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.

Dagstuhl Seminar on Computational Counting – November 30, 2010

The problem

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

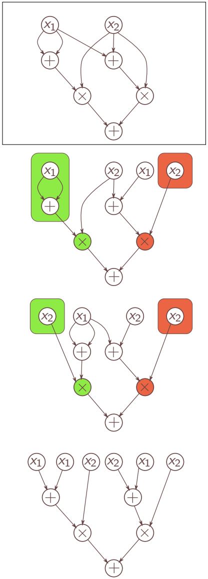
- Formal polynomial

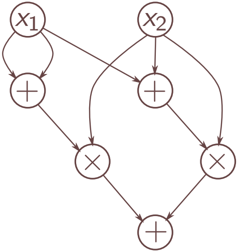
The problem

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

- Formal polynomial
- Smallest possible dimension of the matrix

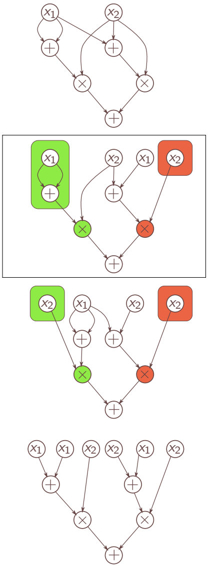
Representations of polynomials

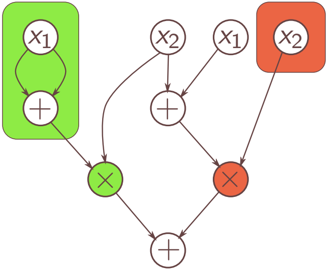




Circuit of size 5

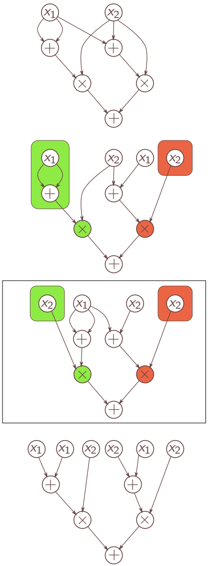
Representations of polynomials

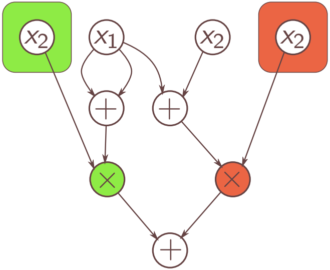




Weakly-skew circuit of size 5

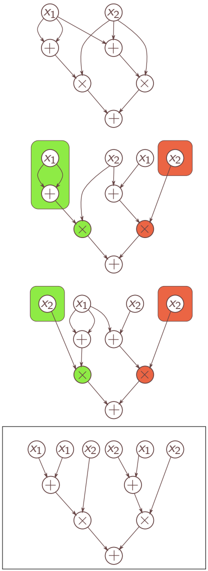
Representations of polynomials

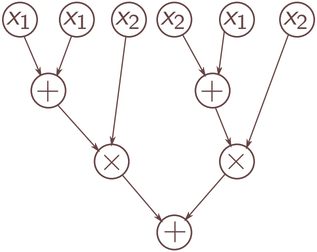




Skew circuit of size 5

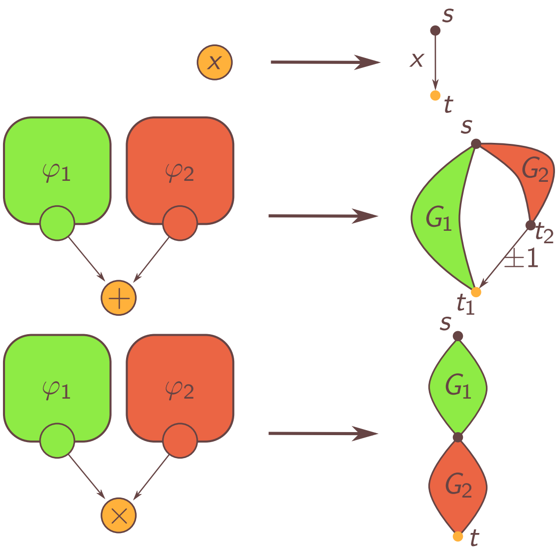
Representations of polynomials





Formula of size 5

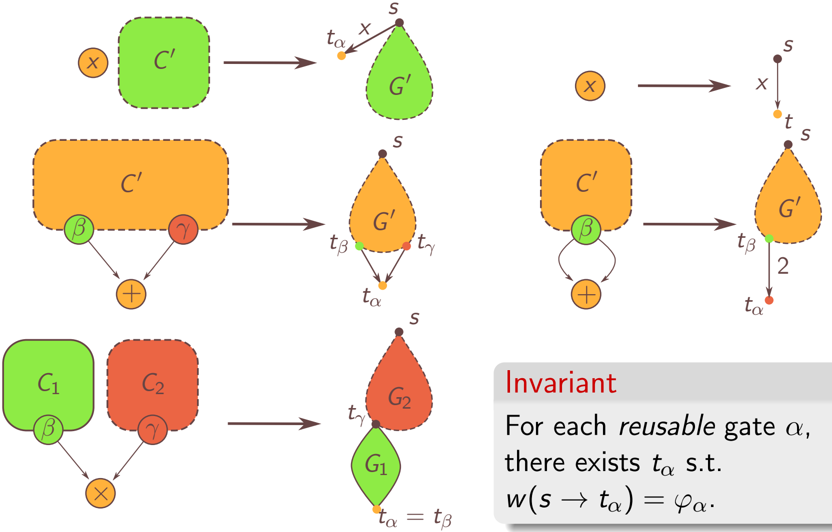
Valiant's construction



Invariant

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

Toda-Malod's construction



Invariant

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

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?

Outline

1. Universality of determinants of symmetric matrices

2. Characteristic 2

Introduction

- Symmetric matrices $\iff$ undirected graphs

Introduction

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

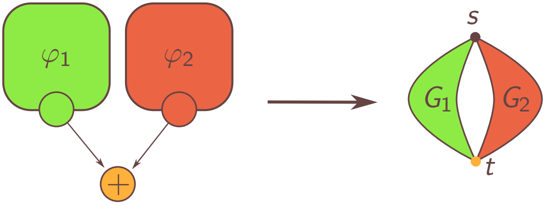
Introduction

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

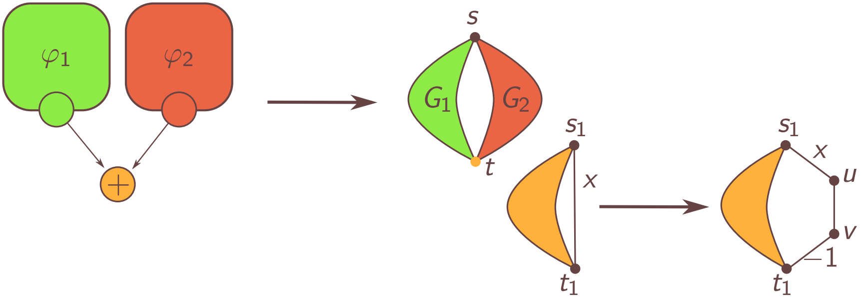
Introduction

- 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

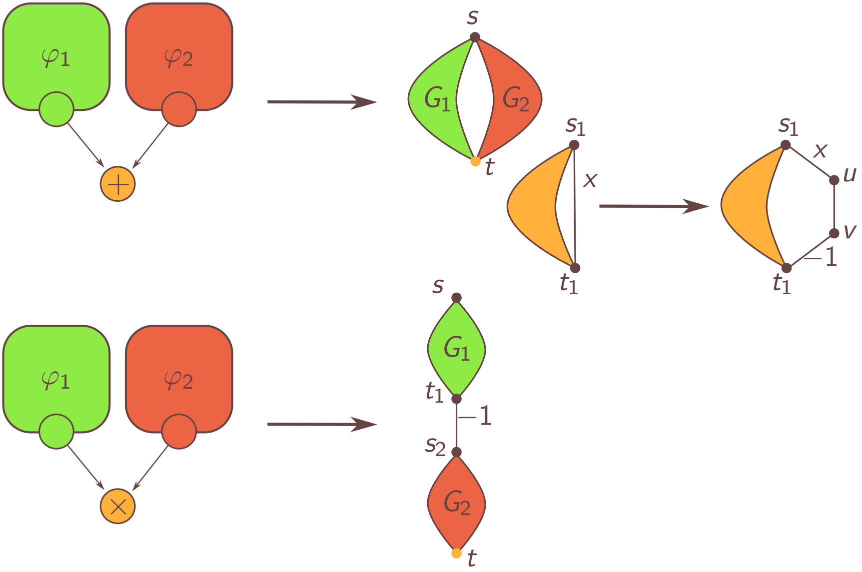
From formulas to symmetric determinants



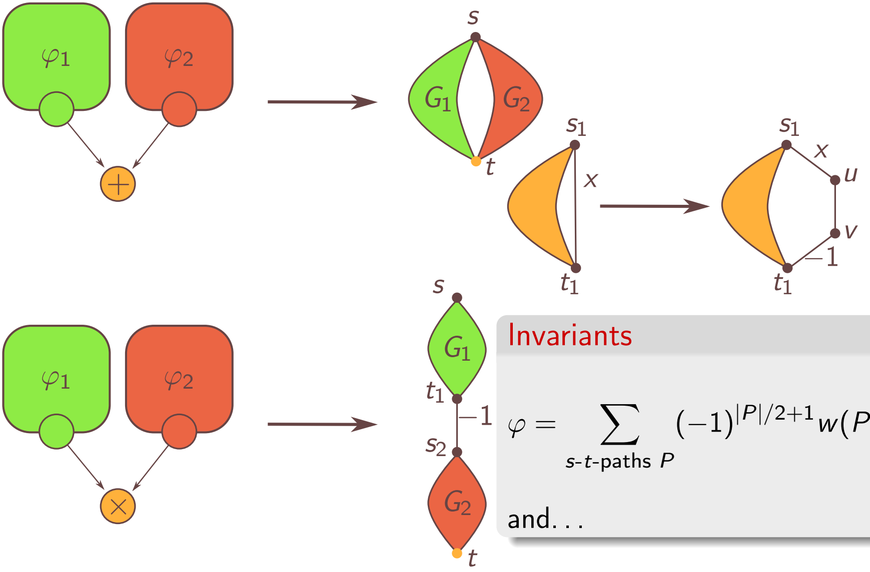
From formulas to symmetric determinants



From formulas to symmetric determinants



From formulas to symmetric determinants



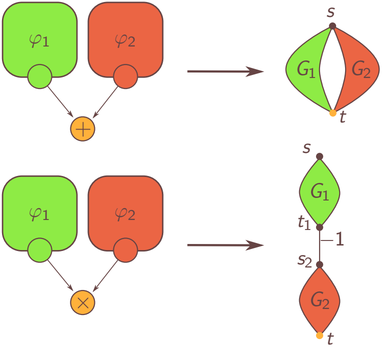
Invariants

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

and...

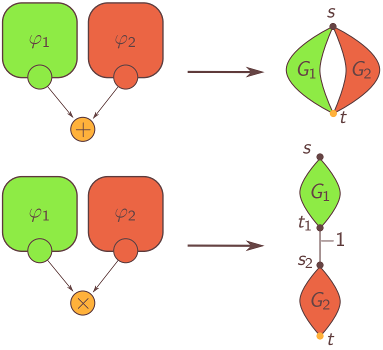
Invariants for formula's construction

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



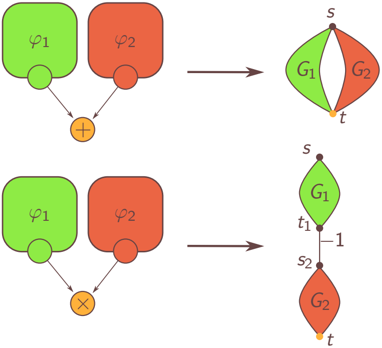
Invariants for formula's construction

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

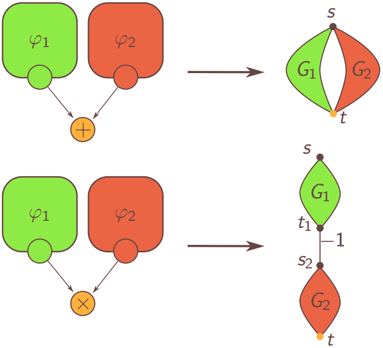


Invariants for formula's construction

Cycle cover = Directed cycle cover!
Edge = Length-2 cycle!

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



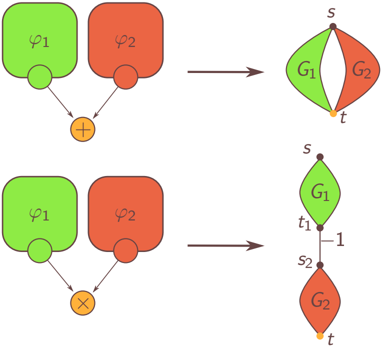
Invariants for formula's construction

⚠ Cycle cover = Directed cycle cover!
Edge = Length-2 cycle!

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

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



Invariants for formula's construction

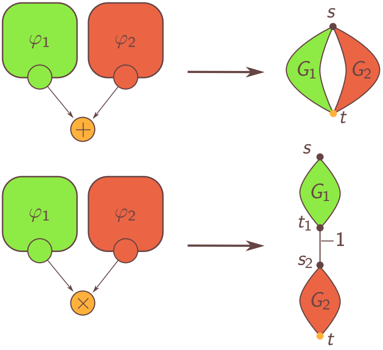
⚠ Cycle cover = Directed cycle cover!
Edge = Length-2 cycle!

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

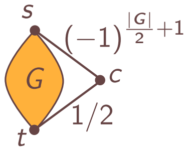
⇝ Perfect matching of weight 1

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

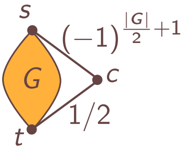
⇝ Perfect matching of weight 1



From G to G'

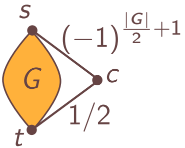


From G to G'



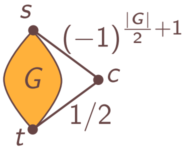
- $|G'|$ is odd: Every odd cycle goes through c.

From G to G'



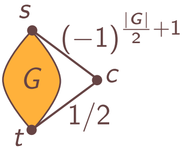
- $|G'|$ is odd: Every odd cycle goes through c.
- Cycle covers in G' $\iff$ $s \to t$-paths in G

From G to G'



- $|G'|$ is odd: Every odd cycle goes through c.
- Cycle covers in G' $\iff$ $s \to t$-paths in G $\iff$ $t \to s$-paths in G

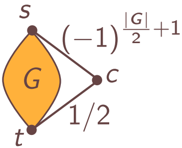
From G to G'



- $|G'|$ is odd: Every odd cycle goes through c.
- Cycle covers in $G' \iff s \to t$-paths in $G \iff t \to s$-paths in G

$$w(s \to t) + w(t \to s) = 2 \times \varphi$$

From G to G'

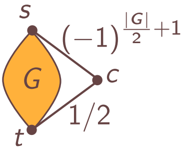


- $|G'|$ is odd: Every odd cycle goes through c.
- Cycle covers in G' $\iff$ $s \to t$-paths in G $\iff$ $t \to s$-paths in G

$$w(s \to t) + w(t \to s) = 2 \times \varphi$$

$\rightsquigarrow$ $\mathrm{char}(\mathbb{K}) \neq 2$

From G to G'



- $|G'|$ is odd: Every odd cycle goes through c.
- Cycle covers in G' $\iff$ $s \to t$-paths in G $\iff$ $t \to s$-paths in G

$$w(s \to t) + w(t \to s) = 2 \times \varphi$$

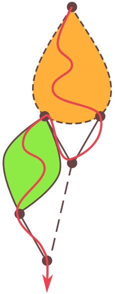
$\rightsquigarrow$ $\mathrm{char}(\mathbb{K}) \neq 2$

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.

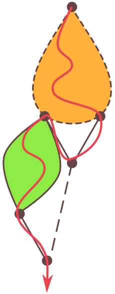
Case of weakly-skew circuits

- Main difficulty:



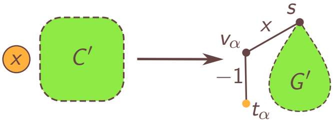
Case of weakly-skew circuits

- Main difficulty:

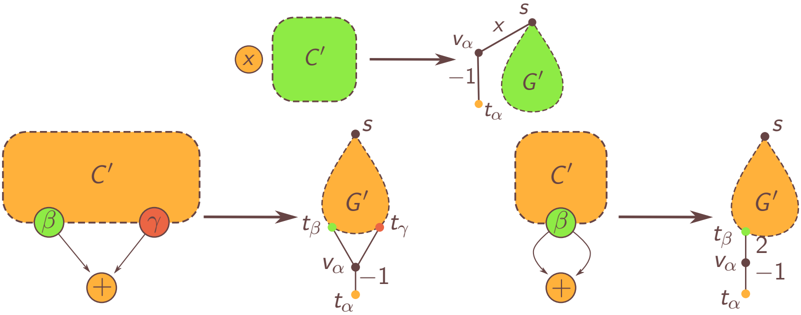


- Definition: A path P is acceptable if $G \setminus P$ admits a cycle cover

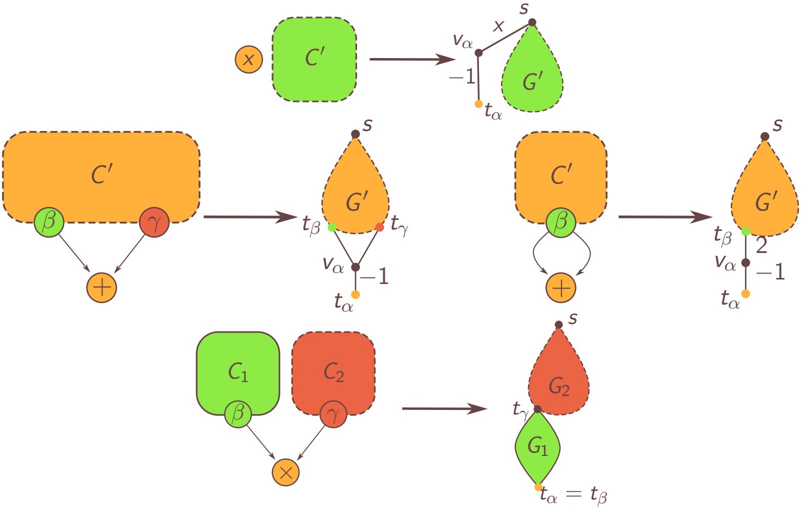
Constructions



Constructions

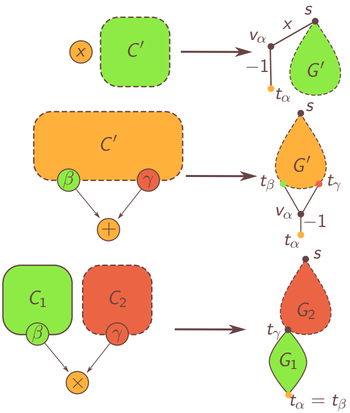


Constructions



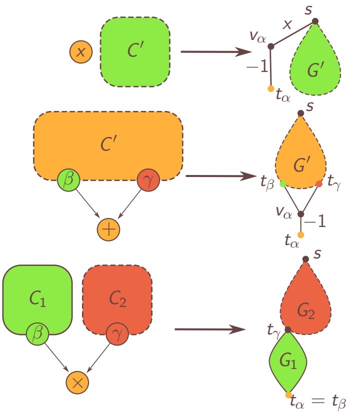
Invariants in the case of weakly-skew circuits

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



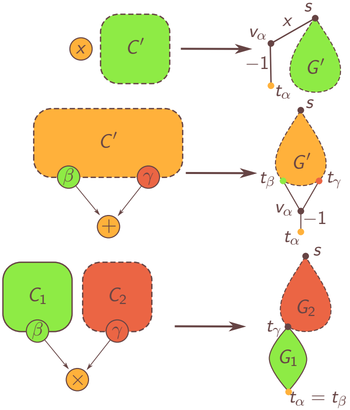
Invariants in the case of weakly-skew circuits

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



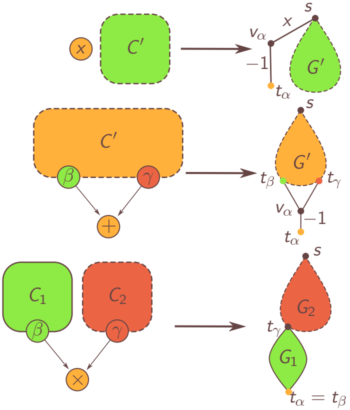
Invariants in the case of weakly-skew circuits

- 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



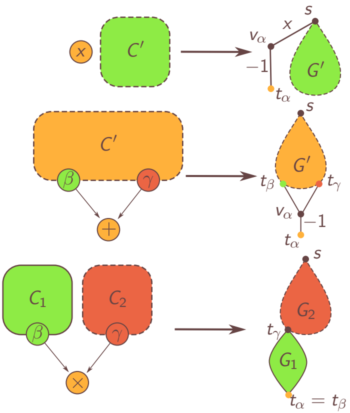
Invariants in the case of weakly-skew circuits

- 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

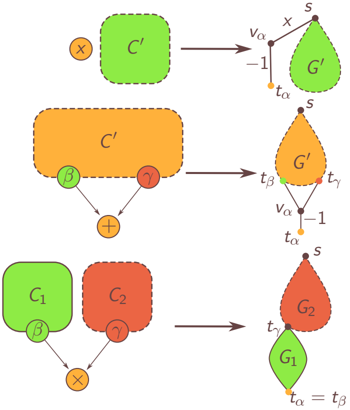
- For each reusable α, there exists t_α s.t.
  - $\varphi_\alpha = \sum_{\substack{\text{acceptable} \\ s\text{-}t_\alpha\text{-paths } P}} (-1)^{\frac{|P|-1}{2}} w(P)$
  - Every s-t_α-path is odd
  - For a s-t_α-path P, $G \setminus P$ is either empty or has a unique cycle cover
  - ⇝ Perfect matching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

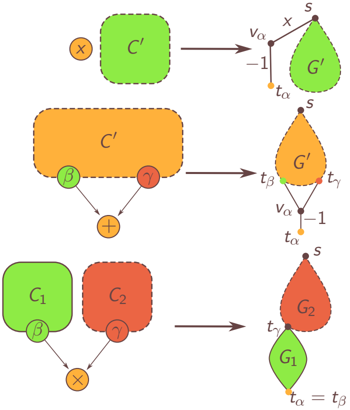
  ⇝ Perfect matching of weight 1
- $|G|$ is odd, every cycle in G is even



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

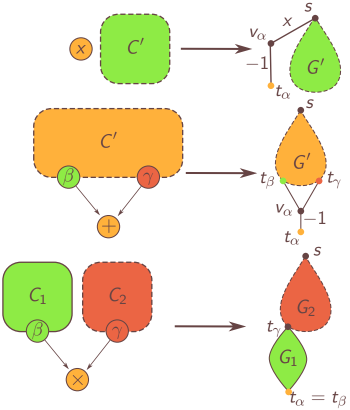
  ⇝ Perfect matching of weight 1
- $|G|$ is odd, every cycle in G is even
- $G \setminus \{s\}$ is either empty or has a unique cycle cover



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 $s \xleftrightarrow{(1/2)\cdot(-1)^{\frac{|G|-1}{2}}} t$: new graph G'.

From G to G'

- Add $s \xleftrightarrow{(1/2)\cdot(-1)^{\frac{|G|-1}{2}}} t$: new graph G'.
- $|G' \setminus \{s,t\}|$ is odd, cycles are even: no cycle cover with $s \leftrightarrow t$.

From G to G'

- Add $s \xleftrightarrow{(1/2)\cdot(-1)^{\frac{|G|-1}{2}}} t$: new graph G'.
- $|G' \setminus \{s,t\}|$ is odd, cycles are even: no cycle cover with $s \leftrightarrow t$.

Cycle covers of $G' \iff s \to t$-paths in $G \iff t \to s$-paths in G.

From G to G'

- Add $s \xleftrightarrow{(1/2)\cdot(-1)^{\frac{|G|-1}{2}}} t$: new graph G'.
- $|G' \setminus \{s,t\}|$ is odd, cycles are even: no cycle cover with $s \leftrightarrow t$.

  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 $s \xleftrightarrow{(1/2)\cdot(-1)^{\frac{|G|-1}{2}}} t$: new graph G'.
- $|G' \setminus \{s,t\}|$ is odd, cycles are even: no cycle cover with $s \leftrightarrow t$.

  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.

Summary

	Formula	Weakly-skew circuit
Non symmetric	$e+1$	$(e+i)+1$
Symmetric	$2e+1$	$2(e+i)+1$

e: size

i: number of input variables

Outline

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 $\Longrightarrow$ not valid for characteristic 2
- Very special case: cycles of length > 2 are counted twice

  $\Longrightarrow$ permutations restricted to pairs and singleton

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

Which polynomials can be represented as determinant of symmetric matrices in 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

  $\implies$ 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?

- $\mathbb{F}$: (finite) field of 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

  $\implies$ 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?

- $\mathbb{F}$: (finite) field of characteristic 2
- Here: Polynomials over $\mathbb{F}[x, y, z]$

A positive result

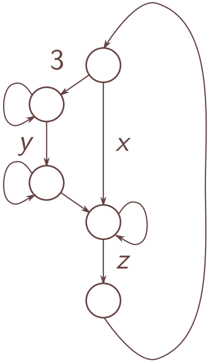
Theorem

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 $p^2 = \det A$.

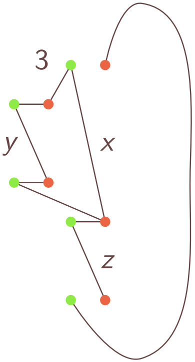


- Toda-Malod's construction

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* $p^2 = \det A$.

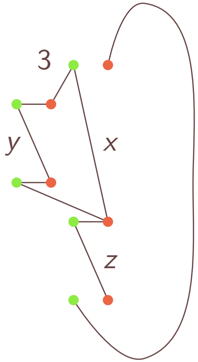


- Toda-Malod's construction
- Undirected graph G':
  - $v \in V \rightsquigarrow v_s$ and v_t .
  - $(u,v) \rightsquigarrow \{u_s, v_t\}$.

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 $p^2 = \det A$.

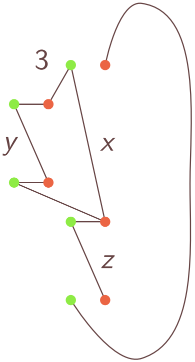


- Toda-Malod's construction
- Undirected graph G':
  - $v \in V \rightsquigarrow v_s$ and v_t .
  - $(u, v) \rightsquigarrow \{u_s, v_t\}$.
- Cycle Covers in $G \iff$ Perfect Matching in G'

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 $p^2 = \det A$.



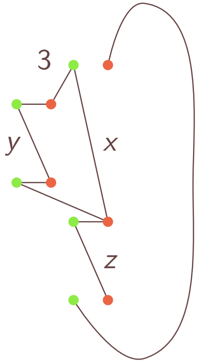
- Toda-Malod's construction
- Undirected graph G':
  - $v \in V \rightsquigarrow v_s$ and v_t .
  - $(u, v) \rightsquigarrow \{u_s, v_t\}$.
- Cycle Covers in $G \iff$ Perfect Matching in G'

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

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 $p \bmod \langle x^2 + \ell_x, y^2 + \ell_y, z^2 + \ell_z \rangle$ is 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* $p \bmod \langle x^2 + \ell_x, y^2 + \ell_y, z^2 + \ell_z \rangle$ *is 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 $p \bmod \langle x^2 + \ell_x, y^2 + \ell_y, z^2 + \ell_z \rangle$ *is 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 $p \bmod \langle x^2 + \ell_x, y^2 + \ell_y, z^2 + \ell_z \rangle$ is 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* $p \bmod \langle x^2 + \ell_x, y^2 + \ell_y, z^2 + \ell_z \rangle$ *is 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

- Modulo: no variable outside the diagonal

Sketch of a proof

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

Sketch of a proof

- Modulo: no variable outside the diagonal
  - If $A_{ij} = A_{ji} = p(x, y, z)$, then "$p^2 \in \det A$" and "$p \notin \det A$"
  - But $p(x, y, z)^2 \equiv \lambda \bmod \langle x^2 + \ell_x, y^2 + \ell_y, z^2 + \ell_z \rangle$, $\lambda \in \mathbb{F}$.

Sketch of a proof

- Modulo: no variable outside the diagonal
  - If $A_{ij} = A_{ji} = p(x, y, z)$, then "$p^2 \in \det A$" and "$p \notin \det A$"
  - But $p(x, y, z)^2 \equiv \lambda \bmod \langle x^2 + \ell_x, y^2 + \ell_y, z^2 + \ell_z \rangle$, $\lambda \in \mathbb{F}$.
- Operations on rows and columns:

Sketch of a proof

- Modulo: no variable outside the diagonal
  - If $A_{ij} = A_{ji} = p(x, y, z)$, then "$p^2 \in \det A$" and "$p \notin \det A$"
  - But $p(x, y, z)^2 \equiv \lambda \bmod \langle x^2 + \ell_x, y^2 + \ell_y, z^2 + \ell_z \rangle$, $\lambda \in \mathbb{F}$.
- Operations on rows and columns:
  - Determinant: unchanged

Sketch of a proof

- Modulo: no variable outside the diagonal
  - If $A_{ij} = A_{ji} = p(x, y, z)$, then "$p^2 \in \det A$" and "$p \notin \det A$"
  - But $p(x, y, z)^2 \equiv \lambda \bmod \langle x^2 + \ell_x, y^2 + \ell_y, z^2 + \ell_z \rangle$, $\lambda \in \mathbb{F}$.
- Operations on rows and columns:
  - Determinant: unchanged
  - Coefficients: linear polynomials

Sketch of a proof

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

Application

- These results raise the questions:

Application

- These results raise the questions:

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

Application

- These results raise the questions:

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 questions:

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 ($\mathrm{VP}_{\mathrm{ws}}$)?

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

Application

- These results raise the questions:

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 ($\mathrm{VP}_{\mathrm{ws}}$)?

- 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.

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, $g_n(\bar{x}) = f_{t(n)}(a_1, \dots, a_m)$, with $a_1, \dots, a_m \in \mathbb{K} \cup \{x_1, \dots, x_n\}$.

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)

Boolean parts

Definition

The boolean part of (f_n) is $bp_f : \{0,1\}^\star \to \{0,1\}$ s.t. for $x \in \{0,1\}^n$, $bp_f(x) = f_n(x)$.

Boolean parts

Definition

The boolean part of (f_n) is $bp_f : \{0,1\}^\star \to \{0,1\}$ s.t. for $x \in \{0,1\}^n$, $bp_f(x) = f_n(x)$.

The boolean part of a class VC is $BP(\mathsf{VC}) = \bigcup_{f \in \mathsf{VC}} bp_f$.

Boolean parts

Definition

The boolean part of (f_n) is $bp_f : \{0,1\}^\star \to \{0,1\}$ s.t. for $x \in \{0,1\}^n$, $bp_f(x) = f_n(x)$.

The boolean part of a class VC is $BP(\mathrm{VC}) = \bigcup_{f \in \mathrm{VC}} bp_f$.

Theorem (Bürgisser)

- $BP(\mathrm{VP}) \subseteq \mathrm{NC}^2/\mathrm{poly}$
- $BP(\mathrm{VNP}) = \oplus\mathrm{P}/\mathrm{poly}$

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.

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

Theorem

$((\mathrm{PER}^*)_n^2) \in \mathrm{VP}$ *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, $\oplus\mathsf{P}/\mathsf{poly} = \mathsf{NC}^2/\mathsf{poly}$, *and* $\mathsf{PH} = \Sigma_2$.

Answer to Bürgisser's problem

Problem

Is the partial permanent VNP-complete in characteristic 2?

Theorem

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

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 $BP(\mathsf{VP}) = BP(\mathsf{VNP})$

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: $\oplus\mathsf{P}/\mathsf{poly} = BP(\mathsf{VNP})$ $\quad BP(VP) \subseteq \mathsf{NC}^2/\mathsf{poly}$

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* $\mathrm{PH} = \Sigma_2$.

Proof sketch. If the case arises,

- $\mathrm{VNP}^2 \subseteq \mathrm{VP}$, thus $BP(\mathrm{VP}) = BP(\mathrm{VNP})$
- Bürgisser: $\oplus\mathrm{P}/\mathrm{poly} = BP(\mathrm{VNP})$ $\quad BP(VP) \subseteq \mathrm{NC}^2/\mathrm{poly}$
- 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

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

Future work

- Convex Geometry: $\mathbb{K} = \mathbb{R}$ and real zero polynomials
  $\rightsquigarrow$ what can be done in that precise case?

Future work

- Convex Geometry: $\mathbb{K} = \mathbb{R}$ and real zero polynomials
  - $\rightsquigarrow$ what can be done in that precise case?
- Characteristic 2:

Future work

- Convex Geometry: $\mathbb{K} = \mathbb{R}$ and real zero polynomials
  $\rightsquigarrow$ what can be done in that precise case?
- Characteristic 2:
  - Characterize polynomials with a symmetric determinantal representation

Future work

- Convex Geometry: $\mathbb{K} = \mathbb{R}$ and real zero polynomials
  $\rightsquigarrow$ what can be done in that precise case?
- Characteristic 2:
  - Characterize polynomials with a symmetric determinantal representation
  - Explore graph polynomials

Future work

- Convex Geometry: $\mathbb{K} = \mathbb{R}$ and real zero polynomials
  $\rightsquigarrow$ what can be done in that precise case?
- Characteristic 2:
  - Characterize polynomials with a symmetric determinantal representation
  - Explore graph polynomials
- Symmetric matrices in Valiant's theory?

Thank you!