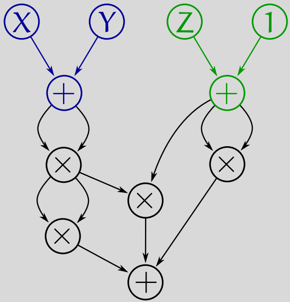
Around sparse polynomials

Bruno Grenet
LIX — École Polytechnique

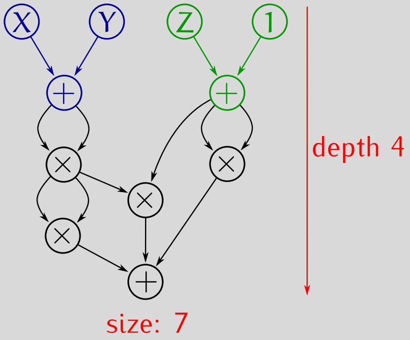
I. The real τ-conjecture

and its variants

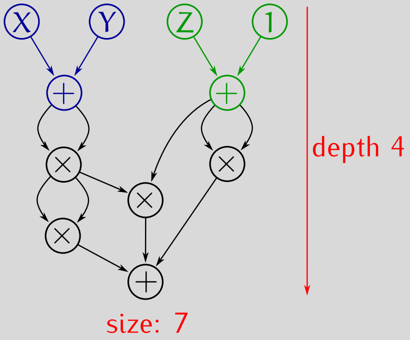
$(X+Y)^4 + (Z+1)^2 + (X+Y)^2(Z+1)$



$(X+Y)^4 + (Z+1)^2 + (X+Y)^2(Z+1)$



$(X+Y)^4 + (Z+1)^2 + (X+Y)^2(Z+1)$



Complexity of a polynomial

$\tau(f) =$ size of its smallest circuit representation *without constant*

Conjecture [Shub & Smale'95]

$\exists c$ s.t. the number of integer roots of $f \in \mathbb{Z}[X]$ is $\leqslant (1 + \tau(f))^c$.

Conjecture [Shub & Smale'95]

$\exists c$ s.t. the number of integer roots of $f \in \mathbb{Z}[X]$ is $\leqslant (1+\tau(f))^c$.

Theorem [Bürgisser'07]

τ-conjecture

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

Conjecture [Shub & Smale'95]

$\exists c$ s.t. the number of integer roots of $f \in \mathbb{Z}[X]$ is $\leqslant (1+\tau(f))^c$.

Theorem [Bürgisser'07]

τ-conjecture

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

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

Conjecture [Shub & Smale'95]

$\exists c$ s.t. the number of integer roots of $f \in \mathbb{Z}[X]$ is $\leqslant (1 + \tau(f))^c$.

Theorem [Bürgisser'07]

τ-conjecture

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

$\implies$ $\tau(\mathrm{PER}_n)$ is not polynomially bounded in n

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

Conjecture [Shub & Smale'95]

$\exists c$ s.t. the number of integer roots of $f \in \mathbb{Z}[X]$ is $\leqslant (1+\tau(f))^c$.

Theorem [Bürgisser'07]

τ-conjecture

$\Longrightarrow$ super-polynomial lower bound for the permanent

$\Longrightarrow$ $\tau(\mathrm{PER}_n)$ is not polynomially bounded in n

$\Longrightarrow$ $\mathsf{VP}^0 \neq \mathsf{VNP}^0$

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

Theorem [Shub & Smale'95]

τ-conjecture $\implies$ $\mathsf{P}_{\mathbb{C}} \neq \mathsf{NP}_{\mathbb{C}}$

The τ-conjecture is hard!

Theorem [Shub & Smale'95]

τ-conjecture $\implies$ $\mathsf{P}_{\mathbb{C}} \neq \mathsf{NP}_{\mathbb{C}}$

Theorem [Cheng'03]

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

Theorem [Shub & Smale'95]

τ-conjecture $\implies$ $\mathsf{P}_{\mathbb{C}} \neq \mathsf{NP}_{\mathbb{C}}$

Theorem [Cheng'03]

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

- False for real roots (Chebyshev polynomials)

Conjecture [Koiran'11]

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

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

Conjecture [Koiran'11]

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

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

Theorem [Koiran'11]

Real τ-conjecture

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

Conjecture [Koiran'11]

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

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

Theorem [Koiran'11]

Real τ-conjecture

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

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

The real τ-conjecture

Conjecture [Koiran'11]

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

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

Theorem [Koiran'11]

Real τ-conjecture

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

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

Theorem

If $f \in \mathbb{R}[X]$ has t monomials, then it has $\leqslant (2t-1)$ real roots.

Theorem

If $f \in \mathbb{R}[X]$ has t monomials, then it has $\leqslant (2t-1)$ real roots.

Proof. Induction on t: f has $\leqslant t-1$ positive real roots

- $t = 1$: No positive real root

Theorem

If $f \in \mathbb{R}[X]$ has t monomials, then it has $\leqslant (2t-1)$ real roots.

Proof. Induction on t: f has $\leqslant t-1$ positive real roots

- $t = 1$: No positive real root
- $t > 1$: Let $c_\alpha X^\alpha$ = lowest degree monomial.

Theorem

If $f \in \mathbb{R}[X]$ has t monomials, then it has $\leqslant (2t-1)$ real roots.

Proof. Induction on t: f has $\leqslant t-1$ positive real roots

- $t = 1$: No positive real root
- $t > 1$: Let $c_\alpha X^\alpha$ = lowest degree monomial.
  - $g = f/X^\alpha$: same positive roots, nonzero constant coefficient

Theorem

If $f \in \mathbb{R}[X]$ has t monomials, then it has $\leqslant (2t-1)$ real roots.

Proof. Induction on t: f has $\leqslant t-1$ positive real roots

- $t = 1$: No positive real root
- $t > 1$: Let $c_\alpha X^\alpha$ = lowest degree monomial.
  - $g = f/X^\alpha$: same positive roots, nonzero constant coefficient
  - g' has $(t-1)$ monomials $\implies$ at most $(t-2)$ positive roots

Theorem

If $f \in \mathbb{R}[X]$ has t monomials, then it has $\leqslant (2t-1)$ real roots.

Proof. Induction on t: f has $\leqslant t-1$ positive real roots

- $t = 1$: No positive real root
- $t > 1$: Let $c_\alpha X^\alpha$ = lowest degree monomial.
  - $g = f/X^\alpha$: same positive roots, nonzero constant coefficient
  - g' has $(t-1)$ monomials $\implies$ at most $(t-2)$ positive roots
  - There is a root of g' between two consecutive roots of g [Rolle'1691]

Theorem

If $f \in \mathbb{R}[X]$ has t monomials, then it has $\leqslant (2t-1)$ real roots.

Proof. Induction on t: f has $\leqslant t-1$ positive real roots

- $t = 1$: No positive real root
- $t > 1$: Let $c_\alpha X^\alpha$ = lowest degree monomial.
  - $g = f/X^\alpha$: same positive roots, nonzero constant coefficient
  - g' has $(t-1)$ monomials $\implies$ at most $(t-2)$ positive roots
  - There is a root of g' between two consecutive roots of g [Rolle'1691]

$f = \sum_{i=1}^{k} \prod_{j=1}^{m} f_{ij}$: $\leqslant 2kt^m - 1$ real roots

Real τ-conjecture ⟹ Permanent is hard

$$\mathrm{SPS}(k, m, t) = \left\{ f = \sum_{i=1}^{k} \prod_{j=1}^{m} f_{ij} : f_{ij}\text{'s are } t\text{-sparse} \right\}$$

Real τ-conjecture $\implies$ Permanent is hard

$$\mathrm{SPS}(k, m, t) = \left\{ f = \sum_{i=1}^{k} \prod_{j=1}^{m} f_{ij} : f_{ij}\text{'s are t-sparse} \right\}$$

Proof sketch. Assume the permanent is easy.

Real τ-conjecture ⟹ Permanent is hard

$$\mathrm{SPS}(k,m,t)=\left\{f=\sum_{i=1}^{k}\prod_{j=1}^{m} f_{ij} : f_{ij}\text{'s are t-sparse}\right\}$$

Proof sketch. Assume the permanent is easy.

- $\prod_{i=1}^{2^n}(X-i)$ has circuits of size poly(n) **[Bürgisser'07-09]**

Real τ-conjecture $\implies$ Permanent is hard

$$\mathrm{SPS}(k,m,t) = \left\{ f = \sum_{i=1}^{k} \prod_{j=1}^{m} f_{ij} : f_{ij}\text{'s are } t\text{-sparse} \right\}$$

Proof sketch. Assume the permanent is easy.

- $\prod_{i=1}^{2^n}(X - i)$ has circuits of size poly(n) **[Bürgisser'07-09]**
- Reduction to depth 4 $\rightsquigarrow$ SPS polynomial of size $2^{o(n)}$ **[Koiran'11]**

Real τ-conjecture $\implies$ Permanent is hard

$$\mathrm{SPS}(k,m,t) = \left\{ f = \sum_{i=1}^{k}\prod_{j=1}^{m} f_{ij} : f_{ij}\text{'s are } t\text{-sparse} \right\}$$

Proof sketch. Assume the permanent is easy.

- $\prod_{i=1}^{2^n}(X-i)$ has circuits of size $\mathrm{poly}(n)$ **[Bürgisser'07-09]**
- Reduction to depth 4 $\rightsquigarrow$ SPS polynomial of size $2^{o(n)}$ **[Koiran'11]**
- Contradiction with real τ-conjecture

Real τ-conjecture $\implies$ Permanent is hard

$$\text{SPS}(k,m,t) = \left\{ f = \sum_{i=1}^{k} \prod_{j=1}^{m} f_{ij} : f_{ij}\text{'s are } t\text{-sparse} \right\}$$

Proof sketch. Assume the permanent is easy.

- $\prod_{i=1}^{2^n}(X-i)$ has circuits of size poly(n) **[Bürgisser'07-09]**
- Reduction to depth 4 $\rightsquigarrow$ SPS polynomial of size $2^{o(n)}$ **[Koiran'11]**
- Contradiction with real τ-conjecture

Theorem [Koiran'11]

Circuit of size t and degree d

$\rightsquigarrow$ Depth-4 circuit of size $t^{\mathcal{O}(\sqrt{d}\log d)}$

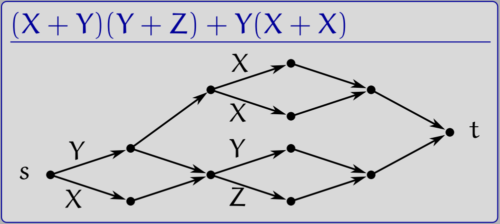
Theorem **[Koiran'11]**

Circuit of size t and degree d

$\rightsquigarrow$ Depth-4 circuit of size $t^{\mathcal{O}(\sqrt{d}\log d)}$

Proof idea.

- Construct an equivalent Arithmetic Branching Program
  $\rightsquigarrow$ size $t^{\log 2d}+1$, depth $\delta = 3d-1$ **[Malod-Portier'08]**



Theorem [Koiran'11]

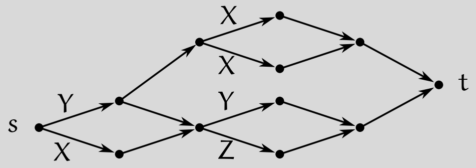
Circuit of size t and degree d

$\rightsquigarrow$ Depth-4 circuit of size $t^{\mathcal{O}(\sqrt{d}\log d)}$

Proof idea.

- Construct an equivalent Arithmetic Branching Program
  $\rightsquigarrow$ size $t^{\log 2d}+1$, depth $\delta = 3d-1$ [Malod-Portier'08]
- ABP $\equiv$ Matrix powering

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



Theorem **[Koiran'11]**

Circuit of size t and degree d

$\rightsquigarrow$ Depth-4 circuit of size $t^{\mathcal{O}(\sqrt{d}\log d)}$

Proof idea.

- Construct an equivalent Arithmetic Branching Program
  $\rightsquigarrow$ size $t^{\log 2d}+1$, depth $\delta = 3d-1$ **[Malod-Portier'08]**
- ABP $\equiv$ Matrix powering
- $M^\delta = (M^{\sqrt{\delta}})^{\sqrt{\delta}}$

$$\mathrm{SPS}(k, m, t) = \left\{ f = \sum_{i=1}^{k} \prod_{j=1}^{m} f_{ij} : f_{ij}\text{'s are t-sparse} \right\}$$

$$\mathrm{SPS}(k,m,t) = \left\{ f = \sum_{i=1}^{k} \prod_{j=1}^{m} f_{ij} : f_{ij}\text{'s are } t\text{-sparse} \right\}$$

τ-conjectures (implying $\text{PER} \notin \mathrm{VP}^0$)

$\forall f \in \mathrm{SPS}(k,m,t)$,

- $\exists \mathbb{L} \in \{\mathbb{R}, \mathbb{Q}_2, \mathbb{Q}_3, \mathbb{Q}_5, \ldots\}$, [Phillipson-Rojas'13]
  $\#\{x \in \mathbb{L} : f(x) = 0\} \leqslant \mathrm{poly}(kmt)$;

$$\mathsf{SPS}(k,m,t) = \left\{ f = \sum_{i=1}^{k} \prod_{j=1}^{m} f_{ij} : f_{ij}\text{'s are } t\text{-sparse} \right\}$$

τ-conjectures (implying $\text{Per} \notin \mathsf{VP}^0$)

$\forall f \in \mathsf{SPS}(k,m,t)$,

- $\exists \mathbb{L} \in \{\mathbb{R}, \mathbb{Q}_2, \mathbb{Q}_3, \mathbb{Q}_5, \dots\}$, [Phillipson-Rojas'13]
  $$\#\{x \in \mathbb{L} : f(x) = 0\} \leqslant \text{poly}(kmt);$$
- $\exists p$, prime, [Koiran-Portier-Rojas'13]
  $$\#\{e \in \mathbb{N} : \exists x \in \mathbb{Z}, \nu_p(x) = e, f(x) = 0\} \leqslant \text{poly}(kmt);$$

$$\mathrm{SPS}(k,m,t) = \left\{ f = \sum_{i=1}^{k} \prod_{j=1}^{m} f_{ij} : f_{ij}\text{'s are } t\text{-sparse} \right\}$$

τ-conjectures (implying $\text{Per} \notin \mathsf{VP}^0$)

$\forall f \in \mathrm{SPS}(k,m,t)$,

- $\exists \mathbb{L} \in \{\mathbb{R}, \mathbb{Q}_2, \mathbb{Q}_3, \mathbb{Q}_5, \ldots\}$, [Phillipson-Rojas'13]
  $$\#\{x \in \mathbb{L} : f(x) = 0\} \leqslant \mathrm{poly}(kmt);$$
- $\exists p$, prime, [Koiran-Portier-Rojas'13]
  $$\#\{e \in \mathbb{N} : \exists x \in \mathbb{Z}, \nu_p(x) = e, f(x) = 0\} \leqslant \mathrm{poly}(kmt);$$
- The Newton polygon of $f(X,Y)$ has $\leqslant \mathrm{poly}(kmt)$ many edges. [Koiran-Portier-Tavenas-Thomassé'13]

$$\mathsf{SPS}(k,m,t) = \left\{ f = \sum_{i=1}^{k} a_i f_i^m \quad : f_i \text{ 's are } t\text{-sparse} \right\}$$

τ-conjectures (implying $\mathrm{PER} \notin \mathsf{VP}^0$)

$\forall f \in \mathsf{SPS}(k,m,t)$,

- $\exists \mathbb{L} \in \{\mathbb{R}, \mathbb{Q}_2, \mathbb{Q}_3, \mathbb{Q}_5, \ldots\}$, [Phillipson-Rojas'13]
  $$\#\{x \in \mathbb{L} : f(x) = 0\} \leqslant \mathrm{poly}(kmt);$$
- $\exists p$, prime, [Koiran-Portier-Rojas'13]
  $$\#\{e \in \mathbb{N} : \exists x \in \mathbb{Z}, v_p(x) = e, f(x) = 0\} \leqslant \mathrm{poly}(kmt);$$
- The Newton polygon of $f(X, Y)$ has $\leqslant \mathrm{poly}(kmt)$ many edges. [Koiran-Portier-Tavenas-Thomassé'13]

$$\mathrm{SPS}(k,m,t) = \left\{ f = \sum_{i=1}^{k} a_i f_i^m \quad : f_i \text{ 's are } t\text{-sparse} \right\}$$

τ-conjectures (implying $\mathrm{P{\scriptstyle ER}} \notin \mathrm{VP}^0$)

$\forall f \in \mathrm{SPS}(k,m,t)$,

- $\exists \mathbb{L} \in \{\mathbb{R}, \mathbb{Q}_2, \mathbb{Q}_3, \mathbb{Q}_5, \ldots\}$, [Phillipson-Rojas'13]
  $$\#\{x \in \mathbb{L} : f(x) = 0\} \leqslant \mathrm{poly}(kmt);$$
- $\exists p$, prime, [Koiran-Portier-Rojas'13]
  $$\#\{e \in \mathbb{N} : \exists x \in \mathbb{Z}, \nu_p(x) = e, f(x) = 0\} \leqslant \mathrm{poly}(kmt);$$
- The Newton polygon of $f(X,Y)$ has $\leqslant \mathrm{poly}(kmt)$ many edges. [Koiran-Portier-Tavenas-Thomassé'13]

- Valid with $2^{(m+\log(kt))^c}$ instead of $\mathrm{poly}(kmt)$.

Known upper bounds

$$\mathrm{SPS}(k, m, t, A) = \left\{ \sum_{i=1}^{k} \prod_{j=1}^{m} f_j^{\alpha_{ij}} : f_j\text{'s are } t\text{-sparse, } \alpha_{ij} \leqslant A \right\}$$

$$\mathrm{SPS}(k,m,t,A)=\left\{\sum_{i=1}^{k}\prod_{j=1}^{m}f_j^{\alpha_{ij}}:f_j\text{'s are t-sparse, }\alpha_{ij}\leqslant A\right\}$$

Theorem

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

- $2kt^{mA}-1$; [Descartes'1637]

$$\mathrm{SPS}(k, m, t, A) = \left\{ \sum_{i=1}^{k} \prod_{j=1}^{m} f_j^{\alpha_{ij}} : f_j\text{'s are } t\text{-sparse}, \ \alpha_{ij} \leqslant A \right\}$$

Theorem

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

- $2kt^{mA} - 1$; [Descartes'1637]
- $t^{\mathcal{O}(m2^{k-1})}$; [G.-Koiran-Portier-Strozecki'11]

$$\mathrm{SPS}(k,m,t,A) = \left\{ \sum_{i=1}^{k} \prod_{j=1}^{m} f_j^{\alpha_{ij}} : f_j\text{'s are } t\text{-sparse}, \ \alpha_{ij} \leqslant A \right\}$$

Theorem

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

- $2kt^{mA} - 1$; [Descartes'1637]
- $t^{\mathcal{O}(m2^{k-1})}$; [G.-Koiran-Portier-Strozecki'11]
- $t^{\mathcal{O}(k^2 m)}$. [Koiran-Portier-Tavenas'13]

$$\mathrm{SPS}(k,m,t,A) = \left\{ \sum_{i=1}^{k} \prod_{j=1}^{m} f_j^{\alpha_{ij}} : f_j\text{'s are } t\text{-sparse}, \alpha_{ij} \leqslant A \right\}$$

Theorem

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

- $2kt^{mA} - 1$; [Descartes'1637]
- $t^{\mathcal{O}(m2^{k-1})}$; [G.-Koiran-Portier-Strozecki'11]
- $t^{\mathcal{O}(k^2 m)}$. [Koiran-Portier-Tavenas'13]

If $f \in \mathrm{SPS}(k,m,t)$, its Newton polygon has at most

- kt^m many edges; number of monomials

$$\mathrm{SPS}(k,m,t,A) = \left\{ \sum_{i=1}^{k} \prod_{j=1}^{m} f_j^{\alpha_{ij}} : f_j\text{'s are } t\text{-sparse}, \alpha_{ij} \leqslant A \right\}$$

Theorem

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

- $2kt^{mA} - 1$; [Descartes'1637]
- $t^{\mathcal{O}(m2^{k-1})}$; [G.-Koiran-Portier-Strozecki'11]
- $t^{\mathcal{O}(k^2 m)}$. [Koiran-Portier-Tavenas'13]

If $f \in \mathrm{SPS}(k,m,t)$, its Newton polygon has at most

- kt^m many edges; number of monomials
- $kt^{2m/3}$ many edges. [Koiran-Portier-Tavenas-Thomassé'13]

- Four different τ-conjectures $\implies$ $\mathsf{VP}^0 \neq \mathsf{VNP}^0$

- Four different τ-conjectures $\implies \mathsf{VP}^0 \neq \mathsf{VNP}^0$
- Use your favorite formulation and tools!

Conclusion

- Four different τ-conjectures $\implies \mathsf{VP}^0 \neq \mathsf{VNP}^0$
- Use your favorite formulation and tools!
  - Wronskian, combinatorial geometry, p-adic geometry, ...

- Four different τ-conjectures $\implies \mathsf{VP}^0 \neq \mathsf{VNP}^0$
- Use your favorite formulation and tools!
  - Wronskian, combinatorial geometry, p-adic geometry, ...
- Links with Khovanskii's fewnomial theory

- Four different τ-conjectures $\implies \mathsf{VP}^0 \neq \mathsf{VNP}^0$
- Use your favorite formulation and tools!
  - Wronskian, combinatorial geometry, p-adic geometry, ...
- Links with Khovanskii's fewnomial theory

Embarrassing Open Problem

Let f, g be t-sparse polynomials.

- What is the maximum number of real roots of $fg + 1$?

- Four different τ-conjectures $\implies \mathsf{VP}^0 \neq \mathsf{VNP}^0$
- Use your favorite formulation and tools!
  - Wronskian, combinatorial geometry, p-adic geometry, …
- Links with Khovanskii's fewnomial theory

Embarrassing Open Problem

Let f, g be t-sparse polynomials.

- What is the maximum number of real roots of $fg + 1$?
- Same question for the different τ-conjectures.

- Four different τ-conjectures $\implies \mathsf{VP}^0 \neq \mathsf{VNP}^0$
- Use your favorite formulation and tools!
  - Wronskian, combinatorial geometry, p-adic geometry, ...
- Links with Khovanskii's fewnomial theory

Embarrassing Open Problem

Let f, g be t-sparse polynomials.

- What is the maximum number of real roots of $fg + 1$?
- Same question for the different τ-conjectures.

- $fg + 1$ has $\leqslant t^2 + 1$ monomials $\rightsquigarrow$ **quadratic bounds**;
- Best known lower bounds: $\mathcal{O}(t)$;

- Four different τ-conjectures $\implies \mathsf{VP}^0 \neq \mathsf{VNP}^0$
- Use your favorite formulation and tools!
  - Wronskian, combinatorial geometry, p-adic geometry, ...
- Links with Khovanskii's fewnomial theory

Embarrassing Open Problem

Let f, g be t-sparse polynomials.

- What is the maximum number of real roots of $fg+1$?
- Same question for the different τ-conjectures.

- $fg+1$ has $\leqslant t^2+1$ monomials $\rightsquigarrow$ **quadratic bounds**;
- Best known lower bounds: $\mathcal{O}(t)$;
- The Newton polygon of $fg+1$ has at most $t^{4/3}$ many edges.

II. Factoring lacunary polynomials

joint work with

A. Chattopdhyay, P. Koiran, N. Portier & Y. Strozecki

Factorization of a polynomial P

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

Factorization of a polynomial P

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

$\mathbb{Z}[X]$

[Lenstra–Lenstra–Lovász'82]

$\downarrow$

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

[A. Lenstra'83, Landau'83]

$\downarrow$

$\mathbb{Q}(\alpha)[X_1, \ldots, X_n]$

[Kaltofen'85, A. Lenstra'87]

Factorization of a polynomial P

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

$\mathbb{Z}[X]$

[Lenstra–Lenstra–Lovász'82]

↓

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

[A. Lenstra'83, Landau'83]

↓

$\mathbb{Q}(\alpha)[X_1, \ldots, X_n]$

[Kaltofen'85, A. Lenstra'87]

$\mathbb{F}_q[X]$

[Berlekamp'67]

↓

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

Factorization of a polynomial P

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

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

$\downarrow$

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

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

Complexity

Polynomial in the **degree** of the polynomials

$\downarrow$

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

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

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

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

$$X^{102}Y^{101} + X^{101}Y^{102} - X^{101}Y^{101} - X - Y + 1$$
$$= (X + Y - 1) \times (X^{101}Y^{101} - 1)$$
$$= (X + Y - 1) \times (XY - 1) \times (1 + XY + \cdots + X^{100}Y^{100})$$

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

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

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

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

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

Definition

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

$$X^{102}Y^{101} + X^{101}Y^{102} - X^{101}Y^{101} - X - Y + 1$$
$$= (X + Y - 1) \times (X^{101}Y^{101} - 1)$$
$$= (X + Y - 1) \times (XY - 1) \times (1 + XY + \cdots + X^{100}Y^{100})$$

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

Definition

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

- Lacunary representation: $\{(\alpha_{1j}, \ldots, \alpha_{nj} : a_j) : 1 \leqslant j \leqslant k\}$

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

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

Definition

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

- Lacunary representation: $\{(\alpha_{1j}, \ldots, \alpha_{nj} : a_j) : 1 \leqslant j \leqslant k\}$
- $\mathrm{size}(P) \simeq \sum_j \mathrm{size}(a_j) + \log(\alpha_{1j}) + \cdots + \log(\alpha_{nj})$

Gap Theorem [Cucker-Koiran-Smale'98]

Let

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

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

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

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

Gap Theorem **[Cucker-Koiran-Smale'98]**

Let

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

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

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

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

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

Factorization of lacunary polynomials

Theorems

There exist deterministic polynomial-time algorithms computing

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

  [Cucker-Koiran-Smale'98]

Theorems

There exist deterministic polynomial-time algorithms computing

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

Factorization of lacunary polynomials

Theorems

There exist deterministic polynomial-time algorithms computing

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

  [Cucker-Koiran-Smale'98]

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

  [H. Lenstra'99]

- **linear** factors of **bivariate** polynomials over $\mathbb{Q}$;

  [Kaltofen-Koiran'05]

Factorization of lacunary polynomials

Theorems

There exist deterministic polynomial-time algorithms computing

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

Observation

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

Observation

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

Gap Theorem

Let

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

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

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

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

$\mathbb{K}$: any field of characteristic 0

Definition

$\mathrm{val}(P) = \max\{v : X^v \text{ divides } P\}$

$\mathbb{K}$: any field of characteristic 0

Definition

$\mathrm{val}(P) = \max\{v : X^v \text{ divides } P\}$

Theorem

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

Then

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

$\mathbb{K}$: any field of characteristic 0

Definition

$\mathrm{val}(P) = \max\{\nu : X^\nu \text{ divides } P\}$

Theorem

Let $P = \sum_{j=1}^{\ell} a_j X^{\alpha_j}(uX+v)^{\beta_j} \not\equiv 0$, with $uv \neq 0$ and $\alpha_1 \leqslant \cdots \leqslant \alpha_\ell$.
Then, if the family $(X^{\alpha_j}(uX+v)^{\beta_j})_j$ is linearly independent,

$$\mathrm{val}(P) \leqslant \alpha_1 + \binom{\ell}{2}.$$

$\mathbb{K}$: any field of characteristic 0

Definition

$\mathrm{val}(P) = \max\{v : X^v \text{ divides } P\}$

Theorem

Let $P = \sum_{j=1}^{\ell} a_j X^{\alpha_j}(uX+v)^{\beta_j} \not\equiv 0$, with $uv \neq 0$ and $\alpha_1 \leqslant \cdots \leqslant \alpha_\ell$.
Then, if the family $(X^{\alpha_j}(uX+v)^{\beta_j})_j$ is linearly independent,

$$\mathrm{val}(P) \leqslant \alpha_1 + \binom{\ell}{2}.$$

- Hajós' Lemma: if $\alpha_1 = \cdots = \alpha_\ell$, $\mathrm{val}(P) \leqslant \alpha_1 + (\ell - 1)$

Definition

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

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

Definition

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

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

Proposition [Bôcher, 1900]

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

Lemma

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

Proof.

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

Lemma

$$\mathrm{val}(\mathrm{wr}(f_1, \ldots, f_\ell)) \geqslant \sum_{j=1}^{\ell} \mathrm{val}(f_j) - \binom{\ell}{2}$$

Lemma

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

$$\mathrm{val}(\mathrm{wr}(f_1, \ldots, f_\ell)) \leqslant \sum_{j=1}^{\ell} \alpha_j = \sum_{j=1}^{\ell} \mathrm{val}(f_j).$$

Lemma

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

Lemma

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

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

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

Lemma

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

Lemma

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

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

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

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

How tight is the bound?

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

How tight is the bound?

- Hajós' Lemma: $\operatorname{val}\left(\sum_{j=1}^{\ell} a_j X^{\alpha}(uX+v)^{\beta_j}\right) \leqslant \alpha + (\ell - 1)$
- Our result: $\operatorname{val}\left(\sum_{j=1}^{\ell} a_j X^{\alpha_j}(uX+v)^{\beta_j}\right) \leqslant \alpha_1 + \binom{\ell}{2}$

How tight is the bound?

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

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

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

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

Theorem

Let

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

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

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

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

Theorem

Let

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

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

$$\alpha_{\ell+1} > \alpha_1 + \binom{\ell}{2} \geqslant \mathrm{val}(Q),$$

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

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

Observation + Gap Theorem (recursively)

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

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

Observation + Gap Theorem (recursively)

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

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

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

Observation + Gap Theorem (recursively)

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

Observation + Gap Theorem (recursively)

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

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

Observation + Gap Theorem (recursively)

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

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

Observation + Gap Theorem (recursively)

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

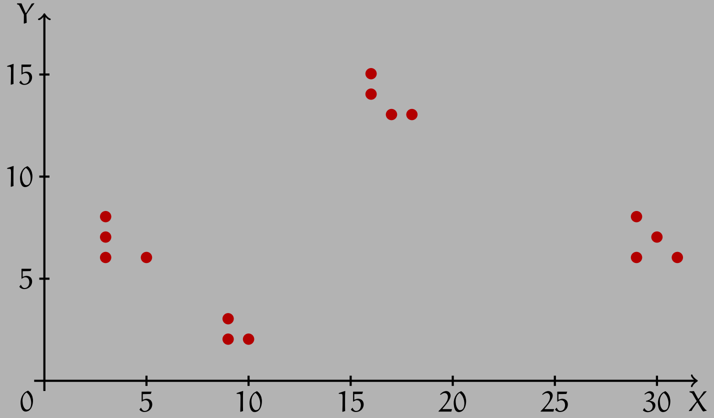
- $P_t = \sum_{j=j_t}^{j_t+\ell_t-1} a_j X^{\alpha_j} Y^{\beta_j}$ with $\alpha_{j_t+\ell_t-1} - \alpha_{j_t} \leqslant \binom{\ell_t}{2}$
- Independent from u and v
- X does not play a special role

Example

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

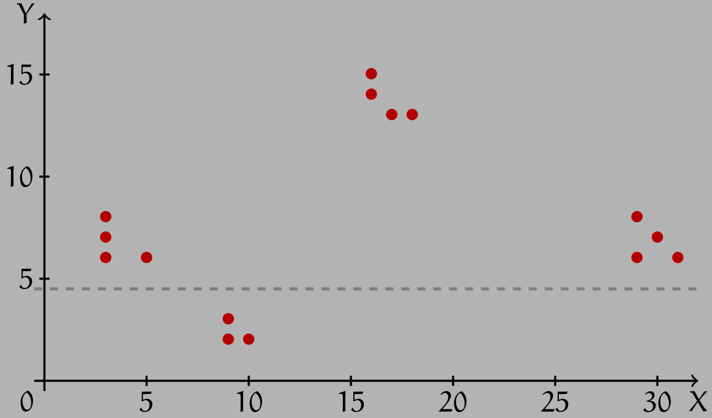
Example

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



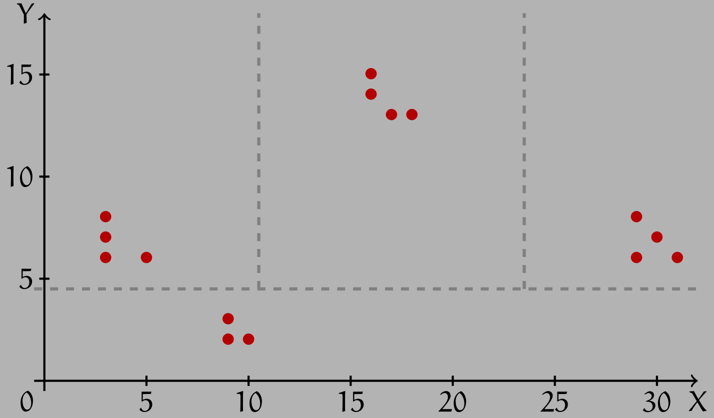
Example

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



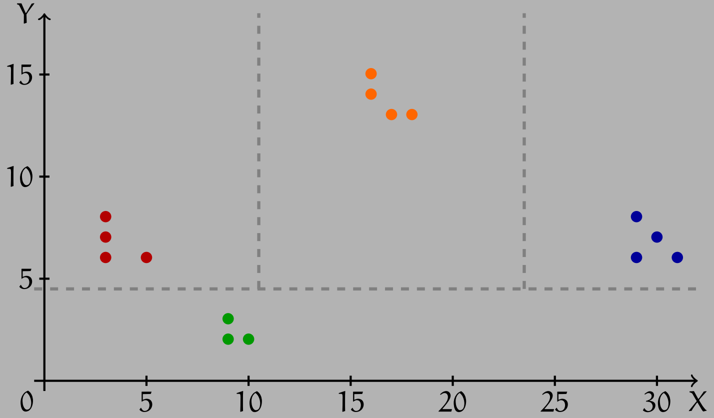
Example

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



Example

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



Example

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

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

Example

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

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

Example

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

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

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

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

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

Example

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

$$P_1 = X^3Y^6(X - Y + 1)(1 - X - Y)$$
$$P_2 = X^9Y^2(X - Y + 1)$$
$$P_3 = X^{16}Y^{13}(X + Y)(X - Y + 1)$$
$$P_4 = X^{29}Y^6(X + Y - 1)(X - Y + 1)$$

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

Example

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

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

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

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

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

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

Complete algorithm

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

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

↓ monomials

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

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

monomials

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

binomials

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

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

Univariate lacunary factorization
[H. Lenstra'99]

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

- **monomials** → $(X, \min_j \alpha_j)$, $(Y, \min_j \beta_j)$
- **binomials** →
  - $(X - a)$: Factors of $\sum_j a_j X^{\alpha_j}$
  - $(Y - uX)$: Roots of $u \mapsto \sum_j a_j u^{\beta_j}$

  Univariate lacunary factorization [H. Lenstra'99]
- **trinomials** → Common factors of $P_t = \sum_{j=j_t}^{j_t+\ell_t-1} a_j X^{\alpha_j} Y^{\beta_j}$ $(\deg(P_t) \leqslant \mathcal{O}(\ell_t^2))$

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

Let $P = \sum_{j=1}^{k} a_j X^{\alpha_j} Y^{\beta_j} \in \mathbb{Q}(\alpha)[X, Y]$ be given in lacunary representation. There exists a **deterministic polynomial-time** algorithm to compute its linear factors, with multiplicities.

monomials — binomials — trinomials

monomials:

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

binomials:

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

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

Univariate lacunary factorization
[H. Lenstra'99]

trinomials:

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

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

Comments

Bottleneck: Factorization of low-degree polynomials

Comments

Bottleneck: Factorization of low-degree polynomials
↳ Complexity measure: $\mathrm{gap}(P)$

Bottleneck: Factorization of low-degree polynomials
↳ Complexity measure: gap(P)

- $\mathrm{gap}(P) = \begin{cases} \mathcal{O}(k \log k + k \log h_P) & \text{[Kaltofen-Koiran]} \\ \mathcal{O}(k^2) & \text{[This work]} \end{cases}$

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

Bottleneck: Factorization of low-degree polynomials
↳ Complexity measure: gap(P)

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

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

- Multiplicities come for free!
  - [Kaltofen-Koiran] Apply k times the algorithm

Bottleneck: Factorization of low-degree polynomials
↳ Complexity measure: gap(P)

- $\mathrm{gap}(P) = \begin{cases} \mathcal{O}(k\log k + k\log h_P) & \text{[Kaltofen-Koiran]} \\ \mathcal{O}(k^2) & \text{[This work]} \end{cases}$

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

- Multiplicities come for free!
  - [Kaltofen-Koiran] Apply k times the algorithm
- Algebraic number field only: based on [H. Lenstra'99]

- **Multilinear** factors, with a new Gap Theorem:

$$\mathrm{val}\left(\sum_{j=1}^{\ell} a_j X^{\alpha_j}(uX+w)^{\beta_j}(vX+t)^{\gamma_j}\right) \leqslant \alpha_1 + 2\binom{\ell}{2};$$

- **Multilinear** factors, with a new Gap Theorem:

$$\operatorname{val}\left(\sum_{j=1}^{\ell} a_j X^{\alpha_j}(uX+w)^{\beta_j}(vX+t)^{\gamma_j}\right) \leqslant \alpha_1 + 2\binom{\ell}{2};$$

- **Multivariate** polynomials: Apply the Gap Theorem with $\mathbb{L} = \mathbb{K}(X_2, \dots, X_n)$;

- **Multilinear** factors, with a new Gap Theorem:

$$\operatorname{val}\left(\sum_{j=1}^{\ell} a_j X^{\alpha_j} (uX+w)^{\beta_j} (vX+t)^{\gamma_j}\right) \leqslant \alpha_1 + 2\binom{\ell}{2};$$

- **Multivariate** polynomials: Apply the Gap Theorem with $\mathbb{L} = \mathbb{K}(X_2, \dots, X_n)$;
- Multilinear factors with $\geqslant 3$ monomials over
  - $\overline{\mathbb{Q}}$: absolute factorization;
  - $\mathbb{R}$, $\mathbb{C}$: approximate factorization;
  - ...

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

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

Theorem

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

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

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

Theorem

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

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

Proposition

$\mathrm{wr}(f_1, \ldots, f_k) \neq 0 \iff f_j$'s linearly independent **over** $\mathbb{F}_{p^s}[X^p]$.

$$\text{Find multilinear factors of } P = \sum_{j=1}^{k} a_j X_1^{\alpha_{1,j}} \cdots X_n^{\alpha_{n,j}}$$
$$\text{where } a_j \in \mathbb{F}_{p^s} \text{ and } p > \deg(P)$$

Find multilinear factors of $P = \sum_{j=1}^{k} a_j X_1^{\alpha_{1,j}} \cdots X_n^{\alpha_{n,j}}$

where $a_j \in \mathbb{F}_{p^s}$ and $p > \deg(P)$

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

$(\geqslant 3)$-nomials → Common factors of $P_t = \sum_{j=j_t}^{j_t+\ell_t-1} a_j \mathbf{X}^{\alpha_j}$ $(\deg(P_t) \leqslant \mathcal{O}(\ell_t^2))$

Low-degree factorization

[Gao'03, Lecerf'10]

Find multilinear factors of $P = \sum_{j=1}^{k} a_j X_1^{\alpha_{1,j}} \cdots X_n^{\alpha_{n,j}}$

where $a_j \in \mathbb{F}_{p^s}$ and $p > \deg(P)$

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

binomials → $(uX^{\beta} - vX^{\gamma})$ $\Updownarrow$ Roots of univariate lacunary polynomials

$(\geqslant 3)$-nomials → Common factors of $P_t = \sum_{j=j_t}^{j_t+\ell_t-1} a_j X^{\alpha_j}$ $(\deg(P_t) \leqslant \mathcal{O}(\ell_t^2))$

Low-degree factorization

[Gao'03, Lecerf'10]

Find multilinear factors of $P = \sum_{j=1}^{k} a_j X_1^{\alpha_{1,j}} \cdots X_n^{\alpha_{n,j}}$

where $a_j \in \mathbb{F}_{p^s}$ and $p > \deg(P)$

- monomials → $(X, \min_j \alpha_j)$, $(Y, \min_j \beta_j)$
- binomials → $(uX^{\beta} - \ldots$ … R… …variate la… polynomials
  - **NP-complete under BPP reductions**
  - [Kipnis-Shamir'99,Bi-Cheng-Rojas'13]
- $(\geqslant 3)$-nomials → Common factors of $P_t = \sum_{j=j_t}^{j_t+\ell_t-1} a_j X^{\alpha_j}$ $(\deg(P_t) \leqslant \mathcal{O}(\ell_t^2))$
  - Low-degree factorization
  - [Gao'03, Lecerf'10]

Conclusion

- Multilinear factors of lacunary multivariate polynomials:

Conclusion

- Multilinear factors of lacunary multivariate polynomials:
  - $(\geqslant 3)$-nomials $\rightsquigarrow$ low-degree polynomials.

Conclusion

- Multilinear factors of lacunary multivariate polynomials:
  - $(\geqslant 3)$-nomials $\rightsquigarrow$ low-degree polynomials.
    - Valid for any field of characteristic 0;

Conclusion

- Multilinear factors of lacunary multivariate polynomials:
  - ($\geqslant 3$)-nomials $\rightsquigarrow$ low-degree polynomials.
    - Valid for any field of characteristic 0;
    - Valid to some extent in positive characteristic.

Conclusion

- Multilinear factors of lacunary multivariate polynomials:
  - $(\geqslant 3)$-nomials $\rightsquigarrow$ low-degree polynomials.
    - Valid for any field of characteristic 0;
    - Valid to some extent in positive characteristic.
  - binomials $\rightsquigarrow$ lacunary univariate polynomials.

Conclusion

- Multilinear factors of lacunary multivariate polynomials:
  - $(\geqslant 3)$-nomials $\rightsquigarrow$ low-degree polynomials.
    - Valid for any field of characteristic 0;
    - Valid to some extent in positive characteristic.
  - binomials $\rightsquigarrow$ lacunary univariate polynomials.
    - Only available for number fields;

Conclusion

- Multilinear factors of lacunary multivariate polynomials:
  - $(\geqslant 3)$-nomials $\rightsquigarrow$ low-degree polynomials.
    - Valid for any field of characteristic 0;
    - Valid to some extent in positive characteristic.
  - binomials $\rightsquigarrow$ lacunary univariate polynomials.
    - Only available for number fields;
    - NP-hard in positive characteristic.

Conclusion

- Multilinear factors of lacunary multivariate polynomials:
  - $(\geqslant 3)$-nomials $\rightsquigarrow$ low-degree polynomials.
    - Valid for any field of characteristic 0;
    - Valid to some extent in positive characteristic.
  - binomials $\rightsquigarrow$ lacunary univariate polynomials.
    - Only available for number fields;
    - NP-hard in positive characteristic.
- New Gap Theorem:

Conclusion

- Multilinear factors of lacunary multivariate polynomials:
  - ($\geqslant 3$)-nomials $\rightsquigarrow$ low-degree polynomials.
    - Valid for any field of characteristic 0;
    - Valid to some extent in positive characteristic.
  - binomials $\rightsquigarrow$ lacunary univariate polynomials.
    - Only available for number fields;
    - NP-hard in positive characteristic.
- New Gap Theorem:
  - Faster algorithm (large coefficients, multiplicities for free);

Conclusion

- Multilinear factors of lacunary multivariate polynomials:
  - $(\geqslant 3)$-nomials $\rightsquigarrow$ low-degree polynomials.
    - Valid for any field of characteristic 0;
    - Valid to some extent in positive characteristic.
  - binomials $\rightsquigarrow$ lacunary univariate polynomials.
    - Only available for number fields;
    - NP-hard in positive characteristic.
- New Gap Theorem:
  - Faster algorithm (large coefficients, multiplicities for free);
  - Easier implementation;

Conclusion

- Multilinear factors of lacunary multivariate polynomials:
  - ($\geqslant 3$)-nomials $\rightsquigarrow$ low-degree polynomials.
    - Valid for any field of characteristic 0;
    - Valid to some extent in positive characteristic.
  - binomials $\rightsquigarrow$ lacunary univariate polynomials.
    - Only available for number fields;
    - NP-hard in positive characteristic.
- New Gap Theorem:
  - Faster algorithm (large coefficients, multiplicities for free);
  - Easier implementation;
  - PIT algorithms for $\sum_j a_j \prod_i f_i^{\alpha_{ij}}$, $\sum_j a_j X^{\alpha_j}(uX^d + v)^{\beta_j}$.

Conclusion

- Multilinear factors of lacunary multivariate polynomials:
  - $(\geqslant 3)$-nomials $\rightsquigarrow$ low-degree polynomials.
    - Valid for any field of characteristic 0;
    - Valid to some extent in positive characteristic.
  - binomials $\rightsquigarrow$ lacunary univariate polynomials.
    - Only available for number fields;
    - NP-hard in positive characteristic.
- New Gap Theorem:
  - Faster algorithm (large coefficients, multiplicities for free);
  - Easier implementation;
  - PIT algorithms for $\sum_j a_j \prod_i f_i^{\alpha_{ij}}$, $\sum_j a_j X^{\alpha_j}(uX^d + v)^{\beta_j}$.
- Extensions: Low-degree/lacunary factors, small characteristic.

Conclusion

- Multilinear factors of lacunary multivariate polynomials:
  - ($\geqslant 3$)-nomials $\rightsquigarrow$ low-degree polynomials.
    - Valid for any field of characteristic 0;
    - Valid to some extent in positive characteristic.
  - binomials $\rightsquigarrow$ lacunary univariate polynomials.
    - Only available for number fields;
    - NP-hard in positive characteristic.
- New Gap Theorem:
  - Faster algorithm (large coefficients, multiplicities for free);
  - Easier implementation;
  - PIT algorithms for $\sum_j a_j \prod_i f_i^{\alpha_{ij}}$, $\sum_j a_j X^{\alpha_j}(uX^d + v)^{\beta_j}$.
- Extensions: Low-degree/lacunary factors, small characteristic.
- Correct bound for the valuation?

Conclusion

Open questions

- Real τ-conjecture and variants:

Open questions

- Real τ-conjecture and variants:
  - Special cases, such as $fg+1$;

Open questions

- Real τ-conjecture and variants:
  - Special cases, such as $fg + 1$;
  - Links with fewnomials theory.

Open questions

- Real τ-conjecture and variants:
  - Special cases, such as $fg + 1$;
  - Links with fewnomials theory.
- Generalize factorization algorithms:

Open questions

- Real τ-conjecture and variants:
  - Special cases, such as $fg + 1$;
  - Links with fewnomials theory.
- Generalize factorization algorithms:
  - Low-degree factors, lacunary factors;

Open questions

- Real τ-conjecture and variants:
  - Special cases, such as $fg + 1$;
  - Links with fewnomials theory.
- Generalize factorization algorithms:
  - Low-degree factors, lacunary factors;
  - Other fields, especially small characteristic;

Open questions

- Real τ-conjecture and variants:
  - Special cases, such as $fg + 1$;
  - Links with fewnomials theory.
- Generalize factorization algorithms:
  - Low-degree factors, lacunary factors;
  - Other fields, especially small characteristic;
  - More general polynomials $\rightsquigarrow$ arithmetic circuits.

Open questions

- Real τ-conjecture and variants:
  - Special cases, such as $fg + 1$;
  - Links with fewnomials theory.
- Generalize factorization algorithms:
  - Low-degree factors, lacunary factors;
  - Other fields, especially small characteristic;
  - More general polynomials $\rightsquigarrow$ arithmetic circuits.
- Practical efficiency