Representations of polynomials, algorithms and lower bounds

Bruno Grenet

LIP, ÉNS de Lyon & IRMAR, U. Rennes 1

Séminaire ECO (LIRMM, Montpellier) — February 25, 2013

Representation of Univariate Polynomials

$$P(X) = X^{10} - 4\,X^8 + 8\,X^7 + 5\,X^3 + 1$$

Representations

- Dense:

$$[1, 0, -4, 8, 0, 0, 0, 5, 0, 0, 1]$$

- Sparse:

$$\Big\{(10:1), (8:-4), (7:8), (3:5), (0:1)\Big\}$$

Representation of Multivariate Polynomials

$$P(X,Y,Z) = X^2Y^3Z^5 - 4\,X^3Y^3Z^2 + 8\,X^5Z^2 + 5\,XYZ + 1$$

Representations

- Dense:

$$[1, \dots, -4, \dots, 8, \dots, 5, \dots, 1]$$

- Lacunary (supersparse):

$$\Big\{(2,3,5:1), (3,3,2:-4), (5,0,2:8), (1,1,1:5), (0:1)\Big\}$$

Representation of Multivariate Polynomials

$$P(X,Y,Z) = X^2Y^3Z^5 - 4\,X^3Y^3Z^2 + 8\,X^5Z^2 + 5\,XYZ + 1$$

Representations

- Dense:

$$[1, \ldots, -4, \ldots, 8, \ldots, 5, \ldots, 1]$$

- Sparse:

$$\Big\{(||, |||, ||||| : 1), (|||, |||, || : -4), (|||||, , || : 8), (|, |, | : 5), (, , : 1)\Big\}$$

- Lacunary (supersparse):

$$\Big\{(2,3,5 : 1), (3,3,2 : -4), (5,0,2 : 8), (1,1,1 : 5), (0 : 1)\Big\}$$

Arithmetic Circuits

$$Q(X,Y,Z) = X^4 + 4X^3Y + 6X^2Y^2 + 4XY^3 + X^2Z + 2XYZ + Y^2Z + X^2 + Y^4 + 2XY + Y^2 + Z^2 + 2Z + 1$$

Arithmetic Circuits

$$Q(X, Y, Z) = (X + Y)^4 + (Z + 1)^2 + (X + Y)^2(Z + 1)$$

Arithmetic Circuits

$$Q(X,Y,Z) = (X+Y)^4 + (Z+1)^2 + (X+Y)^2(Z+1)$$

Arithmetic Circuits

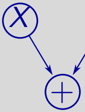
$$\begin{aligned} Q(X,Y,Z) &= (X+Y)^4 + (Z+1)^2 + (X+Y)^2(Z+1) \\ &= (X+Y)^2\big((X+Y)^2 + (Z+1)\big) + (Z+1)^2 \end{aligned}$$

Arithmetic Circuits

$$\begin{aligned} Q(X,Y,Z) &= (X+Y)^4 + (Z+1)^2 + (X+Y)^2(Z+1) \\ &= (X+Y)^4 + \big((Z+1) + (X+Y)^2\big)(Z+1) \end{aligned}$$

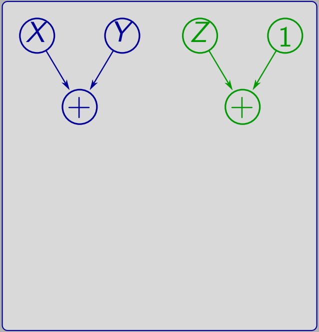
Arithmetic Circuits

$$Q(X,Y,Z) = (X+Y)^4 + (Z+1)^2 + (X+Y)^2(Z+1)$$
$$= (X+Y)^4 + ((Z+1) + (X+Y)^2)(Z+1)$$



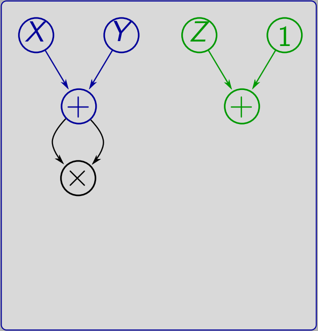
Arithmetic Circuits

$$Q(X,Y,Z) = (X+Y)^4 + (Z+1)^2 + (X+Y)^2(Z+1)$$
$$= (X+Y)^4 + ((Z+1) + (X+Y)^2)(Z+1)$$



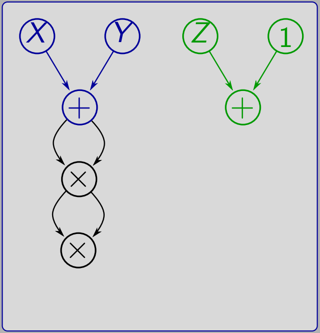
Arithmetic Circuits

$$
\begin{aligned}
Q(X,Y,Z) &= (X+Y)^4 + (Z+1)^2 + (X+Y)^2(Z+1)\\
&= (X+Y)^4 + \big((Z+1) + (X+Y)^2\big)(Z+1)
\end{aligned}
$$



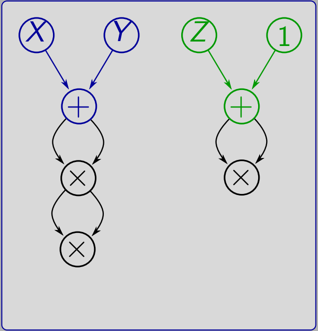
Arithmetic Circuits

$$
\begin{aligned}
Q(X,Y,Z) &= (X+Y)^4 + (Z+1)^2 + (X+Y)^2(Z+1)\\
&= (X+Y)^4 + \big((Z+1) + (X+Y)^2\big)(Z+1)
\end{aligned}
$$



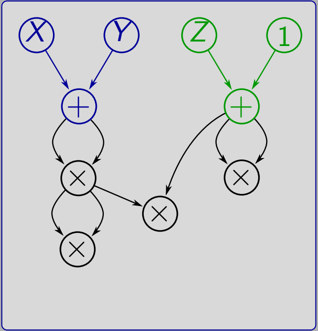
Arithmetic Circuits

$$Q(X,Y,Z) = (X+Y)^4 + (Z+1)^2 + (X+Y)^2(Z+1)$$
$$= (X+Y)^4 + ((Z+1) + (X+Y)^2)(Z+1)$$



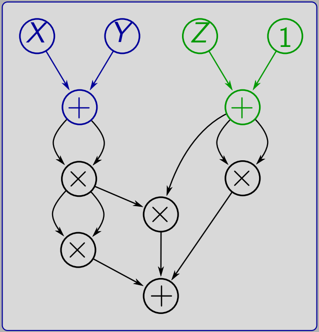
Arithmetic Circuits

$$Q(X,Y,Z) = (X+Y)^4 + (Z+1)^2 + (X+Y)^2(Z+1)$$
$$= (X+Y)^4 + ((Z+1) + (X+Y)^2)(Z+1)$$

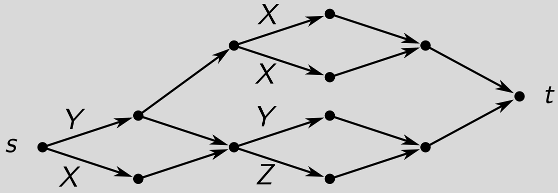


Arithmetic Circuits

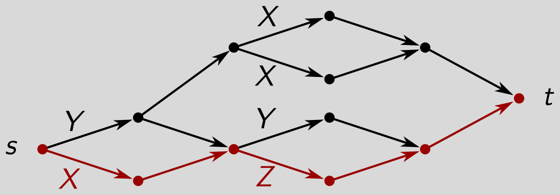
$$Q(X,Y,Z) = (X+Y)^4 + (Z+1)^2 + (X+Y)^2(Z+1)$$
$$= (X+Y)^4 + \big((Z+1) + (X+Y)^2\big)(Z+1)$$



Arithmetic Branching Programs

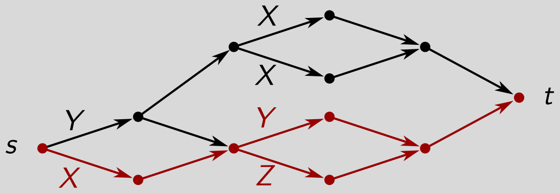


Arithmetic Branching Programs



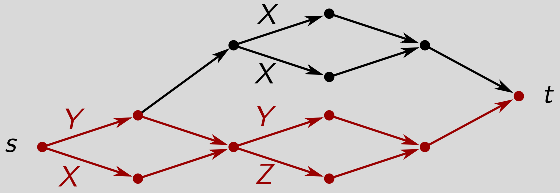
XZ

Arithmetic Branching Programs



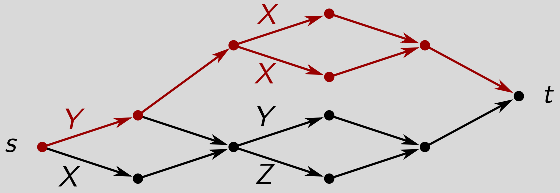
$$X(Y+Z)$$

Arithmetic Branching Programs



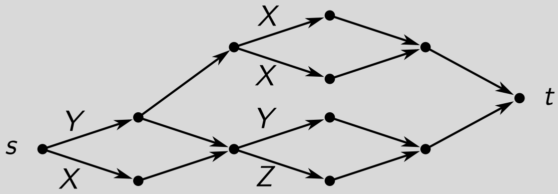
$$(X + Y)(Y + Z)$$

Arithmetic Branching Programs



$2XY$

Arithmetic Branching Programs



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

Some questions

- Links between representations

Some questions

- Links between representations
  - Circuits
  - Branching programs
  - Determinant of matrices

Some questions

- Links between representations
  - Circuits
  - Branching programs
  - Determinant of matrices
- Smallest representations of some polynomials

Some questions

- Links between representations
  - Circuits
  - Branching programs
  - Determinant of matrices
- Smallest representations of some polynomials
  - Determinant
  - Permanent

Some questions

- Links between representations
  - Circuits
  - Branching programs
  - Determinant of matrices
- Smallest representations of some polynomials
  - Determinant
  - Permanent
- Complexity of problems concerning polynomials

Some questions

- Links between representations
  - Circuits
  - Branching programs
  - Determinant of matrices
- Smallest representations of some polynomials
  - Determinant
  - Permanent
- Complexity of problems concerning polynomials
  - Existence of roots — dense, sparse

Some questions

- Links between representations
  - Circuits
  - Branching programs
  - Determinant of matrices
- Smallest representations of some polynomials
  - Determinant
  - Permanent
- Complexity of problems concerning polynomials
  - Existence of roots — dense, sparse
  - Factorization — lacunary

Some questions

- Links between representations
  - Circuits
  - Branching programs
  - Determinant of matrices
- Smallest representations of some polynomials
  - Determinant
  - Permanent
- Complexity of problems concerning polynomials
  - Existence of roots — dense, sparse
  - Factorization — lacunary
  - Polynomial Identity Testing — circuit

Outline

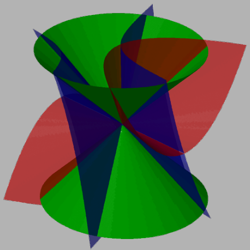
1. Resolution of polynomial systems

2. Determinantal Representations of Polynomials

3. Factorization of lacunary polynomials

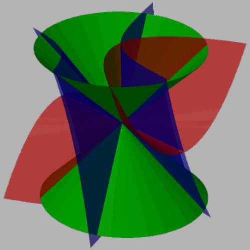
1. Resolution of polynomial systems

Is there a (nonzero) solution?



$$X^2 + Y^2 - Z^2 = 0$$
$$XZ + 3\,XY + YZ + Y^2 = 0$$
$$XZ - Y^2 = 0$$

Is there a (nonzero) solution?

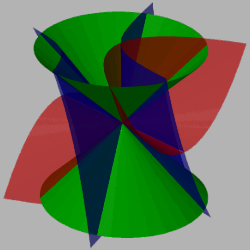


$$X^2 + Y^2 - Z^2 = 0$$
$$XZ + 3\,XY + YZ + Y^2 = 0$$
$$XZ - Y^2 = 0$$

Input: System of polynomials $f = (f_1, f_2, f_3)$, $f_j \in \mathbb{Z}[X, Y, Z]$, **homogeneous**

Question: Is there a point $a = (a_1, a_2, a_3) \in \mathbb{C}^3$, **nonzero**, s.t. $f_1(a) = f_2(a) = f_3(a) = 0$?

Is there a (nonzero) solution?



$$X^2 + Y^2 - Z^2 = 0$$
$$XZ + 3\,XY + YZ + Y^2 = 0$$
$$XZ - Y^2 = 0$$

Input: System of polynomials $f = (f_1, f_2, f_3)$, $f_j \in \mathbb{Z}[X, Y, Z]$, **homogeneous**

Question: Is there a point $a = (a_1, a_2, a_3) \in \mathbb{C}^3$, **nonzero**, s.t. $f(a) = 0$?

More on the homogeneous case

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

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

More on the homogeneous case

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

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

- $s < n + 1$: Always **Yes** ($\rightsquigarrow$ trivial answer)

More on the homogeneous case

Input: $f_1, \dots, f_s \in \mathbb{K}[X_0, \dots, X_n]$, homogeneous
Question: Is there a nonzero $a \in \bar{\mathbb{K}}^{n+1}$ s.t. $f(a) = 0$?

- $s < n + 1$: Always **Yes** ($\rightsquigarrow$ trivial answer)
- $s > n + 1$: **Hard** problem (NP-hard)

More on the homogeneous case

Input: $f_1, \ldots, f_s \in \mathbb{K}[X_0, \ldots, X_n]$, homogeneous
Question: Is there a nonzero $a \in \bar{\mathbb{K}}^{n+1}$ s.t. $f(a) = 0$?

- $s < n+1$: Always **Yes** ($\rightsquigarrow$ trivial answer)
- $s > n+1$: **Hard** problem (NP-hard)
- $s = n+1$: **Resultant**: Algebraic tool to answer the question

More on the homogeneous case

Input: $f_1, \dots, f_s \in \mathbb{K}[X_0, \dots, X_n]$, homogeneous
Question: Is there a nonzero $a \in \bar{\mathbb{K}}^{n+1}$ s.t. $f(a) = 0$?

- $s < n + 1$: Always **Yes** ($\rightsquigarrow$ trivial answer)
- $s > n + 1$: **Hard** problem (NP-hard)
- $s = n + 1$: **Resultant**: Algebraic tool to answer the question

  $\rightsquigarrow$ Trivial? Easy? Hard?

Definitions

PolSys($\mathbb{K}$)

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

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

Definitions

PolSys($\mathbb{K}$)

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

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

HomPolSys($\mathbb{K}$)

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

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

Definitions

PolSys($\mathbb{K}$)

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

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

HomPolSys($\mathbb{K}$)

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

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

Resultant($\mathbb{K}$)

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

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

Upper bounds

Proposition (Koiran'96)

Under the Generalized Riemann Hypothesis, PolSys($\mathbb{Z}$) $\in$ AM.

Upper bounds

Proposition (Koiran'96)

Under the Generalized Riemann Hypothesis, PolSys($\mathbb{Z}$) $\in$ AM.

Class Arthur-Merlin

$$\mathsf{NP} \subseteq \mathsf{AM} = \mathsf{BP} \cdot \mathsf{NP} \subseteq \Pi_2^{\mathsf{P}}$$

Upper bounds

Proposition (Koiran'96)

Under the Generalized Riemann Hypothesis, $\textsc{PolSys}(\mathbb{Z}) \in \mathsf{AM}$.

Corollary

Under GRH, $\textsc{HomPolSys}(\mathbb{Z})$ and $\textsc{Resultant}(\mathbb{Z})$ belong to AM.

Class Arthur-Merlin

$$\mathsf{NP} \subseteq \mathsf{AM} = \mathsf{BP} \cdot \mathsf{NP} \subseteq \Pi_2^{\mathsf{P}}$$

Upper bounds

Proposition (Koiran'96)

Under the Generalized Riemann Hypothesis, $\textsc{PolSys}(\mathbb{Z}) \in \mathsf{AM}$.

Corollary

Under GRH, $\textsc{HomPolSys}(\mathbb{Z})$ and $\textsc{Resultant}(\mathbb{Z})$ belong to AM.

Class Arthur-Merlin

$$\mathsf{NP} \subseteq \mathsf{AM} = \mathsf{BP} \cdot \mathsf{NP} \subseteq \Pi_2^{\mathsf{P}}$$

Positive characteristics

If p is prime, $(\textsc{Hom})\textsc{PolSys}(\mathbb{F}_p)$ & $\textsc{Resultant}(\mathbb{F}_p)$ are in PSPACE.

Known lower bounds

Notation: $\mathbb{F}_0 = \mathbb{Q}$

Known lower bounds

Notation: $\mathbb{F}_0 = \mathbb{Q}$

Proposition (Folklore)

For $p = 0$ or prime, PolSys($\mathbb{F}_p$) & HomPolSys($\mathbb{F}_p$) are **NP-hard**.

Known lower bounds

Notation: $\mathbb{F}_0 = \mathbb{Q}$

Proposition (Folklore)

For $p = 0$ or prime, PolSys($\mathbb{F}_p$) & HomPolSys($\mathbb{F}_p$) are NP-hard.

Proposition (Folklore, see Heintz-Morgenstern'93)

Resultant($\mathbb{Z}$) is NP-hard.

Known lower bounds

Notation: $\mathbb{F}_0 = \mathbb{Q}$

Proposition (Folklore)

For $p = 0$ or prime, PolSys($\mathbb{F}_p$) & HomPolSys($\mathbb{F}_p$) are NP-hard.

Proposition (Folklore, see Heintz-Morgenstern'93)

Resultant($\mathbb{Z}$) is NP-hard.

- Same results with **degree-2** polynomials.

Known lower bounds

Notation: $\mathbb{F}_0 = \mathbb{Q}$

Proposition (Folklore)

For $p = 0$ or prime, PolSys($\mathbb{F}_p$) & HomPolSys($\mathbb{F}_p$) are NP-hard.

Proposition (Folklore, see Heintz-Morgenstern'93)

Resultant($\mathbb{Z}$) is NP-hard.

- Same results with **degree-2** polynomials.

	PolSys	HomPolSys	Resultant
$\mathbb{Z}$	NP-hard	NP-hard	NP-hard
$\mathbb{F}_p$	NP-hard	NP-hard	**Open**

Known lower bounds

Notation: $\mathbb{F}_0 = \mathbb{Q}$

Proposition (Folklore)

For $p = 0$ or prime, PolSys($\mathbb{F}_p$) & HomPolSys($\mathbb{F}_p$) are NP-hard.

Proposition (Folklore, see Heintz-Morgenstern'93)

Resultant($\mathbb{Z}$) is NP-hard.

- Same results with **degree-2** polynomials.

	PolSys	HomPolSys	Resultant
$\mathbb{Z}$	NP-hard	NP-hard	NP-hard
$\mathbb{F}_p$	NP-hard	NP-hard	**Open**

- What happens for Resultant($\mathbb{F}_p$), $p > 0$?

Hardness in positive characteristics

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

Hardness in positive characteristics

- 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

- 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

- 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'10-12)

Let p be a prime number.

Hardness in positive characteristics

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

Theorem (G.-Koiran-Portier'10-12)

Let p be a prime number.

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

Hardness in positive characteristics

- 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'10-12)

Let p be a prime number.

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

Proof idea

$f(X)$: s degree-2 homogeneous polynomials in $\mathbb{F}_p[X_0, \ldots, X_n]$

Proof idea

$f(X)$: s degree-2 homogeneous polynomials in $\mathbb{F}_p[X_0, \ldots, X_n]$

From $f(X)$ to $g(X, Y)$

$$g(X, Y) = \begin{pmatrix} f_1(X) & \\ \vdots & \text{(unchanged)} \\ f_n(X) & \\ & \\ & \\ & \end{pmatrix}$$

Proof idea

$f(X)$: s degree-2 homogeneous polynomials in $\mathbb{F}_p[X_0, \ldots, X_n]$

From $f(X)$ to $g(X, Y)$

$$g(X,Y) = \left(\begin{array}{ll} f_1(X) & \\ \vdots & \\ f_n(X) & \\ f_{n+1}(X) & + \lambda Y_1^2 \\ & \\ & \\ & \end{array} \right)$$

Proof idea

$f(X)$: s degree-2 homogeneous polynomials in $\mathbb{F}_p[X_0, \ldots, X_n]$

From $f(X)$ to $g(X, Y)$

$$g(X,Y) = \begin{pmatrix} f_1(X) & \\ \vdots & \\ f_n(X) & \\ f_{n+1}(X) & + \lambda Y_1^2 \\ f_{n+2}(X) - Y_1^2 & + \lambda Y_2^2 \\ & \\ & \end{pmatrix}$$

Proof idea

$f(X)$: s degree-2 homogeneous polynomials in $\mathbb{F}_p[X_0,\dots,X_n]$

From $f(X)$ to $g(X,Y)$

$$g(X,Y)=\begin{pmatrix} f_1(X) \\ \vdots \\ f_n(X) \\ f_{n+1}(X) \qquad\qquad + \lambda Y_1^2 \\ f_{n+2}(X) - Y_1^2 \qquad + \lambda Y_2^2 \\ \vdots \\ f_{s-1}(X) - Y_{s-n-2}^2 + \lambda Y_{s-n-1}^2 \end{pmatrix}$$

Proof idea

$f(X)$: s degree-2 homogeneous polynomials in $\mathbb{F}_p[X_0, \dots, X_n]$

From $f(X)$ to $g(X, Y)$

$$g(X,Y) = \begin{pmatrix} f_1(X) & & \\ \vdots & & \\ f_n(X) & & \\ f_{n+1}(X) & & +\lambda Y_1^2 \\ f_{n+2}(X) & - Y_1^2 & +\lambda Y_2^2 \\ \vdots & & \\ f_{s-1}(X) & - Y_{s-n-2}^2 & +\lambda Y_{s-n-1}^2 \\ f_s(X) & - Y_{s-n-1}^2 & \end{pmatrix}$$

Proof idea

$f(X)$: s degree-2 homogeneous polynomials in $\mathbb{F}_p[X_0, \ldots, X_n]$

From $f(X)$ to $g(X, Y)$

$$g(X,Y) = \begin{pmatrix} f_1(X) \\ \vdots \\ f_n(X) \\ f_{n+1}(X) + \lambda Y_1^2 \\ f_{n+2}(X) - Y_1^2 + \lambda Y_2^2 \\ \vdots \\ f_{s-1}(X) - Y_{s-n-2}^2 + \lambda Y_{s-n-1}^2 \\ f_s(X) - Y_{s-n-1}^2 \end{pmatrix}$$

Proof idea

$f(X)$: s degree-2 homogeneous polynomials in $\mathbb{F}_p[X_0,\ldots,X_n]$

From $f(X)$ to $g(X,Y)$

$$g(X,Y) = \begin{pmatrix} f_1(X) & & \\ \vdots & & \\ f_n(X) & & \\ f_{n+1}(X) & & +\lambda Y_1^2 \\ f_{n+2}(X) & -\ Y_1^2 & +\lambda Y_2^2 \\ \vdots & & \\ f_{s-1}(X) & -\ Y_{s-n-2}^2 & +\lambda Y_{s-n-1}^2 \\ f_s(X) & -\ Y_{s-n-1}^2 & \end{pmatrix}$$

- $f(a) = 0 \implies g(a,0) = 0$

Proof idea

$f(X)$: s degree-2 homogeneous polynomials in $\mathbb{F}_p[X_0,\dots,X_n]$

From $f(X)$ to $g(X,Y)$

$$g(X,Y) = \begin{pmatrix} f_1(X) & & \\ \vdots & & \\ f_n(X) & & \\ f_{n+1}(X) & & +\lambda Y_1^2 \\ f_{n+2}(X) & -Y_1^2 & +\lambda Y_2^2 \\ \vdots & & \\ f_{s-1}(X) & -Y_{s-n-2}^2 & +\lambda Y_{s-n-1}^2 \\ f_s(X) & -Y_{s-n-1}^2 & \end{pmatrix}$$

- $f(a) = 0 \implies g(a,0) = 0$
- Find λ such that $(g(a,b) = 0 \implies b = 0)$

Proof idea

$f(X)$: s degree-2 homogeneous polynomials in $\mathbb{F}_p[X_0, \dots, X_n]$

From $f(X)$ to $g(X, Y)$

$$g(X,Y) = \begin{pmatrix} f_1(X) & & \\ \vdots & & \\ f_n(X) & & \\ f_{n+1}(X) & & +\lambda Y_1^2 \\ f_{n+2}(X) & - Y_1^2 & +\lambda Y_2^2 \\ \vdots & & \\ f_{s-1}(X) & - Y_{s-n-2}^2 & +\lambda Y_{s-n-1}^2 \\ f_s(X) & - Y_{s-n-1}^2 & \end{pmatrix}$$

- $f(a) = 0 \implies g(a, 0) = 0$
- Find λ such that $(g(a,b) = 0 \implies b = 0 \implies f(a) = 0)$

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.

2. Determinantal Representations of Polynomials

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

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

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

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

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

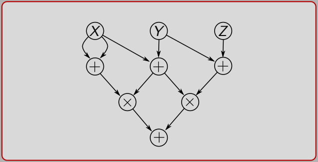
- Complexity of the determinant
- Determinant vs. Permanent: Algebraic "P = NP?"
- Links between circuits, ABPs and the determinant

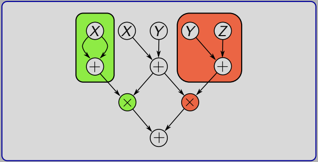
Determinantal representations

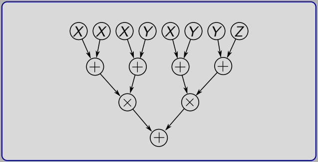
$$2XY+(X+Y)(Y+Z) = \det \begin{vmatrix} 0 & 2 & 0 & 0 & 0 & 0 & 0 & Y & 0 & X & 0 & 0 & 0 & 0 & \frac{1}{2} \\ 2 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & X & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & X & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 &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

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

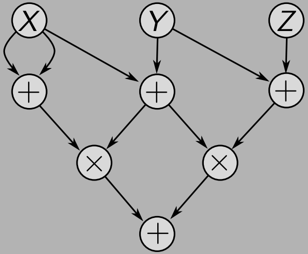
Circuits







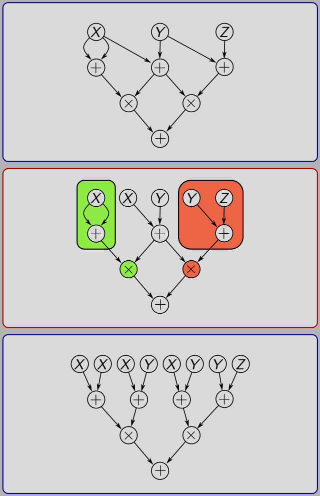
$$2X(X+Y)+(X+Y)(Y+Z)$$



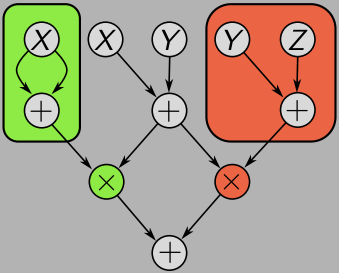
Arithmetic circuit

Size	6
Inputs	3

Circuits



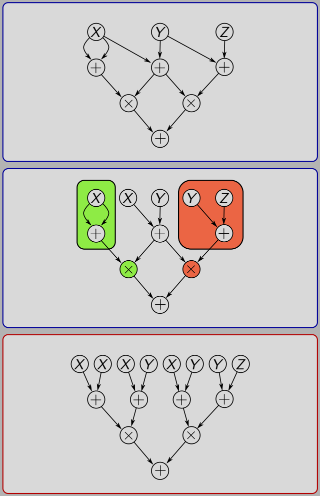
$$2X(X + Y) + (X + Y)(Y + Z)$$



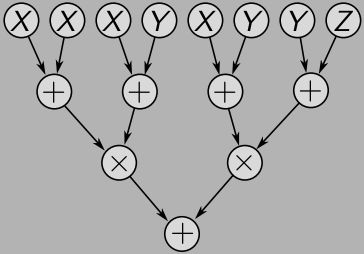
Weakly-skew circuit

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

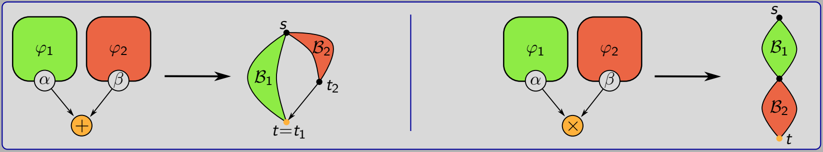
Proposition (Liu-Regan'06, G.-Kaltofen-Koiran-Portier'11)

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

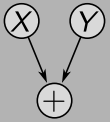
Proposition (Toda'92, Malod-Portier'08)

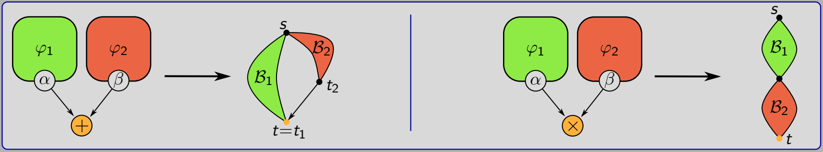
Weakly-skew circuit of size s with i inputs $\rightsquigarrow$ Determinant of a matrix of dimension $(s+i+1)$

From Formulas to Branching Programs

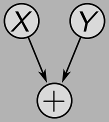


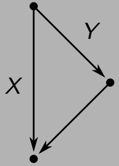
From Formulas to Branching Programs

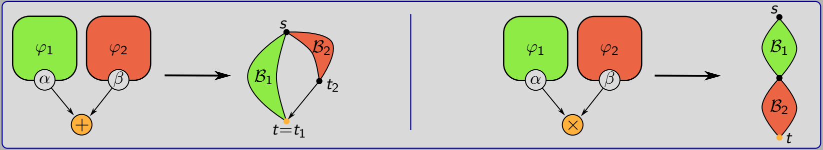




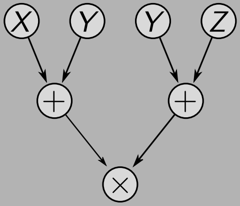
From Formulas to Branching Programs

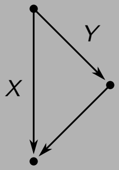


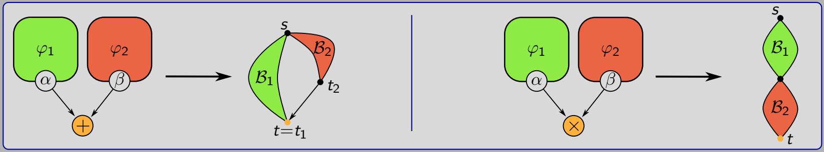




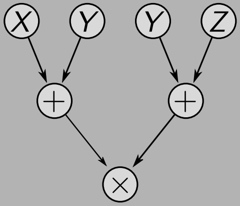
From Formulas to Branching Programs

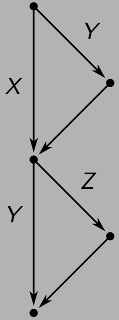


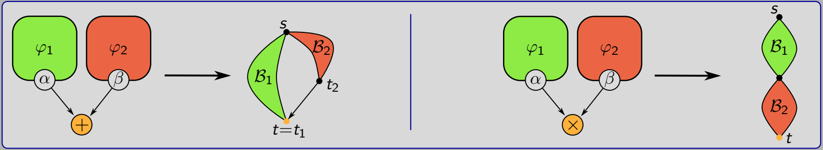




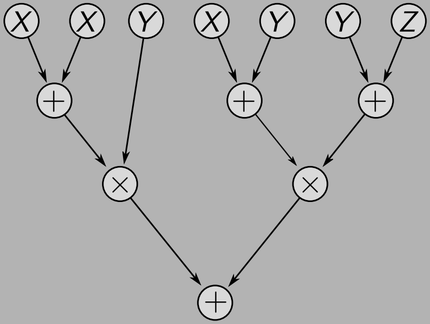
From Formulas to Branching Programs

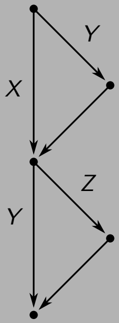


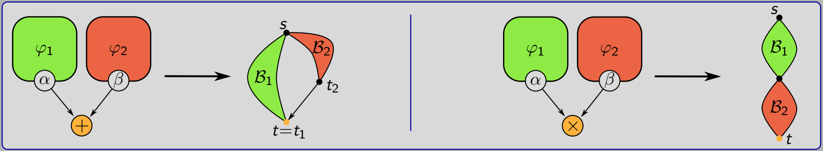




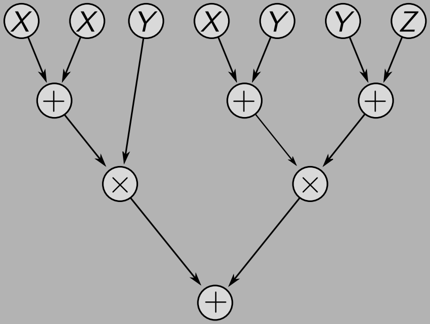
From Formulas to Branching Programs

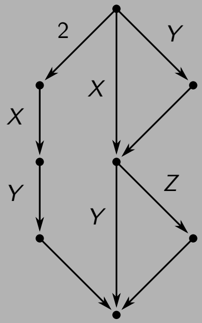


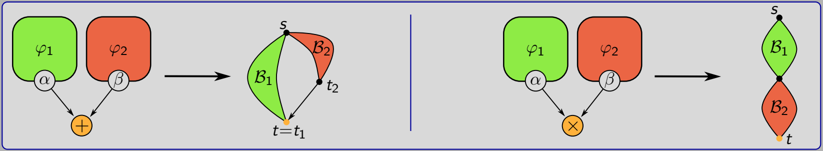




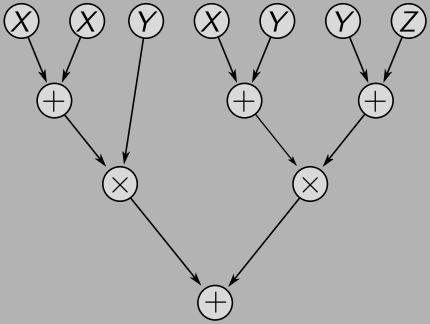
From Formulas to Branching Programs

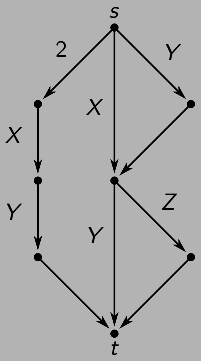


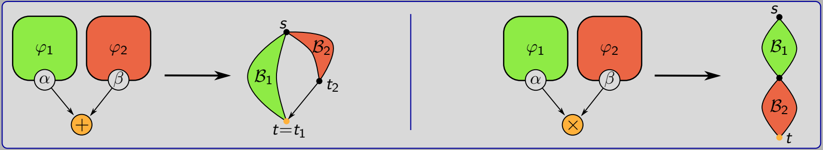




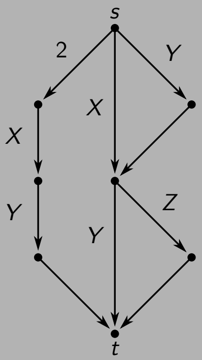
From Formulas to Branching Programs



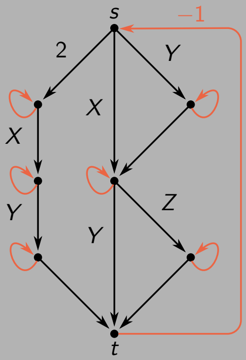




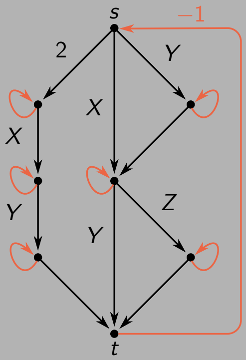
From Branching Programs to Determinants



From Branching Programs to Determinants

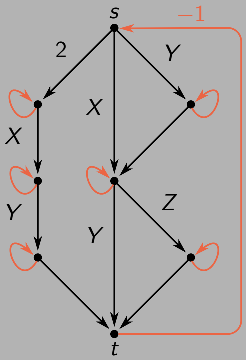


From Branching Programs to Determinants



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

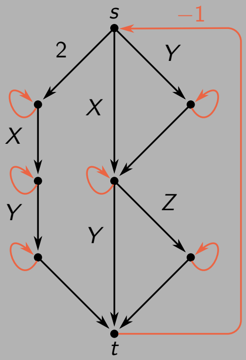
From Branching Programs to Determinants



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

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

From Branching Programs to Determinants

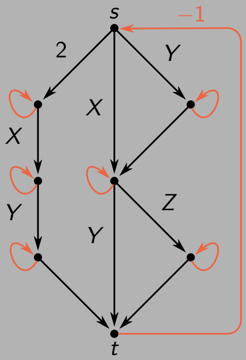


$$M = \begin{pmatrix} 0 & 2 & 0 & 0 & Y & X & 0 & 0 \\ 0 & -1 & X & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & Y & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & Z & Y \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 1 \\ -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

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

- **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

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

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

Branching Program for the Permanent

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

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

Branching Program for the Permanent

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

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

Branching Program for the Permanent

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

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

Theorem (G.'12)

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

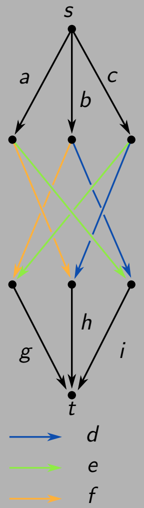
Branching Program for the Permanent

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

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

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 $N = 2^n - 1$**.

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

Permanent versus Determinant

Corollary

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

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

Conjecture (Algebraic P $\neq$ NP)

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

Permanent versus Determinant

Corollary

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

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

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)

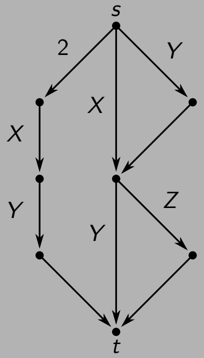
Weakly-skew circuit of **size** s with i **inputs**
$\rightsquigarrow$ Determinant of a matrix of **dimension** $(s+i+1)$

Theorem (G.-Kaltofen-Koiran-Portier'11)

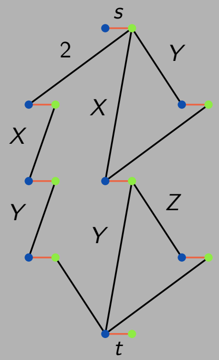
If the underlying field has **characteristic** $\neq 2$,

- 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** $2(s+i)+1$

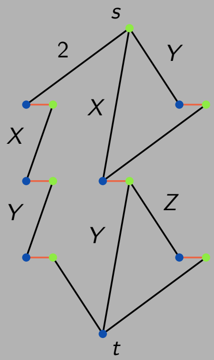
From Branching Programs to Symmetric Determinants



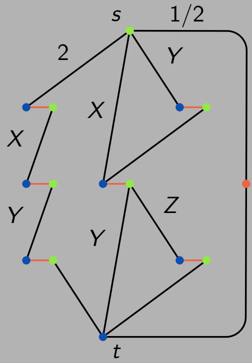
From Branching Programs to Symmetric Determinants



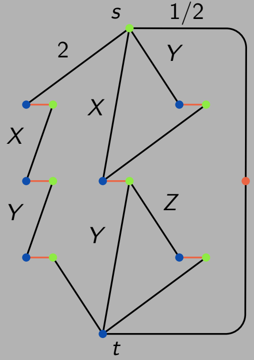
From Branching Programs to Symmetric Determinants



From Branching Programs to Symmetric Determinants

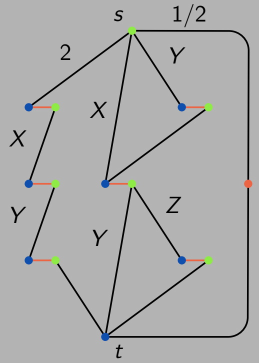


From Branching Programs to Symmetric Determinants



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

From Branching Programs to Symmetric Determinants



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

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

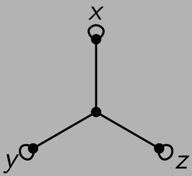
$xy + yz + xz$

SDR in characteristic 2

$$xy + yz + xz = \det \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & x & 0 & 0 \\ 1 & 0 & y & 0 \\ 1 & 0 & 0 & z \end{bmatrix}$$

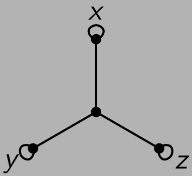
SDR in characteristic 2

$$xy + yz + xz = \det \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & x & 0 & 0 \\ 1 & 0 & y & 0 \\ 1 & 0 & 0 & z \end{bmatrix}$$



SDR in characteristic 2

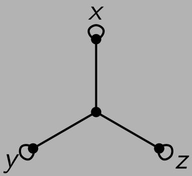
$$xy + yz + xz = \det \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & x & 0 & 0 \\ 1 & 0 & y & 0 \\ 1 & 0 & 0 & z \end{bmatrix}$$



$xz^2 + y^3 + y^2 + z^2$

SDR in characteristic 2

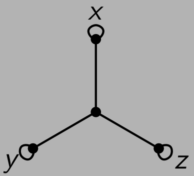
$$xy + yz + xz = \det \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & x & 0 & 0 \\ 1 & 0 & y & 0 \\ 1 & 0 & 0 & z \end{bmatrix}$$



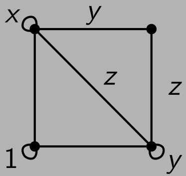
$$xz^2 + y^3 + y^2 + z^2 = \det \begin{bmatrix} x & y & z & 1 \\ y & 0 & z & 0 \\ z & z & y & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}$$

SDR in characteristic 2

$$xy + yz + xz = \det \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & x & 0 & 0 \\ 1 & 0 & y & 0 \\ 1 & 0 & 0 & z \end{bmatrix}$$



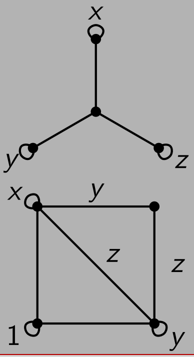
$$xz^2 + y^3 + y^2 + z^2 = \det \begin{bmatrix} x & y & z & 1 \\ y & 0 & z & 0 \\ z & z & y & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}$$



SDR in characteristic 2

$$xy + yz + xz = \det \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & x & 0 & 0 \\ 1 & 0 & y & 0 \\ 1 & 0 & 0 & z \end{bmatrix}$$

$$xz^2 + y^3 + y^2 + z^2 = \det \begin{bmatrix} x & y & z & 1 \\ y & 0 & z & 0 \\ z & z & y & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}$$

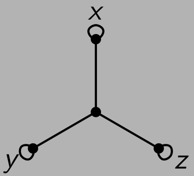


Theorem (G.–Monteil–Thomassé'12)

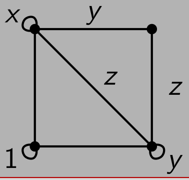
There are polynomials without SDR in characteristic 2, e.g. $xy+z$.

SDR in characteristic 2

$$xy + yz + xz = \det \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & x & 0 & 0 \\ 1 & 0 & y & 0 \\ 1 & 0 & 0 & z \end{bmatrix}$$



$$xz^2 + y^3 + y^2 + z^2 = \det \begin{bmatrix} x & y & z & 1 \\ y & 0 & z & 0 \\ z & z & y & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}$$



Theorem (G.–Monteil–Thomassé'12)

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

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

Determinant and cycle covers

Determinant

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

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

Determinant and cycle covers

Determinant in characteristic 2

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

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

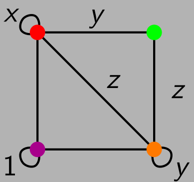
Determinant and cycle covers

Determinant in characteristic 2

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

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

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



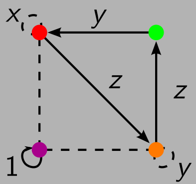
Determinant and cycle covers

Determinant in characteristic 2

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

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

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



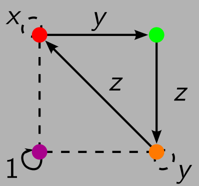
Determinant and cycle covers

Determinant in characteristic 2

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

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

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



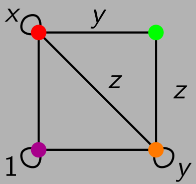
Determinant and partial matchings

Determinant in characteristic 2 of symmetric matrices

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

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

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



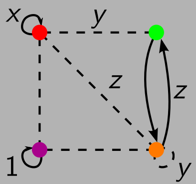
Determinant and partial matchings

Determinant in characteristic 2 of symmetric matrices

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

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

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



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

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

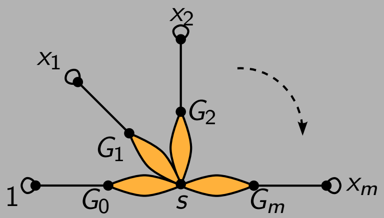
Representable polynomials

Lemma

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

Theorem

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



Obstructions to representability

Theorem

If P is representable, then

$$P \equiv L_1 \times \cdots \times L_k \bmod \langle x_1^2 + 1, \ldots, x_m^2 + 1 \rangle$$

where the L_i's are linear. (linear = degree-1)

Obstructions to representability

Theorem

If P is representable, then

$$P \equiv L_1 \times \cdots \times L_k \bmod \langle x_1^2 + \ell_1^2, \ldots, x_m^2 + \ell_m^2 \rangle$$

where the L_i's are linear. (linear = degree-1)

Obstructions to representability

Theorem

If P is representable, then

$$P \equiv L_1 \times \cdots \times L_k \bmod \langle x_1^2 + \ell_1^2, \ldots, x_m^2 + \ell_m^2 \rangle$$

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

$$P \equiv L_1 \times \cdots \times L_k \bmod \langle x_1^2 + \ell_1^2, \ldots, x_m^2 + \ell_m^2 \rangle$$

where the L_i's are linear. (linear = degree-1)

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

$$\bmod \langle x^2 + 1, y^2 + 1, z^2 + 1 \rangle$$

Obstructions to representability

Theorem

If P is representable, then

$$P \equiv L_1 \times \cdots \times L_k \bmod \langle x_1^2 + \ell_1^2, \ldots, x_m^2 + \ell_m^2 \rangle$$

where the L_i's are linear. (linear = degree-1)

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

$$\bmod \langle x^2+1, y^2+1, z^2+1 \rangle$$

Obstructions to representability

Theorem

If P is representable, then

$$P \equiv L_1 \times \cdots \times L_k \bmod \langle x_1^2 + \ell_1^2, \ldots, x_m^2 + \ell_m^2 \rangle$$

where the L_i's are linear. (linear = degree-1)

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

$$\equiv \det\begin{pmatrix} x & 0 \\ 0 & x+z \end{pmatrix} \qquad \bmod \langle x^2+1, y^2+1, z^2+1 \rangle$$

Obstructions to representability

Theorem

If P is representable, then

$$P \equiv L_1 \times \cdots \times L_k \bmod \langle x_1^2 + \ell_1^2, \ldots, x_m^2 + \ell_m^2 \rangle$$

where the L_i's are linear. (linear = degree-1)

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

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

Obstructions to representability

Theorem

If P is representable, then

$$P \equiv L_1 \times \cdots \times L_k \bmod \langle x_1^2 + \ell_1^2, \ldots, x_m^2 + \ell_m^2 \rangle$$

where the L_i's are linear. (linear = degree-1)

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

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

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

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* $\langle x_1^2 + \ell_1^2, \ldots, x_m^2 + \ell_m^2 \rangle$;

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

Finding a factor

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

Finding a factor

$$(x+y+z+1)\times(x+y+z+1)\times\cdots\times(x+y+z+1)$$

$$\stackrel{?}{\equiv} xy+z \mod \langle x^2, y^2, z^2\rangle$$

Finding a factor

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

Finding a factor

$$(x + y + z + 1) \times (x + y + z + 1) \times \cdots \times (x + y + z + 1)$$

$$\stackrel{?}{\equiv} xy + z \mod \langle x^2, y^2, z^2 \rangle$$

Finding a factor

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

Finding a factor

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

Finding a factor

$$(\qquad z \qquad) \times (x + y + z + 1) \times \cdots \times (x + y + z + 1)$$

$$\overset{?}{\equiv} xy + z \mod \langle x^2, y^2, z^2 \rangle$$

Finding a factor

$$(\qquad z \qquad) \times (x+y+z+1) \times \cdots \times (x+y+z+1)$$

$$\stackrel{?}{\equiv} xy + z \mod \langle x^2, y^2, z^2 \rangle$$

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

Finding a factor

$$(\qquad z \qquad) \times (x + y + z + 1) \times \cdots \times (x + y + z + 1)$$

$$\stackrel{?}{\equiv} xy + z \mod \langle x^2, y^2, z^2 \rangle$$

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

Theorem

Under suitable conditions, P is factorizable if and only if

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

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

Links with coding theory?

Conjecture

Over $\mathbb{F}_2$, there are $\prod_{i=1}^{n}(2^i+1)$ nonzero representable multilinear n-variate polynomials.

Links with coding theory?

Conjecture

Over $\mathbb{F}_2$, there are $\prod_{i=1}^{n}(2^i+1)$ nonzero representable multilinear n-variate polynomials.

- Equals number of self-dual codes of length $2n+2$ over $\mathbb{F}_2$

Links with coding theory?

Conjecture

Over $\mathbb{F}_2$, there are $\prod_{i=1}^{n}(2^i+1)$ nonzero representable multilinear n-variate polynomials.

- Equals number of self-dual codes of length $2n+2$ over $\mathbb{F}_2$

- Linear code of length N: Subspace of the vector space $\mathbb{F}_2^N$

Links with coding theory?

Conjecture

Over $\mathbb{F}_2$, there are $\prod_{i=1}^{n}(2^i+1)$ nonzero representable multilinear n-variate polynomials.

- Equals number of self-dual codes of length $2n+2$ over $\mathbb{F}_2$

- Linear code of length N: Subspace of the vector space $\mathbb{F}_2^N$
- Self-dual code C: for all $x, y \in C$, $x \cdot y = 0$.

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?

3. Factorization of lacunary polynomials

Introduction

Definition (reminder)

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

Introduction

Definition (reminder)

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

- Lacunary representation:

$$\left\{(\alpha_{1j},\dots,\alpha_{nj} : a_j) : 1 \leq j \leq k\right\}$$

Introduction

Definition (reminder)

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

- Lacunary representation:

$$\Big\{(\alpha_{1j},\dots,\alpha_{nj} : a_j) : 1\le j\le k\Big\}$$

- Size:

$$\mathrm{size}(P)\simeq\sum_{j=1}^{k}\mathrm{size}(a_j)+\log(\alpha_{1j})+\cdots+\log(\alpha_{nj})$$

Factorization: dense/sparse vs. lacunary

Factorization of a polynomial P

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

Factorization: dense/sparse vs. lacunary

Factorization of a polynomial P

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

- $\mathbb{F}_q[X]$: randomized polynomial time [Berlekamp'67]

Factorization: dense/sparse vs. lacunary

Factorization of a polynomial P

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

- $\mathbb{F}_q[X]$: randomized polynomial time [Berlekamp'67]
  - $\rightsquigarrow$ $\mathbb{F}_q[X_1, \dots, X_n]$

Factorization: dense/sparse vs. lacunary

Factorization of a polynomial P

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

- $\mathbb{F}_q[X]$: randomized polynomial time [Berlekamp'67]
  - $\rightsquigarrow$ $\mathbb{F}_q[X_1, \dots, X_n]$
- $\mathbb{Z}[X]$: deterministic polynomial time [Lenstra-Lenstra-Lovász'82]

Factorization: dense/sparse vs. lacunary

Factorization of a polynomial P

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

- $\mathbb{F}_q[X]$: randomized polynomial time [Berlekamp'67]
  - $\rightsquigarrow$ $\mathbb{F}_q[X_1, \dots, X_n]$
- $\mathbb{Z}[X]$: deterministic polynomial time [Lenstra–Lenstra–Lovász'82]
  - $\rightsquigarrow$ $\mathbb{Q}(\alpha)[X]$ [A. Lenstra'83, Landau'83]

Factorization: dense/sparse vs. lacunary

Factorization of a polynomial P

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

- $\mathbb{F}_q[X]$: randomized polynomial time [Berlekamp'67]
  - $\rightsquigarrow$ $\mathbb{F}_q[X_1, \dots, X_n]$
- $\mathbb{Z}[X]$: deterministic polynomial time [Lenstra–Lenstra–Lovász'82]
  - $\rightsquigarrow$ $\mathbb{Q}(\alpha)[X]$ [A. Lenstra'83, Landau'83]
  - $\rightsquigarrow$ $\mathbb{Q}(\alpha)[X_1, \dots, X_n]$ [Kaltofen'85, A. Lenstra'87]

Factorization: dense/sparse vs. lacunary

Factorization of a polynomial P

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

- $\mathbb{F}_q[X]$: randomized polynomial time [Berlekamp'67]
  - $\rightsquigarrow$ $\mathbb{F}_q[X_1, \dots, X_n]$
- $\mathbb{Z}[X]$: deterministic polynomial time [Lenstra-Lenstra-Lovász'82]
  - $\rightsquigarrow$ $\mathbb{Q}(\alpha)[X]$ [A. Lenstra'83, Landau'83]
  - $\rightsquigarrow$ $\mathbb{Q}(\alpha)[X_1, \dots, X_n]$ [Kaltofen'85, A. Lenstra'87]

Example

$$X^p - 1 = (X - 1)(1 + X + \cdots + X^{p-1})$$

Factorization: dense/sparse vs. lacunary

Factorization of a polynomial P

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

- $\mathbb{F}_q[X]$: randomized polynomial time [Berlekamp'67]
  - $\rightsquigarrow$ $\mathbb{F}_q[X_1, \dots, X_n]$
- $\mathbb{Z}[X]$: deterministic polynomial time [Lenstra-Lenstra-Lovász'82]
  - $\rightsquigarrow$ $\mathbb{Q}(\alpha)[X]$ [A. Lenstra'83, Landau'83]
  - $\rightsquigarrow$ $\mathbb{Q}(\alpha)[X_1, \dots, X_n]$ [Kaltofen'85, A. Lenstra'87]

Example

$$X^p - 1 = (X - 1)(1 + X + \cdots + X^{p-1})$$

$\Longrightarrow$ restriction to finding **some** factors

Factorization of sparse univariate polynomials

$$P(X) = \sum_{j=1}^{k} a_j X^{\alpha_j} \qquad \text{size}(P) \simeq \sum_{j=1}^{k} \text{size}(a_j) + \log(\alpha_j)$$

Factorization of sparse univariate polynomials

$$P(X) = \sum_{j=1}^{k} a_j X^{\alpha_j} \qquad \mathrm{size}(P) \simeq \sum_{j=1}^{k} \mathrm{size}(a_j) + \log(\alpha_j)$$

Theorem (Cucker-Koiran-Smale'98)

Polynomial-time algorithm to find **integer roots** if $a_j \in \mathbb{Z}$.

Factorization of sparse univariate polynomials

$$P(X) = \sum_{j=1}^{k} a_j X^{\alpha_j} \qquad \mathrm{size}(P) \simeq \sum_{j=1}^{k} \mathrm{size}(a_j) + \log(\alpha_j)$$

Theorem (Cucker-Koiran-Smale'98)

Polynomial-time algorithm to find **integer roots** if $a_j \in \mathbb{Z}$.

Theorem (H. Lenstra'99)

Polynomial-time algorithm to find **factors of degree $\leq d$** if $a_j \in \mathbb{Q}(\alpha)$.

Factorization of lacunary polynomials

Theorem (Kaltofen-Koiran'05)

Polynomial-time algorithm to find **linear factors** of **bivariate** lacunary polynomials over $\mathbb{Q}$.

Factorization of lacunary polynomials

Theorem (Kaltofen-Koiran'05)

Polynomial-time algorithm to find **linear factors** of **bivariate** lacunary polynomials over $\mathbb{Q}$.

Theorem (Kaltofen-Koiran'06)

Polynomial-time algorithm to find **low-degree factors** of **multivariate** lacunary polynomials over $\mathbb{Q}(\alpha)$.

Common ideas

Gap Theorem

$$P = \underbrace{\sum_{j=1}^{\ell} a_j X^{\alpha_j} Y^{\beta_j}}_{P_0} + \underbrace{\sum_{j=\ell+1}^{k} a_j X^{\alpha_j} Y^{\beta_j}}_{P_1}$$

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

Common ideas

Gap Theorem

$$P = \underbrace{\sum_{j=1}^{\ell} a_j X^{\alpha_j} Y^{\beta_j}}_{P_0} + \underbrace{\sum_{j=\ell+1}^{k} a_j X^{\alpha_j} Y^{\beta_j}}_{P_1}$$

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

$$\alpha_{\ell+1} - \alpha_\ell > \operatorname{gap}(P)$$

Common ideas

Gap Theorem

$$P = \underbrace{\sum_{j=1}^{\ell} a_j X^{\alpha_j} Y^{\beta_j}}_{P_0} + \underbrace{\sum_{j=\ell+1}^{k} a_j X^{\alpha_j} Y^{\beta_j}}_{P_1}$$

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

$$\alpha_{\ell+1} - \alpha_\ell > \mathrm{gap}(P),$$

then every factor of P divides both P_0 and P_1.

Common ideas

Gap Theorem

$$P = \underbrace{\sum_{j=1}^{\ell} a_j X^{\alpha_j} Y^{\beta_j}}_{P_0} + \underbrace{\sum_{j=\ell+1}^{k} a_j X^{\alpha_j} Y^{\beta_j}}_{P_1}$$

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

$$\alpha_{\ell+1} - \alpha_\ell > \mathrm{gap}(P),$$

then every factor of P divides both P_0 and P_1.

$\mathrm{gap}(P)$: function of the **algebraic height** of P.

Common algorithmic idea

- Recursively apply the Gap Theorem:

$$P = X^{\alpha_1} P_1 + \cdots + X^{\alpha_s} P_s \text{ with } \deg(P_t) \leq \mathrm{gap}(P)$$

Common algorithmic idea

- Recursively apply the Gap Theorem:

$$P = X^{\alpha_1} P_1 + \cdots + X^{\alpha_s} P_s \text{ with } \deg(P_t) \leq \operatorname{gap}(P)$$

- Factor out $P_1, \ldots, P_s$ using a dense factorization algorithm

Common algorithmic idea

- Recursively apply the Gap Theorem:

$$P = X^{\alpha_1} P_1 + \cdots + X^{\alpha_s} P_s \text{ with } \deg(P_t) \leq \operatorname{gap}(P)$$

- Factor out P_1, …, P_s using a dense factorization algorithm
- Refinements:

Common algorithmic idea

- Recursively apply the Gap Theorem:

$$P = X^{\alpha_1} P_1 + \cdots + X^{\alpha_s} P_s \text{ with } \deg(P_t) \leq \operatorname{gap}(P)$$

- Factor out $P_1, \ldots, P_s$ using a dense factorization algorithm
- Refinements:
  - Factor out $\gcd(P_1, \ldots, P_s)$

Common algorithmic idea

- Recursively apply the Gap Theorem:

$$P = X^{\alpha_1} P_1 + \cdots + X^{\alpha_s} P_s \text{ with } \deg(P_t) \leq \operatorname{gap}(P)$$

- Factor out P_1, …, P_s using a dense factorization algorithm
- Refinements:
  - Factor out $\gcd(P_1, \ldots, P_s)$
  - Factor out only P_1 & check which factors divide the other P_t's

Common algorithmic idea

- Recursively apply the Gap Theorem:

$$P = X^{\alpha_1} P_1 + \cdots + X^{\alpha_s} P_s \text{ with } \deg(P_t) \leq \operatorname{gap}(P)$$

- Factor out P_1, …, P_s using a dense factorization algorithm
- Refinements:
  - Factor out $\gcd(P_1, \ldots, P_s)$
  - Factor out only P_1 & check which factors divide the other P_t's
  - …

Results

Theorem (Chattopadhyay-G.-Koiran-Portier-Strozecki'12)

Polynomial time algorithm to find **multilinear** factors of **bivariate** lacunary polynomials over algebraic number fields.

Results

Theorem (Chattopadhyay-G.-Koiran-Portier-Strozecki'12)

Polynomial time algorithm to find **multilinear** factors of **bivariate** lacunary polynomials over algebraic number fields.

- Linear factors of bivariate lacunary polynomials

  [Kaltofen-Koiran'05]

Results

Theorem (Chattopadhyay-G.-Koiran-Portier-Strozecki'12)

Polynomial time algorithm to find **multilinear** factors of **bivariate** lacunary polynomials over algebraic number fields.

- Linear factors of bivariate lacunary polynomials
  [Kaltofen-Koiran'05]
- gap(P) **independent of the height**

Results

Theorem (Chattopadhyay-G.-Koiran-Portier-Strozecki'12)

Polynomial time algorithm to find **multilinear** factors of **bivariate** lacunary polynomials over algebraic number fields.

- Linear factors of bivariate lacunary polynomials [Kaltofen-Koiran'05]
- gap(P) **independent of the height**
  - $\rightsquigarrow$ More elementary algorithms

Results

Theorem (Chattopadhyay-G.-Koiran-Portier-Strozecki'12)

Polynomial time algorithm to find **multilinear** factors of **bivariate** lacunary polynomials over algebraic number fields.

- Linear factors of bivariate lacunary polynomials [Kaltofen-Koiran'05]
- gap(P) **independent of the height**
  - ⇝ More elementary algorithms
  - ⇝ Gap Theorem valid over **any field of characteristic** 0

Results

Theorem (Chattopadhyay-G.-Koiran-Portier-Strozecki'12)

Polynomial time algorithm to find **multilinear** factors of **bivariate** lacunary polynomials over algebraic number fields.

- Linear factors of bivariate lacunary polynomials [Kaltofen-Koiran'05]
- gap(P) **independent of the height**
  - ⇝ More elementary algorithms
  - ⇝ Gap Theorem valid over **any field of characteristic 0**
- Extension to **multilinear** factors

Results

Theorem (Chattopadhyay-G.-Koiran-Portier-Strozecki'12)

Polynomial time algorithm to find **multilinear** factors of **bivariate** lacunary polynomials over algebraic number fields.

- Linear factors of bivariate lacunary polynomials [Kaltofen-Koiran'05]
- gap(P) **independent of the height**
  - ⇝ More elementary algorithms
  - ⇝ Gap Theorem valid over **any field of characteristic 0**
- Extension to **multilinear** factors
- Results in **positive characteristics**

Linear factors of bivariate polynomials

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

Linear factors of bivariate polynomials

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

Observation

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

Linear factors of bivariate polynomials

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

Observation

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

- Study of polynomials of the form $\sum_j a_j X^{\alpha_j}(uX+v)^{\beta_j}$

Linear factors of bivariate polynomials

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

Observation

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

- Study of polynomials of the form $\sum_j a_j X^{\alpha_j}(uX+v)^{\beta_j}$
- $\mathbb{K}$: any field of characteristic 0

Bound on the valuation

Definition

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

Bound on the valuation

Definition

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

Theorem

Let $P = \sum_{j=1}^{k} a_j X^{\alpha_j}(uX+v)^{\beta_j} \not\equiv 0$, with $uv \neq 0$ and $\alpha_1 \leq \cdots \leq \alpha_k$.

Bound on the valuation

Definition

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

Theorem

Let $P = \sum_{j=1}^{k} a_j X^{\alpha_j} (uX+v)^{\beta_j} \not\equiv 0$, with $uv \neq 0$ and $\alpha_1 \leq \cdots \leq \alpha_k$.

Then

$$\mathrm{val}(P) \leq \max_{1\leq j\leq k} \left(\alpha_j + \binom{k+1-j}{2} \right)$$

Bound on the valuation

Definition

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

Theorem

Let $P = \sum_{j=1}^{k} a_j X^{\alpha_j}(uX+v)^{\beta_j} \not\equiv 0$, with $uv \neq 0$ and $\alpha_1 \leq \cdots \leq \alpha_k$.
Then

$$\mathrm{val}(P) \leq \alpha_1 + \binom{k}{2}$$

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

Bound on the valuation

Definition

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

Theorem

Let $P = \sum_{j=1}^{k} a_j X^{\alpha_j}(uX+v)^{\beta_j} \not\equiv 0$, with $uv \neq 0$ and $\alpha_1 \leq \cdots \leq \alpha_k$.
Then

$$\mathrm{val}(P) \leq \alpha_1 + \binom{k}{2}$$

- $X^{\alpha_j}(uX+v)^{\beta_j}$ linearly independent
- Hajós' Lemma: if $\alpha_1 = \cdots = \alpha_k$, $\mathrm{val}(P) \leq \alpha_1 + (k-1)$

Gap Theorem

Theorem

Let

$$P = \underbrace{\sum_{j=1}^{\ell} a_j X^{\alpha_j}(uX+v)^{\beta_j}}_{P_0} + \underbrace{\sum_{j=\ell+1}^{k} a_j X^{\alpha_j}(uX+v)^{\beta_j}}_{P_1}$$

with $uv \neq 0$, $\alpha_1 \leq \cdots \leq \alpha_k$. 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 $P_0 \equiv 0$ and $P_1 \equiv 0$.

Gap Theorem

Theorem

Let

$$P = \underbrace{\sum_{j=1}^{\ell} a_j X^{\alpha_j}(uX+v)^{\beta_j}}_{P_0} + \underbrace{\sum_{j=\ell+1}^{k} a_j X^{\alpha_j}(uX+v)^{\beta_j}}_{P_1}$$

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

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

then $P \equiv 0$ iff both $P_0 \equiv 0$ and $P_1 \equiv 0$.

The Wronskian

Definition

Let $f_1, \ldots, f_k \in \mathbb{K}[X]$. Then

$$\operatorname{wr}(f_1, \ldots, f_k) = \det \begin{bmatrix} f_1 & f_2 & \ldots & f_k \\ f_1' & f_2' & \ldots & f_k' \\ \vdots & \vdots & & \vdots \\ f_1^{(k-1)} & f_2^{(k-1)} & \ldots & f_k^{(k-1)} \end{bmatrix}.$$

The Wronskian

Definition

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

$$\mathrm{wr}(f_1, \dots, f_k) = \det \begin{bmatrix} f_1 & f_2 & \dots & f_k \\ f_1' & f_2' & \dots & f_k' \\ \vdots & \vdots & & \vdots \\ f_1^{(k-1)} & f_2^{(k-1)} & \dots & f_k^{(k-1)} \end{bmatrix}.$$

Proposition (Bôcher, 1900)

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

Wronskian & valuation

Lemma

$$\mathrm{val}(\mathrm{wr}(f_1,\dots,f_k)) \geq \sum_{j=1}^{k} \mathrm{val}(f_j) - \binom{k}{2}$$

Wronskian & valuation

Lemma

$$\mathrm{val}(\mathrm{wr}(f_1,\dots,f_k)) \geq \sum_{j=1}^{k} \mathrm{val}(f_j) - \binom{k}{2}$$

Lemma

Let $f_j = X^{\alpha_j}(uX+v)^{\beta_j}$, $uv \neq 0$, linearly independent, and s.t. $\alpha_j, \beta_j \geq k-1$. Then

$$\mathrm{val}(\mathrm{wr}(f_1,\dots,f_k)) \leq \sum_{j=1}^{k} \alpha_j.$$

Wronskian & valuation

Lemma

$$\mathrm{val}(\mathrm{wr}(f_1,\dots,f_k)) \geq \sum_{j=1}^{k} \mathrm{val}(f_j) - \binom{k}{2}$$

Lemma

Let $f_j = X^{\alpha_j}(uX+v)^{\beta_j}$, $uv \neq 0$, linearly independent, and s.t. $\alpha_j, \beta_j \geq k-1$. Then

$$\mathrm{val}(\mathrm{wr}(f_1,\dots,f_k)) \leq \sum_{j=1}^{k} \alpha_j.$$

Proof of the theorem. $\mathrm{wr}(P, f_2, \dots, f_k) = a_1\,\mathrm{wr}(f_1,\dots,f_k)$

Wronskian & valuation

Lemma

$$\mathrm{val}(\mathrm{wr}(f_1,\dots,f_k)) \geq \sum_{j=1}^{k} \mathrm{val}(f_j) - \binom{k}{2}$$

Lemma

Let $f_j = X^{\alpha_j}(uX+v)^{\beta_j}$, $uv \neq 0$, linearly independent, and s.t. $\alpha_j, \beta_j \geq k-1$. Then

$$\mathrm{val}(\mathrm{wr}(f_1,\dots,f_k)) \leq \sum_{j=1}^{k} \alpha_j.$$

Proof of the theorem. $\mathrm{wr}(P, f_2, \dots, f_k) = a_1 \,\mathrm{wr}(f_1,\dots,f_k)$

$$\sum_{j=1}^{k} \alpha_j \geq \mathrm{val}(\mathrm{wr}(f_1,\dots,f_k)) \geq \mathrm{val}(P) + \sum_{j=2}^{k} \alpha_j - \binom{k}{2}$$

Finding linear factors

Observation + Gap Theorem

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

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

Finding linear factors

Observation + Gap Theorem

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

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

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

Finding linear factors

Observation + Gap Theorem

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

$$\begin{aligned}
&\iff P(X, uX + v) \equiv 0\\
&\iff P_1(X, uX + v) \equiv \cdots \equiv P_s(X, uX + v) \equiv 0\\
&\iff (Y - uX - v) \text{ divides each } P_t(X, Y)
\end{aligned}$$

Finding linear factors

Observation + Gap Theorem

$$
\begin{aligned}
(Y - uX - v) \text{ divides } P(X,Y)& \\
&\iff P(X, uX+v) \equiv 0 \\
&\iff P_1(X, uX+v) \equiv \cdots \equiv P_s(X, uX+v) \equiv 0 \\
&\iff (Y - uX - v) \text{ divides each } P_t(X,Y)
\end{aligned}
$$

- Find linear factors of low-degree polynomials
  $\rightsquigarrow$ [Kaltofen'82, ..., Lecerf'07]

Finding linear factors

Observation + Gap Theorem

$$
\begin{aligned}
(Y - uX - v) \text{ divides } P(X,Y) \\
&\iff P(X, uX+v) \equiv 0 \\
&\iff P_1(X, uX+v) \equiv \cdots \equiv P_s(X, uX+v) \equiv 0 \\
&\iff (Y - uX - v) \text{ divides each } P_t(X,Y)
\end{aligned}
$$

- Find linear factors of low-degree polynomials
  $\rightsquigarrow$ [Kaltofen'82, ..., Lecerf'07]
- $\mathbb{K} = \mathbb{Q}(\alpha)$: algebraic number field

Some details

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

Some details

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

1. If $u = 0$: Factors of polynomials $\sum_j a_j Y^{\beta_j}$

Some details

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

1. If $u = 0$: Factors of polynomials $\sum_j a_j Y^{\beta_j}$ [H. Lenstra'99]

Some details

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

1. If $u = 0$: Factors of polynomials $\sum_j a_j Y^{\beta_j}$ [H. Lenstra'99]
2. If $v = 0$: $P(X, uX) = \sum_j a_j u^{\beta_j} X^{\alpha_j + \beta_j}$

Some details

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

1. If $u = 0$: Factors of polynomials $\sum_j a_j Y^{\beta_j}$ [H. Lenstra'99]
2. If $v = 0$: $P(X, uX) = \sum_j a_j u^{\beta_j} X^{\alpha_j + \beta_j}$ [H. Lenstra'99]

Some details

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

1. If $u = 0$: Factors of polynomials $\sum_j a_j Y^{\beta_j}$ [H. Lenstra'99]
2. If $v = 0$: $P(X, uX) = \sum_j a_j u^{\beta_j} X^{\alpha_j + \beta_j}$ [H. Lenstra'99]
3. If $u, v \neq 0$:

Some details

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

1. If $u = 0$: Factors of polynomials $\sum_j a_j Y^{\beta_j}$ [H. Lenstra'99]
2. If $v = 0$: $P(X, uX) = \sum_j a_j u^{\beta_j} X^{\alpha_j + \beta_j}$ [H. Lenstra'99]
3. If $u, v \neq 0$:
   - Compute $P = P_1 + \cdots + P_s$ where $P_t = \sum_j a_j X^{\alpha_j} Y^{\beta_j}$ with $\alpha_{\max} \leq \alpha_{\min} + \binom{k}{2}$

Some details

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

1. If $u = 0$: Factors of polynomials $\sum_j a_j Y^{\beta_j}$ [H. Lenstra'99]
2. If $v = 0$: $P(X, uX) = \sum_j a_j u^{\beta_j} X^{\alpha_j + \beta_j}$ [H. Lenstra'99]
3. If $u, v \neq 0$:
   - Compute $P = P_1 + \cdots + P_s$ where $P_t = \sum_j a_j X^{\alpha_j} Y^{\beta_j}$ with $\alpha_{\max} \leq \alpha_{\min} + \binom{k}{2}$
   - Invert the roles of X and Y, to get $\beta_{\max} \leq \beta_{\min} + \binom{k}{2}$

Some details

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

1. If $u = 0$: Factors of polynomials $\sum_j a_j Y^{\beta_j}$ [H. Lenstra'99]
2. If $v = 0$: $P(X, uX) = \sum_j a_j u^{\beta_j} X^{\alpha_j + \beta_j}$ [H. Lenstra'99]
3. If $u, v \neq 0$:
   - Compute $P = P_1 + \cdots + P_s$ where $P_t = \sum_j a_j X^{\alpha_j} Y^{\beta_j}$ with $\alpha_{\max} \leq \alpha_{\min} + \binom{k}{2}$
   - Invert the roles of X and Y, to get $\beta_{\max} \leq \beta_{\min} + \binom{k}{2}$
   - Apply some dense factorization algorithm [Kaltofen'82, …, Lecerf'07]

Positive characteristic

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

Positive characteristic

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

Theorem

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

Then $\mathrm{val}(P) \leq \max_j\left(\alpha_j + \binom{k+1-j}{2}\right)$, provided $P \not\equiv 0$.

Positive characteristic

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

Theorem

Let $P = \sum_{j=1}^{k} a_j X^{\alpha_j}(uX+v)^{\beta_j} \in \mathbb{F}_{p^s}[X]$, where $p > \max_j(\alpha_j + \beta_j)$.
Then $\mathrm{val}(P) \leq \max_j\left(\alpha_j + \binom{k+1-j}{2}\right)$, provided $P \not\equiv 0$.

Theorem

Let $P = \sum_j a_j X^{\alpha_j} Y^{\beta_j} \in \mathbb{F}_{p^s}[X,Y]$, where $p > \max_j(\alpha_j + \beta_j)$.
Finding factors of the form $(uX + vY + w)$ is

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

Positive characteristic

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

Theorem

Let $P = \sum_{j=1}^{k} a_j X^{\alpha_j}(uX+v)^{\beta_j} \in \mathbb{F}_{p^s}[X]$, where $p > \max_j(\alpha_j + \beta_j)$.
Then $\mathrm{val}(P) \leq \max_j\left(\alpha_j + \binom{k+1-j}{2}\right)$, provided $P \not\equiv 0$.

Theorem

Let $P = \sum_j a_j X^{\alpha_j} Y^{\beta_j} \in \mathbb{F}_{p^s}[X,Y]$, where $p > \max_j(\alpha_j + \beta_j)$.
Finding factors of the form $(uX + vY + w)$ is

- doable in **randomized polynomial time** if $uvw \neq 0$;
- **NP-hard** under randomized reductions **otherwise**.

Conclusion

Finding **multilinear factors** of **bivariate** lacunary polynomials

- More elementary proofs for [Kaltofen-Koiran'05]

Conclusion

Finding **multilinear factors** of **bivariate** lacunary polynomials

- More elementary proofs for [Kaltofen-Koiran'05]
- There exists $P = \sum_{j=1}^{k} a_j X^{\alpha_j}(uX+v)^{\beta_j}$ s.t. $\mathrm{val}(P) = \alpha_1 + (2k-3)$

Conclusion

Finding **multilinear factors** of **bivariate** lacunary polynomials

- More elementary proofs for [Kaltofen-Koiran'05]
- There exists $P = \sum_{j=1}^{k} a_j X^{\alpha_j}(uX+v)^{\beta_j}$ s.t. $\mathrm{val}(P) = \alpha_1 + (2k-3)$
- Results in large **positive characteristic**

Conclusion

Finding **multilinear factors** of **bivariate** lacunary polynomials

- More elementary proofs for [Kaltofen-Koiran'05]
- There exists $P = \sum_{j=1}^{k} a_j X^{\alpha_j}(uX+v)^{\beta_j}$ s.t. $\mathrm{val}(P) = \alpha_1 + (2k-3)$
- Results in large **positive characteristic**

Main open problem

Extend to low-degree factors of multivariate polynomials

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!