Symmetric Determinantal Representations of Polynomials

Bruno Grenet[*†]

Joint work with Erich L. Kaltofen[‡], Pascal Koiran[*†] and Natacha Portier[*†]

[*]MC2 – LIP, ÉNS Lyon
[†]Theory Group – DCS, U. of Toronto
[‡]Dept. of Mathematics – North Carolina State U.

Paris – Séminaire CLI – November 16, 2010

The problem

$$(x + 3y)z = \det \begin{pmatrix} 0 & x & 3 & 0 & 0 \\ 0 & 1 & 0 & 0 & z \\ 0 & 0 & 1 & y & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

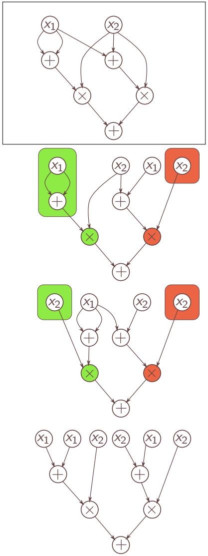
- Formal polynomial

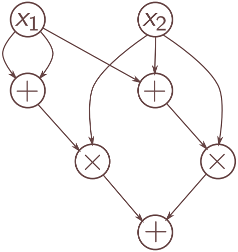
The problem

$$(x+3y)z = \det \begin{pmatrix} 0 & x & 3 & 0 & 0 \\ 0 & 1 & 0 & 0 & z \\ 0 & 0 & 1 & y & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

- Formal polynomial
- Smallest possible dimension of the matrix

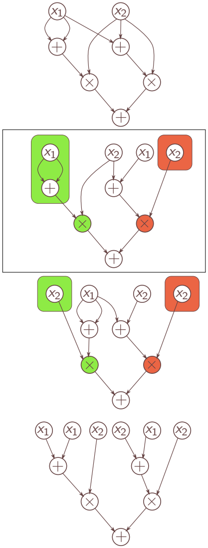
Representations of polynomials

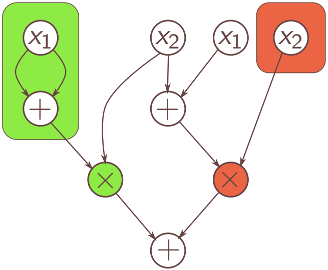




Circuit

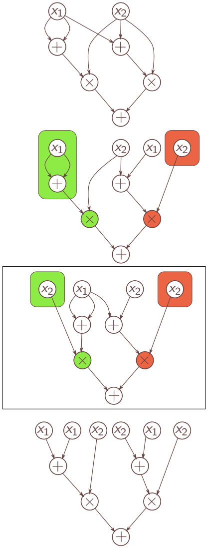
Representations of polynomials

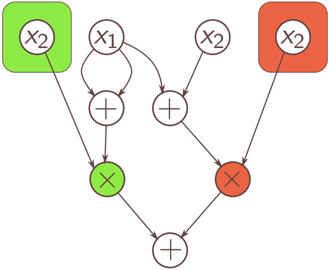




Weakly-skew circuit

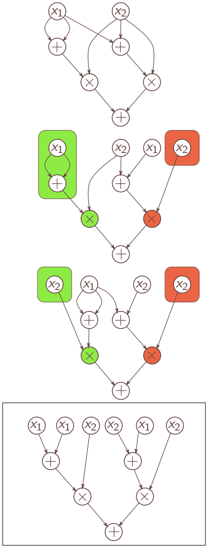
Representations of polynomials

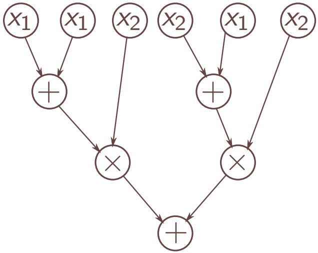




Skew circuit

Representations of polynomials





Formula

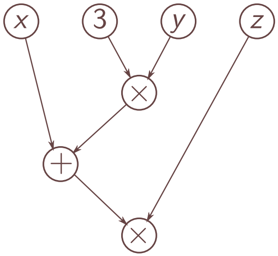
Motivation

L. G. Valiant, Completeness classes in algebra, STOC 79
$\rightsquigarrow$ Universality of the determinant

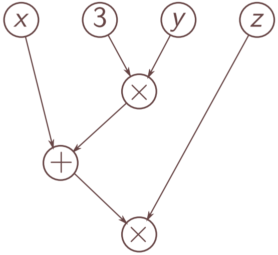
"We conclude that for the problem of finding a subexponential formula for a polynomial when one exists, linear algebra is essentially the only technique in the sense that it is always applicable".

An example

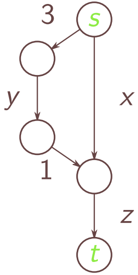
$(x + 3y)z$

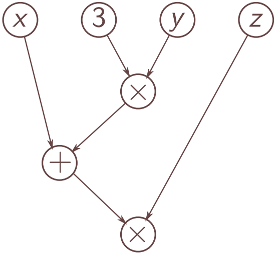


An example



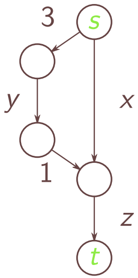
An example



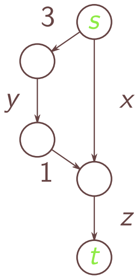


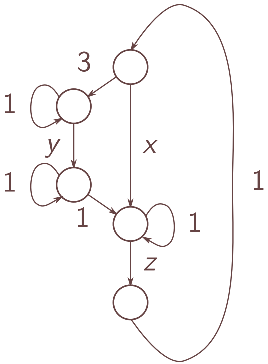
Arithmetic Branching Program

An example

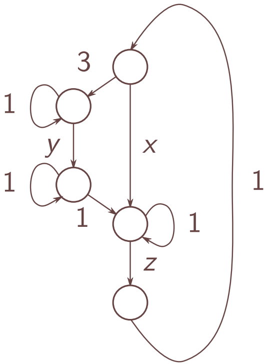


An example



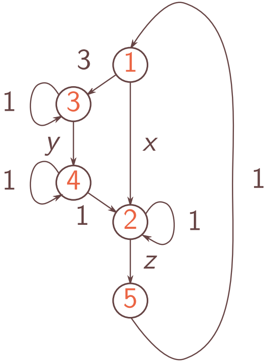


An example



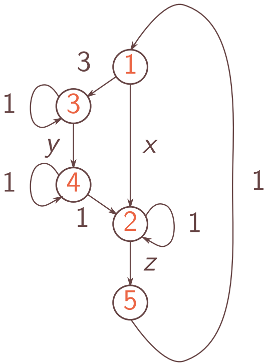
An example

$$\det \begin{pmatrix} 0 & x & 3 & 0 & 0 \\ 0 & 1 & 0 & 0 & z \\ 0 & 0 & 1 & y & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$



An example

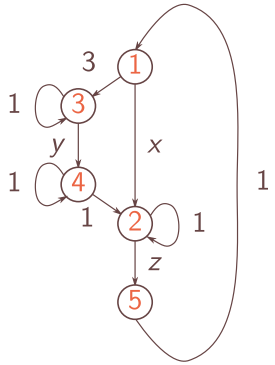
$$\det \begin{pmatrix} 0 & x & 3 & 0 & 0 \\ 0 & 1 & 0 & 0 & z \\ 0 & 0 & 1 & y & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$



$$\det A = \sum_{\sigma} (-1)^{\mathrm{sgn}(\sigma)} \prod_{i=1}^{n} A_{i,\sigma(i)}$$

An example

$$\det \begin{pmatrix} 0 & x & 3 & 0 & 0 \\ 0 & 1 & 0 & 0 & z \\ 0 & 0 & 1 & y & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

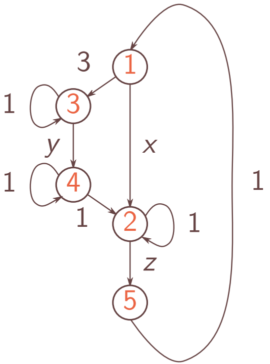


$$\det A = \sum_{\sigma} (-1)^{\mathrm{sgn}(\sigma)} \prod_{i=1}^{n} A_{i,\sigma(i)}$$

- permutation in A = cycle cover in G

An example

$$\det \begin{pmatrix} 0 & x & 3 & 0 & 0 \\ 0 & 1 & 0 & 0 & z \\ 0 & 0 & 1 & y & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$



$$\det A = \sum_{\sigma} (-1)^{\mathrm{sgn}(\sigma)} \prod_{i=1}^{n} A_{i,\sigma(i)}$$

- permutation in A = cycle cover in G
- Up to signs, $\det A$ = sum of the weights of cycle covers in G

Outline

1. From polynomials to determinants
2. From polynomials to determinants of symmetric matrices
3. Characteristic 2

Upper bounds

- $e+2$: L. G. Valiant, in *Completeness classes in algebra* (STOC 79)

Upper bounds

- $e+2$: L. G. Valiant, in *Completeness classes in algebra* (STOC 79)
- $2e+2$: J. von zur Gathen, in *Feasible arithmetic computations: Valiant's hypothesis* (J. Symb. Comput., 1987)

Upper bounds

- $e+2$: L. G. Valiant, in *Completeness classes in algebra* (STOC 79)
- $2e+2$: J. von zur Gathen, in *Feasible arithmetic computations: Valiant's hypothesis* (J. Symb. Comput., 1987)
- $e+1$ if there is at least one addition in the formula: H. Liu and K.W. Regan, in *Improved construction for universality of determinant and permanent* (Inf. Process. Lett., 2006)

Valiant's construction (1/3)

- Input: a formula representing a polynomial $\varphi \in \mathbb{K}[X_1, \ldots, X_n]$ of size e

Valiant's construction (1/3)

- Input: a formula representing a polynomial $\varphi \in \mathbb{K}[X_1, \ldots, X_n]$ of size e

Size of a formula : number of computation gates

Valiant's construction (1/3)

- Input: a formula representing a polynomial $\varphi \in \mathbb{K}[X_1, \ldots, X_n]$ of size e

  Size of a formula : number of computation gates

- Output: a matrix A of dimension $(e+1)$, with entries in $\mathbb{K} \cup \{X_1, \ldots, X_n\}$, s.t. $\det A = \varphi$

Valiant's construction (1/3)

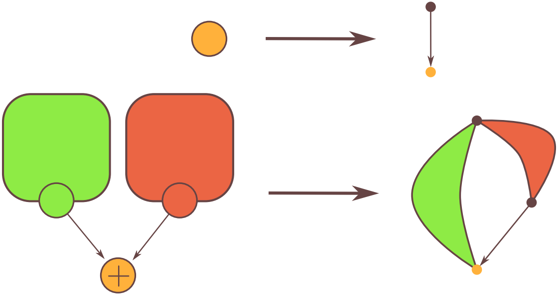
- Input: a formula representing a polynomial $\varphi \in \mathbb{K}[X_1, \dots, X_n]$ of size e

  Size of a formula : number of computation gates

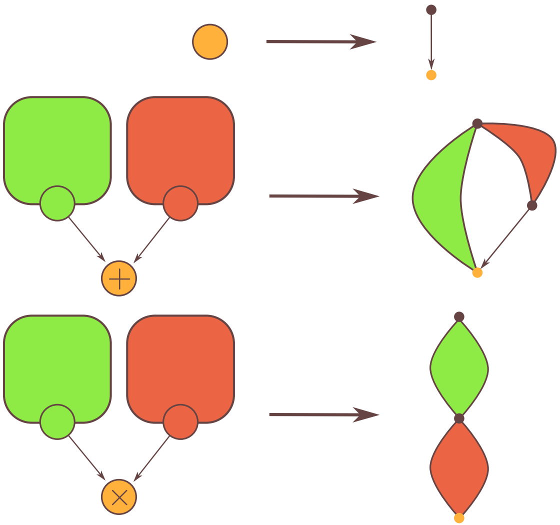
- Output: a matrix A of dimension $(e+1)$, with entries in $\mathbb{K} \cup \{X_1, \dots, X_n\}$, s.t. $\det A = \varphi$
- In between: a graph G of size $(e+1)$ whose adjacency matrix is A

Valiant's construction (2/3)

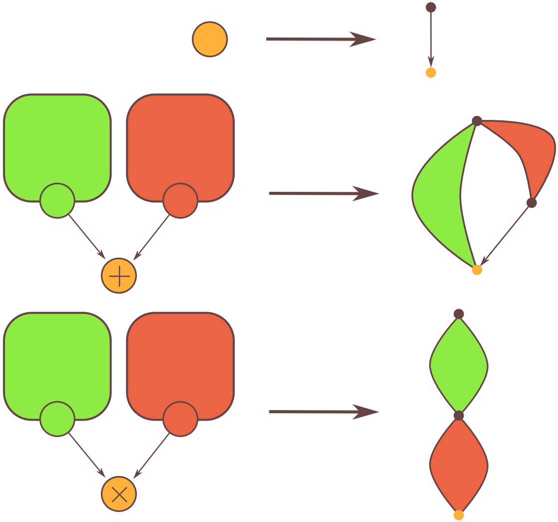
Valiant's construction (2/3)



Valiant's construction (2/3)



Valiant's construction (2/3)



Invariant

$$\varphi = \pm \sum_{s\text{-}t\text{-paths } P} (-1)^{|P|} w(P)$$

Valiant's construction (3/3)

- G s.t. $\varphi = \pm \sum_{s\text{-}t\text{-paths } P} (-1)^{|P|} w(P)$, with s, t distinguished

Valiant's construction (3/3)

- G s.t. $\varphi = \pm \sum_{s\text{-}t\text{-paths } P} (-1)^{|P|} w(P)$, with s, t distinguished

$\rightsquigarrow$ G': merge s and t + add weight-1 loops on vertices $\neq s$.

Valiant's construction (3/3)

- G s.t. $\varphi = \pm \sum_{s\text{-}t\text{-paths } P} (-1)^{|P|} w(P)$, with s, t distinguished

$\rightsquigarrow$ G': merge s and t + add weight-1 loops on vertices $\neq s$.

- s-t-paths $\rightsquigarrow$ *big* cycles

Valiant's construction (3/3)

- G s.t. $\varphi = \pm \sum_{s\text{-}t\text{-paths } P} (-1)^{|P|} w(P)$, with s, t distinguished

$\rightsquigarrow$ G': merge s and t + add weight-1 loops on vertices $\neq s$.

- s-t-paths $\rightsquigarrow$ *big* cycles
- Cycle cover in G': One big cycle + loops

Valiant's construction (3/3)

- G s.t. $\varphi = \pm \sum_{s\text{-}t\text{-paths } P} (-1)^{|P|} w(P)$, with s, t distinguished

$\rightsquigarrow$ G': merge s and t + add weight-1 loops on vertices $\neq s$.

- s-t-paths $\rightsquigarrow$ *big* cycles
- Cycle cover in G': One big cycle + loops

Theorem

For a size-e formula, this construction yields a size-$(e+1)$ graph. Let A be the adjacency matrix of G. Then $\det(A) = \varphi$.

(Weakly-)Skew circuits

- Toda (IEICE Trans. Inf. Syst. 92): Notions of skew and weakly-skew circuits

(Weakly-)Skew circuits

- Toda (IEICE Trans. Inf. Syst. 92): Notions of skew and weakly-skew circuits
  - Skew circuit of size $O(n^{20})$ for the determinant

(Weakly-)Skew circuits

- Toda (IEICE Trans. Inf. Syst. 92): Notions of skew and weakly-skew circuits
  - Skew circuit of size $O(n^{20})$ for the determinant
  - Weakly-skew circuit of size $O(n^7)$.

(Weakly-)Skew circuits

- Toda (IEICE Trans. Inf. Syst. 92): Notions of skew and weakly-skew circuits
  - Skew circuit of size $O(n^{20})$ for the determinant
  - Weakly-skew circuit of size $O(n^7)$.
- Malod (MFCS'06, with Portier): Notion of strongly multiplicatively disjoint circuits

(Weakly-)Skew circuits

- Toda (IEICE Trans. Inf. Syst. 92): Notions of skew and weakly-skew circuits
  - Skew circuit of size $O(n^{20})$ for the determinant
  - Weakly-skew circuit of size $O(n^7)$.
- Malod (MFCS'06, with Portier): Notion of strongly multiplicatively disjoint circuits
  - Study of Valiant's classes, especially VQP

(Weakly-)Skew circuits

- Toda (IEICE Trans. Inf. Syst. 92): Notions of skew and weakly-skew circuits
  - Skew circuit of size $O(n^{20})$ for the determinant
  - Weakly-skew circuit of size $O(n^7)$.
- Malod (MFCS'06, with Portier): Notion of strongly multiplicatively disjoint circuits
  - Study of Valiant's classes, especially VQP
- Koiran and Kaltofen (ISSAC'08): Weakly-skew and skew circuits are linearly equivalent (factor 2)

(Weakly-)Skew circuits

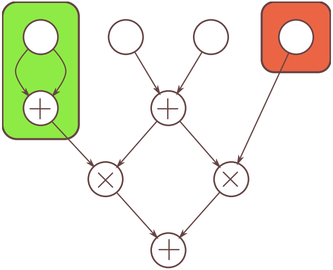
- Toda (IEICE Trans. Inf. Syst. 92): Notions of skew and weakly-skew circuits
  - Skew circuit of size $O(n^{20})$ for the determinant
  - Weakly-skew circuit of size $O(n^7)$.
- Malod (MFCS'06, with Portier): Notion of strongly multiplicatively disjoint circuits
  - Study of Valiant's classes, especially VQP
- Koiran and Kaltofen (ISSAC'08): Weakly-skew and skew circuits are linearly equivalent (factor 2)
  - Skew circuit of size $O(n^5)$ for the determinant

Toda-Malod's construction (1/3)

- Input: a weakly-skew circuit of size e with i variable inputs representing φ

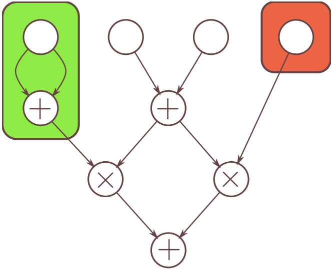
Toda-Malod's construction (1/3)

- Input: a weakly-skew circuit of size e with i variable inputs representing φ



Toda-Malod's construction (1/3)

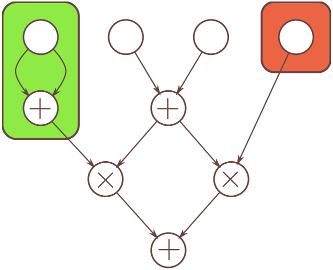
- Input: a weakly-skew circuit of size e with i variable inputs representing φ



$e = 5$ and $i = 4$

Toda-Malod's construction (1/3)

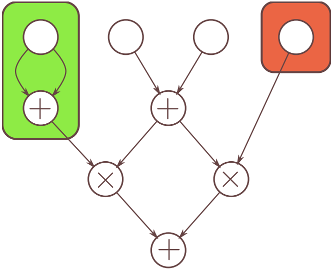
- Input: a weakly-skew circuit of size e with i variable inputs representing φ
- Output: a matrix A of dimension $(e+i+1)$ s.t. $\det A = \varphi$



$e = 5$ and $i = 4$

Toda-Malod's construction (1/3)

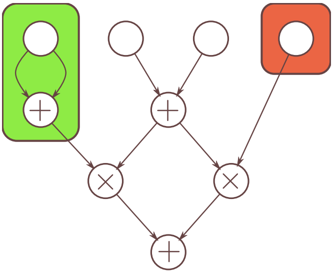
- Input: a weakly-skew circuit of size e with i variable inputs representing φ
- Output: a matrix A of dimension $(e+i+1)$ s.t. $\det A = \varphi$
- In between: a graph G...



$e = 5$ and $i = 4$

Toda-Malod's construction (1/3)

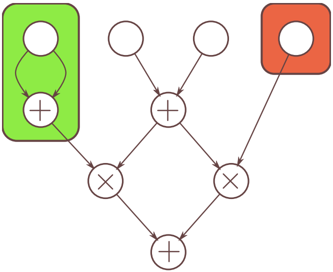
- Input: a weakly-skew circuit of size e with i variable inputs representing φ
- Output: a matrix A of dimension $(e+i+1)$ s.t. $\det A = \varphi$
- In between: a graph G...
- φ_α: polynomial computed by gate α



$e = 5$ and $i = 4$

Toda-Malod's construction (1/3)

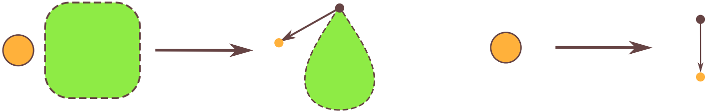
- Input: a weakly-skew circuit of size e with i variable inputs representing φ
- Output: a matrix A of dimension $(e + i + 1)$ s.t. $\det A = \varphi$
- In between: a graph G...



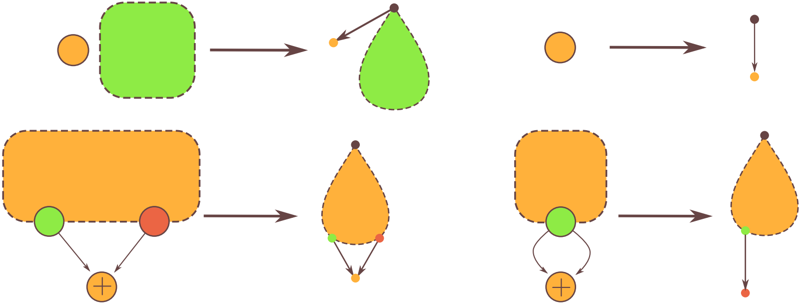
- φ_α: polynomial computed by gate α
- Reusable gate: not in a closed subcircuit

$e = 5$ and $i = 4$

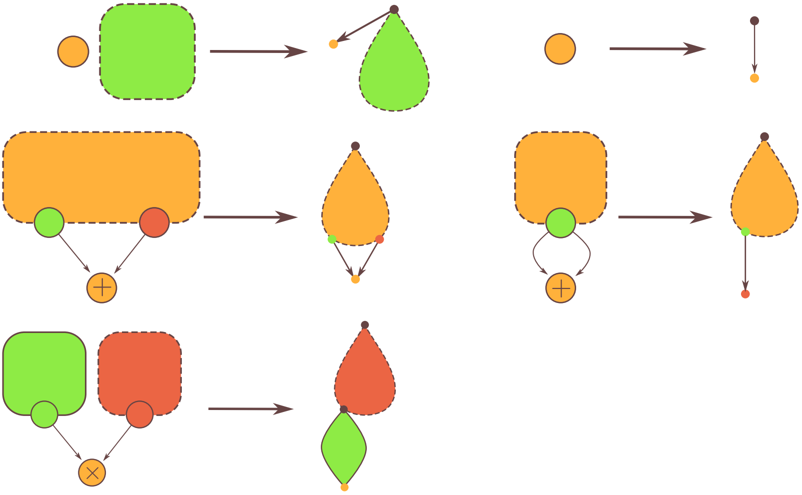
Toda-Malod's construction (2/3)



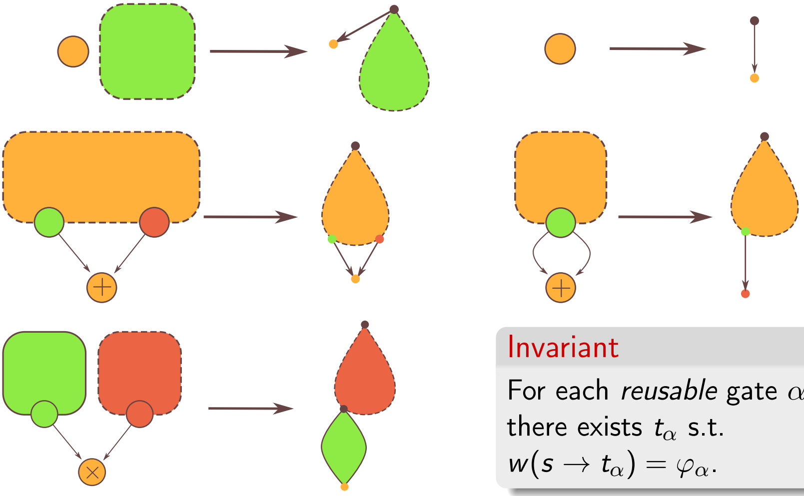
Toda-Malod's construction (2/3)



Toda-Malod's construction (2/3)



Toda-Malod's construction (2/3)



Invariant

For each *reusable* gate α, there exists t_α s.t. $w(s \to t_\alpha) = \varphi_\alpha$.

Toda-Malod's construction (3/3)

- As in Valiant's, $G \rightsquigarrow G'$: same idea

Toda-Malod's construction (3/3)

- As in Valiant's, $G \rightsquigarrow G'$: same idea

Theorem

For a ws circuit of size e with i variable inputs representing φ, this construction yields a size-$(e+i+1)$. The determinant of its adjacency matrix equals φ.

Outline

1. From polynomials to determinants
2. From polynomials to determinants of symmetric matrices
3. Characteristic 2

Motivation from Convex Geometry

- Linear Matrix Expression (LME): for A_i symmetric in $\mathbb{R}^{t\times t}$

$$A_0 + x_1 A_1 + \cdots + x_n A_n$$

Motivation from Convex Geometry

- Linear Matrix Expression (LME): for A_i symmetric in $\mathbb{R}^{t\times t}$

$$A_0 + x_1 A_1 + \cdots + x_n A_n$$

- Lax conjecture: express a *real zero polynomial* f as

$$f = \det A$$

with A LME and $A_0 \succeq 0$.

Motivation from Convex Geometry

- Linear Matrix Expression (LME): for A_i symmetric in $\mathbb{R}^{t\times t}$

$$A_0 + x_1 A_1 + \cdots + x_n A_n$$

- Lax conjecture: express a *real zero polynomial* f as

$$f = \det A$$

with A LME and $A_0 \succeq 0$. $\rightsquigarrow$ disproved

Motivation from Convex Geometry

- Linear Matrix Expression (LME): for A_i symmetric in $\mathbb{R}^{t\times t}$

$$A_0 + x_1 A_1 + \cdots + x_n A_n$$

- Lax conjecture: express a *real zero polynomial* f as

$$f = \det A$$

  with A LME and $A_0 \succeq 0$. $\rightsquigarrow$ disproved
- Drop condition $A_0 \succeq 0 \rightsquigarrow$ exponential size matrices

Motivation from Convex Geometry

- Linear Matrix Expression (LME): for A_i symmetric in $\mathbb{R}^{t\times t}$

$$A_0 + x_1 A_1 + \cdots + x_n A_n$$

- Lax conjecture: express a *real zero polynomial* f as

$$f = \det A$$

  with A LME and $A_0 \succeq 0$. $\rightsquigarrow$ disproved
- Drop condition $A_0 \succeq 0$ $\rightsquigarrow$ exponential size matrices
- What about polynomial size matrices?

Introduction

- Symmetric matrices $\iff$ undirected graphs

Introduction

- Symmetric matrices $\iff$ undirected graphs
- Difficulty: no DAG anymore!

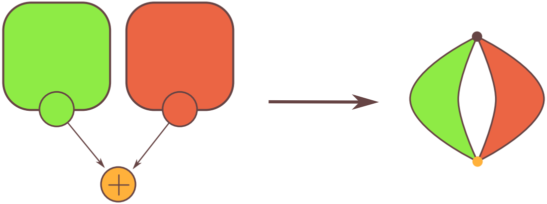
Introduction

- Symmetric matrices $\iff$ undirected graphs
- Difficulty: no DAG anymore!
- Solution: some changes in the construction, and new invariants

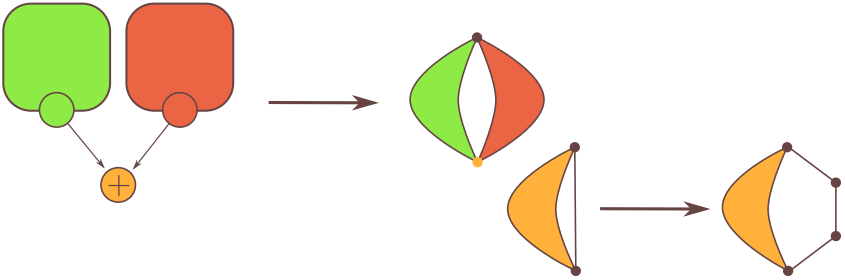
Introduction

- Symmetric matrices $\iff$ undirected graphs
- Difficulty: no DAG anymore!
- Solution: some changes in the construction, and new invariants
- N.B.: $\mathrm{char}(\mathbb{K}) \neq 2$ in this section

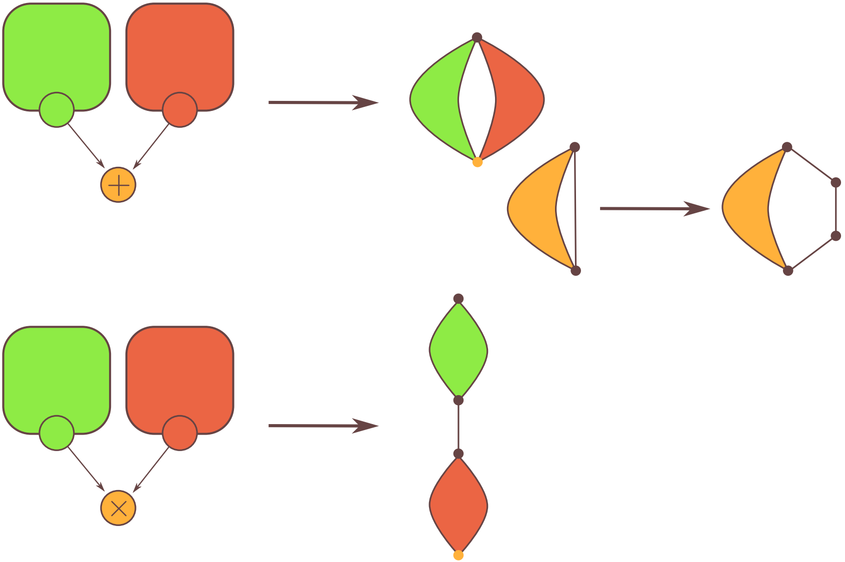
Algorithm



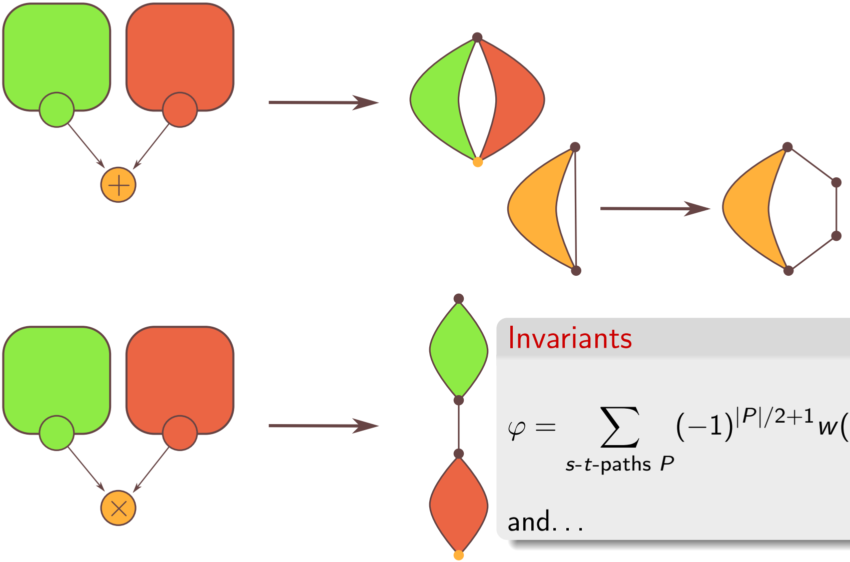
Algorithm



Algorithm



Algorithm



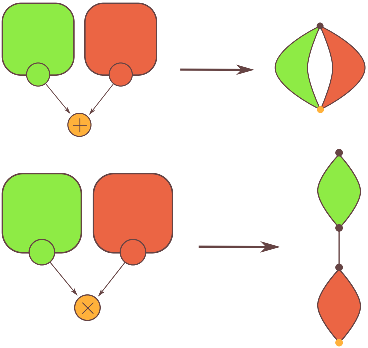
Invariants

$$\varphi = \sum_{s\text{-}t\text{-paths } P} (-1)^{|P|/2+1} w(P)$$

and. . .

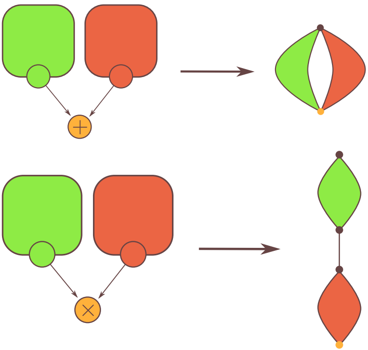
Invariants for formula's construction

- $\varphi = \sum_{s\text{-}t\text{-paths } P} (-1)^{|P|/2+1} w(P)$



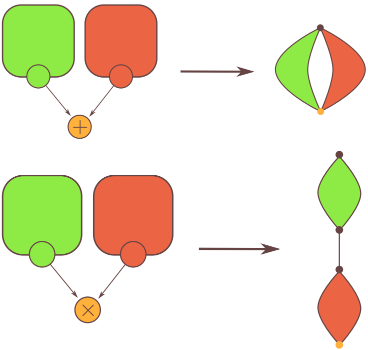
Invariants for formula's construction

- $\varphi = \sum_{s\text{-}t\text{-paths } P} (-1)^{|P|/2+1} w(P)$
- $|G|$ is even, every cycle in G is even, and every s-t-path is even



Invariants for formula's construction

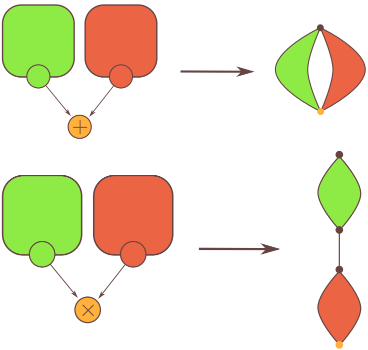
- $\varphi = \sum_{s\text{-}t\text{-paths } P} (-1)^{|P|/2+1} w(P)$
- $|G|$ is even, every cycle in G is even, and every s-t-path is even
- $G \setminus \{s, t\}$ is either empty or has a unique cycle cover



Invariants for formula's construction

- $\varphi = \sum_{s\text{-}t\text{-paths } P} (-1)^{|P|/2+1} w(P)$
- $|G|$ is even, every cycle in G is even, and every s-t-path is even
- $G \setminus \{s, t\}$ is either empty or has a unique cycle cover

⇝ Perfect matching of weight 1

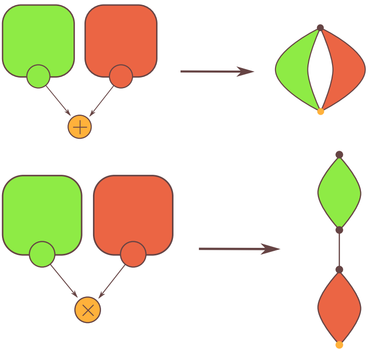


Invariants for formula's construction

- $\varphi = \sum_{s\text{-}t\text{-paths } P} (-1)^{|P|/2+1} w(P)$
- $|G|$ is even, every cycle in G is even, and every s-t-path is even
- $G \setminus \{s,t\}$ is either empty or has a unique cycle cover

$\rightsquigarrow$ Perfect matching of weight 1

- For any s-t-path P, $G \setminus P$ is either empty or has a unique cycle cover



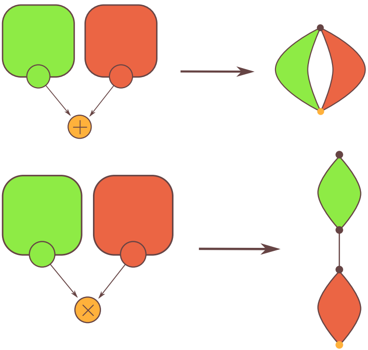
Invariants for formula's construction

- $\varphi = \sum_{s\text{-}t\text{-paths } P} (-1)^{|P|/2+1} w(P)$
- $|G|$ is even, every cycle in G is even, and every s-t-path is even
- $G \setminus \{s,t\}$ is either empty or has a unique cycle cover

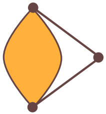
$\rightsquigarrow$ Perfect matching of weight 1

- For any s-t-path P, $G \setminus P$ is either empty or has a unique cycle cover

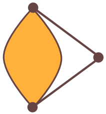
$\rightsquigarrow$ Perfect matching of weight 1



From G to G'

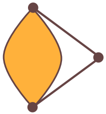


From G to G'



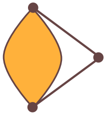
- $|G'|$ is odd. An odd cycle in G' has to go through c

From G to G'



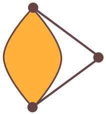
- $|G'|$ is odd. An odd cycle in G' has to go through c
- Cycle covers in G' $\iff$ $s \to t$-paths in G

From G to G'



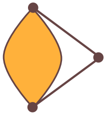
- $|G'|$ is odd. An odd cycle in G' has to go through c
- Cycle covers in $G' \iff s \to t$-paths in $G \iff t \to s$-paths in G

From G to G'



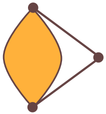
- $|G'|$ is odd. An odd cycle in G' has to go through c
- Cycle covers in G' $\iff$ $s \to t$-paths in G $\iff$ $t \to s$-paths in G
- $(-1)^{|G/2|+1}$ ensures that the signs are OK.

From G to G'



- $|G'|$ is odd. An odd cycle in G' has to go through c
- Cycle covers in $G' \iff s \to t$-paths in $G \iff t \to s$-paths in G
- $(-1)^{|G/2|+1}$ ensures that the signs are OK.
- $1/2$: to deal with $s \to t$ and $t \to s$-paths, implies $\mathrm{char}(\mathbb{K}) \neq 2$

From G to G'



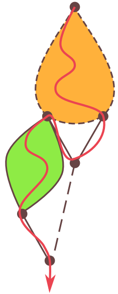
- $|G'|$ is odd. An odd cycle in G' has to go through c
- Cycle covers in $G' \iff s \to t$-paths in $G \iff t \to s$-paths in G
- $(-1)^{|G/2|+1}$ ensures that the signs are OK.
- $1/2$: to deal with $s \to t$ and $t \to s$-paths, implies $\mathrm{char}(\mathbb{K}) \neq 2$

Theorem

For a formula φ of size e, this construction yields a graph of size $2e+3$. The determinant of its adjacency matrix equals φ.

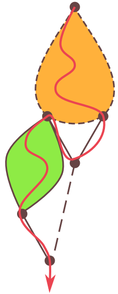
Introduction

- Main difficulty:



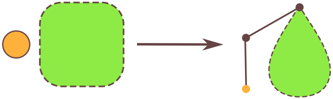
Introduction

- Main difficulty:

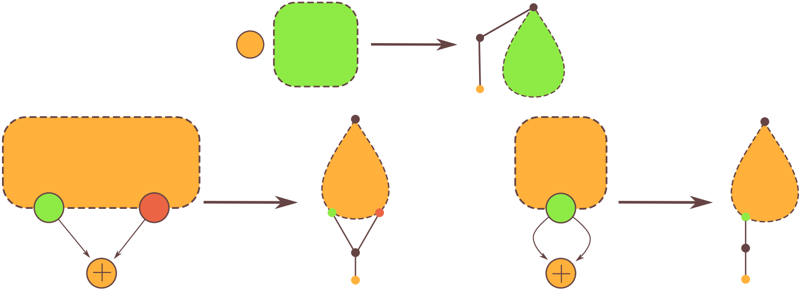


- Definition: an path P is said acceptable if $G \setminus P$ admits a cycle cover

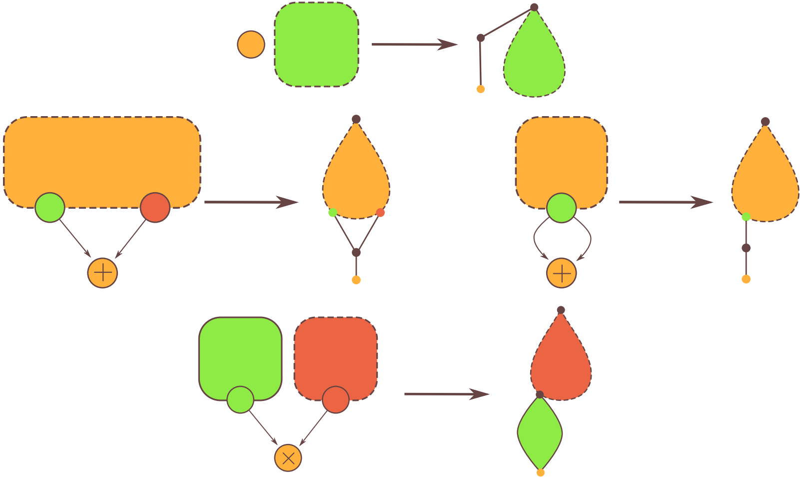
Constructions



Constructions

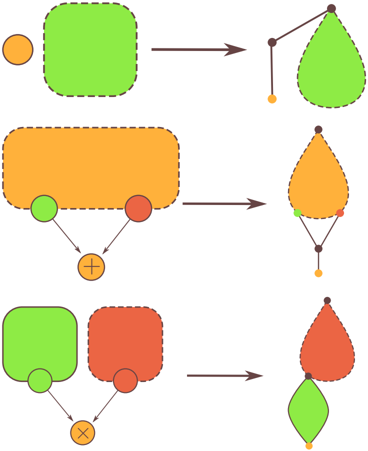


Constructions



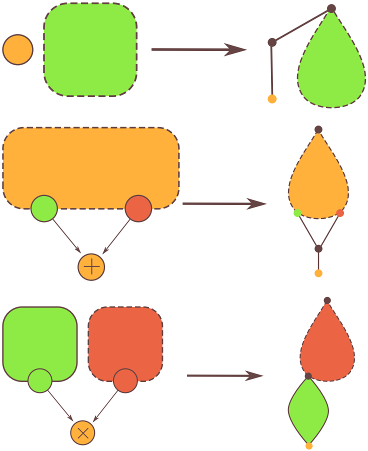
Invariants in the case of weakly-skew circuits

- For each reusable α, there exists t_α s.t.



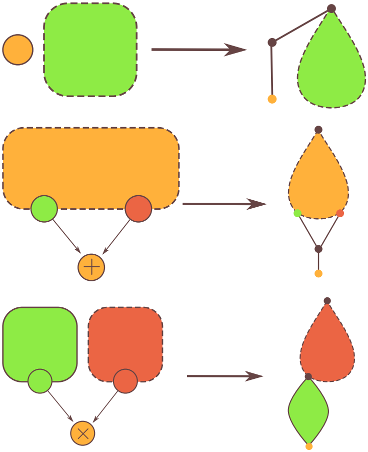
Invariants in the case of weakly-skew circuits

- For each reusable α, there exists t_α s.t.
  - $\varphi_\alpha = \sum_{\substack{\text{acceptable} \\ s\text{-}t_\alpha\text{-paths } P}} (-1)^{\frac{|P|-1}{2}} w(P)$



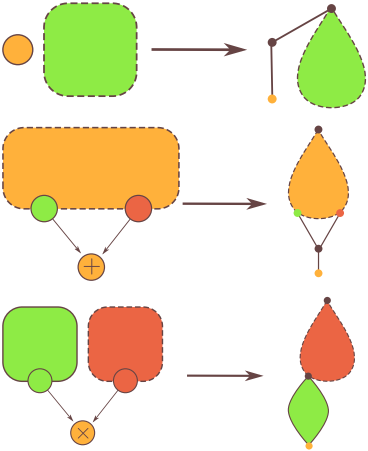
Invariants in the case of weakly-skew circuits

- For each reusable α, there exists t_α s.t.
  - $\varphi_\alpha = \sum_{\substack{\text{acceptable} \\ s\text{-}t_\alpha\text{-paths } P}} (-1)^{\frac{|P|-1}{2}} w(P)$
  - Every s-t_α-path is odd



Invariants in the case of weakly-skew circuits

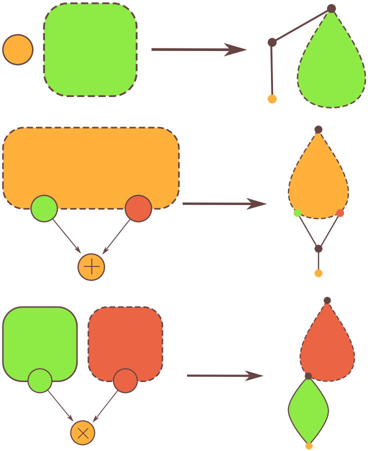
- For each reusable α, there exists t_α s.t.
  - $$\varphi_\alpha = \sum_{\substack{\text{acceptable} \\ s\text{-}t_\alpha\text{-paths } P}} (-1)^{\frac{|P|-1}{2}} w(P)$$
  - Every s-t_α-path is odd
  - For a s-t_α-path P, $G \setminus P$ is either empty or has a unique cycle cover



Invariants in the case of weakly-skew circuits

- For each reusable α, there exists t_α s.t.
  - $\varphi_\alpha = \sum_{\substack{\text{acceptable} \\ s\text{-}t_\alpha\text{-paths } P}} (-1)^{\frac{|P|-1}{2}} w(P)$
  - Every s-t_α-path is odd
  - For a s-t_α-path P, $G \setminus P$ is either empty or has a unique cycle cover

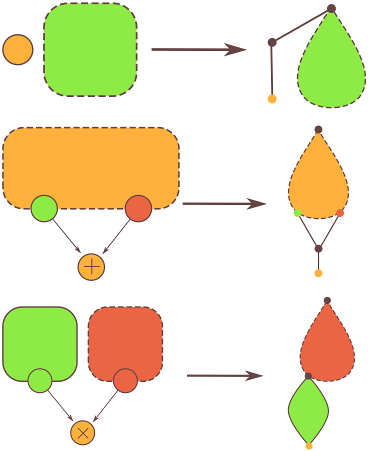
⇝ Perfect matching of weight 1



Invariants in the case of weakly-skew circuits

- For each reusable α, there exists t_α s.t.
  - $$\varphi_\alpha = \sum_{\substack{\text{acceptable} \\ s\text{-}t_\alpha\text{-paths } P}} (-1)^{\frac{|P|-1}{2}} w(P)$$
  - Every s-t_α-path is odd
  - For a s-t_α-path P, $G \setminus P$ is either empty or has a unique cycle cover

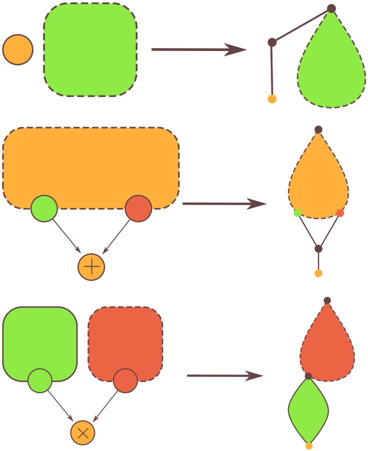
  ⇝ Perfect matching of weight 1
- $|G|$ is odd, every cycle in G is even



Invariants in the case of weakly-skew circuits

- For each reusable α, there exists t_α s.t.
  - $\varphi_\alpha = \sum_{\substack{\text{acceptable} \\ s\text{-}t_\alpha\text{-paths } P}} (-1)^{\frac{|P|-1}{2}} w(P)$
  - Every s-t_α-path is odd
  - For a s-t_α-path P, $G \setminus P$ is either empty or has a unique cycle cover

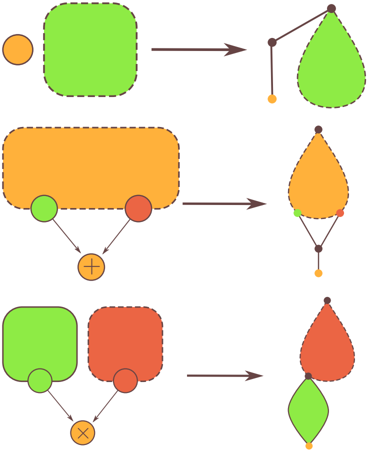
  $\rightsquigarrow$ Perfect matching of weight 1
- $|G|$ is odd, every cycle in G is even
- $G \setminus \{s\}$ is either empty or has a unique cycle cover



Invariants in the case of weakly-skew circuits

- For each reusable α, there exists t_α s.t.
  - $\varphi_\alpha = \sum_{\substack{\text{acceptable} \\ s\text{-}t_\alpha\text{-paths } P}} (-1)^{\frac{|P|-1}{2}} w(P)$
  - Every s-t_α-path is odd
  - For a s-t_α-path P, $G \setminus P$ is either empty or has a unique cycle cover
  - $\rightsquigarrow$ Perfect matching of weight 1
- $|G|$ is odd, every cycle in G is even
- $G \setminus \{s\}$ is either empty or has a unique cycle cover

$\rightsquigarrow$ Perfect matching of weight 1



From G to G'

- Add an edge between s and t, of weight $\frac{1}{2}(-1)^{\frac{|G|-1}{2}} \rightsquigarrow G'$.

From G to G'

- Add an edge between s and t, of weight $\frac{1}{2}(-1)^{\frac{|G|-1}{2}} \rightsquigarrow G'$.
- $|G' \setminus \{s,t\}|$ is odd, cycles are even: no cycle cover with $s \leftrightarrow t$.

From G to G'

- Add an edge between s and t, of weight $\frac{1}{2}(-1)^{\frac{|G|-1}{2}} \rightsquigarrow G'$.
- $|G' \setminus \{s,t\}|$ is odd, cycles are even: no cycle cover with $s \leftrightarrow t$.
- As for every path P, $G' \setminus P$ has an only cycle cover, of weight 1:

From G to G'

- Add an edge between s and t, of weight $\frac{1}{2}(-1)^{\frac{|G|-1}{2}} \rightsquigarrow G'$.
- $|G' \setminus \{s,t\}|$ is odd, cycles are even: no cycle cover with $s \leftrightarrow t$.
- As for every path P, $G' \setminus P$ has an only cycle cover, of weight 1:
  Cycle covers of $G' \iff s \to t$-paths in $G \iff t \to s$-paths in G.

From G to G'

- Add an edge between s and t, of weight $\frac{1}{2}(-1)^{\frac{|G|-1}{2}} \rightsquigarrow G'$.
- $|G' \setminus \{s,t\}|$ is odd, cycles are even: no cycle cover with $s \leftrightarrow t$.
- As for every path P, $G' \setminus P$ has an only cycle cover, of weight 1:
  Cycle covers of $G' \iff s \to t$-paths in $G \iff t \to s$-paths in G.
- With some sign considerations, we get:

From G to G'

- Add an edge between s and t, of weight $\frac{1}{2}(-1)^{\frac{|G|-1}{2}} \rightsquigarrow G'$.
- $|G' \setminus \{s,t\}|$ is odd, cycles are even: no cycle cover with $s \leftrightarrow t$.
- As for every path P, $G' \setminus P$ has an only cycle cover, of weight 1:
  Cycle covers of $G' \iff s \to t$-paths in $G \iff t \to s$-paths in G.
- With some sign considerations, we get:

Theorem

For a weakly skew circuit of size e, with i input variables, computing a polynomial φ, this construction yields a graph G' with $2(e+i)+1$ vertices. The adjacency matrix of G' has its determinant equal to φ.

Outline

1. From polynomials to determinants
2. From polynomials to determinants of symmetric matrices
3. Characteristic 2

Introduction

- Scalar $1/2$ in the constructions $\implies$ not valid for characteristic 2

Introduction

- Scalar $1/2$ in the constructions $\implies$ not valid for characteristic 2
- Very special case: cycles of length > 2 are counted twice

Introduction

- Scalar $1/2$ in the constructions $\implies$ not valid for characteristic 2
- Very special case: cycles of length > 2 are counted twice

  $\implies$ permutations restricted to pairs and singleton

Introduction

- Scalar $1/2$ in the constructions $\implies$ not valid for characteristic 2
- Very special case: cycles of length > 2 are counted twice

  $\implies$ permutations restricted to pairs and singleton

  $\implies$ cycle covers replaced by monomer-dimer covers

Introduction

- Scalar $1/2$ in the constructions $\implies$ not valid for characteristic 2
- Very special case: cycles of length > 2 are counted twice

  $\implies$ permutations restricted to pairs and singleton

  $\implies$ cycle covers replaced by monomer-dimer covers

Which polynomials can be represented as determinant of symmetric matrices in characteristic 2?

A positive result

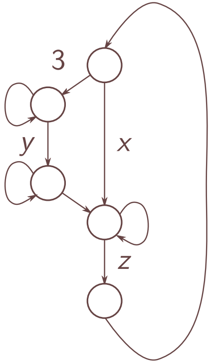
Theorem

Let p be a polynomial, represented by a weakly-skew circuit of size e with i input variables. Then there exists a symmetric matrix A of size $2(e+i)+2$ such that $p^2 = \det A$.

A positive result

Theorem

Let p be a polynomial, represented by a weakly-skew circuit of size e with i input variables. Then there exists a symmetric matrix A of size $2(e+i)+2$ *such that* $p^2 = \det A$.

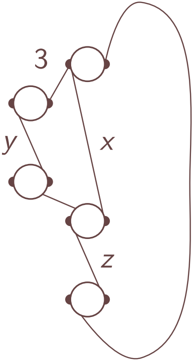


- Toda-Malod's construction

A positive result

Theorem

Let p be a polynomial, represented by a weakly-skew circuit of size e with i input variables. Then there exists a symmetric matrix A of size $2(e+i)+2$ such that $p^2 = \det A$.

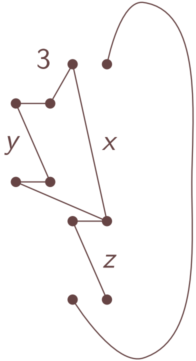


- Toda-Malod's construction
- Undirected graph G':
  - $v \in V \rightsquigarrow v_s$ and v_t.

A positive result

Theorem

Let p be a polynomial, represented by a weakly-skew circuit of size e with i input variables. Then there exists a symmetric matrix A of size $2(e+i)+2$ *such that* $p^2 = \det A$.

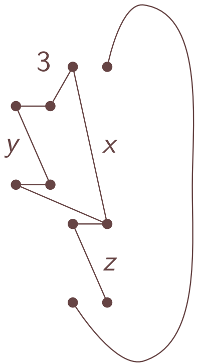


- Toda-Malod's construction
- Undirected graph G':
  - $v \in V \rightsquigarrow v_s$ and v_t.
  - $(u, v) \rightsquigarrow \{u_s, v_t\}$.

A positive result

Theorem

Let p be a polynomial, represented by a weakly-skew circuit of size e with i input variables. Then there exists a symmetric matrix A of size $2(e+i)+2$ such that $p^2 = \det A$.

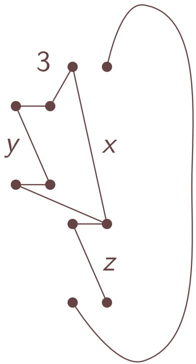


- Toda-Malod's construction
- Undirected graph G':
  - $v \in V \rightsquigarrow v_s$ and v_t.
  - $(u,v) \rightsquigarrow \{u_s, v_t\}$.
- Cycle Covers in $G \iff$ Perfect Matching in G'

A positive result

Theorem

Let p be a polynomial, represented by a weakly-skew circuit of size e with i input variables. Then there exists a symmetric matrix A of size $2(e+i)+2$ such that $p^2 = \det A$.



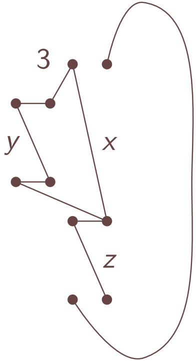
- Toda-Malod's construction
- Undirected graph G':
  - $v \in V \rightsquigarrow v_s$ and v_t.
  - $(u, v) \rightsquigarrow \{u_s, v_t\}$.
- Cycle Covers in $G \iff$ Perfect Matching in G'

$\rightsquigarrow \det M_G = \sum_\mu w(\mu)$

A positive result

Theorem

Let p be a polynomial, represented by a weakly-skew circuit of size e with i input variables. Then there exists a symmetric matrix A of size $2(e+i)+2$ such that $p^2 = \det A$.



- Toda-Malod's construction
- Undirected graph G':
  - $v \in V \rightsquigarrow v_s$ and v_t.
  - $(u, v) \rightsquigarrow \{u_s, v_t\}$.
- Cycle Covers in $G \iff$ Perfect Matching in G'

$\rightsquigarrow$ $\det M_G = \sum_\mu w(\mu)$

- $\det M_{G'} = \sum_\mu w(\mu)^2 = \left(\sum_\mu w(\mu)\right)^2$

A negative result

Theorem (G., Monteil, Thomassé)

If there exists a symmetric matrix A such that $p = \det A$, then $p \bmod \langle x^2+\epsilon_x, y^2+\epsilon_y, z^2+\epsilon_z\rangle$ can be written as a product of degree-1 polynomials.

A negative result

Theorem (G., Monteil, Thomassé)

If there exists a symmetric matrix A such that $p = \det A$, then $p \bmod \langle x^2 + \epsilon_x, y^2 + \epsilon_y, z^2 + \epsilon_z \rangle$ can be written as a product of degree-1 polynomials.

Conjecture

This is not sufficient.

A negative result

Theorem (G., Monteil, Thomassé)

If there exists a symmetric matrix A such that $p = \det A$, then $p \bmod \langle x^2 + \epsilon_x, y^2 + \epsilon_y, z^2 + \epsilon_z \rangle$ can be written as a product of degree-1 polynomials.

Conjecture

This is not sufficient.

- Example: $xy + z$ has no symmetric determinantal representation.

A negative result

Theorem (G., Monteil, Thomassé)

If there exists a symmetric matrix A such that $p = \det A$, then $p \bmod \langle x^2+\epsilon_x, y^2+\epsilon_y, z^2+\epsilon_z\rangle$ can be written as a product of degree-1 polynomials.

Conjecture

This is not sufficient.

- Example: $xy+z$ has no symmetric determinantal representation.
- Conjecture: nor does $xy^2+yz^2+zx^2$.

A negative result

Theorem (G., Monteil, Thomassé)

If there exists a symmetric matrix A such that $p = \det A$, then $p \bmod \langle x^2 + \epsilon_x, y^2 + \epsilon_y, z^2 + \epsilon_z \rangle$ can be written as a product of degree-1 polynomials.

Conjecture

This is not sufficient.

- Example: $xy + z$ has no symmetric determinantal representation.
- Conjecture: nor does $xy^2 + yz^2 + zx^2$.
- Characterization?

Sketch of a proof

- Quotient: no variable outside the diagonal

Sketch of a proof

- Quotient: no variable outside the diagonal
  - If $A_{ij} = A_{ji} = p(x)$, then "$p(x)^2 \in \det A$" and "$p(x) \notin \det A$"

Sketch of a proof

- Quotient: no variable outside the diagonal
  - If $A_{ij} = A_{ji} = p(x)$, then "$p(x)^2 \in \det A$" and "$p(x) \notin \det A$"
  - But $p(x)^2 \equiv \lambda \in \mathbb{F}$.

Sketch of a proof

- Quotient: no variable outside the diagonal
  - If $A_{ij} = A_{ji} = p(x)$, then "$p(x)^2 \in \det A$" and "$p(x) \notin \det A$"
  - But $p(x)^2 \equiv \lambda \in \mathbb{F}$.
- Operations on rows and columns:

Sketch of a proof

- Quotient: no variable outside the diagonal
  - If $A_{ij} = A_{ji} = p(x)$, then "$p(x)^2 \in \det A$" and "$p(x) \notin \det A$"
  - But $p(x)^2 \equiv \lambda \in \mathbb{F}$.
- Operations on rows and columns:
  - Determinant unchanged

Sketch of a proof

- Quotient: no variable outside the diagonal
  - If $A_{ij} = A_{ji} = p(x)$, then "$p(x)^2 \in \det A$" and "$p(x) \notin \det A$"
  - But $p(x)^2 \equiv \lambda \in \mathbb{F}$.
- Operations on rows and columns:
  - Determinant unchanged
  - Coefficients remains linear polynomials

Sketch of a proof

- Quotient: no variable outside the diagonal
  - If $A_{ij} = A_{ji} = p(x)$, then "$p(x)^2 \in \det A$" and "$p(x) \notin \det A$"
  - But $p(x)^2 \equiv \lambda \in \mathbb{F}$.
- Operations on rows and columns:
  - Determinant unchanged
  - Coefficients remains linear polynomials
  - The matrix becomes diagonal

Application

- These results raise the question:

Application

- These results raise the question:

If p^2 has a small (weakly-skew) circuit, what about p?

Application

- These results raise the question:

If p^2 has a small (weakly-skew) circuit, what about p?

If f is a family of polynomials s.t. $f^2 \in \mathrm{VP}$ ($\mathrm{VP}_{\mathrm{ws}}$), does f belong to VP ($\mathrm{VP}_{\mathrm{ws}}$)?

Application

- These results raise the question:

If p^2 has a small (weakly-skew) circuit, what about p?

If f is a family of polynomials s.t. $f^2 \in \mathsf{VP}$ ($\mathsf{VP}_{\mathsf{ws}}$), does f belong to VP ($\mathsf{VP}_{\mathsf{ws}}$)?

- It appears to be related to an open problem of Bürgisser:

Application

- These results raise the question:

If p^2 has a small (weakly-skew) circuit, what about p?

If f is a family of polynomials s.t. $f^2 \in \mathsf{VP}$ ($\mathsf{VP}_{\mathsf{ws}}$), does f belong to VP ($\mathsf{VP}_{\mathsf{ws}}$)?

- It appears to be related to an open problem of Bürgisser:

Is the partial permanent VNP-complete in characteristic 2?

Valiant's classes

- Complexity of a polynomial: size of the smallest circuit computing it.

Valiant's classes

- Complexity of a polynomial: size of the smallest circuit computing it.

Definition

A family (f_n) of polynomials is in VP if for all n, the number of variables, the degree, and the complexity of f_n are polynomially bounded in n.

Valiant's classes

- Complexity of a polynomial: size of the smallest circuit computing it.

Definition

A family (f_n) of polynomials is in VP if for all n, the number of variables, the degree, and the complexity of f_n are polynomially bounded in n.

A family (f_n) of polynomials is in VNP if there exists a family $(g_n(y_1, \dots, y_{v(n)})) \in \mathrm{VP}$ s.t.

$$f_n(x_1, \dots, x_{u(n)}) = \sum_{\bar{\epsilon} \in \{0,1\}^{v(n)-u(n)}} g_n(x_1, \dots, x_{u(n)}, \bar{\epsilon}).$$

Valiant's classes

- Complexity of a polynomial: size of the smallest circuit computing it.

Definition

A family (f_n) of polynomials is in VP if for all n, the number of variables, the degree, and the complexity of f_n are polynomially bounded in n.

A family (f_n) of polynomials is in VNP if there exists a family $(g_n(y_1,\dots,y_{v(n)})) \in \mathrm{VP}$ s.t.

$$f_n(x_1,\dots,x_{u(n)}) = \sum_{\bar\epsilon\in\{0,1\}^{v(n)-u(n)}} g_n(x_1,\dots,x_{u(n)},\bar\epsilon).$$

- $(\mathrm{DET}_n) \in \mathrm{VP}$, $(\mathrm{PER}_n) \in \mathrm{VNP}$, ...

VNP-completeness

Definition

A family (g_n) is a p-projection of a family (f_n) is there exists a polynomial t s.t. for all n, $g_n(\bar{x}) = f_{t(n)}(a_1, \dots, a_n)$, with $a_1, \dots, a_n \in \mathbb{K} \cup \{x_1, \dots, x_n\}$.

VNP-completeness

Definition

A family (g_n) is a p-projection of a family (f_n) is there exists a polynomial t s.t. for all n, $g_n(\bar{x}) = f_{t(n)}(a_1, \ldots, a_n)$, with $a_1, \ldots, a_n \in \mathbb{K} \cup \{x_1, \ldots, x_n\}$.

A family $(f_n) \in$ VNP is VNP-complete if every family in VNP is a p-projection of (f_n).

VNP-completeness

Definition

A family (g_n) is a p-projection of a family (f_n) is there exists a polynomial t s.t. for all n, $g_n(\bar{x}) = f_{t(n)}(a_1, \ldots, a_n)$, with $a_1, \ldots, a_n \in \mathbb{K} \cup \{x_1, \ldots, x_n\}$.

A family $(f_n) \in \mathrm{VNP}$ is VNP-complete if every family in VNP is a p-projection of (f_n).

- (PER_n) is VNP-complete in characteristic $\neq 2$

VNP-completeness

Definition

A family (g_n) is a p-projection of a family (f_n) is there exists a polynomial t s.t. for all n, $g_n(\bar{x}) = f_{t(n)}(a_1, \ldots, a_n)$, with $a_1, \ldots, a_n \in \mathbb{K} \cup \{x_1, \ldots, x_n\}$.

A family $(f_n) \in$ VNP is VNP-complete if every family in VNP is a p-projection of (f_n).

- (PER_n) is VNP-complete in characteristic $\neq 2$
- (HC_n) is VNP-complete (in any characteristic)

Partial Permanent

$$\operatorname{per}^* M = \sum_{\pi} \prod_{i \in \operatorname{def}(\pi)} M_{i,\pi(i)}$$

where π ranges over the injective partial maps from $[n]$ to $[n]$.

Partial Permanent

$$\operatorname{per}^* M = \sum_{\pi} \prod_{i \in \operatorname{def}(\pi)} M_{i,\pi(i)}$$

where π ranges over the injective partial maps from $[n]$ to $[n]$.

Lemma

Let $G = K_{n,n}$. Let A and B be the respective adjacency and biadjacency matrices of G. Then in characteristic 2,

$$\det(A + I_{2n}) = (\operatorname{per}^* B)^2$$

where I_{2n} is the identity matrix.

Partial Permanent

$$\operatorname{per}^* M = \sum_{\pi} \prod_{i \in \operatorname{def}(\pi)} M_{i,\pi(i)}$$

where π ranges over the injective partial maps from $[n]$ to $[n]$.

Lemma

Let $G = K_{n,n}$. Let A and B be the respective adjacency and biadjacency matrices of G. Then in characteristic 2,

$$\det(A + I_{2n}) = (\operatorname{per}^* B)^2$$

where I_{2n} is the identity matrix.

Same kind of ideas as the previous proof.

Partial permanents as family of polynomials

(PER_n^*): family of polynomials defined as partial permanents of $n \times n$ matrices of indeterminates.

Partial permanents as family of polynomials

(PER_n^*): family of polynomials defined as partial permanents of $n \times n$ matrices of indeterminates.

($(\mathrm{PER}^*)_n^2$): family of polynomials defined as square of partial permanents of $n \times n$ matrices of indeterminates.

Partial permanents as family of polynomials

(PER^*_n): family of polynomials defined as partial permanents of $n \times n$ matrices of indeterminates.

$((\mathrm{PER}^*)^2_n)$: family of polynomials defined as square of partial permanents of $n \times n$ matrices of indeterminates.

Theorem

$((\mathrm{PER}^*)^2_n) \in \mathrm{VP}$ *in characteristic* 2.

Partial permanents as family of polynomials

(PER^*_n): family of polynomials defined as partial permanents of $n \times n$ matrices of indeterminates.

$((\mathrm{PER}^*)^2_n)$: family of polynomials defined as square of partial permanents of $n \times n$ matrices of indeterminates.

Theorem

$((\mathrm{PER}^*)^2_n) \in \mathrm{VP}$ *in characteristic* 2.

Proof. $((\mathrm{PER}^*)^2_n)$ is a p-projection of (DET_n).

Answer to Bürgisser's problem

Problem

Is the partial permanent VNP-complete in characteristic 2?

Answer to Bürgisser's problem

Problem

Is the partial permanent VNP-complete in characteristic 2?

Theorem

If it is the case, $\oplus\mathrm{P}/\mathrm{poly} = \mathrm{NC}^2/\mathrm{poly}$, *and* $\mathrm{PH} = \Sigma_2$.

Answer to Bürgisser's problem

Problem

Is the partial permanent VNP-complete in characteristic 2?

Theorem

If it is the case, $\oplus\mathsf{P}/\mathsf{poly} = \mathsf{NC}^2/\mathsf{poly}$, *and* $\mathsf{PH} = \Sigma_2$.

Proof sketch. If the case arises,

Answer to Bürgisser's problem

Problem

Is the partial permanent VNP-complete in characteristic 2?

Theorem

If it is the case, $\oplus\mathsf{P}/\mathrm{poly} = \mathsf{NC}^2/\mathrm{poly}$*, and* $\mathsf{PH} = \Sigma_2$*.*

Proof sketch. If the case arises,

- $\mathsf{VNP}^2 \subseteq \mathsf{VP}$, thus $BP(\mathsf{VP}) = BP(\mathsf{VNP})$ (Bürgisser's boolean part)

Answer to Bürgisser's problem

Problem

Is the partial permanent VNP-complete in characteristic 2?

Theorem

If it is the case, $\oplus\mathsf{P}/\text{poly} = \mathsf{NC}^2/\text{poly}$, *and* $\mathsf{PH} = \Sigma_2$.

Proof sketch. If the case arises,

- $\mathsf{VNP}^2 \subseteq \mathsf{VP}$, thus $BP(\mathsf{VP}) = BP(\mathsf{VNP})$ (Bürgisser's boolean part)
- Bürgisser: $\oplus\mathsf{P}/\text{poly} = BP(\mathsf{VNP})$ $\quad BP(VP) \subseteq \mathsf{NC}^2/\text{poly}$

Answer to Bürgisser's problem

Problem

Is the partial permanent VNP-complete in characteristic 2?

Theorem

If it is the case, $\oplus\mathsf{P}/\mathsf{poly} = \mathsf{NC}^2/\mathsf{poly}$, *and* $\mathsf{PH} = \Sigma_2$.

Proof sketch. If the case arises,

- $\mathsf{VNP}^2 \subseteq \mathsf{VP}$, thus $BP(\mathsf{VP}) = BP(\mathsf{VNP})$ (Bürgisser's boolean part)
- Bürgisser: $\oplus\mathsf{P}/\mathsf{poly} = BP(\mathsf{VNP})$ $BP(VP) \subseteq \mathsf{NC}^2/\mathsf{poly}$
- Karp-Lipton Theorem

Conclusion

- We obtained Symmetric Determinantal Representations for Formulas and Weakly-Skew Circuits of linear size

Conclusion

- We obtained Symmetric Determinantal Representations for Formulas and Weakly-Skew Circuits of linear size
- Improvement of Valiant's and Malod's constructions

Conclusion

- We obtained Symmetric Determinantal Representations for Formulas and Weakly-Skew Circuits of linear size
- Improvement of Valiant's and Malod's constructions
- By-product (in characteristic $\neq 2$):

Conclusion

- We obtained Symmetric Determinantal Representations for Formulas and Weakly-Skew Circuits of linear size
- Improvement of Valiant's and Malod's constructions
- By-product (in characteristic $\neq 2$):

Theorem

Let M be an $n \times n$ matrix. Then there exists a symmetric matrix M' of size $O(n^5)$ s.t. $\det M = \det M'$.

Conclusion

- We obtained Symmetric Determinantal Representations for Formulas and Weakly-Skew Circuits of linear size
- Improvement of Valiant's and Malod's constructions
- By-product (in characteristic $\neq 2$):

Theorem

Let M be an $n \times n$ matrix. Then there exists a symmetric matrix M' of size $O(n^5)$ s.t. $\det M = \det M'$.

- For characteristic 2:

Conclusion

- We obtained Symmetric Determinantal Representations for Formulas and Weakly-Skew Circuits of linear size
- Improvement of Valiant's and Malod's constructions
- By-product (in characteristic $\neq 2$):

Theorem

Let M be an $n \times n$ matrix. Then there exists a symmetric matrix M' of size $O(n^5)$ s.t. $\det M = \det M'$.

- For characteristic 2:
  - Answer to Bürgisser's Open Problem

Conclusion

- We obtained Symmetric Determinantal Representations for Formulas and Weakly-Skew Circuits of linear size
- Improvement of Valiant's and Malod's constructions
- By-product (in characteristic $\neq 2$):

Theorem

Let M be an $n \times n$ matrix. Then there exists a symmetric matrix M' of size $O(n^5)$ s.t. $\det M = \det M'$.

- For characteristic 2:
  - Answer to Bürgisser's Open Problem
  - Proof of a negative result

Future work

- In Convex Geometry: $\mathbb{K} = \mathbb{R}$ and polynomials are *real zero polynomials*.

Future work

- In Convex Geometry: $\mathbb{K} = \mathbb{R}$ and polynomials are *real zero polynomials*.

$\rightsquigarrow$ what can be done in that precise case?

Future work

- In Convex Geometry: $\mathbb{K} = \mathbb{R}$ and polynomials are *real zero polynomials*.

$\rightsquigarrow$ what can be done in that precise case?

- Characterize polynomials with a symmetric determinantal representation in characteristic 2.

Future work

- In Convex Geometry: $\mathbb{K} = \mathbb{R}$ and polynomials are *real zero polynomials*.

$\rightsquigarrow$ what can be done in that precise case?

- Characterize polynomials with a symmetric determinantal representation in characteristic 2.
- Symmetric matrices in Valiant's theory?

Thank you!