The Limited Power of Powering

Polynomial Identity Testing and a Depth-four Lower Bound for the Permanent

Bruno Grenet

ÉNS Lyon

Pascal Koiran

ÉNS Lyon

Natacha Portier

ÉNS Lyon

Yann Strozecki

U. Paris Sud XI

Journées Nationales du Calcul Formel
CIRM, Marseille – November 18, 2011

Representation of Univariate Polynomials

$$P(X) = X^{10} + 5X^6 + 3X^2 + 1$$

Representations

- Dense: $[1, 0, 0, 0, 5, 0, 0, 0, 3, 0, 1]$
- Sparse: $\{(10, 1), (6, 5), (2, 3), (0, 1)\}$

Representation of Multivariate Polynomials

$$P(x, y, z) = x^5 y^3 z^2 + 5xy^4 z + 3yz + 1$$

Representations

- Dense: $[1, \ldots, 5, \ldots, 3, \ldots, 1]$
- Sparse: $\{(5; 3; 2, 1), (1; 4; 1, 5), (0; 1; 1, 3), (0, 1)\}$

$\rightsquigarrow$ Dense representation no longer relevant!

Representation of Multivariate Polynomials

$$P(x, y, z) = x^5 y^3 z^2 + 5xy^4 z + 3yz + 1$$

Representations

- Dense: $[1, \ldots, 5, \ldots, 3, \ldots, 1]$
- Sparse: $\{(5; 3; 2, 1), (1; 4; 1, 5), (0; 1; 1, 3), (0, 1)\}$

$\rightsquigarrow$ Dense representation no longer relevant!

Sparse representation not always relevant either.

Arithmetic Circuits

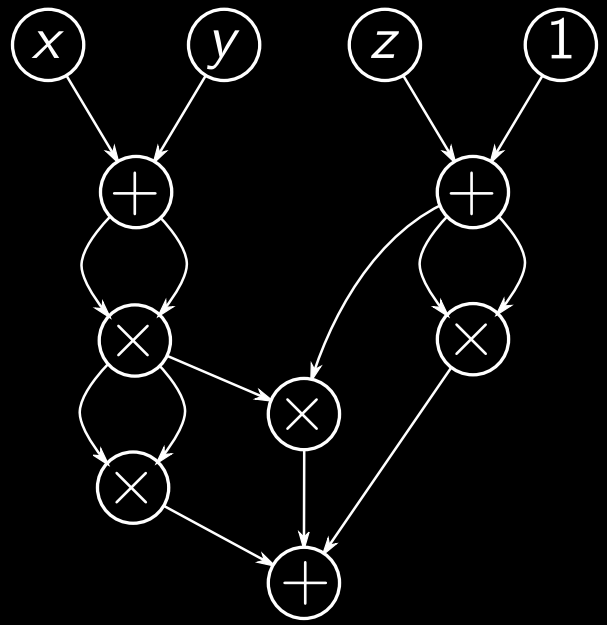
$$Q(x,y,z) = x^4 + 4\,x^3y + 6\,x^2y^2 + 4\,xy^3 + x^2z + 2\,xyz + y^2z + x^2 + y^4 + 2\,xy + y^2 + z^2 + 2\,z + 1$$

Arithmetic Circuits

$$Q(x, y, z) = (x + y)^4 + (z + 1)^2 + (x + y)^2(z + 1)$$

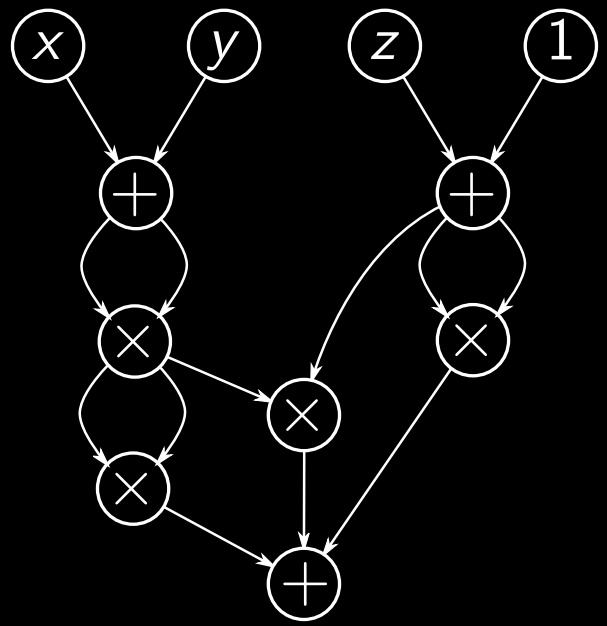
Arithmetic Circuits

$$Q(x, y, z) = (x + y)^4 + (z + 1)^2 + (x + y)^2(z + 1)$$



Arithmetic Circuits

$$Q(x, y, z) = (x + y)^4 + (z + 1)^2 + (x + y)^2(z + 1)$$



$\rightsquigarrow$ Straight Line Programs

Algebraic Complexity Theory

Complexity of a polynomial = size of its smallest circuit

Algebraic Complexity Theory

Complexity of a polynomial = size of its smallest circuit

- Which polynomials have low/high complexity?

Algebraic Complexity Theory

Complexity of a polynomial = size of its smallest circuit

- Which polynomials have low/high complexity?
  - Polynomial complexity: Determinant

$$\det((x_{ij})_{1\leq i,j\leq n}) = \sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} x_{i\sigma(i)}$$

Algebraic Complexity Theory

Complexity of a polynomial = size of its smallest circuit

- Which polynomials have low/high complexity?
  - Polynomial complexity: Determinant
  - Non-polynomial complexity: Permanent?

$$\mathrm{per}((x_{ij})_{1\leq i,j\leq n}) = \sum_{\sigma\in\mathfrak{S}_n} \prod_{i=1}^{n} x_{i\sigma(i)}$$

Algebraic Complexity Theory

Complexity of a polynomial = size of its smallest circuit

- Which polynomials have low/high complexity?
  - Polynomial complexity: Determinant
  - Non-polynomial complexity: Permanent?

  } "Algebraic P vs NP"

$$\mathrm{per}((x_{ij})_{1\leq i,j\leq n}) = \sum_{\sigma\in\mathfrak{S}_n} \prod_{i=1}^{n} x_{i\sigma(i)}$$

Algebraic Complexity Theory

Complexity of a polynomial = size of its smallest circuit

- Which polynomials have low/high complexity?
  - Polynomial complexity: Determinant
  - Non-polynomial complexity: Permanent?

  } "Algebraic P vs NP"

Conjecture (Algebraic P $\neq$ NP)

The complexity of the permanent is super-polynomial.

$$\mathrm{per}((x_{ij})_{1\leq i,j\leq n}) = \sum_{\sigma\in\mathfrak{S}_n} \prod_{i=1}^{n} x_{i\sigma(i)}$$

Algebraic Complexity Theory

Complexity of a polynomial = size of its smallest circuit

- Which polynomials have low/high complexity?
  - Polynomial complexity: Determinant
  - Non-polynomial complexity: Permanent?

  } "Algebraic P vs NP"

Conjecture (Algebraic P $\neq$ NP)

The complexity of the permanent is super-polynomial.

- (Boolean) Complexity of problems on circuits

Algebraic Complexity Theory

Complexity of a polynomial = size of its smallest circuit

- Which polynomials have low/high complexity?
  - Polynomial complexity: Determinant
  - Non-polynomial complexity: Permanent?

} "Algebraic P vs NP"

Conjecture (Algebraic P $\neq$ NP)

The complexity of the permanent is super-polynomial.

- (Boolean) Complexity of problems on circuits
  - Polynomial Identity Testing

Algebraic Complexity Theory

Complexity of a polynomial = size of its smallest circuit

- Which polynomials have low/high complexity?
  - Polynomial complexity: Determinant
  - Non-polynomial complexity: Permanent?

  } "Algebraic P vs NP"

Conjecture (Algebraic P $\neq$ NP)

The complexity of the permanent is super-polynomial.

- (Boolean) Complexity of problems on circuits
  - Polynomial Identity Testing
  - Roots finding, factorization, ...

Permanent & Polynomial Identity Testing

- PIT: randomized polynomial-time algorithm

  [Schwartz'80, Zippel'79, DeMillo-Lipton'78]

Permanent & Polynomial Identity Testing

- PIT: randomized polynomial-time algorithm

  [Schwartz'80, Zippel'79, DeMillo-Lipton'78]

Theorem (Kabanets-Impagliazzo'03, Agrawal'05)

Derandomization of PIT algorithm
$\Longrightarrow$ *Super-polynomial lower bound for the permanent*

Permanent & Polynomial Identity Testing

- PIT: randomized polynomial-time algorithm

  [Schwartz'80, Zippel'79, DeMillo-Lipton'78]

Theorem (Kabanets-Impagliazzo'03, Agrawal'05)

Derandomization of PIT algorithm
$\Longrightarrow$ *Super-polynomial lower bound for the permanent*

$\rightsquigarrow$ Connections between PIT and lower bounds already in [Heintz-Schnorr'80]

The τ-conjecture

Conjecture (Shub & Smale, 1995)

For any $f \in \mathbb{Z}[X]$ of complexity $\tau(f)$,

$$\#\{n \in \mathbb{Z} : f(n) = 0\} \leq \mathsf{poly}(\tau(f)).$$

The τ-conjecture

Conjecture (Shub & Smale, 1995)

For any $f \in \mathbb{Z}[X]$ of complexity $\tau(f)$,

$$\#\{n \in \mathbb{Z} : f(n) = 0\} \leq \mathsf{poly}(\tau(f)).$$

Theorem (Bürgisser, 2006)

τ-conjecture

$$\Longrightarrow \textit{ super-polynomial lower bound for the permanent}$$

Sum of products of sparse polynomials

Definition

Let $\mathrm{SPS}(k, m, t, A)$ the class of polynomials

$$f(X) = \sum_{i=1}^{k} \prod_{j=1}^{m} f_j(X)^{\alpha_{ij}}$$

where the $f_j \in \mathbb{R}[X]$ are t-sparse and $0 \leq \alpha_{ij} \leq A$.

Sum of products of sparse polynomials

Definition

Let $\mathrm{SPS}(k, m, t, A)$ the class of polynomials

$$f(X) = \sum_{i=1}^{k} \prod_{j=1}^{m} f_j(X)^{\alpha_{ij}}$$

where the $f_j \in \mathbb{R}[X]$ are t-sparse and $0 \leq \alpha_{ij} \leq A$.

- Descartes' rule of signs:

$$t\text{-sparse} \implies \text{at most } 2t - 1 \text{ real roots}$$

Sum of products of sparse polynomials

Definition

Let $\mathrm{SPS}(k, m, t, A)$ the class of polynomials

$$f(X) = \sum_{i=1}^{k} \prod_{j=1}^{m} f_j(X)^{\alpha_{ij}}$$

where the $f_j \in \mathbb{R}[X]$ are t-sparse and $0 \leq \alpha_{ij} \leq A$.

- Descartes' rule of signs:

$$t\text{-sparse} \implies \text{at most } 2t - 1 \text{ real roots}$$

- $\prod_{j=1}^{m} f_j(X)^{\alpha_j}$: at most $2m(t-1)+1$ real roots

Sum of products of sparse polynomials

Definition

Let $\mathrm{SPS}(k, m, t, A)$ the class of polynomials

$$f(X) = \sum_{i=1}^{k} \prod_{j=1}^{m} f_j(X)^{\alpha_{ij}}$$

where the $f_j \in \mathbb{R}[X]$ are t-sparse and $0 \leq \alpha_{ij} \leq A$.

- Descartes' rule of signs:

$$t\text{-sparse} \implies \text{at most } 2t - 1 \text{ real roots}$$

- $\prod_{j=1}^{m} f_j(X)^{\alpha_j}$: at most $2m(t-1)+1$ real roots
- f is $(k \times t^{mA})$-sparse

The real τ-conjecture

Conjecture (Koiran, 2011)

Let $f \in \mathrm{SPS}(k, m, t, A)$, then

$$\#\{x \in \mathbb{R} : f(x) = 0\} \leq \mathrm{poly}(k, m, t, A)$$

The real τ-conjecture

Conjecture (Koiran, 2011)

Let $f \in \mathrm{SPS}(k, m, t, A)$, then

$$\#\{x \in \mathbb{R} : f(x) = 0\} \leq \mathrm{poly}(k, m, t, A)$$

Theorem (Koiran, 2011)

Real τ-conjecture

$\Longrightarrow$ *Super-polynomial lower bound for the permanent*

The real τ-conjecture

Conjecture (Koiran, 2011)

Let $f \in \mathrm{SPS}(k, m, t, A)$, then

$$\#\{x \in \mathbb{R} : f(x) = 0\} \leq \mathrm{poly}(k, m, t, A)$$

Theorem (Koiran, 2011)

Real τ-conjecture
$\implies$ *Super-polynomial lower bound for the permanent*

1. Upper bound on the number of real roots of $f \in \mathrm{SPS}(k, m, t, A)$
2. Lower bound for the permanent

Upper bound for the number of real roots of SPS polynomials

Theorem

There exists $C > 0$ such that the number of real roots of any $f = \sum_{i=1}^{k} \prod_{j=1}^{m} f_j^{\alpha_{ij}} \in \mathrm{SPS}(k, m, t, A)$ is at most

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

Upper bound for the number of real roots of SPS polynomials

Theorem

There exists $C > 0$ such that the number of real roots of any $f = \sum_{i=1}^{k} \prod_{j=1}^{m} f_j^{\alpha_{ij}} \in \mathrm{SPS}(k, m, t, A)$ is at most

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

- Independent of A.

Upper bound for the number of real roots of SPS polynomials

Theorem

There exists $C > 0$ such that the number of real roots of any $f = \sum_{i=1}^{k} \prod_{j=1}^{m} f_j^{\alpha_{ij}} \in \mathrm{SPS}(k, m, t, A)$ is at most

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

- 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

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

The permanent family

$$\mathrm{PER}_n(x_{11}, \ldots, x_{nn}) = \mathrm{per} \begin{pmatrix} x_{11} & \cdots & x_{1n} \\ \vdots & & \vdots \\ x_{n1} & \cdots & x_{nn} \end{pmatrix} = \sum_{\sigma \in \mathfrak{S}_n} \prod_{i=1}^{n} x_{i\sigma(i)}$$

The permanent family

$$\mathrm{PER}_n(x_{11}, \ldots, x_{nn}) = \mathrm{per}\begin{pmatrix} x_{11} & \cdots & x_{1n} \\ \vdots & & \vdots \\ x_{n1} & \cdots & x_{nn} \end{pmatrix} = \sum_{\sigma \in \mathfrak{S}_n} \prod_{i=1}^{n} x_{i\sigma(i)}$$

Conjecture (Algebraic P $\neq$ NP)

$n \mapsto \tau(\mathrm{PER}_n)$ grows faster than any polynomial function.

The permanent family

$$\mathrm{PER}_n(x_{11},\ldots,x_{nn}) = \mathrm{per}\begin{pmatrix} x_{11} & \cdots & x_{1n} \\ \vdots & & \vdots \\ x_{n1} & \cdots & x_{nn} \end{pmatrix} = \sum_{\sigma\in\mathfrak{S}_n}\prod_{i=1}^{n} x_{i\sigma(i)}$$

Conjecture (Algebraic P $\neq$ NP)

$n \mapsto \tau(\mathrm{PER}_n)$ grows faster than any polynomial function.

- The conjecture for depth-4 circuits implies the general case [Agrawal-Vinay'08, Koiran'11]

Multivariate SPS polynomials

Definition

$(P_n)_{n\geq 0} \in \mathrm{mSPS}(k, m)$ if

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

where

- $f_{j,n}$ is $Q(n)$-sparse;

Multivariate SPS polynomials

Definition

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

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

where

- $\mathrm{bitsize}(\alpha_{ij,n}) \leq Q(n)$;
- $f_{j,n}$ is $Q(n)$-sparse;
- $f_{j,n}$ has complexity at most $Q(n)$.

Multivariate SPS polynomials

Definition

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

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

where

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

Multivariate SPS polynomials

Definition

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

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

where

- $\mathrm{bitsize}(\alpha_{ij,n}) \leq Q(n)$;
- $f_{j,n}$ is $Q(n)$-sparse;
- $f_{j,n}$ has complexity at most $Q(n)$.

Multivariate SPS polynomials

Definition

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

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

where

- $\mathrm{bitsize}(\alpha_{ij,n}) \leq Q(n)$;
- $f_{j,n}$ is $Q(n)$-sparse;
- $f_{j,n}$ has complexity at most $Q(n)$.

- $\mathrm{mSPS}(k, m) \subsetneq$ depth-4 circuits
- Possibly exponential-size circuits

Lower bound for the permanent

Theorem

For any fixed k and m, (PER_n) does not have $\mathrm{mSPS}(k, m)$ circuits.

Conclusion

- First result toward the real τ-conjecture

Conclusion

- First result toward the real τ-conjecture
- Implementation of Koiran's Theorem in a particular case

Conclusion

- First result toward the real τ-conjecture
- Implementation of Koiran's Theorem in a particular case
- Links with Polynomial Identity Testing

Conclusion

- First result toward the real τ-conjecture
- Implementation of Koiran's Theorem in a particular case
- Links with Polynomial Identity Testing

- Update: Agrawal *et al.*, arXiv:1111.0582

Conclusion

- First result toward the real τ-conjecture
- Implementation of Koiran's Theorem in a particular case
- Links with Polynomial Identity Testing

- Update: Agrawal *et al.*, arXiv:1111.0582

Open Problem

Let f, g be t-sparse polynomials.
$\rightsquigarrow$ What is the maximum number of roots of $fg + 1$?

Conclusion

- First result toward the real τ-conjecture
- Implementation of Koiran's Theorem in a particular case
- Links with Polynomial Identity Testing

- Update: Agrawal *et al.*, arXiv:1111.0582

Open Problem

Let f, g be t-sparse polynomials.
$\rightsquigarrow$ What is the maximum number of roots of $fg + 1$?

$$4t - 3 \leq \max_{f,g} \#\{x \in \mathbb{R} : f(x)g(x) + 1 = 0\} \leq 2t^2$$

Conclusion

- First result toward the real τ-conjecture
- Implementation of Koiran's Theorem in a particular case
- Links with Polynomial Identity Testing

- Update: Agrawal *et al.*, arXiv:1111.0582

Open Problem

Let f, g be t-sparse polynomials.
$\rightsquigarrow$ What is the maximum number of roots of $fg + 1$?

$$4t - 3 \leq \max_{f,g} \#\{x \in \mathbb{R} : f(x)g(x) + 1 = 0\} \leq 2t^2$$

arXiv:1107.1434