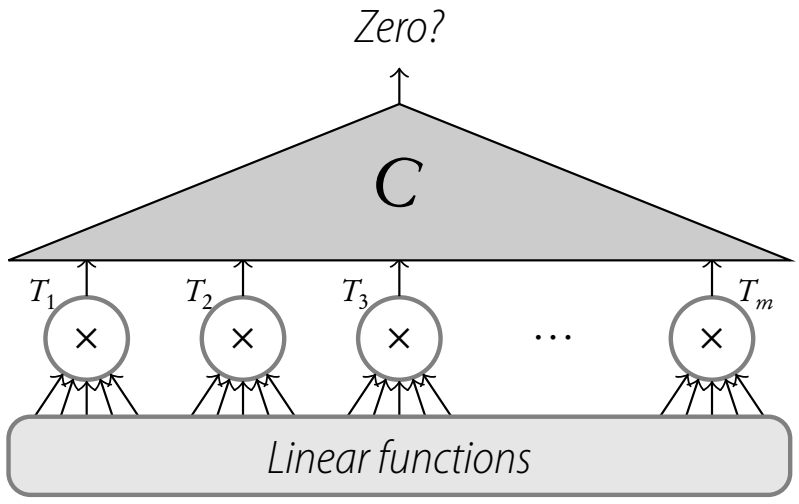
General philosophy

If you have black-box PITs for a class $\mathscr{C}$, then you have determinant/permanent lower bounds for (almost) $\mathscr{C}'$.

[KabanetsImpagliazzo03], [Agrawal05], [DvirShpilkaYehudayoff08] etc...

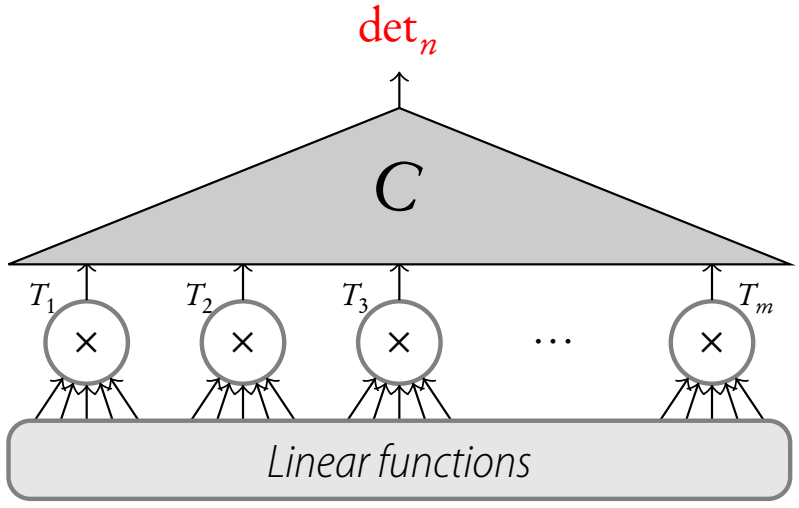
PITs & Lower bounds

Theorem



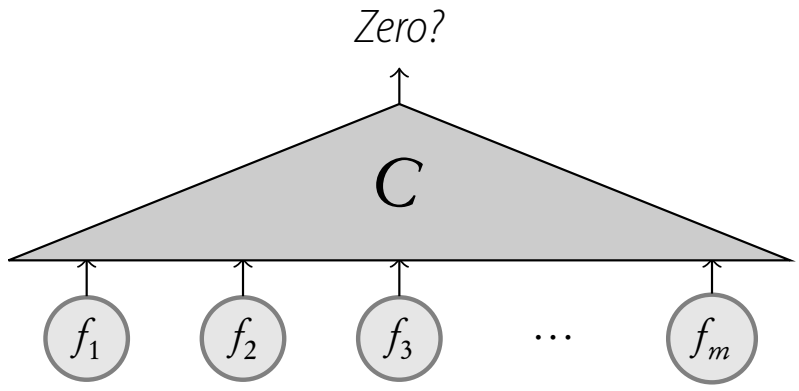
Black-box PIT if $\mathbf{trdeg}\{T_1, \cdots, T_m\} = O(1)$.

Theorem



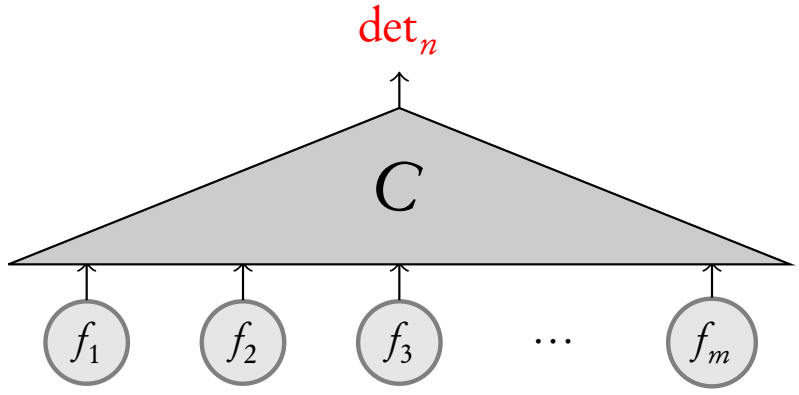
Then, $\mathrm{trdeg}\{T_1, \cdots, T_m\} = \Omega(n)$.

Theorem



Black-box PIT if $\mathbf{trdeg}\{f_1, \cdots, f_m\} = O(1)$.

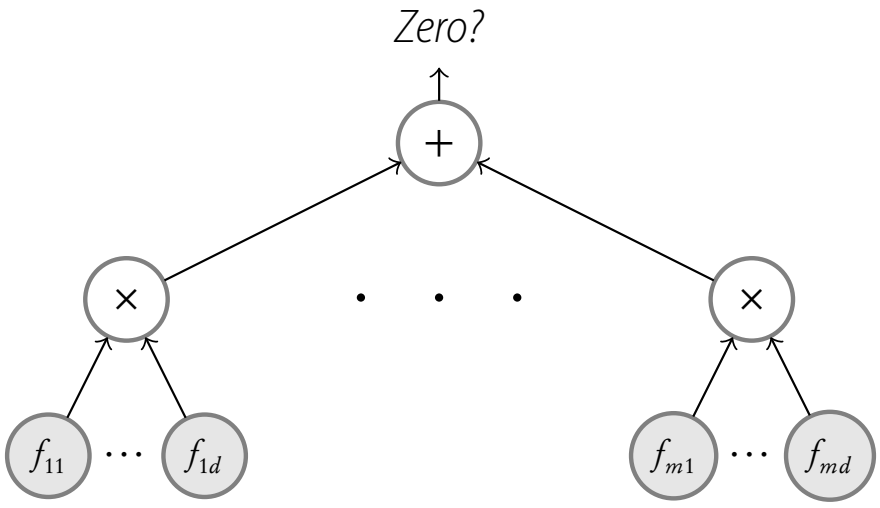
Theorem



If $\mathrm{trdeg}\{f_1, \cdots, f_m\} = k$, *then* $\mathrm{size}(f_i) \geq 2^{n/k^2}$

PITs & Lower bounds

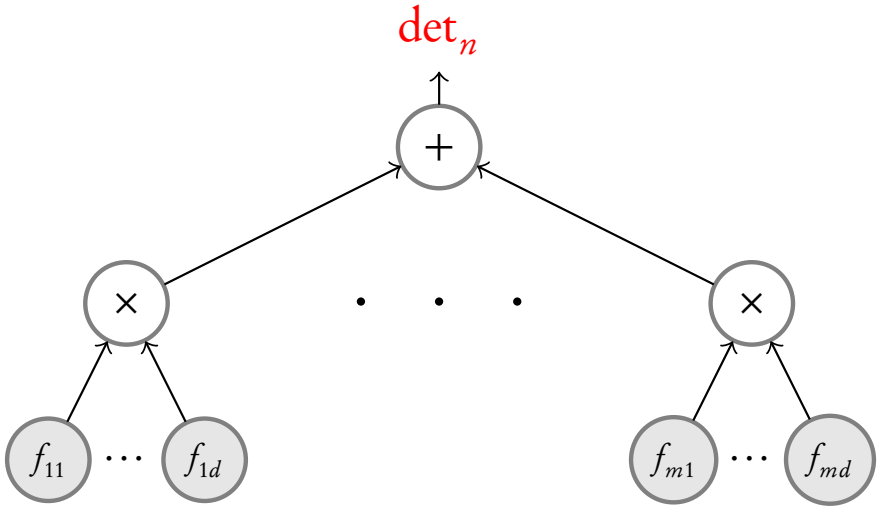
Theorem



Black-box PIT if at most $O(1)$ *of the* f_i*'s depend on any* x_j.

PITs & Lower bounds

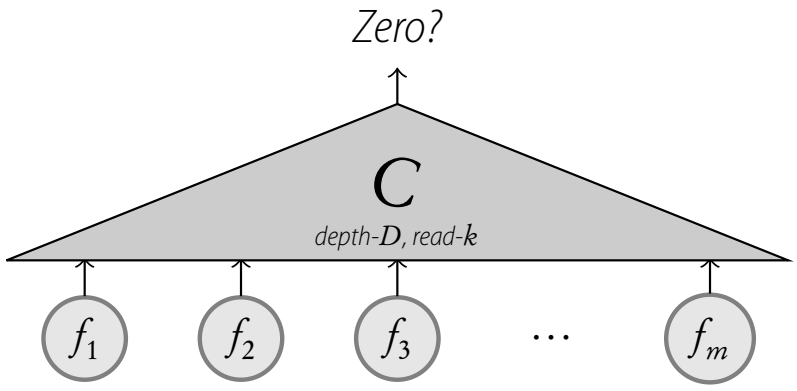
Theorem



If at most k *of the* f_i*'s depend on any* x_j*, then* $\text{size}(f_i) \geq 2^{n/k^3}$

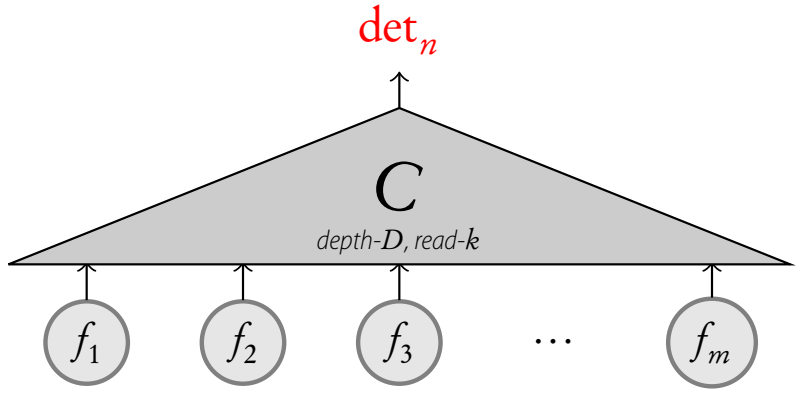
PITs & Lower bounds

Theorem



Black-box PIT if at most $O(1)$ *of the* f_i*'s depend on any* x_j.

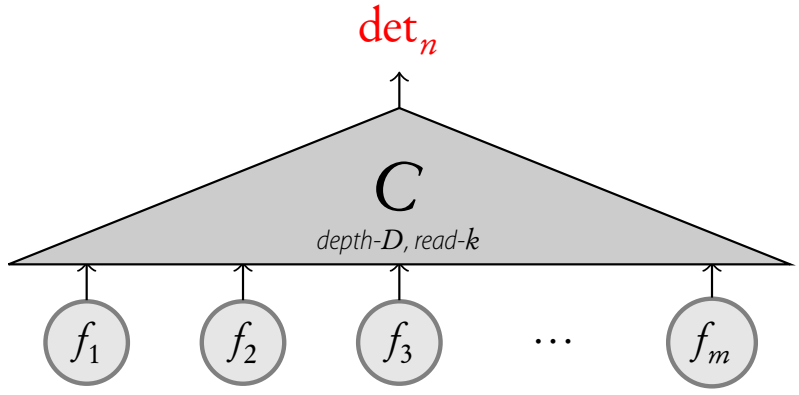
Theorem



If at most $O(1)$ *of the* f_i*'s depend on any* x_j*, then* $\text{size}(f_i) \geq 2^{\Omega(n)}$*, assuming a conjecture about determinants is true.*

$$M = \begin{vmatrix} x_{11} & x_{12} & x_{13} & x_{14} & x_{15} & x_{16} & x_{17} & x_{18} \\ x_{21} & x_{22} & x_{23} & x_{24} & x_{25} & x_{26} & x_{27} & x_{28} \\ x_{31} & x_{32} & x_{33} & x_{34} & x_{35} & x_{36} & x_{37} & x_{38} \\ x_{41} & x_{42} & x_{43} & x_{44} & x_{45} & x_{46} & x_{47} & x_{48} \\ x_{51} & x_{52} & x_{53} & x_{54} & x_{55} & x_{56} & x_{57} & x_{58} \\ x_{61} & x_{62} & x_{63} & x_{64} & x_{65} & x_{66} & x_{67} & x_{68} \\ x_{71} & x_{72} & x_{73} & x_{74} & x_{75} & x_{76} & x_{77} & x_{78} \\ x_{81} & x_{82} & x_{83} & x_{84} & x_{85} & x_{86} & x_{87} & x_{88} \end{vmatrix}$$

Theorem

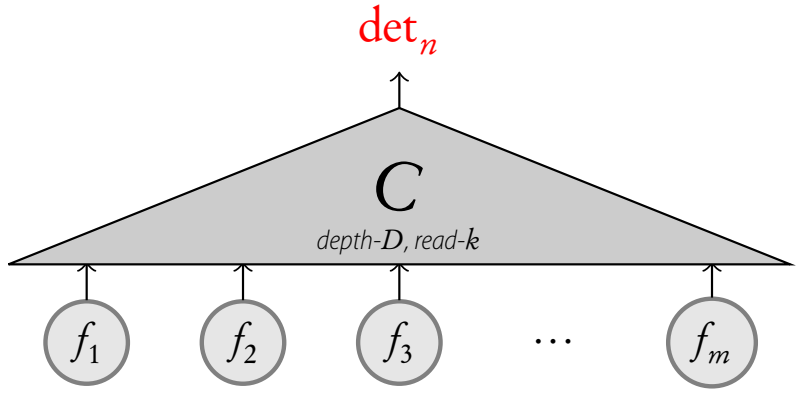


If at most $O(1)$ *of the* f_i*'s depend on any* x_j*, then* $\text{size}(f_i) \geq 2^{\Omega(n)}$*, assuming a conjecture about determinants is true.*

$$M_1 = \begin{vmatrix} x_{22} & x_{23} & x_{24} & x_{25} & x_{26} & x_{27} & x_{28} \\ x_{32} & x_{33} & x_{34} & x_{35} & x_{36} & x_{37} & x_{38} \\ x_{42} & x_{43} & x_{44} & x_{45} & x_{46} & x_{47} & x_{48} \\ x_{52} & x_{53} & x_{54} & x_{55} & x_{56} & x_{57} & x_{58} \\ x_{62} & x_{63} & x_{64} & x_{65} & x_{66} & x_{67} & x_{68} \\ x_{72} & x_{73} & x_{74} & x_{75} & x_{76} & x_{77} & x_{78} \\ x_{82} & x_{83} & x_{84} & x_{85} & x_{86} & x_{87} & x_{88} \end{vmatrix}$$

PITs & Lower bounds

Theorem

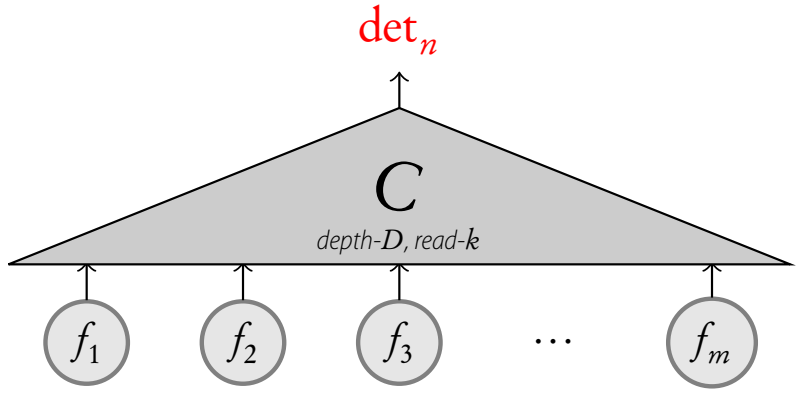


If at most $O(1)$ *of the* f_i*'s depend on any* x_j*, then* $\text{size}(f_i) \geq 2^{\Omega(n)}$*, assuming a conjecture about determinants is true.*

$$M_{13} = \begin{vmatrix} x_{22} & x_{24} & x_{25} & x_{26} & x_{27} & x_{28} \\ x_{42} & x_{44} & x_{45} & x_{46} & x_{47} & x_{48} \\ x_{52} & x_{54} & x_{55} & x_{56} & x_{57} & x_{58} \\ x_{62} & x_{64} & x_{65} & x_{66} & x_{67} & x_{68} \\ x_{72} & x_{74} & x_{75} & x_{76} & x_{77} & x_{78} \\ x_{82} & x_{84} & x_{85} & x_{86} & x_{87} & x_{88} \end{vmatrix}$$

PITs & Lower bounds

Theorem



If at most $O(1)$ *of the* f_i*'s depend on any* x_j*, then* $\text{size}(f_i) \geq 2^{\Omega(n)}$*, assuming a conjecture about determinants is true.*

*Baby version of conjecture**

$$\det \begin{bmatrix} M_{135} & M_{136} & M_{137} & M_{138} \\ M_{145} & M_{146} & M_{147} & M_{148} \\ M_{235} & M_{236} & M_{237} & M_{238} \\ M_{245} & M_{246} & M_{247} & M_{248} \end{bmatrix} \stackrel{?}{=} 0$$

*: so much so that it even is true

An illustrative example

Theorem

If $\det_n = C(f_1, \cdots, f_k)$, *then one of the* f_i*'s has* $2^{n/k^2}$ *monomials .*

Proof

$$\mathscr{J}(\det_n, f_1, \cdots, f_k) \quad =$$

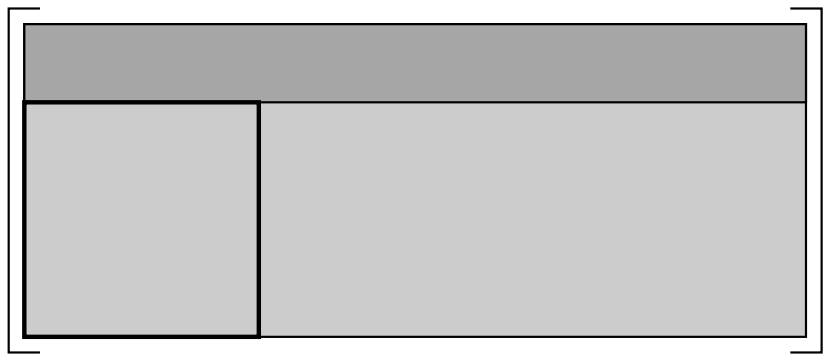
An illustrative example

Theorem

If $\det_n = C(f_1, \cdots, f_k)$, *then one of the* f_i*'s has* $2^{n/k^2}$ *monomials .*

Proof

$$\mathcal{J}(\det_n, f_1, \cdots, f_k) \quad =$$



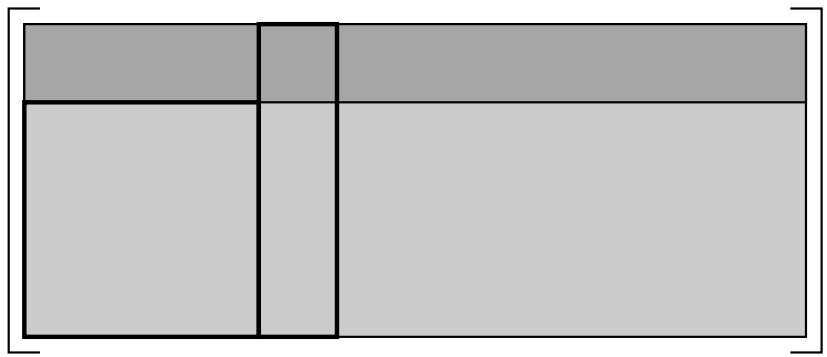
An illustrative example

Theorem

If $\det_n = C(f_1, \cdots, f_k)$, *then one of the* f_i*'s has* $2^{n/k^2}$ *monomials .*

Proof

$$\mathcal{J}(\det_n, f_1, \cdots, f_k) \quad =$$



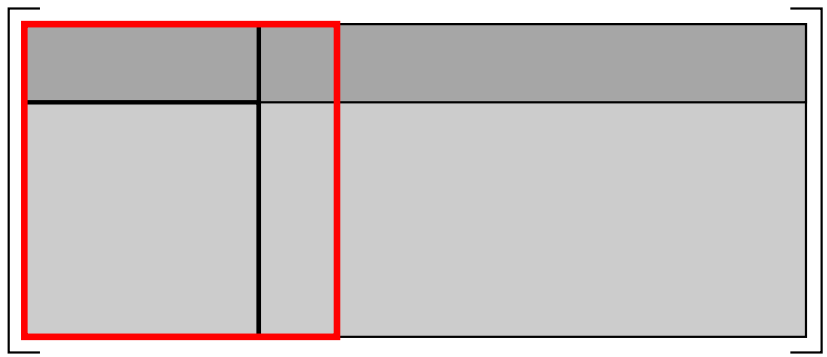
An illustrative example

Theorem

If $\det_n = C(f_1, \cdots, f_k)$, *then one of the* f_i*'s has* $2^{n/k^2}$ *monomials .*

Proof

$$\mathcal{J}(\det_n, f_1, \cdots, f_k) \quad =$$



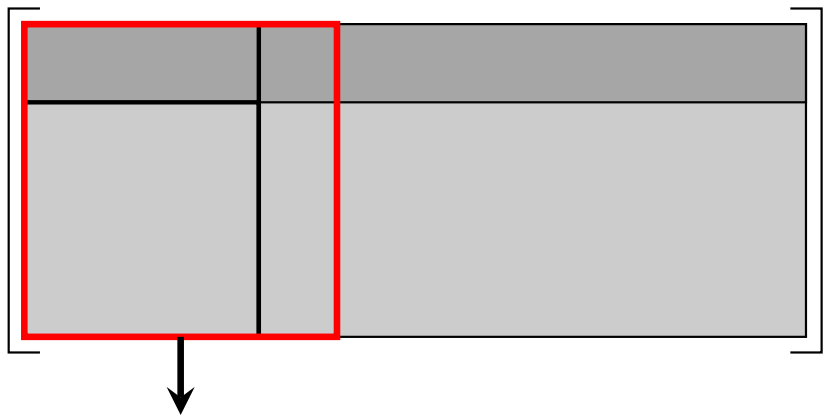
An illustrative example

Theorem

If $\det_n = C(f_1, \cdots, f_k)$, *then one of the* f_i*'s has* $2^{n/k^2}$ *monomials .*

Proof

$$\mathcal{J}(\det_n, f_1, \cdots, f_k) =$$



$$\sum_{i=1}^{k} M_i \cdot g_i = 0$$

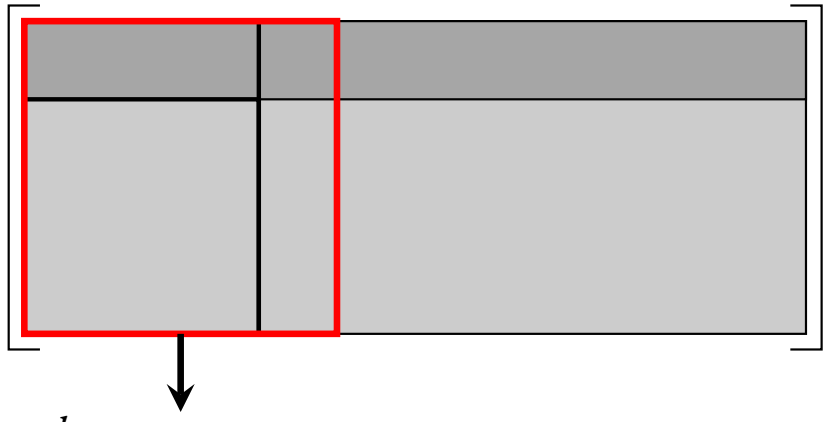
An illustrative example

Theorem

If $\det_n = C(f_1, \cdots, f_k)$, *then one of the* f_i*'s has* $2^{n/k^2}$ *monomials .*

Proof

$$\mathcal{J}(\det_n, f_1, \cdots, f_k) \quad =$$



$$\sum_{i=1}^{k} M_i \cdot g_i \quad = \quad 0$$

Is this possible?!

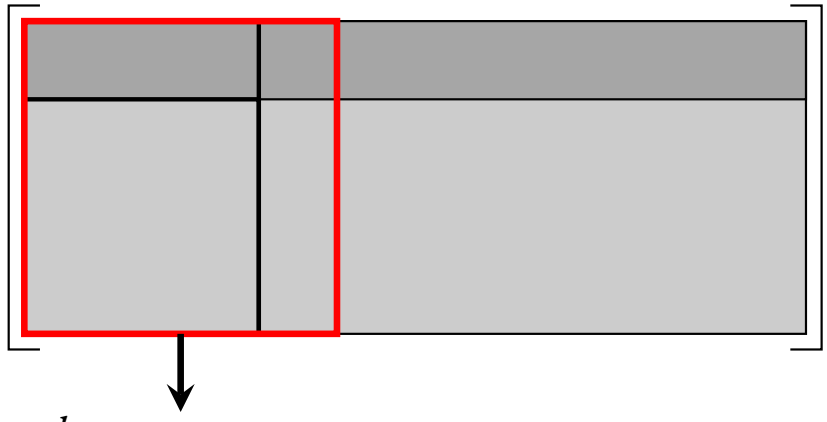
An illustrative example

Theorem

If $\det_n = C(f_1, \cdots, f_k)$, *then one of the* f_i*'s has* $2^{n/k^2}$ *monomials .*

Proof

$$\mathcal{J}(\det_n, f_1, \cdots, f_k) \quad =$$



$$\sum_{i=1}^{k} M_i \cdot g_i \quad = \quad 0$$

Is this possible?!

Not unless $\mathbf{size}(g_i) > 2^{n/k}$

Hanc marginis exiguitas non caperet.

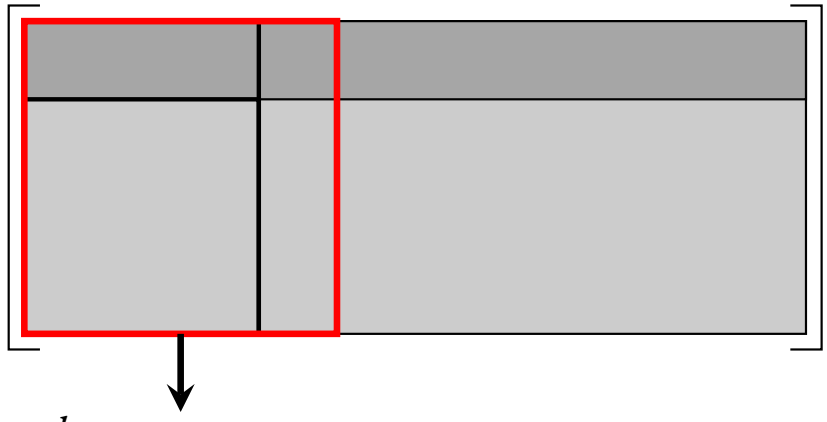
An illustrative example

Theorem

If $\det_n = C(f_1, \cdots, f_k)$, *then one of the* f_i*'s has* $2^{n/k^2}$ *monomials .*

Proof

$$\mathcal{J}(\det_n, f_1, \cdots, f_k) \quad =$$



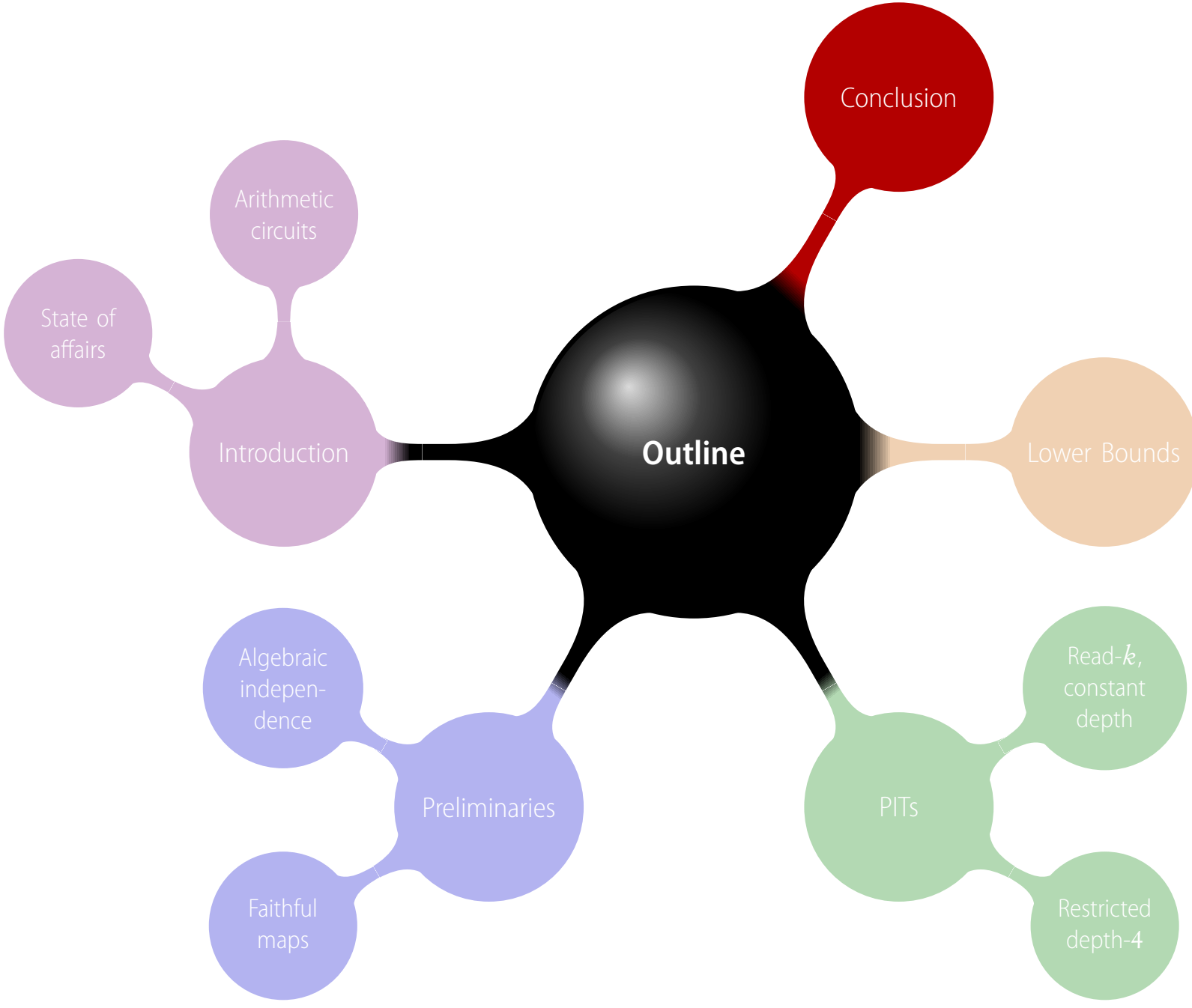
$$\sum_{i=1}^{k} M_i \cdot g_i \quad = \quad 0$$

Is this possible?!

Not unless $\mathbf{size}(g_i) > 2^{n/k}$

Hanc marginis exiguitas non caperet.

□


Outline
Introduction
Arithmetic circuits
State of affairs
Preliminaries
Algebraic indepen-dence
Faithful maps
Lower Bounds
PITs
Read-k, constant depth
Restricted depth-4
Conclusion

Concluding Remarks

- Generalizes all known polynomial time black-box PITs for sub-classes of constant depth formulae.
- Unified approach.
- Simpler proofs.

Open Problems

Models not hit by the Jacobian (yet!)

- Arbitrary depth, read-k formulae

  However, Jacobian gives a quasipoly blackbox test for arbitrary depth read-1 formulae

- Diagonal circuits: $\ell_1^d + \cdots + \ell_m^d \stackrel{?}{=} 0$

  Polynomial time non-blackbox known [Saxena08]

Others problems

- Conjecture on independence of minors
- Jacobian and circuit reconstructions
- Fields of small characteristic

Open Problems

Models not hit by the Jacobian (yet!)

- Arbitrary depth, read-k formulae

  However, Jacobian gives a quasipoly blackbox test for arbitrary depth read-1 formulae

- Diagonal circuits: $\ell_1^d + \cdots + \ell_m^d \stackrel{?}{=} 0$

  Polynomial time non-blackbox known [Saxena08]

Others problems

- Conjecture on independence of minors [Soon]
- Jacobian and circuit reconstructions on going
- Fields of small characteristic

Open Problems

Models not hit by the Jacobian (yet!)

- Arbitrary depth, read-k formulae

  However, Jacobian gives a quasipoly blackbox test for arbitrary depth read-1 formulae

- Diagonal circuits: $\ell_1^d + \cdots + \ell_m^d \stackrel{?}{=} 0$

  Polynomial time non-blackbox known [Saxena08]

Others problems

- Conjecture on independence of minors — [Soon]
- Jacobian and circuit reconstructions — on going
- Fields of small characteristic

Thank You

Questions?

谢谢

问题?

Tak

Spørgsmål?