

# Representations of polynomials, algorithms and lower bounds



**Bruno Grenet**

ÉNS Lyon & IRMAR (Rennes)

# Introduction

**Polynomials**  
(formal)

# Introduction

## Lists

- ▶ Coefficients  $\rightsquigarrow$  dense
- ▶ Monomials  $\neq 0 \rightsquigarrow$  sparse  
 $\rightsquigarrow$  lacunary

**Polynomials**  
(formal)



# Introduction

## Lists

- ▶ Coefficients  $\rightsquigarrow$  dense
- ▶ Monomials  $\neq 0 \rightsquigarrow$  sparse  
 $\rightsquigarrow$  lacunary

## Combinatorial objects

- ▶ Circuits, formulas
- ▶ Branching programs
- ▶ Graphs (determinants)

## Polynomials (formal)

## Algorithmic

Root Finding  
Factorization  
Identity Testing

# Introduction

## Lists

- ▶ Coefficients  $\rightsquigarrow$  dense
- ▶ Monomials  $\neq 0 \rightsquigarrow$  sparse  
 $\rightsquigarrow$  lacunary

## Combinatorial objects

- ▶ Circuits, formulas
- ▶ Branching programs
- ▶ Graphs (determinants)

## Polynomials (formal)

## Algorithmic

Root Finding  
Factorization  
Identity Testing

## Complexity

Permanent v. determinant  
Algebraic "P = NP ?"  
Expressivity

# Introduction

## Lists

- ▶ Coefficients  $\rightsquigarrow$  dense
- ▶ Monomials  $\neq 0 \rightsquigarrow$  sparse  
 $\rightsquigarrow$  lacunary

## Combinatorial objects

- ▶ Circuits, formulas
- ▶ Branching programs
- ▶ Graphs (determinants)

## Polynomials (formal)

## Algorithmic

Root Finding  
Factorization  
Identity Testing

## Complexity

Permanent v. determinant  
Algebraic "P = NP ?"  
Expressivity

## Tool

Combinatorics  
Semi-definite Prog.  
Correcting Codes

# Introduction

## Lists

- ▶ Coefficients  $\rightsquigarrow$  dense
- ▶ Monomials  $\neq 0 \rightsquigarrow$  sparse  
 $\rightsquigarrow$  lacunary

## Combinatorial objects

- ▶ Circuits, formulas
- ▶ Branching programs
- ▶ Graphs (determinants)

## Polynomials (formal)

## Algorithmic

Root Finding  
Factorization  
Identity Testing

Symbolic Computation

## Complexity

Permanent v. determinant  
Algebraic "P = NP ?"  
Expressivity

Algebraic Complexity

## Tool

Combinatorics  
Semi-definite Prog.  
Correcting Codes

Applications



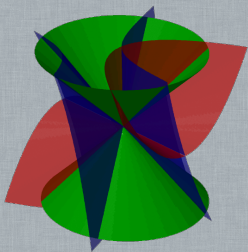
# Outline

1. Resolution of polynomial systems
2. Determinantal Representations of Polynomials
3. Real  $\tau$ -conjecture
4. Factorization of lacunary polynomials

# Resolution of polynomial systems

joint work with Pascal Koiran and Natacha Portier

Is there a (nonzero) solution?

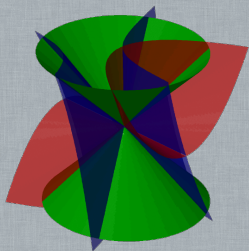


$$X^2 + Y^2 - Z^2 = 0$$

$$XZ + 3XY + YZ + Y^2 = 0$$

$$XZ - Y^2 = 0$$

Is there a (nonzero) solution?



$$X^2 + Y^2 - Z^2 = 0$$

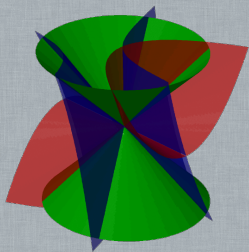
$$XZ + 3XY + YZ + Y^2 = 0$$

$$XZ - Y^2 = 0$$

**Input:** System of polynomials  $f = (f_1, \dots, f_s)$ ,  
 $f_j \in \mathbb{K}[X_0, \dots, X_n]$ , **homogeneous**

**Question:** Is there a point  $a \in \overline{\mathbb{K}}^{n+1}$ , **nonzero**, s.t.  $f(a) = 0$ ?

# Is there a (nonzero) solution?



$$X^2 + Y^2 - Z^2 = 0$$

$$XZ + 3XY + YZ + Y^2 = 0$$

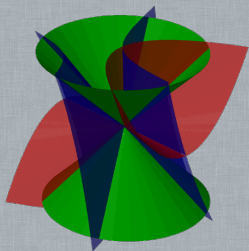
$$XZ - Y^2 = 0$$

**Input:** System of polynomials  $f = (f_1, \dots, f_s)$ ,  
 $f_j \in \mathbb{K}[X_0, \dots, X_n]$ , **homogeneous**

**Question:** Is there a point  $a \in \overline{\mathbb{K}}^{n+1}$ , **nonzero**, s.t.  $f(a) = 0$ ?

- ▶  $s < n + 1$ : **Trivial** (always true)

# Is there a (nonzero) solution?



$$X^2 + Y^2 - Z^2 = 0$$

$$XZ + 3XY + YZ + Y^2 = 0$$

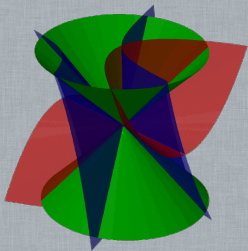
$$XZ - Y^2 = 0$$

**Input:** System of polynomials  $f = (f_1, \dots, f_s)$ ,  
 $f_j \in \mathbb{K}[X_0, \dots, X_n]$ , **homogeneous**

**Question:** Is there a point  $a \in \overline{\mathbb{K}}^{n+1}$ , **nonzero**, s.t.  $f(a) = 0$ ?

- ▶  $s < n + 1$ : **Trivial** (always true)
- ▶  $s > n + 1$ : **NP-Hard**

# Is there a (nonzero) solution?



$$X^2 + Y^2 - Z^2 = 0$$

$$XZ + 3XY + YZ + Y^2 = 0$$

$$XZ - Y^2 = 0$$

**Input:** System of polynomials  $f = (f_1, \dots, f_s)$ ,  
 $f_j \in \mathbb{K}[X_0, \dots, X_n]$ , **homogeneous**

**Question:** Is there a point  $a \in \overline{\mathbb{K}}^{n+1}$ , **nonzero**, s.t.  $f(a) = 0$ ?

- ▶  $s < n + 1$ : **Trivial** (always true)
- ▶  $s > n + 1$ : **NP-Hard**
- ▶  $s = n + 1$ : **Resultant**: Algebraic tool to answer the question

# Definitions

## PolSys( $\mathbb{K}$ )

---

**Input:**  $f_1, \dots, f_s \in \mathbb{K}[X_1, \dots, X_n]$

**Question:** Is there  $\mathbf{a} \in \overline{\mathbb{K}}^n$  s.t.  $f(\mathbf{a}) = 0$ ?



# Definitions

## PolSys( $\mathbb{K}$ )

---

**Input:**  $f_1, \dots, f_s \in \mathbb{K}[X_1, \dots, X_n]$

**Question:** Is there  $\mathbf{a} \in \overline{\mathbb{K}}^n$  s.t.  $f(\mathbf{a}) = 0$ ?

## HomPolSys( $\mathbb{K}$ )

---

**Input:**  $f_1, \dots, f_s \in \mathbb{K}[X_0, \dots, X_n]$ , **homogeneous**

**Question:** Is there a **nonzero**  $\mathbf{a} \in \overline{\mathbb{K}}^{n+1}$  s.t.  $f(\mathbf{a}) = 0$ ?

# Definitions

## POLSYS( $\mathbb{K}$ )

**Input:**  $f_1, \dots, f_s \in \mathbb{K}[X_1, \dots, X_n]$

**Question:** Is there  $\mathbf{a} \in \overline{\mathbb{K}}^n$  s.t.  $f(\mathbf{a}) = 0$ ?

## HOMPOLSYS( $\mathbb{K}$ )

**Input:**  $f_1, \dots, f_s \in \mathbb{K}[X_0, \dots, X_n]$ , **homogeneous**

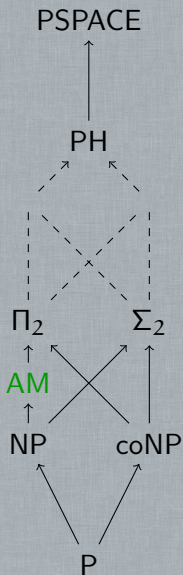
**Question:** Is there a **nonzero**  $\mathbf{a} \in \overline{\mathbb{K}}^{n+1}$  s.t.  $f(\mathbf{a}) = 0$ ?

## RESULTANT( $\mathbb{K}$ )

**Input:**  $f_1, \dots, f_{n+1} \in \mathbb{K}[X_0, \dots, X_n]$ , homogeneous

**Question:** Is there a nonzero  $\mathbf{a} \in \overline{\mathbb{K}}^{n+1}$  s.t.  $f(\mathbf{a}) = 0$ ?

# Known results

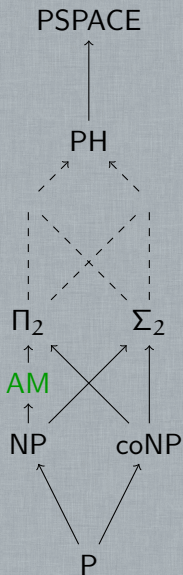


## Upper bounds

- ▶ Under GRH,  $PolSys(\mathbb{Z}) \in AM$

[Koiran'96]

# Known results



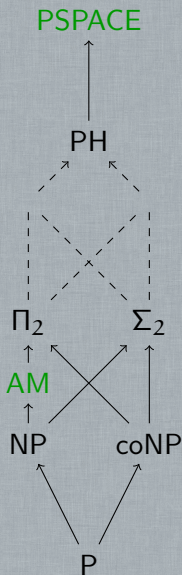
## Upper bounds

► Under GRH,  $\text{PoLSys}(\mathbb{Z}) \in \text{AM}$

[Koiran'96]

$\implies \text{HomPoLSys}(\mathbb{Z}), \text{RESULTANT}(\mathbb{Z}) \in \text{AM}$

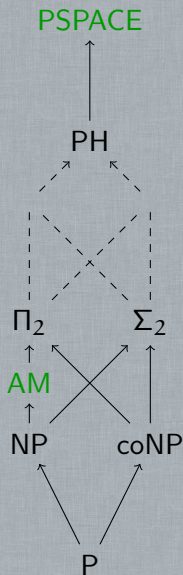
# Known results



## Upper bounds

- ▶ Under GRH,  $PolSys(\mathbb{Z}) \in AM$  [Koiran'96]  
 $\implies HomPolSys(\mathbb{Z}), RESULTANT(\mathbb{Z}) \in AM$
- ▶  $PolSys(\mathbb{F}_p) \in PSPACE$

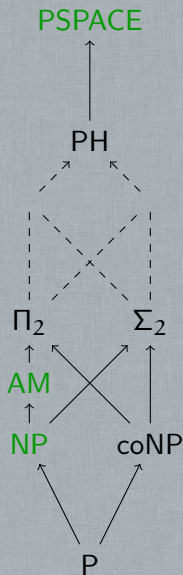
# Known results



## Upper bounds

- ▶ Under GRH,  $\text{PoLSys}(\mathbb{Z}) \in \text{AM}$  [Koiran'96]  
     $\implies \text{HomPoLSys}(\mathbb{Z}), \text{RESULTANT}(\mathbb{Z}) \in \text{AM}$
- ▶  $\text{PoLSys}(\mathbb{F}_p) \in \text{PSPACE}$   
     $\implies \text{HomPoLSys}(\mathbb{F}_p), \text{RESULTANT}(\mathbb{F}_p) \in \text{PSPACE}$

# Known results

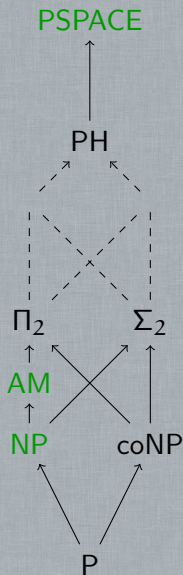


## Upper bounds

- ▶ Under GRH,  $\text{PoLSys}(\mathbb{Z}) \in \text{AM}$  [Koiran'96]  
 $\implies \text{HomPoLSys}(\mathbb{Z}), \text{RESULTANT}(\mathbb{Z}) \in \text{AM}$
- ▶  $\text{PoLSys}(\mathbb{F}_p) \in \text{PSPACE}$   
 $\implies \text{HomPoLSys}(\mathbb{F}_p), \text{RESULTANT}(\mathbb{F}_p) \in \text{PSPACE}$

## Lower bounds: NP-hardness

# Known results



## Upper bounds

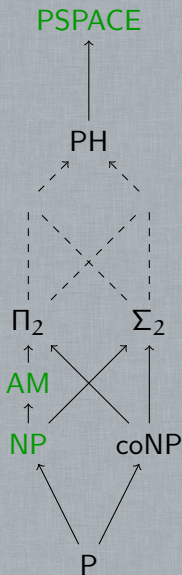
- ▶ Under GRH,  $\text{PoLSys}(\mathbb{Z}) \in \text{AM}$  [Koiran'96]  
 $\implies \text{HomPoLSys}(\mathbb{Z}), \text{RESULTANT}(\mathbb{Z}) \in \text{AM}$
- ▶  $\text{PoLSys}(\mathbb{F}_p) \in \text{PSPACE}$   
 $\implies \text{HomPoLSys}(\mathbb{F}_p), \text{RESULTANT}(\mathbb{F}_p) \in \text{PSPACE}$

## Lower bounds: NP-hardness

- ▶  $(\text{Hom})\text{PoLSys}(\mathbb{Z})$  and  $(\text{Hom})\text{PoLSys}(\mathbb{F}_p)$  [Folklore]



# Known results



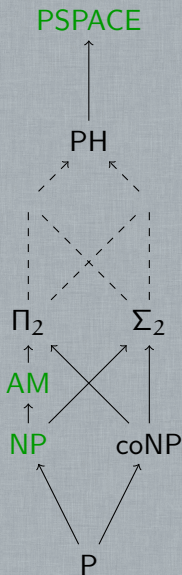
## Upper bounds

- ▶ Under GRH,  $\text{PoLSys}(\mathbb{Z}) \in \text{AM}$  [Koiran'96]  
     $\implies \text{HomPoLSys}(\mathbb{Z}), \text{RESULTANT}(\mathbb{Z}) \in \text{AM}$
- ▶  $\text{PoLSys}(\mathbb{F}_p) \in \text{PSPACE}$   
     $\implies \text{HomPoLSys}(\mathbb{F}_p), \text{RESULTANT}(\mathbb{F}_p) \in \text{PSPACE}$

## Lower bounds: NP-hardness

- ▶  $(\text{Hom})\text{PoLSys}(\mathbb{Z})$  and  $(\text{Hom})\text{PoLSys}(\mathbb{F}_p)$  [Folklore]
- ▶  $\text{RESULTANT}(\mathbb{Z})$  [Heintz-Morgenstern'93]

# Known results



## Upper bounds

- ▶ Under GRH,  $\text{PoLSys}(\mathbb{Z}) \in \text{AM}$  [Koiran'96]  
     $\implies \text{HomPoLSys}(\mathbb{Z}), \text{RESULTANT}(\mathbb{Z}) \in \text{AM}$
- ▶  $\text{PoLSys}(\mathbb{F}_p) \in \text{PSPACE}$   
     $\implies \text{HomPoLSys}(\mathbb{F}_p), \text{RESULTANT}(\mathbb{F}_p) \in \text{PSPACE}$

## Lower bounds: NP-hardness

- ▶  $(\text{Hom})\text{PoLSys}(\mathbb{Z})$  and  $(\text{Hom})\text{PoLSys}(\mathbb{F}_p)$  [Folklore]
- ▶  $\text{RESULTANT}(\mathbb{Z})$  [Heintz-Morgenstern'93]

What about  $\text{RESULTANT}(\mathbb{F}_p)$ ?

# Hardness in positive characteristics

- ▶  $\text{HomPolSys}(\mathbb{F}_p)$  is NP-hard:  
# homogeneous polynomials  $\geq$  # variables

# Hardness in positive characteristics

- ▶  $\text{HomPolSys}(\mathbb{F}_p)$  is NP-hard:  
# homogeneous polynomials  $\geq$  # variables
- ▶ Two strategies:
  - Reduce the number of polynomials
  - Increase the number of variables

# Hardness in positive characteristics

- ▶  $\text{HomPolSys}(\mathbb{F}_p)$  is NP-hard:  
# homogeneous polynomials  $\geq$  # variables
- ▶ Two strategies:
  - Reduce the number of polynomials
  - Increase the number of variables

# Hardness in positive characteristics

- ▶  $\text{HomPolSys}(\mathbb{F}_p)$  is NP-hard:  
# homogeneous polynomials  $\geq$  # variables
- ▶ Two strategies:
  - Reduce the number of polynomials
  - Increase the number of variables

## Theorem

[G.-Koiran-Portier'10-13]

Let  $p$  be a prime number.

# Hardness in positive characteristics

- ▶  $\text{HomPolSys}(\mathbb{F}_p)$  is NP-hard:  
# homogeneous polynomials  $\geq$  # variables
- ▶ Two strategies:
  - Reduce the number of polynomials
  - Increase the number of variables

## Theorem

[G.-Koiran-Portier'10-13]

Let  $p$  be a prime number.

- ▶  $\text{RESULTANT}(\mathbb{F}_p)$  is NP-hard for **sparse** polynomials.

# Hardness in positive characteristics

- ▶  $\text{HomPolSys}(\mathbb{F}_p)$  is NP-hard:  
# homogeneous polynomials  $\geq$  # variables
- ▶ Two strategies:
  - Reduce the number of polynomials
  - Increase the number of variables

## Theorem

[G.-Koiran-Portier'10-13]

Let  $p$  be a prime number.

- ▶  $\text{Resultant}(\mathbb{F}_p)$  is NP-hard for **sparse** polynomials.
- ▶  $\text{Resultant}(\mathbb{F}_q)$  is NP-hard for **dense** polynomials for some  $q = p^s$ .



# Conclusion

- ▶ **NP-hardness results** for square homogeneous systems of polynomials over finite fields

# Conclusion

- ▶ **NP-hardness results** for square homogeneous systems of polynomials over finite fields
- ▶ Result on the **evaluation** of the resultant polynomial

# Conclusion

- ▶ **NP-hardness results** for square homogeneous systems of polynomials over finite fields
- ▶ Result on the **evaluation** of the resultant polynomial

## Main open problem

- ▶ Improve the PSPACE upper bound in positive characteristics...
- ▶ ... or the NP lower bound.

# Determinantal Representations of Polynomials

joint works with

Erich L. Kaltofen, Pascal Koiran and Natacha Portier

&

Thierry Monteil and Stéphan Thomassé

# Determinantal representations

$$2XY + (X+Y)(Y+Z) = \det \begin{pmatrix} 0 & 2 & 0 & 0 & Y & X & 0 & 0 \\ 0 & -1 & X & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & Y & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & Z & Y \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 1 \\ -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

# Determinantal representations

$$2XY + (X+Y)(Y+Z) = \det \begin{vmatrix} 0 & 2 & 0 & 0 & 0 & 0 & 0 & Y & 0 & X & 0 & 0 & 0 & 0 & \frac{1}{2} \\ 2 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & X & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & X & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & Y & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & Y & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ Y & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ X & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & Z & 0 & Y \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & Z & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & Y & 0 & 1 & 0 & 1 \\ \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{vmatrix}$$

# Determinantal representations

$$2XY + (X+Y)(Y+Z) = \det \begin{vmatrix} 0 & 2 & 0 & 0 & 0 & 0 & 0 & Y & 0 & X & 0 & 0 & 0 & 0 & \frac{1}{2} \\ 2 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & X & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & X & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & Y & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & Y & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ Y & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ X & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & Z & 0 & Y \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & Z & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & Y & 0 & 1 & 0 & 1 \\ \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{vmatrix}$$

- Complexity of the determinant

# Determinantal representations

$$2XY + (X+Y)(Y+Z) = \det \begin{vmatrix} 0 & 2 & 0 & 0 & 0 & 0 & 0 & Y & 0 & X & 0 & 0 & 0 & 0 & \frac{1}{2} \\ 2 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & X & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & X & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & Y & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & Y & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ Y & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ X & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & Z & 0 & Y & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & Z & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & Y & 0 & 1 & 0 & 1 \\ \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{vmatrix}$$

- ▶ Complexity of the determinant
- ▶ Determinant vs. Permanent: Algebraic "P = NP?"



# Determinantal representations

$$2XY + (X+Y)(Y+Z) = \det \begin{vmatrix} 0 & 2 & 0 & 0 & 0 & 0 & 0 & Y & 0 & X & 0 & 0 & 0 & 0 & \frac{1}{2} \\ 2 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & X & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & X & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & Y & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & Y & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ Y & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ X & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & Z & 0 & Y \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & Z & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & Y & 0 & 1 & 0 & 1 \\ \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{vmatrix}$$

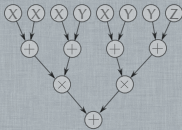
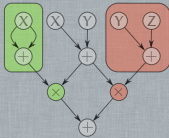
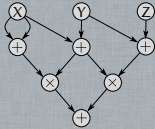
- ▶ Complexity of the determinant
- ▶ Determinant vs. Permanent: Algebraic "P = NP?"
- ▶ Links between circuits, ABPs and the determinant

# Determinantal representations

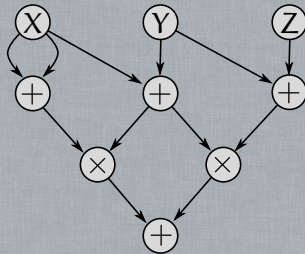
$$2XY + (X+Y)(Y+Z) = \det \begin{vmatrix} 0 & 2 & 0 & 0 & 0 & 0 & 0 & Y & 0 & X & 0 & 0 & 0 & 0 & \frac{1}{2} \\ 2 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & X & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & X & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & Y & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & Y & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ Y & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ X & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & Z & 0 & Y \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & Z & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & Y & 0 & 1 & 0 & 1 \\ \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{vmatrix}$$

- ▶ Complexity of the determinant
- ▶ Determinant vs. Permanent: Algebraic “P = NP?”
- ▶ Links between circuits, ABPs and the determinant
- ▶ Convex optimization

# Circuits



$$2X(X + Y) + (X + Y)(Y + Z)$$

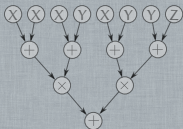
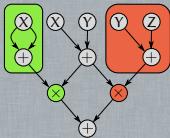
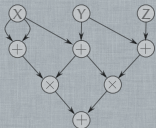


**Arithmetic circuit**

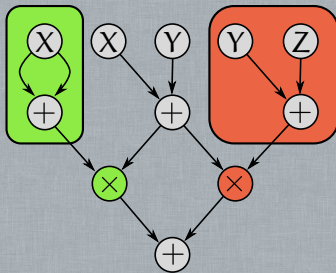
Size 6

Inputs 3

# Circuits



$$2X(X + Y) + (X + Y)(Y + Z)$$

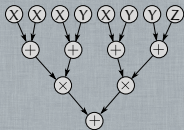
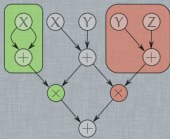
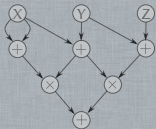


**Weakly-skew circuit**

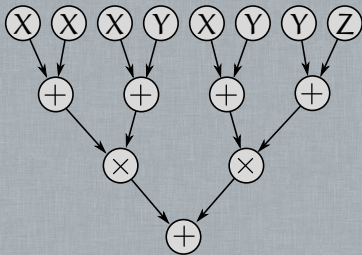
Size 6

Inputs 5

# Circuits



$$2X(X + Y) + (X + Y)(Y + Z)$$



**Formula**

Size 7

Inputs 8

# Results

## Proposition

[Valiant'79]

Formula of **size**  $s \rightsquigarrow$  Determinant of a matrix of **dimension**  $(s + 2)$

# Results

## Proposition

[Liu-Regan'06, G.-Kaltofen-Koiran-Portier'11]

Formula of **size**  $s \rightsquigarrow$  Determinant of a matrix of **dimension**  $(s + 1)$

# Results

## Proposition

[Liu-Regan'06, G.-Kaltofen-Koiran-Portier'11]

Formula of **size**  $s \rightsquigarrow$  Determinant of a matrix of **dimension**  $(s + 1)$

## Proposition

[Toda'92, Malod-Portier'08]

Weakly-skew circuit of **size**  $s$  with  $i$  **inputs**

$\rightsquigarrow$  Determinant of a matrix of **dimension**  $(s + i + 1)$



# Results

## Proposition

[Liu-Regan'06, G.-Kaltofen-Koiran-Portier'11]

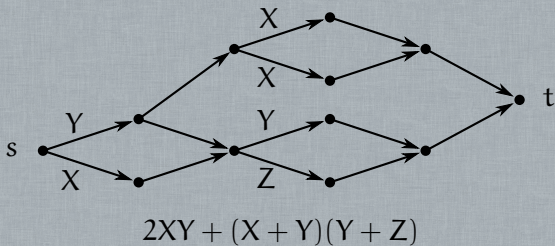
Formula of **size**  $s \rightsquigarrow$  Determinant of a matrix of **dimension**  $(s + 1)$

## Proposition

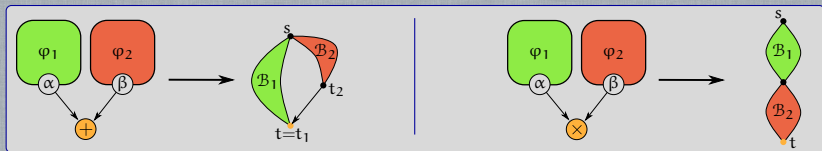
[Toda'92, Malod-Portier'08]

Weakly-skew circuit of **size**  $s$  with  $i$  **inputs**

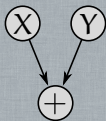
$\rightsquigarrow$  Determinant of a matrix of **dimension**  $(s + i + 1)$



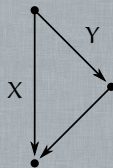
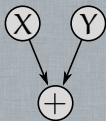
# From Formulas to Branching Programs



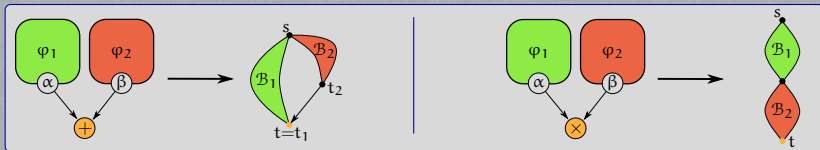
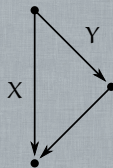
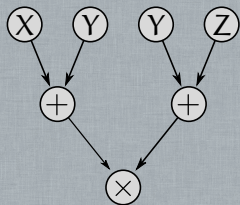
# From Formulas to Branching Programs



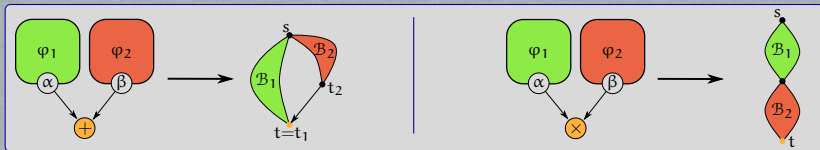
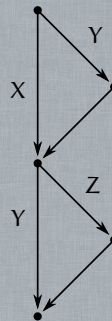
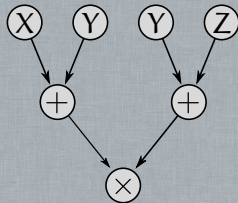
# From Formulas to Branching Programs



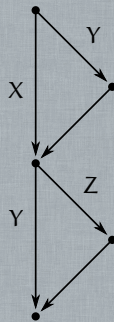
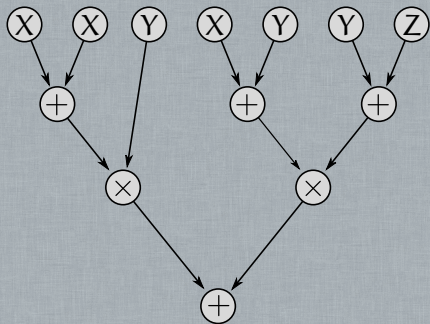
# From Formulas to Branching Programs



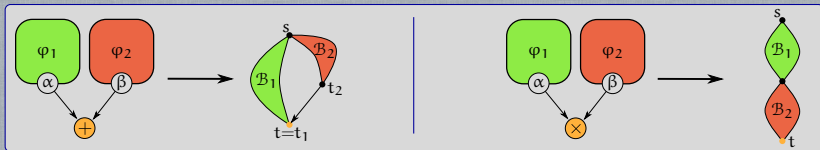
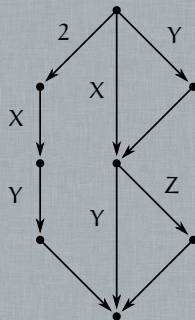
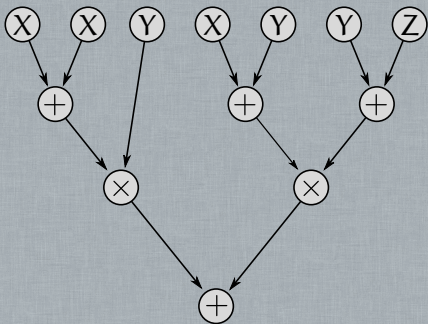
# From Formulas to Branching Programs



# From Formulas to Branching Programs

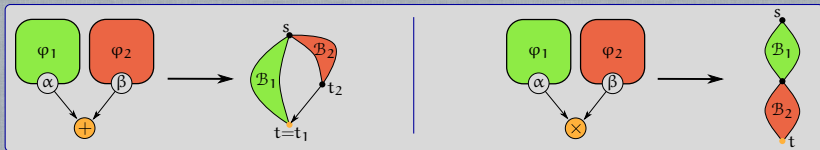
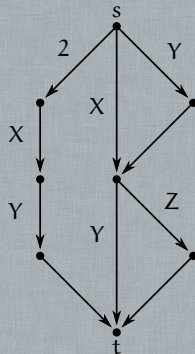
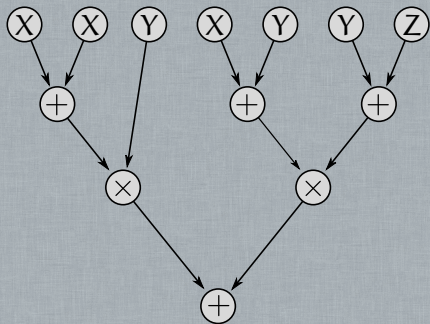


# From Formulas to Branching Programs

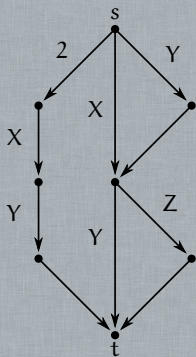




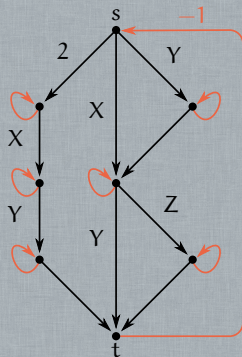
# From Formulas to Branching Programs



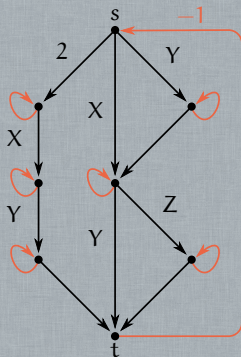
# From Branching Programs to Determinants



# From Branching Programs to Determinants

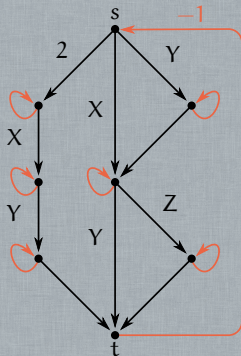


# From Branching Programs to Determinants



$$M = \begin{pmatrix} 0 & 2 & 0 & 0 & Y & X & 0 & 0 \\ 0 & -1 & X & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & Y & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & Z & Y \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 1 \\ -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

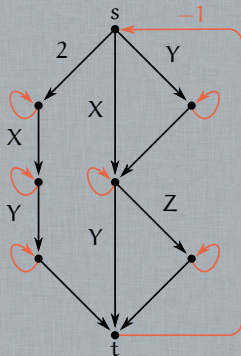
# From Branching Programs to Determinants



$$M = \begin{pmatrix} 0 & 2 & 0 & 0 & Y & X & 0 & 0 \\ 0 & -1 & X & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & Y & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & Z & Y \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 1 \\ -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\det M = \sum_{\sigma \in \mathfrak{S}_n} (-1)^{\epsilon(\sigma)} \prod_{i=1}^n M_{i, \sigma(i)}$$

# From Branching Programs to Determinants

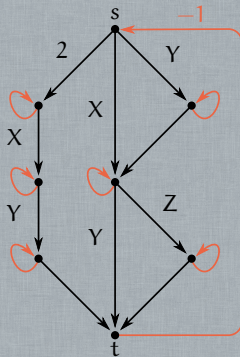


$$M = \begin{pmatrix} 0 & 2 & 0 & 0 & Y & X & 0 & 0 \\ 0 & -1 & X & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & Y & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & Z & Y \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 1 \\ -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\det M = \sum_{\sigma \in \mathfrak{S}_n} (-1)^{\epsilon(\sigma)} \prod_{i=1}^n M_{i, \sigma(i)}$$

► **Cycle covers**  $\iff$  **Permutations**

# From Branching Programs to Determinants



$$M = \begin{pmatrix} 0 & 2 & 0 & 0 & Y & X & 0 & 0 \\ 0 & -1 & X & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & Y & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & Z & Y \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 1 \\ -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\det M = \sum_{\sigma \in \mathfrak{S}_n} (-1)^{\epsilon(\sigma)} \prod_{i=1}^n M_{i, \sigma(i)}$$

- ▶ **Cycle covers**  $\iff$  **Permutations**
- ▶ Up to signs,  **$\det(M)$  = sum of the weights** of the cycle covers of  $G$

# Branching Program for the Permanent

$$\text{per } A = \sum_{\sigma \in \mathfrak{S}_n} \prod_{i=1}^n A_{i, \sigma(i)}$$



# Branching Program for the Permanent

$$\text{per } A = \sum_{\sigma \in \mathfrak{S}_n} \prod_{i=1}^n A_{i, \sigma(i)}$$

$$\text{per} \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} = aei + bfg + cdh + afh + bdi + ceg$$

# Branching Program for the Permanent

$$\text{per } A = \sum_{\sigma \in \mathfrak{S}_n} \prod_{i=1}^n A_{i, \sigma(i)}$$

$$\text{per} \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} = aei + bfg + cdh + afh + bdi + ceg$$

## Theorem

[G.'12]

There exists a **branching program of size  $2^n$**  representing the **permanent of dimension  $n$** .



# Permanent versus Determinant

## Corollary

The **permanent of dimension  $n$**  is a projection of the **determinant of dimension  $N = 2^n - 1$** .

# Permanent versus Determinant

## Corollary

The **permanent of dimension  $n$**  is a projection of the **determinant of dimension  $N = 2^n - 1$** .

$$\text{per} \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} = \det \begin{pmatrix} 0 & a & d & g & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & i & f & 0 \\ 0 & 0 & 1 & 0 & 0 & c & i \\ 0 & 0 & 0 & 1 & c & 0 & f \\ e & 0 & 0 & 0 & 1 & 0 & 0 \\ h & 0 & 0 & 0 & 0 & 1 & 0 \\ b & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

# Permanent versus Determinant

## Corollary

The **permanent of dimension  $n$**  is a projection of the **determinant of dimension  $N = 2^n - 1$** .

$$\text{per} \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} = \det \begin{pmatrix} 0 & a & d & g & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & i & f & 0 \\ 0 & 0 & 1 & 0 & 0 & c & i \\ 0 & 0 & 0 & 1 & c & 0 & f \\ e & 0 & 0 & 0 & 1 & 0 & 0 \\ h & 0 & 0 & 0 & 0 & 1 & 0 \\ b & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

## Conjecture

[Algebraic  $P \neq NP$ ]

The **permanent of dimension  $n$**  is **not** a projection of the **determinant of dimension  $N = n^{O(1)}$** .

# Permanent versus Determinant

## Corollary

The **permanent of dimension  $n$**  is a projection of the **determinant of dimension  $N = 2^n - 1$** .

$$\text{per} \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} = \det \begin{pmatrix} 0 & a & d & g & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & i & f & 0 \\ 0 & 0 & 1 & 0 & 0 & c & i \\ 0 & 0 & 0 & 1 & c & 0 & f \\ e & 0 & 0 & 0 & 1 & 0 & 0 \\ h & 0 & 0 & 0 & 0 & 1 & 0 \\ b & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

## Conjecture

[Algebraic  $P \neq NP$ ]

The **permanent of dimension  $n$**  is **not** a projection of the **determinant of dimension  $N = 2^{O(n)}$** .

# Results

## Proposition

[Liu-Regan'06, G.-Kaltofen-Koiran-Portier'11]

Formula of **size**  $s \rightsquigarrow$  Determinant of a matrix of **dimension**  $(s + 1)$

## Proposition

[Toda'92, Malod-Portier'08]

Weakly-skew circuit of **size**  $s$  with  $i$  **inputs**  
 $\rightsquigarrow$  Determinant of a matrix of **dimension**  $(s + i + 1)$

# Results

## Proposition

[Liu-Regan'06, G.-Kaltofen-Koiran-Portier'11]

Formula of **size**  $s$   $\rightsquigarrow$  Determinant of a matrix of **dimension**  $(s + 1)$

## Proposition

[Toda'92, Malod-Portier'08]

Weakly-skew circuit of **size**  $s$  with  $i$  **inputs**  
 $\rightsquigarrow$  Determinant of a matrix of **dimension**  $(s + i + 1)$

## Theorem

[G.-Kaltofen-Koiran-Portier'11]

If the underlying field has **characteristic**  $\neq 2$ ,



# Results

## Proposition

[Liu-Regan'06, G.-Kaltofen-Koiran-Portier'11]

Formula of **size**  $s \rightsquigarrow$  Determinant of a matrix of **dimension**  $(s + 1)$

## Proposition

[Toda'92, Malod-Portier'08]

Weakly-skew circuit of **size**  $s$  with  $i$  **inputs**  
 $\rightsquigarrow$  Determinant of a matrix of **dimension**  $(s + i + 1)$

## Theorem

[G.-Kaltofen-Koiran-Portier'11]

If the underlying field has **characteristic**  $\neq 2$ ,

- ▶ Formula of **size**  $s \rightsquigarrow$  **Symmetric** determinant of **dimension**  $2s + 1$

# Results

## Proposition

[Liu-Regan'06, G.-Kaltofen-Koiran-Portier'11]

Formula of **size**  $s \rightsquigarrow$  Determinant of a matrix of **dimension**  $(s + 1)$

## Proposition

[Toda'92, Malod-Portier'08]

Weakly-skew circuit of **size**  $s$  with  **$i$  inputs**  
 $\rightsquigarrow$  Determinant of a matrix of **dimension**  $(s + i + 1)$

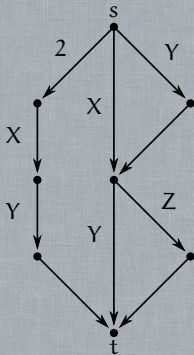
## Theorem

[G.-Kaltofen-Koiran-Portier'11]

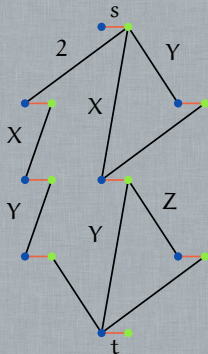
If the underlying field has **characteristic**  $\neq 2$ ,

- ▶ Formula of **size**  $s \rightsquigarrow$  **Symmetric** determinant of **dimension**  $2s + 1$
- ▶ Weakly-skew circuit of **size**  $s$  with  **$i$  inputs**  
 $\rightsquigarrow$  **Symmetric** determinant of **dimension**  $2(s + i) + 1$

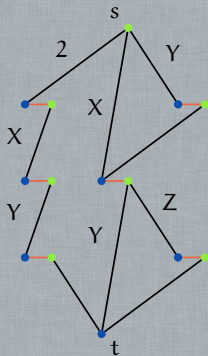
# From Branching Programs to Symmetric Determinants



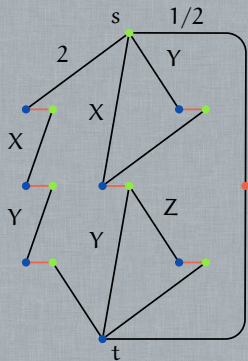
# From Branching Programs to Symmetric Determinants



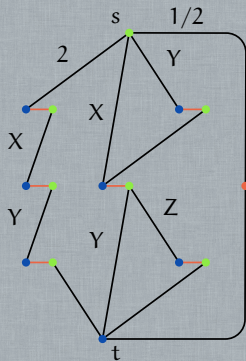
# From Branching Programs to Symmetric Determinants



# From Branching Programs to Symmetric Determinants

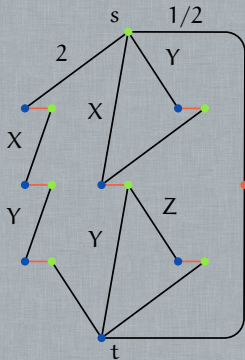


# From Branching Programs to Symmetric Determinants



$$S = \begin{vmatrix} 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & Y & 0 & X & 0 & 0 & 0 & 0 & \frac{1}{2} \\ 2 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & X & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & X & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & Y & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & Y & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ Y & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ X & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & Z & 0 & Y \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & Z & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{vmatrix}$$

# From Branching Programs to Symmetric Determinants



$$S = \begin{pmatrix} 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & Y & 0 & X & 0 & 0 & 0 & 0 & \frac{1}{2} \\ 2 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & X & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & X & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & Y & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & Y & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ Y & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ X & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & Z & 0 & Y \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & Z & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & Y & 0 & 1 & 0 & 1 & 0 \\ \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

## Corollary

The **determinant of dimension  $n$**  is a projection of the **symmetric determinant of dimension  $\frac{2}{3}n^3 + o(n^3)$** .



## SDR in characteristic 2

### Theorem

[G., Monteil, Thomassé'13]

There are polynomials **without SDR** in characteristic 2, e.g.  $xy+z$ .

## SDR in characteristic 2

### Theorem

[G., Monteil, Thomassé'13]

There are polynomials **without SDR** in characteristic 2, e.g.  $xy+z$ .

- ▶ A polynomial is said **representable** if it has an SDR.

# SDR in characteristic 2

## Theorem

[G., Monteil, Thomassé'13]

There are polynomials **without SDR** in characteristic 2, e.g.  $xy+z$ .

- ▶ A polynomial is said **representable** if it has an SDR.

## Determinant

$\mathfrak{S}_n$  = Permutation group of  $\{1, \dots, n\}$

$$\det A = \sum_{\sigma \in \mathfrak{S}_n} (-1)^{\epsilon(\sigma)} \prod_{i=1}^n A_{i, \sigma(i)}$$

# SDR in characteristic 2

## Theorem

[G., Monteil, Thomassé'13]

There are polynomials **without SDR** in characteristic 2, e.g.  $xy+z$ .

- ▶ A polynomial is said **representable** if it has an SDR.

## Determinant in characteristic 2

$\mathfrak{S}_n$  = Permutation group of  $\{1, \dots, n\}$

$$\det A = \sum_{\sigma \in \mathfrak{S}_n} \prod_{i=1}^n A_{i, \sigma(i)}$$

# SDR in characteristic 2

## Theorem

[G., Monteil, Thomassé'13]

There are polynomials **without SDR** in characteristic 2, e.g.  $xy+z$ .

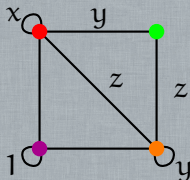
- ▶ A polynomial is said **representable** if it has an SDR.

## Determinant in characteristic 2

$\mathfrak{S}_n$  = Permutation group of  $\{1, \dots, n\}$

$$\det A = \sum_{\sigma \in \mathfrak{S}_n} \prod_{i=1}^n A_{i, \sigma(i)}$$

$$\begin{array}{c} \bullet \quad \bullet \quad \bullet \quad \bullet \\ \bullet \quad \left[ \begin{array}{cccc} x & y & 1 & z \\ y & 0 & 0 & z \\ 1 & 0 & 1 & 1 \\ z & z & 1 & y \end{array} \right] \end{array}$$



# SDR in characteristic 2

## Theorem

[G., Monteil, Thomassé'13]

There are polynomials **without SDR** in characteristic 2, e.g.  $xy+z$ .

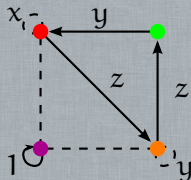
- ▶ A polynomial is said **representable** if it has an SDR.

## Determinant in characteristic 2

$\mathfrak{S}_n$  = Permutation group of  $\{1, \dots, n\}$

$$\det A = \sum_{\sigma \in \mathfrak{S}_n} \prod_{i=1}^n A_{i, \sigma(i)}$$

•	•	•	•
•	$\begin{bmatrix} x & y & 1 & z \\ y & 0 & 0 & z \\ 1 & 0 & 1 & 1 \\ z & z & 1 & y \end{bmatrix}$		
•			
•			
•			



# SDR in characteristic 2

## Theorem

[G., Monteil, Thomassé'13]

There are polynomials **without SDR** in characteristic 2, e.g.  $xy+z$ .

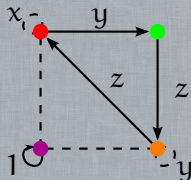
- ▶ A polynomial is said **representable** if it has an SDR.

## Determinant in characteristic 2

$\mathfrak{S}_n$  = Permutation group of  $\{1, \dots, n\}$

$$\det A = \sum_{\sigma \in \mathfrak{S}_n} \prod_{i=1}^n A_{i, \sigma(i)}$$

•	•	•	•	
•	$x$	$y$	$1$	$z$
•	$y$	$0$	$0$	$z$
•	$1$	$0$	$1$	$1$
•	$z$	$z$	$1$	$y$



## SDR in characteristic 2

### Theorem

[G., Monteil, Thomassé'13]

There are polynomials **without SDR** in characteristic 2, e.g.  $xy+z$ .

- ▶ A polynomial is said **representable** if it has an SDR.

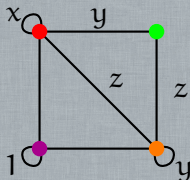
### Determinant in characteristic 2 of symmetric matrices

$\mathfrak{I}_n =$  Involutions of  $\{1, \dots, n\}$

$$\det A = \sum_{\sigma \in \mathfrak{I}_n} \prod_{i=1}^n A_{i, \sigma(i)}$$

•	•	•	•
•	•	•	•
•	•	•	•
•	•	•	•

$$\begin{bmatrix} x & y & 1 & z \\ y & 0 & 0 & z \\ 1 & 0 & 1 & 1 \\ z & z & 1 & y \end{bmatrix}$$





## SDR in characteristic 2

### Theorem

[G., Monteil, Thomassé'13]

There are polynomials **without SDR** in characteristic 2, e.g.  $xy+z$ .

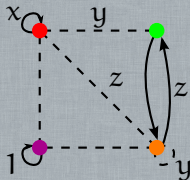
- ▶ A polynomial is said **representable** if it has an SDR.

### Determinant in characteristic 2 of symmetric matrices

$\mathfrak{I}_n =$  Involutions of  $\{1, \dots, n\}$

$$\det A = \sum_{\sigma \in \mathfrak{I}_n} \prod_{i=1}^n A_{i, \sigma(i)}$$

$$\begin{array}{cccc} \bullet & \bullet & \bullet & \bullet \\ \bullet & \left[ \begin{array}{cccc} x & y & 1 & z \\ y & 0 & 0 & z \\ 1 & 0 & 1 & 1 \\ z & z & 1 & y \end{array} \right] \end{array}$$



# Representable polynomials

## Lemma

- ▶  $P$  and  $Q$  are representable  $\implies P \times Q$  is representable.

# Representable polynomials

## Lemma

- ▶  $P$  and  $Q$  are representable  $\implies P \times Q$  is representable.
- ▶ For all  $P$ ,  $P^2$  is representable.

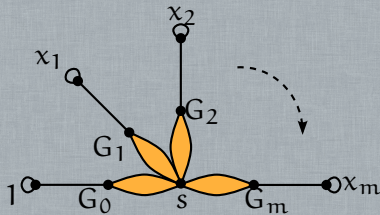
# Representable polynomials

## Lemma

- ▶  $P$  and  $Q$  are representable  $\implies P \times Q$  is representable.
- ▶ For all  $P$ ,  $P^2$  is representable.

## Theorem

$L(x_1, \dots, x_m) = P_0^2 + x_1 P_1^2 + \dots + x_m P_m^2$  is representable.



# Obstructions to representability

## Theorem

If  $P$  is representable, then

$$P \equiv L_1 \times \cdots \times L_k \pmod{\langle x_1^2 + 1, \dots, x_m^2 + 1 \rangle}$$

where the  $L_i$ 's are linear.

(linear = degree-1)

# Obstructions to representability

## Theorem

If  $P$  is representable, then

$$P \equiv L_1 \times \cdots \times L_k \pmod{\langle x_1^2 + \ell_1^2, \dots, x_m^2 + \ell_m^2 \rangle}$$

where the  $L_i$ 's are linear.

(linear = degree-1)

# Obstructions to representability

## Theorem

If  $P$  is representable, then

$$P \equiv L_1 \times \cdots \times L_k \pmod{\langle x_1^2 + \ell_1^2, \dots, x_m^2 + \ell_m^2 \rangle}$$

where the  $L_i$ 's are linear.

(linear = degree-1)

$$xz + y^2 = \det \begin{pmatrix} x & y \\ y & z \end{pmatrix}$$

# Obstructions to representability

## Theorem

If  $P$  is representable, then

$$P \equiv L_1 \times \cdots \times L_k \pmod{\langle x_1^2 + \ell_1^2, \dots, x_m^2 + \ell_m^2 \rangle}$$

where the  $L_i$ 's are linear.

(linear = degree-1)

$$xz + y^2 = \det \begin{pmatrix} x & y \\ y & z \end{pmatrix} \equiv \det \begin{pmatrix} x & 1 \\ 1 & z \end{pmatrix} \pmod{\langle x^2 + 1, y^2 + 1, z^2 + 1 \rangle}$$



# Obstructions to representability

## Theorem

If  $P$  is representable, then

$$P \equiv L_1 \times \cdots \times L_k \pmod{\langle x_1^2 + \ell_1^2, \dots, x_m^2 + \ell_m^2 \rangle}$$

where the  $L_i$ 's are linear.

(linear = degree-1)

$$xz + y^2 = \det \begin{pmatrix} x & y \\ y & z \end{pmatrix} \equiv \det \begin{pmatrix} x & 1 \\ 1 & z \end{pmatrix} \equiv \det \begin{pmatrix} x & 1+x \\ 1+x & x+z \end{pmatrix} \\ \pmod{\langle x^2 + 1, y^2 + 1, z^2 + 1 \rangle}$$

# Obstructions to representability

## Theorem

If  $P$  is representable, then

$$P \equiv L_1 \times \cdots \times L_k \pmod{\langle x_1^2 + \ell_1^2, \dots, x_m^2 + \ell_m^2 \rangle}$$

where the  $L_i$ 's are linear.

(linear = degree-1)

$$\begin{aligned}xz + y^2 &= \det \begin{pmatrix} x & y \\ y & z \end{pmatrix} \equiv \det \begin{pmatrix} x & 1 \\ 1 & z \end{pmatrix} \equiv \det \begin{pmatrix} x & 1+x \\ 1+x & x+z \end{pmatrix} \\ &\equiv \det \begin{pmatrix} x & 0 \\ 0 & x+z \end{pmatrix} \pmod{\langle x^2 + 1, y^2 + 1, z^2 + 1 \rangle}\end{aligned}$$

# Obstructions to representability

## Theorem

If  $P$  is representable, then

$$P \equiv L_1 \times \cdots \times L_k \pmod{\langle x_1^2 + \ell_1^2, \dots, x_m^2 + \ell_m^2 \rangle}$$

where the  $L_i$ 's are linear.

(linear = degree-1)

$$\begin{aligned}xz + y^2 &= \det \begin{pmatrix} x & y \\ y & z \end{pmatrix} \equiv \det \begin{pmatrix} x & 1 \\ 1 & z \end{pmatrix} \equiv \det \begin{pmatrix} x & 1+x \\ 1+x & x+z \end{pmatrix} \\ &\equiv \det \begin{pmatrix} x & 0 \\ 0 & x+z \end{pmatrix} \equiv x(x+z) \pmod{\langle x^2 + 1, y^2 + 1, z^2 + 1 \rangle}\end{aligned}$$

# Obstructions to representability

## Theorem

If  $P$  is representable, then

$$P \equiv L_1 \times \cdots \times L_k \pmod{\langle x_1^2 + \ell_1^2, \dots, x_m^2 + \ell_m^2 \rangle}$$

where the  $L_i$ 's are linear.

(linear = degree-1)

$$\begin{aligned}xz + y^2 &= \det \begin{pmatrix} x & y \\ y & z \end{pmatrix} \equiv \det \begin{pmatrix} x & 1 \\ 1 & z \end{pmatrix} \equiv \det \begin{pmatrix} x & 1+x \\ 1+x & x+z \end{pmatrix} \\ &\equiv \det \begin{pmatrix} x & 0 \\ 0 & x+z \end{pmatrix} \equiv x(x+z) \pmod{\langle x^2 + 1, y^2 + 1, z^2 + 1 \rangle}\end{aligned}$$

Such a  $P$  is said **factorizable modulo**  $\langle x_1^2 + \ell_1^2, \dots, x_m^2 + \ell_m^2 \rangle$ .

# Multilinear polynomials

## Theorem

---

Let  $P$  be a **multilinear** polynomial. The following propositions are equivalent:

- (i)  $P$  is representable;

# Multilinear polynomials

## Theorem

Let  $P$  be a **multilinear** polynomial. The following propositions are equivalent:

- (i)  $P$  is representable;
- (ii)  $\forall \ell$ ,  $P$  is factorizable *modulo*  $\langle x_1^2 + \ell_1^2, \dots, x_m^2 + \ell_m^2 \rangle$ ;

# Multilinear polynomials

## Theorem

Let  $P$  be a **multilinear** polynomial. The following propositions are equivalent:

- (i)  $P$  is representable;
- (ii)  $\forall \ell$ ,  $P$  is factorizable *modulo*  $\langle x_1^2 + \ell_1^2, \dots, x_m^2 + \ell_m^2 \rangle$ ;
- (iii)  $\exists \ell$ ,  $P$  is factorizable *modulo*  $\langle x_1^2 + \ell_1^2, \dots, x_m^2 + \ell_m^2 \rangle$ .

# Multilinear polynomials

## Theorem

Let  $P$  be a **multilinear** polynomial. The following propositions are equivalent:

- (i)  $P$  is representable;
- (ii)  $\forall \ell$ ,  $P$  is factorizable *modulo*  $\langle x_1^2 + \ell_1^2, \dots, x_m^2 + \ell_m^2 \rangle$ ;
- (iii)  $\exists \ell$ ,  $P$  is factorizable *modulo*  $\langle x_1^2 + \ell_1^2, \dots, x_m^2 + \ell_m^2 \rangle$ .

Is  $xy + z$  representable?



# Multilinear polynomials

## Theorem

Let  $P$  be a **multilinear** polynomial. The following propositions are equivalent:

- (i)  $P$  is representable;
- (ii)  $\forall \ell$ ,  $P$  is factorizable *modulo*  $\langle x_1^2 + \ell_1^2, \dots, x_m^2 + \ell_m^2 \rangle$ ;
- (iii)  $\exists \ell$ ,  $P$  is factorizable *modulo*  $\langle x_1^2 + \ell_1^2, \dots, x_m^2 + \ell_m^2 \rangle$ .

Is  $xy + z$  representable?

$\rightsquigarrow$  Factorization in  $\mathbb{F}[x_1, \dots, x_m] / \langle x_1^2 + \ell_1^2, \dots, x_m^2 + \ell_m^2 \rangle$

# Finding a factor

$$(x + y + z + 1) \times (x + y + z + 1) \times \cdots \times (x + y + z + 1) \\ \stackrel{?}{\equiv} xy + z \pmod{\langle x^2, y^2, z^2 \rangle}$$

# Finding a factor

$$(x + y + z + 1) \times (x + y + z + 1) \times \cdots \times (x + y + z + 1) \\ \stackrel{?}{\equiv} xy + z \pmod{\langle x^2, y^2, z^2 \rangle}$$

# Finding a factor

$$(x + y + z + 1) \times (x + y + z + 1) \times \cdots \times (x + y + z + 1) \\ \stackrel{?}{\equiv} xy + z \pmod{\langle x^2, y^2, z^2 \rangle}$$

# Finding a factor

$$(x + y + z + 1) \times (x + y + z + 1) \times \cdots \times (x + y + z + 1) \\ \stackrel{?}{\equiv} xy + z \pmod{\langle x^2, y^2, z^2 \rangle}$$

# Finding a factor

$$(x + y + z) \times (x + y + z + 1) \times \cdots \times (x + y + z + 1) \\ \stackrel{?}{\equiv} xy + z \pmod{\langle x^2, y^2, z^2 \rangle}$$

# Finding a factor

$$(x + y + z) \times (x + y + z + 1) \times \cdots \times (x + y + z + 1) \\ \stackrel{?}{\equiv} xy + z \pmod{\langle x^2, y^2, z^2 \rangle}$$

# Finding a factor

$$\begin{aligned} & ( \quad z \quad ) \times (x + y + z + 1) \times \cdots \times (x + y + z + 1) \\ & \stackrel{?}{\equiv} xy + z \pmod{\langle x^2, y^2, z^2 \rangle} \end{aligned}$$



# Finding a factor

$$\begin{aligned} & ( \quad z \quad ) \times (x + y + z + 1) \times \cdots \times (x + y + z + 1) \\ & \stackrel{?}{\equiv} xy + z \pmod{\langle x^2, y^2, z^2 \rangle} \end{aligned}$$

$$\text{lin}(xy + yz + y + z + 1) = y + z + 1$$

# Finding a factor

$$\left( \quad z \quad \right) \times (x + y + z + 1) \times \cdots \times (x + y + z + 1) \\ \stackrel{?}{\equiv} xy + z \pmod{\langle x^2, y^2, z^2 \rangle}$$

$$\text{lin}(xy + yz + y + z + 1) = y + z + 1$$

## Theorem

Under *suitable* conditions,  $P$  is factorizable if and only if

$$P \equiv \text{lin}(P) \times \frac{1}{\alpha_i} \frac{\partial P}{\partial x_i} \pmod{\langle x_1^2, \dots, x_m^2 \rangle},$$

where  $\alpha_i x_i$  is a monomial of  $\text{lin}(P)$ .

# Conclusion

Same **expressiveness**:

- ▶ (Weakly-)Skew circuits

# Conclusion

Same **expressiveness**:

- ▶ (Weakly-)Skew circuits
- ▶ Branching Programs

# Conclusion

Same **expressiveness**:

- ▶ (Weakly-)Skew circuits
- ▶ Branching Programs
- ▶ Determinants

# Conclusion

Same **expressiveness**:

- ▶ (Weakly-)Skew circuits
- ▶ Branching Programs
- ▶ Determinants
- ▶ Symmetric Determinants in characteristic  $\neq 2$

# Conclusion

Same **expressiveness**:

- ▶ (Weakly-)Skew circuits
- ▶ Branching Programs
- ▶ Determinants
- ▶ Symmetric Determinants in characteristic  $\neq 2$

In characteristic 2, some polynomials have no SDR.

# Conclusion

Same **expressiveness**:

- ▶ (Weakly-)Skew circuits
- ▶ Branching Programs
- ▶ Determinants
- ▶ Symmetric Determinants in characteristic  $\neq 2$

In characteristic 2, some polynomials have no SDR.

- ▶ Characterization for multilinear polynomials



# Conclusion

Same **expressiveness**:

- ▶ (Weakly-)Skew circuits
- ▶ Branching Programs
- ▶ Determinants
- ▶ Symmetric Determinants in characteristic  $\neq 2$

In characteristic 2, some polynomials have no SDR.

- ▶ Characterization for multilinear polynomials
- ▶ Algorithms to build SDRs

# Conclusion

Same **expressiveness**:

- ▶ (Weakly-)Skew circuits
- ▶ Branching Programs
- ▶ Determinants
- ▶ Symmetric Determinants in characteristic  $\neq 2$

In characteristic 2, some polynomials have no SDR.

- ▶ Characterization for multilinear polynomials
- ▶ Algorithms to build SDRs

## Main open question

[Algebraic “P = NP?”]

What is the **smallest N** s.t. the **permanent of dimension n** is a projection of the **determinant of dimension N**?

# Real $\tau$ -conjecture

joint work with Pascal Koiran, Natacha Portier and Yann Strozecki

# The $\tau$ -conjecture

$\tau(f)$  = minimal number of  $+$  and  $\times$  needed to evaluate  $f$ ,  
from constant  $-1$  and variables

# The $\tau$ -conjecture

$\tau(f)$  = minimal number of  $+$  and  $\times$  needed to evaluate  $f$ ,  
from constant  $-1$  and variables

## Conjecture

[Shub-Smale'95]

The number of **integer roots** of any  $f \in \mathbb{Z}[X]$  is  $\leq \text{poly}(\tau(f))$ .

# The $\tau$ -conjecture

$\tau(f)$  = minimal number of  $+$  and  $\times$  needed to evaluate  $f$ ,  
from constant  $-1$  and variables

## Conjecture

[Shub-Smale'95]

The number of **integer roots** of any  $f \in \mathbb{Z}[X]$  is  $\leq \text{poly}(\tau(f))$ .

## Theorems

$\tau$ -conjecture

$$\implies P_{\mathbb{C}} \neq NP_{\mathbb{C}}$$

[Shub-Smale'95]

# The $\tau$ -conjecture

$\tau(f)$  = minimal number of  $+$  and  $\times$  needed to evaluate  $f$ ,  
from constant  $-1$  and variables

## Conjecture

[Shub-Smale'95]

The number of **integer roots** of any  $f \in \mathbb{Z}[X]$  is  $\leq \text{poly}(\tau(f))$ .

## Theorems

$\tau$ -conjecture

$\implies P_{\mathbb{C}} \neq NP_{\mathbb{C}}$  [Shub-Smale'95]

$\implies$  super-polynomial lower bound for the permanent  
( $VP^0 \neq VNP^0$ ) [Bürgisser'07]

# The $\tau$ -conjecture

$\tau(f)$  = minimal number of  $+$  and  $\times$  needed to evaluate  $f$ ,  
from constant  $-1$  and variables

## Conjecture

[Shub-Smale'95]

The number of **integer roots** of any  $f \in \mathbb{Z}[X]$  is  $\leq \text{poly}(\tau(f))$ .

## Theorems

$\tau$ -conjecture

$\implies P_{\mathbb{C}} \neq NP_{\mathbb{C}}$  [Shub-Smale'95]

$\implies$  super-polynomial lower bound for the permanent  
( $VP^0 \neq VNP^0$ ) [Bürgisser'07]

## Theorem

[Cheng'03]

Extended  $\tau$ -conjecture  $\implies$  Merel torsion theorem, ...



# The $\tau$ -conjecture

$\tau(f)$  = minimal number of  $+$  and  $\times$  needed to evaluate  $f$ ,  
from constant  $-1$  and variables

## Conjecture

[Shub-Smale'95]

The number of **integer roots** of any  $f \in \mathbb{Z}[X]$  is  $\leq \text{poly}(\tau(f))$ .

## Theorems

$\tau$ -conjecture

$\implies P_{\mathbb{C}} \neq NP_{\mathbb{C}}$  [Shub-Smale'95]

$\implies$  super-polynomial lower bound for the permanent  
( $VP^0 \neq VNP^0$ ) [Bürgisser'07]

## Theorem

[Cheng'03]

Extended  $\tau$ -conjecture  $\implies$  Merel torsion theorem, ...

- ▶ False for real roots (Chebyshev polynomials)

# The real $\tau$ -conjecture

## Conjecture

[Koiran'11]

Let  $f = \sum_{i=1}^k \prod_{j=1}^m f_{ij}$  where the  $f_{ij}$ 's are  $t$ -sparse polynomials.

Then  $f$  has  $\leq \text{poly}(k, m, t)$  real roots.

# The real $\tau$ -conjecture

## Conjecture

[Koiran'11]

Let  $f = \sum_{i=1}^k \prod_{j=1}^m f_{ij}$  where the  $f_{ij}$ 's are  $t$ -sparse polynomials.

Then  $f$  has  $\leq \text{poly}(k, m, t)$  real roots.

## Theorem

[Koiran'11]

Real  $\tau$ -conjecture

$\implies$  Super-polynomial lower bound for the permanent

# The real $\tau$ -conjecture

## Conjecture

[Koiran'11]

Let  $f = \sum_{i=1}^k \prod_{j=1}^m f_{ij}$  where the  $f_{ij}$ 's are  $t$ -sparse polynomials.

Then  $f$  has  $\leq \text{poly}(k, m, t)$  real roots.

## Theorem

[Koiran'11]

Real  $\tau$ -conjecture

$\implies$  Super-polynomial lower bound for the permanent

- ▶ Enough to bound the number of **integer roots**

# The real $\tau$ -conjecture

## Conjecture

[Koiran'11]

Let  $f = \sum_{i=1}^k \prod_{j=1}^m f_{ij}$  where the  $f_{ij}$ 's are  $t$ -sparse polynomials.

Then  $f$  has  $\leq \text{poly}(k, m, t)$  real roots.

## Theorem

[Koiran'11]

Real  $\tau$ -conjecture

$\implies$  Super-polynomial lower bound for the permanent

- ▶ Enough to bound the number of **integer roots**

$\rightsquigarrow$  Adelic  $\tau$ -conjecture

[Phillipson-Rojas'13]

# The real $\tau$ -conjecture

## Conjecture

[Koiran'11]

Let  $f = \sum_{i=1}^k \prod_{j=1}^m f_{ij}$  where the  $f_{ij}$ 's are  $t$ -sparse polynomials.

Then  $f$  has  $\leq \text{poly}(k, m, t)$  real roots.

## Theorem

[Koiran'11]

Real  $\tau$ -conjecture

$\implies$  Super-polynomial lower bound for the permanent

- ▶ Enough to bound the number of **integer roots**

$\rightsquigarrow$  Adelic  $\tau$ -conjecture

[Phillipson-Rojas'13]

- ▶ Case  $k = 1$ : Follows from **Descartes' rule**.

# The real $\tau$ -conjecture

## Conjecture

[Koiran'11]

Let  $f = \sum_{i=1}^k \prod_{j=1}^m f_{ij}$  where the  $f_{ij}$ 's are  $t$ -sparse polynomials.

Then  $f$  has  $\leq \text{poly}(k, m, t)$  real roots.

## Theorem

[Koiran'11]

Real  $\tau$ -conjecture

$\implies$  Super-polynomial lower bound for the permanent

- ▶ Enough to bound the number of **integer roots**

$\rightsquigarrow$  Adelic  $\tau$ -conjecture

[Phillipson-Rojas'13]

- ▶ Case  $k = 1$ : Follows from **Descartes' rule**.
- ▶ Case  $k = 2$ : Open.

# The real $\tau$ -conjecture

## Conjecture

[Koiran'11]

Let  $f = \sum_{i=1}^k \prod_{j=1}^m f_{ij}$  where the  $f_{ij}$ 's are  $t$ -sparse polynomials.

Then  $f$  has  $\leq \text{poly}(k, m, t)$  real roots.

## Theorem

[Koiran'11]

Real  $\tau$ -conjecture

$\implies$  Super-polynomial lower bound for the permanent

- ▶ Enough to bound the number of **integer roots**

$\rightsquigarrow$  Adelic  $\tau$ -conjecture

[Phillipson-Rojas'13]

- ▶ Case  $k = 1$ : Follows from **Descartes' rule**.
- ▶ Case  $k = 2$ : Open.
- ▶ Toy question: Number of real roots of  $fg + 1$ ?



# The limited power of powering

$$\text{SPS}(k, m, t, A) = \left\{ \sum_{i=1}^k \prod_{j=1}^m f_j^{\alpha_{ij}} \mid \begin{array}{l} f_j \text{'s are } t\text{-sparse} \\ \alpha_{ij} \leq A \end{array} \right\}$$

# The limited power of powering

$$\text{SPS}(k, m, t, A) = \left\{ \sum_{i=1}^k \prod_{j=1}^m f_j^{\alpha_{ij}} \mid \begin{array}{l} f_j \text{'s are } t\text{-sparse} \\ \alpha_{ij} \leq A \end{array} \right\}$$

## Theorem

[G.-Koiran-Portier-Strozecki'11]

If  $f \in \text{SPS}(k, m, t, A)$ , its number of real roots is at most

$$C \cdot \left[ e \cdot \left( 1 + \frac{t^m}{2^{k-1} - 1} \right) \right]^{2^{k-1} - 1} \quad \text{for some } C.$$

# The limited power of powering

$$\text{SPS}(k, m, t, A) = \left\{ \sum_{i=1}^k \prod_{j=1}^m f_j^{\alpha_{ij}} \mid \begin{array}{l} f_j \text{'s are } t\text{-sparse} \\ \alpha_{ij} \leq A \end{array} \right\}$$

## Theorem

[G.-Koiran-Portier-Strozecki'11]

If  $f \in \text{SPS}(k, m, t, A)$ , its number of real roots is at most

$$C \cdot \left[ e \cdot \left( 1 + \frac{t^m}{2^{k-1} - 1} \right) \right]^{2^{k-1} - 1} \quad \text{for some } C.$$

- ▶ Independent of  $A$ .

# The limited power of powering

$$\text{SPS}(k, m, t, A) = \left\{ \sum_{i=1}^k \prod_{j=1}^m f_j^{\alpha_{ij}} \mid \begin{array}{l} f_j \text{'s are } t\text{-sparse} \\ \alpha_{ij} \leq A \end{array} \right\}$$

## Theorem

[G.-Koiran-Portier-Strozecki'11]

If  $f \in \text{SPS}(k, m, t, A)$ , its number of real roots is at most

$$C \cdot \left[ e \cdot \left( 1 + \frac{t^m}{2^{k-1} - 1} \right) \right]^{2^{k-1} - 1} \quad \text{for some } C.$$

- ▶ Independent of  $A$ .
- ▶ If  $k$  and  $m$  are fixed, this is **polynomial in  $t$** .

## Case $k = 2$

### Proposition

The polynomial

$$f = \prod_{j=1}^m f_j^{\alpha_j} + \prod_{j=1}^m f_j^{\beta_j}$$

has at most  $2mt^m + 4m(t-1)$  real roots.

## Case $k = 2$

### Proposition

The polynomial

$$f = \prod_{j=1}^m f_j^{\alpha_j} + \prod_{j=1}^m f_j^{\beta_j}$$

has at most  $2mt^m + 4m(t-1)$  real roots.

**Proof sketch.** Let  $F = f / \prod_j f_j^{\alpha_j} = 1 + \prod_j f_j^{\beta_j - \alpha_j}$ .

## Case $k = 2$

### Proposition

The polynomial

$$f = \prod_{j=1}^m f_j^{\alpha_j} + \prod_{j=1}^m f_j^{\beta_j}$$

has at most  $2mt^m + 4m(t-1)$  real roots.

**Proof sketch.** Let  $F = f / \prod_j f_j^{\alpha_j} = 1 + \prod_j f_j^{\beta_j - \alpha_j}$ . Then

$$F' = \underbrace{\prod_{j=1}^m f_j^{\beta_j - \alpha_j - 1}}_{\leq 2m(t-1) \text{ roots and poles}} \times \underbrace{\sum_{j=1}^m (\beta_j - \alpha_j) f_j' \prod_{\ell \neq j} f_\ell}_{\leq 2mt^m - 1 \text{ roots}}$$

# Multivariate SPS polynomials

## Definition

$(P_n)_{n \geq 0} \in m\text{SPS}(k, m)$  if there exists a polynomial  $Q$  s.t.

$$P_n(x_1, \dots, x_{Q(n)}) = \sum_{i=1}^k \prod_{j=1}^m f_{j,n}^{\alpha_{ij,n}}(\vec{x})$$

where

- ▶  $f_{j,n}$  is  $Q(n)$ -sparse;



# Multivariate SPS polynomials

## Definition

$(P_n)_{n \geq 0} \in \text{mSPS}(k, m)$  if there exists a polynomial  $Q$  s.t.

$$P_n(x_1, \dots, x_{Q(n)}) = \sum_{i=1}^k \prod_{j=1}^m f_{j,n}^{\alpha_{ij,n}}(\vec{x})$$

where

- ▶  $\log(\alpha_{ij,n}) \leq Q(n)$ ;
- ▶  $f_{j,n}$  is  $Q(n)$ -sparse;
- ▶  $f_{j,n}$  has complexity at most  $Q(n)$  or GRH is assumed.

# Multivariate SPS polynomials

## Definition

$(P_n)_{n \geq 0} \in \text{mSPS}(k, m)$  if there exists a polynomial  $Q$  s.t.

$$P_n(x_1, \dots, x_{Q(n)}) = \sum_{i=1}^k \prod_{j=1}^m f_{j,n}^{\alpha_{ij,n}}(\vec{x})$$

where

- ▶  $\log(\alpha_{ij,n}) \leq Q(n)$ ;
- ▶  $f_{j,n}$  is  $Q(n)$ -sparse;
- ▶  $f_{j,n}$  has complexity at most  $Q(n)$  or GRH is assumed.

- ▶ exponential-size depth-4 circuits
- ▶ polynomial-size circuits with polynomial-depth

# Lower bound for the permanent

## Theorem

For fixed  $k$  and  $m$ ,  $(PER_n)$  does not have  $mSPS(k, m)$  circuits.

# Lower bound for the permanent

## Theorem

For fixed  $k$  and  $m$ ,  $(\text{PER}_n)$  does not have  $m\text{SPS}(k, m)$  circuits.

**Proof sketch.**  $(\text{PER}_n) \in m\text{SPS}(k, m)$

$$\implies \text{PW}_n(X) = \prod_{i=1}^{2^n} (X - i) \in \text{SPS}(k, m, \text{poly}(n), 2^{\text{poly}(n)})$$

# Lower bound for the permanent

## Theorem

For fixed  $k$  and  $m$ ,  $(\text{PER}_n)$  does not have  $m\text{SPS}(k, m)$  circuits.

**Proof sketch.**  $(\text{PER}_n) \in m\text{SPS}(k, m)$

$$\implies \text{PW}_n(X) = \prod_{i=1}^{2^n} (X - i) \in \text{SPS}(k, m, \text{poly}(n), 2^{\text{poly}(n)})$$

But  $\text{PW}_n$  has  $2^n$  roots: contradiction.

# Links with PIT

## Theorem

For fixed  $k$  and  $m$ , we can test for zero  $f \in \text{SPS}(k, m, t, \mathbb{A})$  in time polynomial in  $t$  and  $\mathbb{A}$ .

# Links with PIT

## Theorem

For fixed  $k$  and  $m$ , we can test for zero  $f \in \text{SPS}(k, m, t, A)$  in time polynomial in  $t$  and  $A$ .

## Proposition

With an oracle testing for zero  $\sum_{i=1}^k \prod_{j=1}^m a_{ij}^{\alpha_{ij}}$ , PIT algorithm in time polynomial in  $t$  and  $\log(A)$ .

# Links with PIT

## Theorem

For fixed  $k$  and  $m$ , we can test for zero  $f \in \text{SPS}(k, m, t, A)$  in time polynomial in  $t$  and  $A$ .

## Proposition

With an oracle testing for zero  $\sum_{i=1}^k \prod_{j=1}^m a_{ij}^{\alpha_{ij}}$ , PIT algorithm in time polynomial in  $t$  and  $\log(A)$ .

**Remark.** Works also with mSPS polynomials (Kronecker substitution).



# Conclusion

- ▶ Real  $\tau$ -conjecture  $\implies VP^0 \neq VNP^0$

# Conclusion

- ▶ Real  $\tau$ -conjecture  $\implies VP^0 \neq VNP^0$
- ▶ Use your favorite real analysis tools!

# Conclusion

- ▶ Real  $\tau$ -conjecture  $\implies VP^0 \neq VNP^0$
- ▶ Use your favorite real analysis tools!
- ▶ Adelic formulation: replace **real roots** by **p-adic roots**

# Conclusion

- ▶ Real  $\tau$ -conjecture  $\implies VP^0 \neq VNP^0$
- ▶ Use your favorite real analysis tools!
- ▶ Adelic formulation: replace **real roots** by **p-adic roots**
- ▶ Update: Number of real roots for  $f \in \text{SPS}(k, m, t, A) \leq t^{O(mk^2)}$   
[Koiran-Portier-Tavenas'13]

# Conclusion

- ▶ Real  $\tau$ -conjecture  $\implies VP^0 \neq VNP^0$
- ▶ Use your favorite real analysis tools!
- ▶ Adelic formulation: replace **real roots** by **p-adic roots**
- ▶ Update: Number of real roots for  $f \in \text{SPS}(k, m, t, A) \leq t^{O(mk^2)}$   
[Koiran-Portier-Tavenas'13]

## Embarrassing Open Problem

Let  $f, g$  be  $t$ -sparse polynomials.

$\rightsquigarrow$  What is the maximum number of roots of  $fg + 1$ ?

# Factorization of lacunary polynomials

joint work with Arakdev Chattopadhyay, Pascal Koiran, Natacha Portier and  
Yann Strozecki

# Classical factorization algorithms

## Factorization of a polynomial $P$

Find  $F_1, \dots, F_t$ , irreducible, s.t.  $P = F_1 \times \dots \times F_t$ .

# Classical factorization algorithms

## Factorization of a polynomial $P$

Find  $F_1, \dots, F_t$ , irreducible, s.t.  $P = F_1 \times \dots \times F_t$ .

$\mathbb{Z}[X]$   
[Lenstra-Lenstra-Lovász'82]



$\mathbb{Q}(\alpha)[X]$   
[A. Lenstra'83, Landau'83]



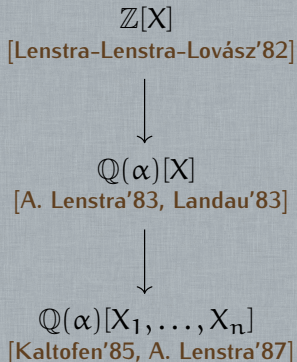
$\mathbb{Q}(\alpha)[X_1, \dots, X_n]$   
[Kaltofen'85, A. Lenstra'87]



# Classical factorization algorithms

## Factorization of a polynomial $P$

Find  $F_1, \dots, F_t$ , irreducible, s.t.  $P = F_1 \times \dots \times F_t$ .



# Classical factorization algorithms

## Factorization of a polynomial $P$

Find  $F_1, \dots, F_t$ , irreducible, s.t.  $P = F_1 \times \dots \times F_t$ .

$\mathbb{Z}[X]$   
[Lenstra-Lenstra-Lovász'82]



$\mathbb{Q}(\alpha)[X]$

$\mathbb{F}_q[X]$   
[Berlekamp'67]



## Complexity

Polynomial in the **degree** of the polynomials

$\mathbb{Q}(\alpha)[X_1, \dots, X_n]$   
[Kaltofen'85, A. Lenstra'87]

$\mathbb{F}_q[X_1, \dots, X_n]$

# Lacunary polynomials

$$X^{102}Y^{101} + X^{101}Y^{102} - X^{101}Y^{101} - X - Y + 1$$

# Lacunary polynomials

$$\begin{aligned} X^{102}Y^{101} + X^{101}Y^{102} - X^{101}Y^{101} - X - Y + 1 \\ = (X + Y - 1) \times (X^{101}Y^{101} - 1) \end{aligned}$$

# Lacunary polynomials

$$\begin{aligned} & X^{102}Y^{101} + X^{101}Y^{102} - X^{101}Y^{101} - X - Y + 1 \\ &= (X + Y - 1) \times (X^{101}Y^{101} - 1) \\ &= (X + Y - 1) \times (XY - 1) \times (1 + XY + \dots + X^{100}Y^{100}) \end{aligned}$$

# Lacunary polynomials

$$\begin{aligned} & X^{102}Y^{101} + X^{101}Y^{102} - X^{101}Y^{101} - X - Y + 1 \\ &= (X + Y - 1) \times (X^{101}Y^{101} - 1) \\ &= (X + Y - 1) \times (XY - 1) \times (1 + XY + \dots + X^{100}Y^{100}) \end{aligned}$$

- ▶ Algorithms polynomial in  $\log(\deg(P))$

# Lacunary polynomials

$$\begin{aligned} & X^{102}Y^{101} + X^{101}Y^{102} - X^{101}Y^{101} - X - Y + 1 \\ &= (X + Y - 1) \times (X^{101}Y^{101} - 1) \\ &= (X + Y - 1) \times (XY - 1) \times (1 + XY + \dots + X^{100}Y^{100}) \end{aligned}$$

- ▶ Algorithms polynomial in  $\log(\deg(P))$
- ▶ **Some** factors only

# Lacunary polynomials

$$\begin{aligned} X^{102}Y^{101} + X^{101}Y^{102} - X^{101}Y^{101} - X - Y + 1 \\ = (X + Y - 1) \times (X^{101}Y^{101} - 1) \\ = (X + Y - 1) \times (XY - 1) \times (1 + XY + \dots + X^{100}Y^{100}) \end{aligned}$$

- ▶ Algorithms polynomial in  $\log(\deg(P))$
- ▶ **Some** factors only

## Definition

$$P(X_1, \dots, X_n) = \sum_{j=1}^k a_j X_1^{\alpha_{1j}} \dots X_n^{\alpha_{nj}}$$



# Lacunary polynomials

$$\begin{aligned} X^{102}Y^{101} + X^{101}Y^{102} - X^{101}Y^{101} - X - Y + 1 \\ = (X + Y - 1) \times (X^{101}Y^{101} - 1) \\ = (X + Y - 1) \times (XY - 1) \times (1 + XY + \dots + X^{100}Y^{100}) \end{aligned}$$

- ▶ Algorithms polynomial in  $\log(\deg(P))$
- ▶ **Some** factors only

## Definition

$$P(X_1, \dots, X_n) = \sum_{j=1}^k a_j X_1^{\alpha_{1j}} \dots X_n^{\alpha_{nj}}$$

- ▶ Lacunary representation:  $\{(\alpha_{1j}, \dots, \alpha_{nj} : a_j) : 1 \leq j \leq k\}$

# Lacunary polynomials

$$\begin{aligned} X^{102}Y^{101} + X^{101}Y^{102} - X^{101}Y^{101} - X - Y + 1 \\ = (X + Y - 1) \times (X^{101}Y^{101} - 1) \\ = (X + Y - 1) \times (XY - 1) \times (1 + XY + \dots + X^{100}Y^{100}) \end{aligned}$$

- ▶ Algorithms polynomial in  $\log(\deg(P))$
- ▶ **Some** factors only

## Definition

$$P(X_1, \dots, X_n) = \sum_{j=1}^k a_j X_1^{\alpha_{1j}} \dots X_n^{\alpha_{nj}}$$

- ▶ Lacunary representation:  $\{(\alpha_{1j}, \dots, \alpha_{nj} : a_j) : 1 \leq j \leq k\}$
- ▶  $\text{size}(P) \simeq \sum_j \text{size}(a_j) + \log(\alpha_{1j}) + \dots + \log(\alpha_{nj})$

# Integral roots of integral polynomials

## Gap Theorem

[Cucker-Koiran-Smale'98]

Let

$$P(X) = \underbrace{\sum_{j=1}^{\ell} a_j X^{\alpha_j}}_Q + \underbrace{\sum_{j=\ell+1}^k a_j X^{\alpha_j}}_R \in \mathbb{Z}[X]$$

with  $\alpha_1 \leq \alpha_2 \leq \dots \leq \alpha_k$ .

# Integral roots of integral polynomials

## Gap Theorem

[Cucker-Koiran-Smale'98]

Let

$$P(X) = \underbrace{\sum_{j=1}^{\ell} a_j X^{\alpha_j}}_Q + \underbrace{\sum_{j=\ell+1}^k a_j X^{\alpha_j}}_R \in \mathbb{Z}[X]$$

with  $\alpha_1 \leq \alpha_2 \leq \dots \leq \alpha_k$ . Suppose that

$$\alpha_{\ell+1} - \alpha_{\ell} > 1 + \log \left( \max_{j \leq \ell} |a_j| \right)$$

# Integral roots of integral polynomials

## Gap Theorem

[Cucker-Koiran-Smale'98]

Let

$$P(X) = \underbrace{\sum_{j=1}^{\ell} a_j X^{\alpha_j}}_Q + \underbrace{\sum_{j=\ell+1}^k a_j X^{\alpha_j}}_R \in \mathbb{Z}[X]$$

with  $\alpha_1 \leq \alpha_2 \leq \dots \leq \alpha_k$ . Suppose that

$$\alpha_{\ell+1} - \alpha_{\ell} > 1 + \log \left( \max_{j \leq \ell} |a_j| \right),$$

then for all  $x \in \mathbb{Z}$ ,  $|x| \geq 2$ ,  $P(x) = 0 \implies Q(x) = R(x) = 0$ .

# Integral roots of integral polynomials

## Gap Theorem

[Cucker-Koiran-Smale'98]

Let

$$P(X) = \underbrace{\sum_{j=1}^{\ell} a_j X^{\alpha_j}}_Q + \underbrace{\sum_{j=\ell+1}^k a_j X^{\alpha_j}}_R \in \mathbb{Z}[X]$$

with  $\alpha_1 \leq \alpha_2 \leq \dots \leq \alpha_k$ . Suppose that

$$\alpha_{\ell+1} - \alpha_{\ell} > 1 + \log \left( \max_{j \leq \ell} |a_j| \right),$$

then for all  $x \in \mathbb{Z}$ ,  $|x| \geq 2$ ,  $P(x) = 0 \implies Q(x) = R(x) = 0$ .

$$-9 + X^2 + 6X^7 + 2X^8$$

# Integral roots of integral polynomials

## Gap Theorem

[Cucker-Koiran-Smale'98]

Let

$$P(X) = \underbrace{\sum_{j=1}^{\ell} a_j X^{\alpha_j}}_Q + \underbrace{\sum_{j=\ell+1}^k a_j X^{\alpha_j}}_R \in \mathbb{Z}[X]$$

with  $\alpha_1 \leq \alpha_2 \leq \dots \leq \alpha_k$ . Suppose that

$$\alpha_{\ell+1} - \alpha_{\ell} > 1 + \log \left( \max_{j \leq \ell} |a_j| \right),$$

then for all  $x \in \mathbb{Z}$ ,  $|x| \geq 2$ ,  $P(x) = 0 \implies Q(x) = R(x) = 0$ .

$$-9 + X^2 + 6X^7 + 2X^8 = -9 + X^2 + X^7(6 + 2X)$$

# Integral roots of integral polynomials

## Gap Theorem

[Cucker-Koiran-Smale'98]

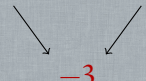
Let

$$P(X) = \underbrace{\sum_{j=1}^{\ell} a_j X^{\alpha_j}}_Q + \underbrace{\sum_{j=\ell+1}^k a_j X^{\alpha_j}}_R \in \mathbb{Z}[X]$$

with  $\alpha_1 \leq \alpha_2 \leq \dots \leq \alpha_k$ . Suppose that

$$\alpha_{\ell+1} - \alpha_{\ell} > 1 + \log \left( \max_{j \leq \ell} |a_j| \right),$$

then for all  $x \in \mathbb{Z}$ ,  $|x| \geq 2$ ,  $P(x) = 0 \implies Q(x) = R(x) = 0$ .

$$-9 + X^2 + 6X^7 + 2X^8 = -9 + X^2 + X^7(6 + 2X)$$


-3



# Integral roots of integral polynomials

## Gap Theorem

[Cucker-Koiran-Smale'98]

Let

$$P(X) = \underbrace{\sum_{j=1}^{\ell} a_j X^{\alpha_j}}_Q + \underbrace{\sum_{j=\ell+1}^k a_j X^{\alpha_j}}_R \in \mathbb{Z}[X]$$

with  $\alpha_1 \leq \alpha_2 \leq \dots \leq \alpha_k$ . Suppose that

$$\alpha_{\ell+1} - \alpha_{\ell} > 1 + \log \left( \max_{j \leq \ell} |a_j| \right),$$

then for all  $x \in \mathbb{Z}$ ,  $|x| \geq 2$ ,  $P(x) = 0 \implies Q(x) = R(x) = 0$ .

$$-9 + X^2 + 6X^7 + 2X^8 = -9 + X^2 + X^7(6 + 2X)$$

$-3$  + check 0, 1 and  $-1$

# Integral roots of integral polynomials

## Gap Theorem

[Cucker-Koiran-Smale'98]

Let

$$P(X) = \underbrace{\sum_{j=1}^{\ell} a_j X^{\alpha_j}}_Q + \underbrace{\sum_{j=\ell+1}^k a_j X^{\alpha_j}}_R \in \mathbb{Z}[X]$$

with  $\alpha_1 \leq \alpha_2 \leq \dots \leq \alpha_k$ . Suppose that

$$\alpha_{\ell+1} - \alpha_{\ell} > 1 + \log \left( \max_{j \leq \ell} |a_j| \right),$$

then for all  $x \in \mathbb{Z}$ ,  $|x| \geq 2$ ,  $P(x) = 0 \implies Q(x) = R(x) = 0$ .

$$-9 + X^2 + 6X^7 + 2X^8 = -9 + X^2 + X^7(6 + 2X)$$

$-3$  + check 0, 1 and  $-1$

# Factorization of lacunary polynomials

## Theorems

Deterministic polynomial time (in  $\log(\deg P)$ ) algorithms for:

- ▶ **linear** factors of **univariate** polynomials over  $\mathbb{Z}$ ;

[Cucker-Koiran-Smale'98]

# Factorization of lacunary polynomials

## Theorems

Deterministic polynomial time (in  $\log(\deg P)$ ) algorithms for:

- ▶ **linear** factors of **univariate** polynomials over  $\mathbb{Z}$ ;

[Cucker-Koiran-Smale'98]

- ▶ **low-degree** factors of **univariate** polynomials over  $\mathbb{Q}(\alpha)$ ;

[H. Lenstra'99]

# Factorization of lacunary polynomials

## Theorems

Deterministic polynomial time (in  $\log(\deg P)$ ) algorithms for:

- ▶ **linear** factors of **univariate** polynomials over  $\mathbb{Z}$ ;  
[Cucker-Koiran-Smale'98]
- ▶ **low-degree** factors of **univariate** polynomials over  $\mathbb{Q}(\alpha)$ ;  
[H. Lenstra'99]
- ▶ **linear** factors of **bivariate** polynomials over  $\mathbb{Q}$ ;  
[Kaltofen-Koiran'05]

# Factorization of lacunary polynomials

## Theorems

Deterministic polynomial time (in  $\log(\deg P)$ ) algorithms for:

- ▶ **linear** factors of **univariate** polynomials over  $\mathbb{Z}$ ;  
[Cucker-Koiran-Smale'98]
- ▶ **low-degree** factors of **univariate** polynomials over  $\mathbb{Q}(\alpha)$ ;  
[H. Lenstra'99]
- ▶ **linear** factors of **bivariate** polynomials over  $\mathbb{Q}$ ;  
[Kaltofen-Koiran'05]
- ▶ **low-degree** factors of **multivariate** polynomials over  $\mathbb{Q}(\alpha)$ .  
[Kaltofen-Koiran'06]

# Linear factors of bivariate polynomials

## Observation

$(Y - uX - v)$  divides  $P(X, Y) \iff P(X, uX + v) \equiv 0$

# Linear factors of bivariate polynomials

## Observation

$(Y - uX - v)$  divides  $P(X, Y) \iff P(X, uX + v) \equiv 0$

## Gap Theorem

[Chattopadhyay-G.-Koiran-Portier-Strozecki'13]

Let

$$P = \underbrace{\sum_{j=1}^{\ell} a_j X^{\alpha_j} (uX + v)^{\beta_j}}_Q + \underbrace{\sum_{j=\ell+1}^k a_j X^{\alpha_j} (uX + v)^{\beta_j}}_R$$

with  $uv \neq 0$ ,  $\alpha_1 \leq \dots \leq \alpha_k$ .



# Linear factors of bivariate polynomials

## Observation

$(Y - uX - v)$  divides  $P(X, Y) \iff P(X, uX + v) \equiv 0$

## Gap Theorem

[Chattopadhyay-G.-Koiran-Portier-Strozecki'13]

Let

$$P = \underbrace{\sum_{j=1}^{\ell} a_j X^{\alpha_j} (uX + v)^{\beta_j}}_Q + \underbrace{\sum_{j=\ell+1}^k a_j X^{\alpha_j} (uX + v)^{\beta_j}}_R$$

with  $uv \neq 0$ ,  $\alpha_1 \leq \dots \leq \alpha_k$ . If  $\ell$  is the smallest index s.t.

$$\alpha_{\ell+1} > \alpha_1 + \binom{\ell}{2},$$

then  $P \equiv 0$  iff both  $Q \equiv 0$  and  $R \equiv 0$ .

# Linear factors of bivariate polynomials

## Observation

$(Y - uX - v)$  divides  $P(X, Y) \iff P(X, uX + v) \equiv 0$

## Gap Theorem

[Chattopadhyay-G.-Koiran-Portier-Strozecki'13]

Let

$$P = \underbrace{\sum_{j=1}^{\ell} a_j X^{\alpha_j} Y^{\beta_j}}_Q + \underbrace{\sum_{j=\ell+1}^k a_j X^{\alpha_j} Y^{\beta_j}}_R$$

with  $uv \neq 0$ ,  $\alpha_1 \leq \dots \leq \alpha_k$ . If  $\ell$  is the smallest index s.t.

$$\alpha_{\ell+1} > \alpha_1 + \binom{\ell}{2},$$

then  $(Y - uX - v)$  divides  $P$  iff it divides both  $Q$  and  $R$ .

# Linear factors of bivariate polynomials

## Observation

$(Y - uX - v)$  divides  $P(X, Y) \iff P(X, uX + v) \equiv 0$

## Gap Theorem

[Chattopadhyay-G.-Koiran-Portier-Strozecki'13]

Let

$$P = \underbrace{\sum_{j=1}^{\ell} a_j X^{\alpha_j} Y^{\beta_j}}_Q + \underbrace{\sum_{j=\ell+1}^k a_j X^{\alpha_j} Y^{\beta_j}}_R$$

with  $uv \neq 0$ ,  $\alpha_1 \leq \dots \leq \alpha_k$ . If  $\ell$  is the smallest index s.t.

$$\alpha_{\ell+1} > \alpha_1 + \binom{\ell}{2},$$

then every linear factor of  $P$  divides both  $Q$  and  $R$  if  $uv \neq 0$ .

# Bound on the valuation

## Definition

$\text{val}(P)$  = degree of the **lowest degree monomial** of  $P \in \mathbb{K}[X]$

▶  $\text{val}(X^3 + 2X^5 - X^{17}) = 3$

# Bound on the valuation

## Definition

$\text{val}(P) = \text{degree of the lowest degree monomial of } P \in \mathbb{K}[X]$

▶  $\text{val}(X^3 + 2X^5 - X^{17}) = 3$

## Theorem

Let  $P = \sum_{j=1}^{\ell} a_j X^{\alpha_j} (uX+v)^{\beta_j} \neq 0$ , with  $uv \neq 0$  and  $\alpha_1 \leq \dots \leq \alpha_{\ell}$ .

Then

$$\text{val}(P) \leq \max_{1 \leq j \leq \ell} \left( \alpha_j + \binom{\ell + 1 - j}{2} \right).$$

# Bound on the valuation

## Definition

$\text{val}(P) =$  degree of the **lowest degree monomial** of  $P \in \mathbb{K}[X]$

▶  $\text{val}(X^3 + 2X^5 - X^{17}) = 3$

## Theorem

Let  $P = \sum_{j=1}^{\ell} a_j X^{\alpha_j} (uX+v)^{\beta_j} \neq 0$ , with  $uv \neq 0$  and  $\alpha_1 \leq \dots \leq \alpha_{\ell}$ .

Then

$$\text{val}(P) \leq \alpha_1 + \binom{\ell}{2}.$$

▶  $X^{\alpha_j} (uX + v)^{\beta_j}$  linearly independent

# Bound on the valuation

## Definition

$\text{val}(P) = \text{degree of the lowest degree monomial of } P \in \mathbb{K}[X]$

▶  $\text{val}(X^3 + 2X^5 - X^{17}) = 3$

## Theorem

Let  $P = \sum_{j=1}^{\ell} a_j X^{\alpha_j} (uX+v)^{\beta_j} \neq 0$ , with  $uv \neq 0$  and  $\alpha_1 \leq \dots \leq \alpha_{\ell}$ .

Then

$$\text{val}(P) \leq \alpha_1 + \binom{\ell}{2}.$$

- ▶  $X^{\alpha_j} (uX+v)^{\beta_j}$  linearly independent
- ▶ Hajós' Lemma: if  $\alpha_1 = \dots = \alpha_{\ell}$ ,  $\text{val}(P) \leq \alpha_1 + (\ell - 1)$

# The Wronskian

## Definition

Let  $f_1, \dots, f_\ell \in \mathbb{K}[X]$ . Then

$$\text{wr}(f_1, \dots, f_\ell) = \det \begin{bmatrix} f_1 & f_2 & \dots & f_\ell \\ f_1' & f_2' & \dots & f_\ell' \\ \vdots & \vdots & & \vdots \\ f_1^{(\ell-1)} & f_2^{(\ell-1)} & \dots & f_\ell^{(\ell-1)} \end{bmatrix}.$$



# The Wronskian

## Definition

Let  $f_1, \dots, f_\ell \in \mathbb{K}[X]$ . Then

$$\text{wr}(f_1, \dots, f_\ell) = \det \begin{bmatrix} f_1 & f_2 & \dots & f_\ell \\ f_1' & f_2' & \dots & f_\ell' \\ \vdots & \vdots & & \vdots \\ f_1^{(\ell-1)} & f_2^{(\ell-1)} & \dots & f_\ell^{(\ell-1)} \end{bmatrix}.$$

## Proposition

[Bôcher, 1900]

$\text{wr}(f_1, \dots, f_\ell) \neq 0 \iff$  the  $f_j$ 's are linearly independent.

# Wronskian & valuation

## Lemma

$$\text{val}(\text{wr}(f_1, \dots, f_\ell)) \geq \sum_{j=1}^{\ell} \text{val}(f_j) - \binom{\ell}{2}$$

Proof.

$$\begin{array}{c|cccc} & \text{val}(f_1) & \text{val}(f_2) & \dots & \text{val}(f_\ell) \\ 0 & f_1 & f_2 & \dots & f_\ell \\ -1 & f'_1 & f'_2 & \dots & f'_\ell \\ \vdots & \vdots & \vdots & & \vdots \\ -(\ell-1) & f_1^{(\ell-1)} & f_2^{(\ell-1)} & \dots & f_\ell^{(\ell-1)} \end{array}$$

# Wronskian & valuation

## Lemma

$$\text{val}(\text{wr}(f_1, \dots, f_\ell)) \geq \sum_{j=1}^{\ell} \text{val}(f_j) - \binom{\ell}{2}$$

## Lemma

Let  $f_j = X^{\alpha_j}(uX + v)^{\beta_j}$ ,  $uv \neq 0$ , linearly independent, and s.t.  $\alpha_j, \beta_j \geq \ell$ . Then

$$\text{val}(\text{wr}(f_1, \dots, f_\ell)) \leq \sum_{j=1}^{\ell} \alpha_j = \sum_{j=1}^{\ell} \text{val}(f_j).$$

# Wronskian & valuation

## Lemma

$$\text{val}(\text{wr}(f_1, \dots, f_\ell)) \geq \sum_{j=1}^{\ell} \text{val}(f_j) - \binom{\ell}{2}$$

## Lemma

Let  $f_j = X^{\alpha_j}(uX + v)^{\beta_j}$ ,  $uv \neq 0$ , linearly independent, and s.t.  $\alpha_j, \beta_j \geq \ell$ . Then

$$\text{val}(\text{wr}(f_1, \dots, f_\ell)) \leq \sum_{j=1}^{\ell} \alpha_j = \sum_{j=1}^{\ell} \text{val}(f_j).$$

**Proof of the theorem.**  $\text{wr}(P, f_2, \dots, f_\ell) = \alpha_1 \text{wr}(f_1, \dots, f_\ell)$

# Wronskian & valuation

## Lemma

$$\text{val}(\text{wr}(f_1, \dots, f_\ell)) \geq \sum_{j=1}^{\ell} \text{val}(f_j) - \binom{\ell}{2}$$

## Lemma

Let  $f_j = X^{\alpha_j}(uX + v)^{\beta_j}$ ,  $uv \neq 0$ , linearly independent, and s.t.  $\alpha_j, \beta_j \geq \ell$ . Then

$$\text{val}(\text{wr}(f_1, \dots, f_\ell)) \leq \sum_{j=1}^{\ell} \alpha_j = \sum_{j=1}^{\ell} \text{val}(f_j).$$

**Proof of the theorem.**  $\text{wr}(P, f_2, \dots, f_\ell) = \alpha_1 \text{wr}(f_1, \dots, f_\ell)$

$$\sum_{j=1}^{\ell} \alpha_j \geq \text{val}(\text{wr}(f_1, \dots, f_\ell)) \geq \text{val}(P) + \sum_{j=2}^{\ell} \alpha_j - \binom{\ell}{2}$$

# How far from optimality?

► Hajós' Lemma:  $\text{val} \left( \sum_{j=1}^{\ell} a_j X^{\alpha} (uX + v)^{\beta_j} \right) \leq \alpha + (\ell - 1)$

# How far from optimality?

▶ Hajós' Lemma:  $\text{val} \left( \sum_{j=1}^{\ell} a_j X^{\alpha} (uX + v)^{\beta_j} \right) \leq \alpha + (\ell - 1)$

▶ Our result:  $\text{val} \left( \sum_{j=1}^{\ell} a_j X^{\alpha_j} (uX + v)^{\beta_j} \right) \leq \alpha_1 + \binom{\ell}{2}$

# How far from optimality?

- ▶ Hajós' Lemma:  $\text{val} \left( \sum_{j=1}^{\ell} a_j X^{\alpha} (uX + v)^{\beta_j} \right) \leq \alpha + (\ell - 1)$
- ▶ Our result:  $\text{val} \left( \sum_{j=1}^{\ell} a_j X^{\alpha_j} (uX + v)^{\beta_j} \right) \leq \alpha_1 + \binom{\ell}{2}$
- ▶ Lemmas: bounds attained, but not simultaneously  $\rightsquigarrow$  trade-off?



# How far from optimality?

- ▶ Hajós' Lemma:  $\text{val} \left( \sum_{j=1}^{\ell} a_j X^{\alpha} (uX + v)^{\beta_j} \right) \leq \alpha + (\ell - 1)$
- ▶ Our result:  $\text{val} \left( \sum_{j=1}^{\ell} a_j X^{\alpha_j} (uX + v)^{\beta_j} \right) \leq \alpha_1 + \binom{\ell}{2}$
- ▶ Lemmas: bounds attained, but not simultaneously  $\rightsquigarrow$  trade-off?
- ▶  $\forall \ell \geq 3, \exists P = \sum_{j=1}^{\ell} a_j X^{\alpha_j} (uX + v)^{\beta_j}$  s.t.  $\text{val}(P) = \alpha_1 + (2\ell - 3)$

# How far from optimality?

- ▶ Hajós' Lemma:  $\text{val} \left( \sum_{j=1}^{\ell} a_j X^{\alpha} (uX + v)^{\beta_j} \right) \leq \alpha + (\ell - 1)$
- ▶ Our result:  $\text{val} \left( \sum_{j=1}^{\ell} a_j X^{\alpha_j} (uX + v)^{\beta_j} \right) \leq \alpha_1 + \binom{\ell}{2}$
- ▶ Lemmas: bounds attained, but not simultaneously  $\rightsquigarrow$  trade-off?
- ▶  $\forall \ell \geq 3, \exists P = \sum_{j=1}^{\ell} a_j X^{\alpha_j} (uX + v)^{\beta_j}$  s.t.  $\text{val}(P) = \alpha_1 + (2\ell - 3)$

$$X^{2\ell-3} = (1+X)^{2\ell+3} - 1 - \sum_{j=3}^{\ell} \frac{2\ell-3}{2j-5} \binom{\ell+j-5}{2j-6} X^{2j-5} (1+X)^{\ell-1-j}$$

# Gap Theorem

## Theorem

Let

$$P = \underbrace{\sum_{j=1}^{\ell} a_j X^{\alpha_j} (uX + v)^{\beta_j}}_Q + \underbrace{\sum_{j=\ell+1}^k a_j X^{\alpha_j} (uX + v)^{\beta_j}}_R$$

with  $uv \neq 0$ ,  $\alpha_1 \leq \dots \leq \alpha_k$ . If

$$\alpha_{\ell+1} > \max_{1 \leq j \leq \ell} \left( \alpha_j + \binom{\ell+1-j}{2} \right),$$

then  $P \equiv 0$  iff both  $Q \equiv 0$  and  $R \equiv 0$ .

# Gap Theorem

## Theorem

Let

$$P = \underbrace{\sum_{j=1}^{\ell} a_j X^{\alpha_j} (uX + v)^{\beta_j}}_Q + \underbrace{\sum_{j=\ell+1}^k a_j X^{\alpha_j} (uX + v)^{\beta_j}}_R$$

with  $uv \neq 0$ ,  $\alpha_1 \leq \dots \leq \alpha_k$ . If

$$\alpha_{\ell+1} > \max_{1 \leq j \leq \ell} \left( \alpha_j + \binom{\ell+1-j}{2} \right) \geq \text{val}(Q),$$

then  $P \equiv 0$  iff both  $Q \equiv 0$  and  $R \equiv 0$ .

$$P = \left( c_{\text{val}(Q)} X^{\text{val}(Q)} + \dots \right) + X^{\alpha_{\ell+1}} \left( a_{\ell+1} (uX + v)^{\beta_{\ell+1}} + \dots \right)$$

# Gap Theorem

## Theorem

Let

$$P = \underbrace{\sum_{j=1}^{\ell} a_j X^{\alpha_j} (uX + v)^{\beta_j}}_Q + \underbrace{\sum_{j=\ell+1}^k a_j X^{\alpha_j} (uX + v)^{\beta_j}}_R$$

with  $uv \neq 0$ ,  $\alpha_1 \leq \dots \leq \alpha_k$ . If  $\ell$  is the smallest index s.t.

$$\alpha_{\ell+1} > \alpha_1 + \binom{\ell}{2},$$

then  $P \equiv 0$  iff both  $Q \equiv 0$  and  $R \equiv 0$ .

$$P = \left( c_{\text{val}(Q)} X^{\text{val}(Q)} + \dots \right) + X^{\alpha_{\ell+1}} \left( a_{\ell+1} (uX + v)^{\beta_{\ell+1}} + \dots \right)$$

# Finding linear factors

## Observation + Gap Theorem (recursively)

$(Y - uX - v)$  divides  $P(X, Y)$

$$\iff P(X, uX + v) \equiv 0$$

# Finding linear factors

## Observation + Gap Theorem (recursively)

$(Y - uX - v)$  divides  $P(X, Y)$

$$\iff P(X, uX + v) \equiv 0$$

$$\iff P_1(X, uX + v) \equiv \dots \equiv P_s(X, uX + v) \equiv 0$$

# Finding linear factors

## Observation + Gap Theorem (recursively)

$(Y - uX - v)$  divides  $P(X, Y)$

$$\iff P(X, uX + v) \equiv 0$$

$$\iff P_1(X, uX + v) \equiv \dots \equiv P_s(X, uX + v) \equiv 0$$

$$\iff (Y - uX - v) \text{ divides each } P_t(X, Y)$$



# Finding linear factors

## Observation + Gap Theorem (recursively)

$(Y - uX - v)$  divides  $P(X, Y)$

$$\iff P(X, uX + v) \equiv 0$$

$$\iff P_1(X, uX + v) \equiv \dots \equiv P_s(X, uX + v) \equiv 0$$

$$\iff (Y - uX - v) \text{ divides each } P_t(X, Y)$$

►  $P_t = \sum_{j=j_t}^{j_t+\ell_t-1} a_j X^{\alpha_j} Y^{\beta_j}$  with  $\alpha_{j_t+\ell_t-1} - \alpha_{j_t} \leq \binom{\ell_t}{2}$

# Finding linear factors

## Observation + Gap Theorem (recursively)

$(Y - uX - v)$  divides  $P(X, Y)$

$$\iff P(X, uX + v) \equiv 0$$

$$\iff P_1(X, uX + v) \equiv \dots \equiv P_s(X, uX + v) \equiv 0$$

$$\iff (Y - uX - v) \text{ divides each } P_t(X, Y)$$

- ▶  $P_t = \sum_{j=j_t}^{j_t+\ell_t-1} a_j X^{\alpha_j} Y^{\beta_j}$  with  $\alpha_{j_t+\ell_t-1} - \alpha_{j_t} \leq \binom{\ell_t}{2}$
- ▶ Independent from  $u$  and  $v$

# Finding linear factors

## Observation + Gap Theorem (recursively)

$(Y - uX - v)$  divides  $P(X, Y)$

$$\iff P(X, uX + v) \equiv 0$$

$$\iff P_1(X, uX + v) \equiv \dots \equiv P_s(X, uX + v) \equiv 0$$

$$\iff (Y - uX - v) \text{ divides each } P_t(X, Y)$$

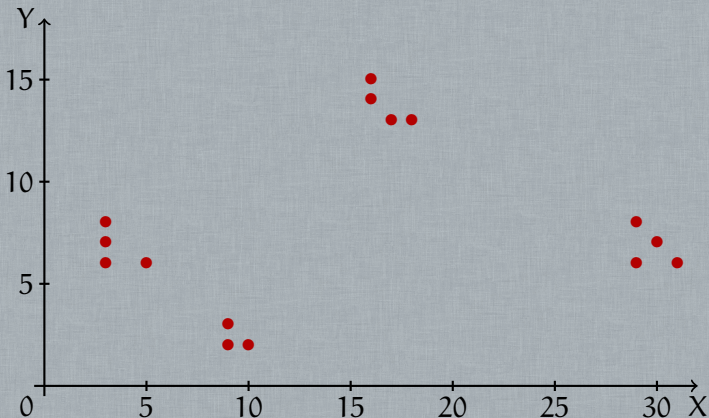
- ▶  $P_t = \sum_{j=j_t}^{j_t+\ell_t-1} a_j X^{\alpha_j} Y^{\beta_j}$  with  $\alpha_{j_t+\ell_t-1} - \alpha_{j_t} \leq \binom{\ell_t}{2}$
- ▶ Independent from  $u$  and  $v$
- ▶  $X$  does not play a special role

## Example

$$\begin{aligned} P = & X^{31}Y^6 - 2X^{30}Y^7 + X^{29}Y^8 - X^{29}Y^6 + X^{18}Y^{13} \\ & - X^{16}Y^{15} + X^{17}Y^{13} + X^{16}Y^{14} + X^{10}Y^2 - X^9Y^3 \\ & + X^9Y^2 - X^5Y^6 + X^3Y^8 - 2X^3Y^7 + X^3Y^6 \end{aligned}$$

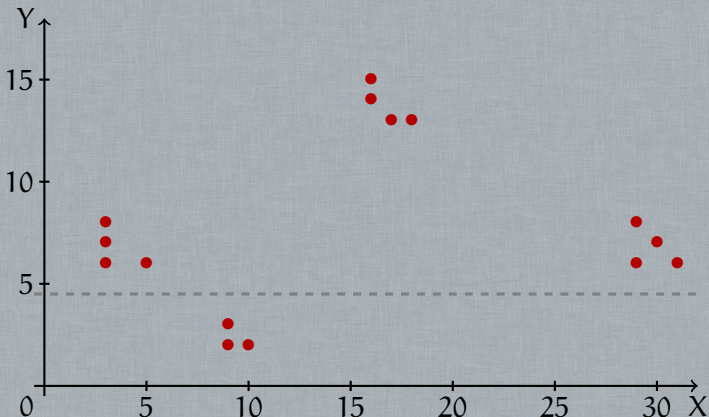
# Example

$$P = X^{31}Y^6 - 2X^{30}Y^7 + X^{29}Y^8 - X^{29}Y^6 + X^{18}Y^{13} \\ - X^{16}Y^{15} + X^{17}Y^{13} + X^{16}Y^{14} + X^{10}Y^2 - X^9Y^3 \\ + X^9Y^2 - X^5Y^6 + X^3Y^8 - 2X^3Y^7 + X^3Y^6$$



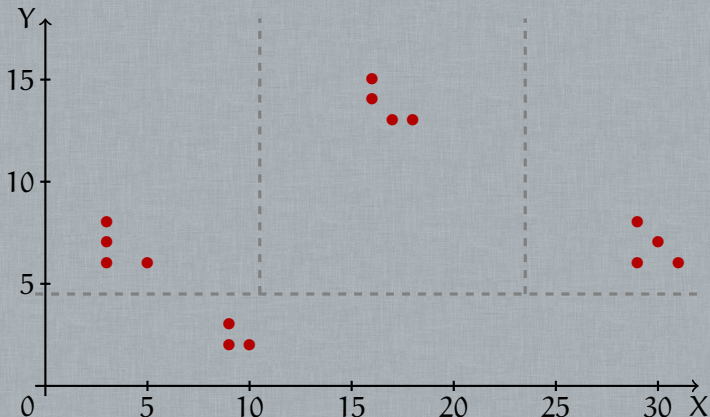
# Example

$$P = X^{31}Y^6 - 2X^{30}Y^7 + X^{29}Y^8 - X^{29}Y^6 + X^{18}Y^{13} \\ - X^{16}Y^{15} + X^{17}Y^{13} + X^{16}Y^{14} + X^{10}Y^2 - X^9Y^3 \\ + X^9Y^2 - X^5Y^6 + X^3Y^8 - 2X^3Y^7 + X^3Y^6$$



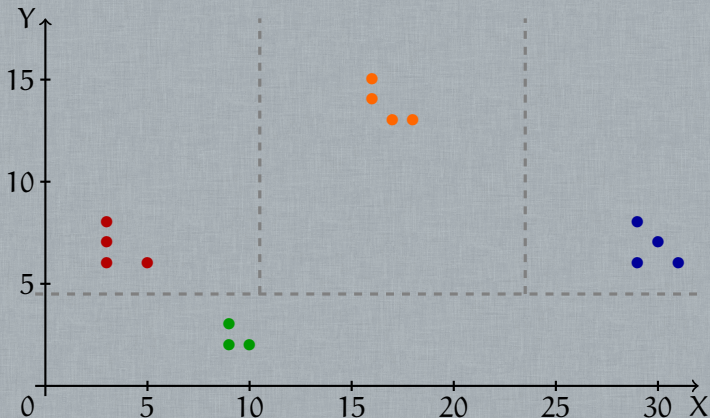
# Example

$$\begin{aligned} P = & X^{31}Y^6 - 2X^{30}Y^7 + X^{29}Y^8 - X^{29}Y^6 + X^{18}Y^{13} \\ & - X^{16}Y^{15} + X^{17}Y^{13} + X^{16}Y^{14} + X^{10}Y^2 - X^9Y^3 \\ & + X^9Y^2 - X^5Y^6 + X^3Y^8 - 2X^3Y^7 + X^3Y^6 \end{aligned}$$



# Example

$$P = X^{31}Y^6 - 2X^{30}Y^7 + X^{29}Y^8 - X^{29}Y^6 + X^{18}Y^{13} \\ - X^{16}Y^{15} + X^{17}Y^{13} + X^{16}Y^{14} + X^{10}Y^2 - X^9Y^3 \\ + X^9Y^2 - X^5Y^6 + X^3Y^8 - 2X^3Y^7 + X^3Y^6$$





## Example

$$\begin{aligned} P = & X^{31}Y^6 - 2X^{30}Y^7 + X^{29}Y^8 - X^{29}Y^6 + X^{18}Y^{13} \\ & - X^{16}Y^{15} + X^{17}Y^{13} + X^{16}Y^{14} + X^{10}Y^2 - X^9Y^3 \\ & + X^9Y^2 - X^5Y^6 + X^3Y^8 - 2X^3Y^7 + X^3Y^6 \end{aligned}$$

$$P_1 = X^3Y^6(-X^2 + Y^2 - 2Y + 1)$$

## Example

$$\begin{aligned} P = & X^{31}Y^6 - 2X^{30}Y^7 + X^{29}Y^8 - X^{29}Y^6 + X^{18}Y^{13} \\ & - X^{16}Y^{15} + X^{17}Y^{13} + X^{16}Y^{14} + X^{10}Y^2 - X^9Y^3 \\ & + X^9Y^2 - X^5Y^6 + X^3Y^8 - 2X^3Y^7 + X^3Y^6 \end{aligned}$$

$$P_1 = X^3Y^6(X - Y + 1)(1 - X - Y)$$

## Example

$$\begin{aligned} P = & X^{31}Y^6 - 2X^{30}Y^7 + X^{29}Y^8 - X^{29}Y^6 + X^{18}Y^{13} \\ & - X^{16}Y^{15} + X^{17}Y^{13} + X^{16}Y^{14} + X^{10}Y^2 - X^9Y^3 \\ & + X^9Y^2 - X^5Y^6 + X^3Y^8 - 2X^3Y^7 + X^3Y^6 \end{aligned}$$

$$P_1 = X^3Y^6(X - Y + 1)(1 - X - Y)$$

$$P_2 = X^9Y^2(X - Y + 1)$$

$$P_3 = X^{16}Y^{13}(X + Y)(X - Y + 1)$$

$$P_4 = X^{29}Y^6(X + Y - 1)(X - Y + 1)$$

## Example

$$\begin{aligned} P = & X^{31}Y^6 - 2X^{30}Y^7 + X^{29}Y^8 - X^{29}Y^6 + X^{18}Y^{13} \\ & - X^{16}Y^{15} + X^{17}Y^{13} + X^{16}Y^{14} + X^{10}Y^2 - X^9Y^3 \\ & + X^9Y^2 - X^5Y^6 + X^3Y^8 - 2X^3Y^7 + X^3Y^6 \end{aligned}$$

$$P_1 = X^3Y^6(X - Y + 1)(1 - X - Y)$$

$$P_2 = X^9Y^2(X - Y + 1)$$

$$P_3 = X^{16}Y^{13}(X + Y)(X - Y + 1)$$

$$P_4 = X^{29}Y^6(X + Y - 1)(X - Y + 1)$$

$\implies$  linear factors of  $P$ :  $(X - Y + 1, 1)$

## Example

$$\begin{aligned} P = & X^{31}Y^6 - 2X^{30}Y^7 + X^{29}Y^8 - X^{29}Y^6 + X^{18}Y^{13} \\ & - X^{16}Y^{15} + X^{17}Y^{13} + X^{16}Y^{14} + X^{10}Y^2 - X^9Y^3 \\ & + X^9Y^2 - X^5Y^6 + X^3Y^8 - 2X^3Y^7 + X^3Y^6 \end{aligned}$$

$$P_1 = X^3Y^6(X - Y + 1)(1 - X - Y)$$

$$P_2 = X^9Y^2(X - Y + 1)$$

$$P_3 = X^{16}Y^{13}(X + Y)(X - Y + 1)$$

$$P_4 = X^{29}Y^6(X + Y - 1)(X - Y + 1)$$

$\implies$  linear factors of  $P$ :  $(X - Y + 1, 1)$ ,  $(X, 3)$ ,  $(Y, 2)$

# Complete algorithm

Find linear factors of  $P(X, Y) = \sum_{j=1}^k a_j X^{\alpha_j} Y^{\beta_j}$

# Complete algorithm

Find linear factors of  $P(X, Y) = \sum_{j=1}^k \alpha_j X^{\alpha_j} Y^{\beta_j}$

monomials

$(X, \min_j \alpha_j)$   
 $(Y, \min_j \beta_j)$

# Complete algorithm

Find linear factors of  $P(X, Y) = \sum_{j=1}^k a_j X^{\alpha_j} Y^{\beta_j}$

monomials

binomials

$(X, \min_j \alpha_j)$   
 $(Y, \min_j \beta_j)$

$(X - a)$   
Factors of  $\sum_j a_j X^{\alpha_j}$   

---

 $(Y - uX)$   
Roots of  $u \mapsto \sum_j a_j u^{\beta_j}$

Univariate lacunary factorization  
[H. Lenstra'99]



# Complete algorithm

Find linear factors of  $P(X, Y) = \sum_{j=1}^k a_j X^{\alpha_j} Y^{\beta_j}$

monomials

binomials

trinomials

$(X, \min_j \alpha_j)$   
 $(Y, \min_j \beta_j)$

$(X - a)$   
Factors of  $\sum_j a_j X^{\alpha_j}$   

---

 $(Y - uX)$   
Roots of  $u \mapsto \sum_j a_j u^{\beta_j}$

Univariate lacunary factorization  
[H. Lenstra'99]

Common factors of  
 $\sum_{j=j_t}^{j_t + \ell_t - 1} a_j X^{\alpha_j} Y^{\beta_j}$   
 $P_t = \sum_{j=j_t}^{j_t + \ell_t - 1} a_j X^{\alpha_j} Y^{\beta_j}$   
with  $\deg(P_t) \leq \mathcal{O}(\ell_t^2)$

Low-degree factorization  
[Kaltofen'82, ..., Lecerf'07]

# Comments

Bottleneck: Factorization of low-degree polynomials

# Comments

Bottleneck: Factorization of low-degree polynomials

↳ Complexity measure:  $\text{gap}(P)$

# Comments

Bottleneck: Factorization of low-degree polynomials

↳ Complexity measure:  $\text{gap}(P)$

$$\blacktriangleright \text{gap}(P) = \begin{cases} \mathcal{O}(k \log k + k \log h_P) & [\text{Kaltofen-Koiran}'05] \\ \mathcal{O}(k^2) & [\text{CGKPS}'13] \end{cases}$$

$$h_P = \max_j |a_j| \text{ if } P \in \mathbb{Z}[X, Y]$$

# Comments

Bottleneck: Factorization of low-degree polynomials

↳ Complexity measure:  $\text{gap}(P)$

$$\text{gap}(P) = \begin{cases} \mathcal{O}(k \log k + k \log h_P) & \text{[Kaltofen-Koiran'05]} \\ \mathcal{O}(k^2) & \text{[CGKPS'13]} \end{cases}$$

$h_P = \max_j |a_j|$  if  $P \in \mathbb{Z}[X, Y]$

- ▶ Algebraic number field only: based on [H. Lenstra'99]

# Positive characteristics

$$(1 + X)^{2^n} + (1 + X)^{2^{n+1}} = X^{2^n}(X + 1) \pmod{2}$$

# Positive characteristics

$$(1 + X)^{2^n} + (1 + X)^{2^{n+1}} = X^{2^n}(X + 1) \pmod{2}$$

## Theorem

Let  $P = \sum_{j=1}^{\ell} a_j X^{\alpha_j} (uX + v)^{\beta_j} \in \mathbb{F}_p^s[X]$ , where  $p > \max_j(\alpha_j + \beta_j)$ .

Then  $\text{val}(P) \leq \max_j(\alpha_j + \binom{\ell+1-j}{2})$ , provided  $P \neq 0$ .

# Positive characteristics

$$(1 + X)^{2^n} + (1 + X)^{2^{n+1}} = X^{2^n}(X + 1) \pmod{2}$$

## Theorem

Let  $P = \sum_{j=1}^{\ell} a_j X^{\alpha_j} (uX + v)^{\beta_j} \in \mathbb{F}_p^s[X]$ , where  $p > \max_j(\alpha_j + \beta_j)$ .

Then  $\text{val}(P) \leq \max_j(\alpha_j + \binom{\ell+1-j}{2})$ , provided  $P \neq 0$ .

## Theorem

[Chattopadhyay-G.-Koiran-Portier-Strozecki'13]

Let  $P = \sum_j a_j X^{\alpha_j} Y^{\beta_j} \in \mathbb{F}_p^s[X, Y]$ , where  $p > \max_j(\alpha_j + \beta_j)$ .

Factors of the form  $(uX + vY + w)$  are

- ▶ computable in **randomized polynomial time** if  $uvw \neq 0$ ;



# Positive characteristics

$$(1 + X)^{2^n} + (1 + X)^{2^{n+1}} = X^{2^n}(X + 1) \pmod{2}$$

## Theorem

Let  $P = \sum_{j=1}^{\ell} a_j X^{\alpha_j} (uX + v)^{\beta_j} \in \mathbb{F}_p^s[X]$ , where  $p > \max_j(\alpha_j + \beta_j)$ .

Then  $\text{val}(P) \leq \max_j(\alpha_j + \binom{\ell+1-j}{2})$ , provided  $P \neq 0$ .

## Theorem

[Chattopadhyay-G.-Koiran-Portier-Strozecki'13]

Let  $P = \sum_j a_j X^{\alpha_j} Y^{\beta_j} \in \mathbb{F}_p^s[X, Y]$ , where  $p > \max_j(\alpha_j + \beta_j)$ .

Factors of the form  $(uX + vY + w)$  are

- ▶ computable in **randomized polynomial time** if  $uvw \neq 0$ ;
- ▶ **NP-hard** to detect under randomized reductions **otherwise**.

# Conclusion

- ▶ Computing linear factors of lacunary bivariate polynomials

# Conclusion

- ▶ Computing linear factors of lacunary bivariate polynomials
  - Reduction to  $\begin{cases} \text{univariate lacunary polynomials} \\ \text{low-degree bivariate polynomials} \end{cases}$

# Conclusion

- ▶ Computing linear factors of lacunary bivariate polynomials
  - Reduction to  $\begin{cases} \text{univariate lacunary polynomials} \\ \text{low-degree bivariate polynomials} \end{cases}$
  - Also works for **multilinear** factors

# Conclusion

- ▶ Computing linear factors of lacunary bivariate polynomials
  - Reduction to  $\left\{ \begin{array}{l} \text{univariate lacunary polynomials} \\ \text{low-degree bivariate polynomials} \end{array} \right.$
  - Also works for **multilinear** factors
  - Also works for **multivariate** polynomials

# Conclusion

- ▶ Computing linear factors of lacunary bivariate polynomials
  - Reduction to  $\left\{ \begin{array}{l} \text{univariate lacunary polynomials} \\ \text{low-degree bivariate polynomials} \end{array} \right.$
  - Also works for **multilinear** factors
  - Also works for **multivariate** polynomials
- ▶ New Gap Theorem (independent of the height)

# Conclusion

- ▶ Computing linear factors of lacunary bivariate polynomials
  - Reduction to  $\left\{ \begin{array}{l} \text{univariate lacunary polynomials} \\ \text{low-degree bivariate polynomials} \end{array} \right.$
  - Also works for **multilinear** factors
  - Also works for **multivariate** polynomials
- ▶ New Gap Theorem (independent of the height)
  - Easy to implement

# Conclusion

- ▶ Computing linear factors of lacunary bivariate polynomials
  - Reduction to  $\left\{ \begin{array}{l} \text{univariate lacunary polynomials} \\ \text{low-degree bivariate polynomials} \end{array} \right.$
  - Also works for **multilinear** factors
  - Also works for **multivariate** polynomials
- ▶ New Gap Theorem (independent of the height)
  - Easy to implement
  - **Large coefficients**



# Conclusion

- ▶ Computing linear factors of lacunary bivariate polynomials
  - Reduction to  $\left\{ \begin{array}{l} \text{univariate lacunary polynomials} \\ \text{low-degree bivariate polynomials} \end{array} \right.$
  - Also works for **multilinear** factors
  - Also works for **multivariate** polynomials
- ▶ New Gap Theorem (independent of the height)
  - Easy to implement
  - **Large coefficients**
  - Partial results for other fields (positive characteristic, absolute factorization)

# Conclusion

- ▶ Computing linear factors of lacunary bivariate polynomials
  - Reduction to  $\left\{ \begin{array}{l} \text{univariate lacunary polynomials} \\ \text{low-degree bivariate polynomials} \end{array} \right.$
  - Also works for **multilinear** factors
  - Also works for **multivariate** polynomials
- ▶ New Gap Theorem (independent of the height)
  - Easy to implement
  - **Large coefficients**
  - Partial results for other fields (positive characteristic, absolute factorization)
  - Two Gap Theorems: mix both!

# Conclusion

- ▶ Computing linear factors of lacunary bivariate polynomials
  - Reduction to  $\left\{ \begin{array}{l} \text{univariate lacunary polynomials} \\ \text{low-degree bivariate polynomials} \end{array} \right.$
  - Also works for **multilinear** factors
  - Also works for **multivariate** polynomials
- ▶ New Gap Theorem (independent of the height)
  - Easy to implement
  - **Large coefficients**
  - Partial results for other fields (positive characteristic, absolute factorization)
  - Two Gap Theorems: mix both!

## Open questions

Can one find **low-degree** factors? And **lacunary** factors?  
What about **smaller characteristics**?

# Conclusion

# Summary

Representations of polynomials, algorithms and lower bounds

# Summary

Representations of polynomials, algorithms and lower bounds

- ▶ Representations of polynomials:

# Summary

## Representations of polynomials, algorithms and lower bounds

- ▶ Representations of polynomials:
  - By circuits, branching programs, (symmetric) determinants

# Summary

## Representations of polynomials, algorithms and lower bounds

- ▶ Representations of polynomials:
  - By circuits, branching programs, (symmetric) determinants
  - As lists: dense, sparse, lacunary



# Summary

## Representations of polynomials, algorithms and lower bounds

- ▶ Representations of polynomials:
  - By circuits, branching programs, (symmetric) determinants
  - As lists: dense, sparse, lacunary
- ▶ Algorithms:

# Summary

## Representations of polynomials, algorithms and lower bounds

- ▶ Representations of polynomials:
  - By circuits, branching programs, (symmetric) determinants
  - As lists: dense, sparse, lacunary
- ▶ Algorithms:
  - Construction of determinantal representations

# Summary

## Representations of polynomials, algorithms and lower bounds

- ▶ Representations of polynomials:
  - By circuits, branching programs, (symmetric) determinants
  - As lists: dense, sparse, lacunary
- ▶ Algorithms:
  - Construction of determinantal representations
  - Factorization of lacunary polynomials

# Summary

## Representations of polynomials, algorithms and lower bounds

- ▶ Representations of polynomials:
  - By circuits, branching programs, (symmetric) determinants
  - As lists: dense, sparse, lacunary
- ▶ Algorithms:
  - Construction of determinantal representations
  - Factorization of lacunary polynomials
  - Polynomial identity testing for several representations

# Summary

## Representations of polynomials, algorithms and lower bounds

- ▶ Representations of polynomials:
  - By circuits, branching programs, (symmetric) determinants
  - As lists: dense, sparse, lacunary
- ▶ Algorithms:
  - Construction of determinantal representations
  - Factorization of lacunary polynomials
  - Polynomial identity testing for several representations
- ▶ Lower Bounds:

# Summary

## Representations of polynomials, algorithms and lower bounds

- ▶ Representations of polynomials:
  - By circuits, branching programs, (symmetric) determinants
  - As lists: dense, sparse, lacunary
- ▶ Algorithms:
  - Construction of determinantal representations
  - Factorization of lacunary polynomials
  - Polynomial identity testing for several representations
- ▶ Lower Bounds:
  - For the resolution of polynomial systems

# Summary

## Representations of polynomials, algorithms and lower bounds

- ▶ **Representations of polynomials:**
  - By circuits, branching programs, (symmetric) determinants
  - As lists: dense, sparse, lacunary
- ▶ **Algorithms:**
  - Construction of determinantal representations
  - Factorization of lacunary polynomials
  - Polynomial identity testing for several representations
- ▶ **Lower Bounds:**
  - For the resolution of polynomial systems
  - For the symmetric determinantal representations in characteristic 2

# Summary

## Representations of polynomials, algorithms and lower bounds

### ▶ Representations of polynomials:

- By circuits, branching programs, (symmetric) determinants
- As lists: dense, sparse, lacunary

### ▶ Algorithms:

- Construction of determinantal representations
- Factorization of lacunary polynomials
- Polynomial identity testing for several representations

### ▶ Lower Bounds:

- For the resolution of polynomial systems
- For the symmetric determinantal representations in characteristic 2
- For the arithmetic complexity of the permanent



# Summary

## Representations of polynomials, algorithms and lower bounds

- ▶ **Representations of polynomials:**
  - By circuits, branching programs, (symmetric) determinants
  - As lists: dense, sparse, lacunary
- ▶ **Algorithms:**
  - Construction of determinantal representations
  - Factorization of lacunary polynomials
  - Polynomial identity testing for several representations
- ▶ **Lower Bounds:**
  - For the resolution of polynomial systems
  - For the symmetric determinantal representations in characteristic 2
  - For the arithmetic complexity of the permanent

Thank you!