Fewestnomials in determinantal ideals

Jan Draisma (Bern/Eindhoven)

CCAAGGS, June 2022

joint with Thomas Kahle and Finn Wiersig

Fewestnomials in ideals

Definition

K a field, $I \subseteq K[x_1, \ldots, x_n]$ an ideal

$\rightsquigarrow c(I) := \min\{\text{number of terms in } f \mid f \in I \setminus \{0\}\}$

Fewestnomials in ideals

Definition
K a field, $I \subseteq K[x_1, \dots, x_n]$ an ideal
$\rightsquigarrow c(I) := \min\{\text{number of terms in } f \mid f \in I \setminus \{0\}\}$

Example
$c(I) = 1 \Leftrightarrow$ some power of $x_1 \cdot x_2 \cdots x_n$ lies in I.
Can be checked by a Gröbner basis computation.

Fewestnomials in ideals

Definition

K a field, $I \subseteq K[x_1, \dots, x_n]$ an ideal
$\rightsquigarrow c(I) := \min\{\text{number of terms in } f \mid f \in I \setminus \{0\}\}$

Example

$c(I) = 1 \Leftrightarrow$ some power of $x_1 \cdot x_2 \cdots x_n$ lies in I.
Can be checked by a Gröbner basis computation.

Questions

- What is $c(I)$ for your favourite I?
- Is $c(I)$ computable from generators of I?
- Why should you care?

The curious case of $c(I) = 2$

Philosophy [Eisenbud-Sturmfels, 1996]

Ideals *spanned* by binomials have many beautiful properties.

This condition is much stronger than $c(I) = 2$.

The curious case of $c(I) = 2$

Philosophy [Eisenbud-Sturmfels, 1996]

Ideals *spanned* by binomials have many beautiful properties.

This condition is much stronger than $c(I) = 2$.

Example [Jensen-Kahle-Kathän, 2017]

For $n \in \mathbb{Z}_{\geq 1}$, $I_n := ((x-z)^2, nx - y - (n-1)z) \subseteq \mathbb{Q}[x, y, z]$ has $c(I_n) = 2$ and $x^n - yz^{n-1}$ is the lowest-degree binomial in I_n.

The curious case of $c(I) = 2$

Philosophy [Eisenbud-Sturmfels, 1996]

Ideals *spanned* by binomials have many beautiful properties.

This condition is much stronger than $c(I) = 2$.

Example [Jensen-Kahle-Kathän, 2017]

For $n \in \mathbb{Z}_{\geq 1}$, $I_n := ((x - z)^2, nx - y - (n-1)z) \subseteq \mathbb{Q}[x, y, z]$ has $c(I_n) = 2$ and $x^n - yz^{n-1}$ is the lowest-degree binomial in I_n.

Theorem [Jensen-Kahle-Kathän, 2017]

$\exists$ algorithm that, on input $I \subseteq \mathbb{Q}[x_1, \ldots, x_n]$, decides $c(I) \stackrel{?}{=} 2$.

The curious case of $c(I) = 2$

Philosophy [Eisenbud-Sturmfels, 1996]

Ideals *spanned* by binomials have many beautiful properties.

This condition is much stronger than $c(I) = 2$.

Example [Jensen-Kahle-Kathän, 2017]

For $n \in \mathbb{Z}_{\geq 1}$, $I_n := ((x-z)^2, nx - y - (n-1)z) \subseteq \mathbb{Q}[x, y, z]$ has $c(I_n) = 2$ and $x^n - yz^{n-1}$ is the lowest-degree binomial in I_n.

Theorem [Jensen-Kahle-Kathän, 2017]

$\exists$ algorithm that, on input $I \subseteq \mathbb{Q}[x_1, \ldots, x_n]$, decides $c(I) \stackrel{?}{=} 2$.

Question: Is $c(I)$ computable?
Special cases: What if $n = 1$ or if I is linearly generated?

The curious case of $c(I) = 2$

Outline of the Jensen-Kahle-Kathän algorithm:

- Rule out $c(I) = 1$, pass to $I \subseteq \mathbb{Q}[x_1^{\pm}, \ldots, x_n^{\pm}]$.
- If $x^\alpha - a \cdot x^0 \in I$, then $\mathrm{Trop}(I) \subseteq \alpha^\perp$.
- Compute a basis $\alpha_1, \ldots, \alpha_m \in \mathbb{Z}^n$ of $\mathrm{Trop}(I)^\perp$.
- After a monomial coordinate change: $\alpha_i = e_i$, so $x^{\alpha_i} = x_i$.
- Need to look for binomials in $J := \mathbb{Q}[x_1^{\pm}, \ldots, x_m^{\pm}] \cap I$.

The curious case of $c(I) = 2$

Outline of the Jensen-Kahle-Kathän algorithm:

- Rule out $c(I) = 1$, pass to $I \subseteq \mathbb{Q}[x_1^{\pm}, \ldots, x_n^{\pm}]$.
- If $x^\alpha - a \cdot x^0 \in I$, then $\mathrm{Trop}(I) \subseteq \alpha^\perp$.
- Compute a basis $\alpha_1, \ldots, \alpha_m \in \mathbb{Z}^n$ of $\mathrm{Trop}(I)^\perp$.
- After a monomial coordinate change: $\alpha_i = e_i$, so $x^{\alpha_i} = x_i$.
- Need to look for binomials in $J := \mathbb{Q}[x_1^{\pm}, \ldots, x_m^{\pm}] \cap I$.

- $\mathrm{Trop}(J) = \{0\} \subseteq \mathbb{R}^m$.
- Hence $A := \mathbb{Q}[x_1^{\pm}, \ldots, x_m^{\pm}]/J$ is finite-dimensional.
- Let $M_i \in \mathrm{End}(A)$ be multiplication with x_i.
- Then need to find $\alpha \in \mathbb{Z}^m$ s.t. $M_1^{\alpha_1} \cdots M_m^{\alpha_m} = a \cdot \mathrm{id}_A$.
- This had already been solved in number theory.

Our results

K algebraically closed
$X \subseteq K^n$ closed subvariety
$I(X) \subseteq K[x_1, \ldots, x_n] \rightsquigarrow c(X) := c(I(X))$

Our results

K algebraically closed
$X \subseteq K^n$ closed subvariety
$I(X) \subseteq K[x_1, \ldots, x_n] \rightsquigarrow c(X) := c(I(X))$

Theorem 1 [D-Kahle-Wiersig, 2021]
For a very general r-dimensional *linear space* $X \subseteq K^n$ we have $c(X) = r + 1$.

Our results

K algebraically closed
$X \subseteq K^n$ closed subvariety
$I(X) \subseteq K[x_1, \dots, x_n] \rightsquigarrow c(X) := c(I(X))$

Theorem 1 [D-Kahle-Wiersig, 2021]
For a very general r-dimensional *linear space* $X \subseteq K^n$ we have $c(X) = r + 1$.

Theorem 2 [D-Kahle-Wiersig, 2021]
For $X := \{A \in K^{m \times n} \mid \mathrm{rk}(A) \leq r\}$ we have $c(X) = (r + 1)!$

Our results

K algebraically closed
$X \subseteq K^n$ closed subvariety
$I(X) \subseteq K[x_1, \ldots, x_n] \rightsquigarrow c(X) := c(I(X))$

Theorem 1 [D-Kahle-Wiersig, 2021]
For a very general r-dimensional *linear space* $X \subseteq K^n$ we have $c(X) = r + 1$.

Theorem 2 [D-Kahle-Wiersig, 2021]
For $X := \{A \in K^{m \times n} \mid \mathrm{rk}(A) \leq r\}$ we have $c(X) = (r+1)!$

Theorem 3 [D-Kahle-Wiersig, 2021]
For r even, $X := \{A \mid A^T = -A, \mathrm{rk}(A) \leq r\} \subseteq K^{m(m-1)/2}$ we have $c(X) = (r+1)!! = (r+1)(r-1)(r-3)\cdots 3 \cdot 1$.

Our results

K algebraically closed
$X \subseteq K^n$ closed subvariety
$I(X) \subseteq K[x_1, \dots, x_n] \rightsquigarrow c(X) := c(I(X))$

Theorem 1 [D-Kahle-Wiersig, 2021]
For a very general r-dimensional *linear space* $X \subseteq K^n$ we have $c(X) = r + 1$.

Theorem 2 [D-Kahle-Wiersig, 2021]
For $X := \{A \in K^{m \times n} \mid \mathrm{rk}(A) \leq r\}$ we have $c(X) = (r+1)!$

Theorem 3 [D-Kahle-Wiersig, 2021]
For r even, $X := \{A \mid A^T = -A, \mathrm{rk}(A) \leq r\} \subseteq K^{m(m-1)/2}$ we have $c(X) = (r+1)!! = (r+1)(r-1)(r-3)\cdots 3 \cdot 1$.

... and in each case we know all $f \in I(X)$ with $c(X)$ terms.

Theorem 1 $\Rightarrow$ Theorem 2

Know: for a very general r-space $X \subseteq K^n$, $c(X) = r + 1$.
To show: $c(\{rk(A) \leq r\}) \geq (r + 1)!$

- Induction: assume true for $(m - 1, r)$ and $(m - 1, r - 1)$.

Theorem 1 $\Rightarrow$ Theorem 2

Know: for a very general r-space $X \subseteq K^n$, $c(X) = r + 1$.
To show: $c(\{rk(A) \leq r\}) \geq (r + 1)!$

- Induction: assume true for $(m - 1, r)$ and $(m - 1, r - 1)$.
- Let $f \in K[x_{ij} \mid i \in [m], j \in [n]] \setminus \{0\}$ vanish on $\{\text{rk} \leq r\}$.

Theorem 1 $\Rightarrow$ Theorem 2

Know: for a very general r-space $X \subseteq K^n$, $c(X) = r + 1$.
To show: $c(\{rk(A) \leq r\}) \geq (r+1)!$

- Induction: assume true for $(m-1, r)$ and $(m-1, r-1)$.
- Let $f \in K[x_{ij} \mid i \in [m], j \in [n]] \setminus \{0\}$ vanish on $\{\text{rk} \leq r\}$.
- Expand $f(A, x_m) = \sum_{\alpha \in \mathbb{Z}^n_{\geq 0}} f_\alpha(A) x_m^\alpha$ where

A	$m-1$
x_m	1

Theorem 1 $\Rightarrow$ Theorem 2

Know: for a very general r-space $X \subseteq K^n$, $c(X) = r + 1$.
To show: $c(\{rk(A) \leq r\}) \geq (r + 1)!$

- Induction: assume true for $(m - 1, r)$ and $(m - 1, r - 1)$.
- Let $f \in K[x_{ij} \mid i \in [m], j \in [n]] \setminus \{0\}$ vanish on $\{\mathrm{rk} \leq r\}$.
- Expand $f(A, x_m) = \sum_{\alpha \in \mathbb{Z}^n_{\geq 0}} f_\alpha(A) x_m^\alpha$ where $\begin{array}{|c|}\hline A \\ \hline x_m \\ \hline \end{array} \begin{array}{l} m-1 \\ 1 \end{array}$
- Each $f_\alpha \neq 0$ vanishes on $\{\mathrm{rk} \leq (r - 1)\} \rightsquigarrow \geq r!$ terms.

Theorem 1 $\Rightarrow$ Theorem 2

Know: for a very general r-space $X \subseteq K^n$, $c(X) = r + 1$.
To show: $c(\{rk(A) \leq r\}) \geq (r+1)!$

- Induction: assume true for $(m-1, r)$ and $(m-1, r-1)$.
- Let $f \in K[x_{ij} \mid i \in [m], j \in [n]] \setminus \{0\}$ vanish on $\{\text{rk} \leq r\}$.
- Expand $f(A, x_m) = \sum_{\alpha \in \mathbb{Z}^n_{\geq 0}} f_\alpha(A) x_m^\alpha$ where

A	$m-1$
x_m	1

- Each $f_\alpha \neq 0$ vanishes on $\{\text{rk} \leq (r-1)\} \rightsquigarrow \geq r!$ terms.
- If an $f_\alpha \neq 0$ vanishes on all rank-$\leq r$ matrices, done.

Theorem 1 $\Rightarrow$ Theorem 2

Know: for a very general r-space $X \subseteq K^n$, $c(X) = r + 1$.
To show: $c(\{rk(A) \leq r\}) \geq (r + 1)!$

- Induction: assume true for $(m - 1, r)$ and $(m - 1, r - 1)$.
- Let $f \in K[x_{ij} \mid i \in [m], j \in [n]] \setminus \{0\}$ vanish on $\{\text{rk} \leq r\}$.
- Expand $f(A, x_m) = \sum_{\alpha \in \mathbb{Z}^n_{\geq 0}} f_\alpha(A) x_m^\alpha$ where $\begin{array}{|c|}\hline A \\ \hline x_m \\ \hline \end{array} \begin{array}{c} m-1 \\ 1 \end{array}$
- Each $f_\alpha \neq 0$ vanishes on $\{\text{rk} \leq (r - 1)\} \rightsquigarrow \geq r!$ terms.
- If an $f_\alpha \neq 0$ vanishes on all rank-$\leq r$ matrices, done.
- Take $A \in K^{(m-1) \times n}$ very general of rank r. Then $f_\alpha(A) \neq 0$ for all α with $f_\alpha \neq 0$. Theorem 1 applied to the row space X of A yields that $f_\alpha \neq 0$ for at least $(r + 1)$ distinct α.

$\rightsquigarrow$ f has at least $(r + 1) \cdot r! = (r + 1)!$ terms $\square$

A subtlety in Theorem 1

Theorem 1
For a very general r-space $X \subseteq K^n$ we have $c(X) = r + 1$.

A subtlety in Theorem 1

Theorem 1
For a very general r-space $X \subseteq K^n$ we have $c(X) = r + 1$.

Question
$X \subseteq K^n$ subspace of dimension r, and no *linear* polynomial with $< r + 1$ terms vanishes on X $\Rightarrow c(X) = r + 1$?

A subtlety in Theorem 1

Theorem 1
For a very general r-space $X \subseteq K^n$ we have $c(X) = r + 1$.

Question
$X \subseteq K^n$ subspace of dimension r, and no *linear* polynomial with $< r + 1$ terms vanishes on X $\Rightarrow c(X) = r + 1$?

Answer
NO: Take $K^6 = \bigwedge^2 K^4$, $X = \bigwedge^2 U \subseteq K^6$ with $U \subseteq K^4$ sufficiently general of dimension 3.

A subtlety in Theorem 1

Theorem 1
For a very general r-space $X \subseteq K^n$ we have $c(X) = r + 1$.

Question
$X \subseteq K^n$ subspace of dimension r, and no *linear* polynomial with $< r + 1$ terms vanishes on X $\Rightarrow c(X) = r + 1$?

Answer
NO: Take $K^6 = \bigwedge^2 K^4$, $X = \bigwedge^2 U \subseteq K^6$ with $U \subseteq K^4$ sufficiently general of dimension 3.

Then X defines the uniform matroid of rank 3 on K^6, but the 4×4-Pfaffian $x_{12}x_{24} - x_{13}x_{24} + x_{14}x_{23}$ vanishes on X and has $3 < 4$ terms.

Proof of Theorem 1

Theorem 1
For a very general r-space $X \subseteq K^n$ we have $c(X) = r + 1$.

Theorem 1
For a very general r-space $X \subseteq K^n$ we have $c(X) = r + 1$.

• If $F \subseteq K[x_1, ..., x_n]_d$ is a linear subspace spanned by s monomials and some nonzero element of F vanishes on X, then on *each* element of $\mathrm{Gr}(r, K^n)$ some nonzero element of F vanishes.

Proof of Theorem 1

Theorem 1
For a very general r-space $X \subseteq K^n$ we have $c(X) = r + 1$.

• If $F \subseteq K[x_1, \ldots, x_n]_d$ is a linear subspace spanned by s monomials and some nonzero element of F vanishes on X, then on *each* element of $\mathrm{Gr}(r, K^n)$ some nonzero element of F vanishes.

• Then gF has the latter property for every $g \in \mathrm{GL}_n(K)$.

Theorem 1
For a very general r-space $X \subseteq K^n$ we have $c(X) = r + 1$.

- If $F \subseteq K[x_1, ..., x_n]_d$ is a linear subspace spanned by s monomials and some nonzero element of F vanishes on X, then on *each* element of $\mathrm{Gr}(r, K^n)$ some nonzero element of F vanishes.
- Then gF has the latter property for every $g \in \mathrm{GL}_n(K)$.
- Then also $F' := \mathrm{gin}_{\succ}(F)$ does, where $x_1 \succ x_2 \succ ...$

Theorem 1
For a very general r-space $X \subseteq K^n$ we have $c(X) = r + 1$.

• If $F \subseteq K[x_1, ..., x_n]_d$ is a linear subspace spanned by s monomials and some nonzero element of F vanishes on X, then on *each* element of $\mathrm{Gr}(r, K^n)$ some nonzero element of F vanishes.

• Then gF has the latter property for every $g \in \mathrm{GL}_n(K)$.

• Then also $F' := \mathrm{gin}_{\succ}(F)$ does, where $x_1 \succ x_2 \succ ...$

• Hence $F' \not\subseteq K[x_1, ..., x_r]_d$, as no polynomial in $x_1, ..., x_r$ vanishes on $K^r \times \{0\}^{n-r}$.

Theorem 1
For a very general r-space $X \subseteq K^n$ we have $c(X) = r + 1$.

• If $F \subseteq K[x_1, \ldots, x_n]_d$ is a linear subspace spanned by s monomials and some nonzero element of F vanishes on X, then on *each* element of $\mathrm{Gr}(r, K^n)$ some nonzero element of F vanishes.

• Then gF has the latter property for every $g \in \mathrm{GL}_n(K)$.

• Then also $F' := \mathrm{gin}_{\succ}(F)$ does, where $x_1 \succ x_2 \succ \ldots$

• Hence $F' \not\subseteq K[x_1, \ldots, x_r]_d$, as no polynomial in $x_1, \ldots, x_r$ vanishes on $K^r \times \{0\}^{n-r}$.

• Hence F' contains a monomial x^β divisible by some x_j, $j > r$, but then $(|F| =)|F'| \geq r + 1$. $\square$

Characterisation of equality

If $f \in I \subseteq K[x_1, ..., x_n]$, then also:

- $c \cdot x^{\alpha} \cdot f \in I$ for all $c \in K^*$, $\alpha \in \mathbb{Z}^n_{\geq 0}$

Characterisation of equality

If $f \in I \subseteq K[x_1, \ldots, x_n]$, then also:

- $c \cdot x^\alpha \cdot f \in I$ for all $c \in K^*$, $\alpha \in \mathbb{Z}^n_{\geq 0}$
- $f^p \in I$ where p is the char. exp. of K.

and these operations preserve the number of terms.

Characterisation of equality

If $f \in I \subseteq K[x_1, \dots, x_n]$, then also:

- $c \cdot x^\alpha \cdot f \in I$ for all $c \in K^*$, $\alpha \in \mathbb{Z}^n_{\geq 0}$
- $f^p \in I$ where p is the char. exp. of K.

and these operations preserve the number of terms.

Theorem 1' [D-Kahle-Wiersig, 2021]

For $r \geq 2$, the only $(r+1)$-term polynomials that vanish on a very general r-space $X \subseteq K^n$ are $c \cdot x^\alpha \cdot \ell^{p^e}$ where ℓ is a linear form with $r+1$ terms.

Characterisation of equality

If $f \in I \subseteq K[x_1, \dots, x_n]$, then also:

- $c \cdot x^\alpha \cdot f \in I$ for all $c \in K^*$, $\alpha \in \mathbb{Z}^n_{\geq 0}$
- $f^p \in I$ where p is the char. exp. of K.

and these operations preserve the number of terms.

Theorem 1' [D-Kahle-Wiersig, 2021]
For $r \geq 2$, the only $(r+1)$-term polynomials that vanish on a very general r-space $X \subseteq K^n$ are $c \cdot x^\alpha \cdot \ell^{p^e}$ where ℓ is a linear form with $r+1$ terms.

Theorem 2' [D-Kahle-Wiersig, 2021]
For $r \geq 2$, the only $(r+1)!$-term polynomials that vanish on rank-r matrices are $c \cdot x^\alpha \cdot \det^{p^e}$ where det is some $(r+1) \times (r+1)$-minor.

Characterisation of equality

If $f \in I \subseteq K[x_1, \dots, x_n]$, then also:

- $c \cdot x^\alpha \cdot f \in I$ for all $c \in K^*$, $\alpha \in \mathbb{Z}^n_{\geq 0}$
- $f^p \in I$ where p is the char. exp. of K.

and these operations preserve the number of terms.

Theorem 1' [D-Kahle-Wiersig, 2021]
For $r \geq 2$, the only $(r+1)$-term polynomials that vanish on a very general r-space $X \subseteq K^n$ are $c \cdot x^\alpha \cdot \ell^{p^e}$ where ℓ is a linear form with $r+1$ terms.

Theorem 2' [D-Kahle-Wiersig, 2021]
For $r \geq 2$, the only $(r+1)!$-term polynomials that vanish on rank-r matrices are $c \cdot x^\alpha \cdot \det^{p^e}$ where det is some $(r+1) \times (r+1)$-minor.

Theorem 3'. $(r+2)$-Pfaffians in the skew-symmetric case.

Key proof ingredient

Definition

reverse lexicographic order $\succ$ defined by $x^{\alpha} \succ x^{\beta}$ if the *largest i* with $\alpha_i \neq \beta_i$ satisfies $\alpha_i < \beta_i$.

Key proof ingredient

Definition

reverse lexicographic order $\succ$ defined by $x^\alpha \succ x^\beta$ if the *largest i* with $\alpha_i \neq \beta_i$ satisfies $\alpha_i < \beta_i$.

So $x_1^d \succ x_1^{d-1}x_2 \succ x_1^{d-2}x_2^2 \succ ... \succ x_2^d \succ x_1^{d-1}x_3 \succ x_1^{d-2}x_2x_3 \succ ... \succ x_2^{d-1}x_3 \succ x_1^{d-2}x_3^2 \succ ...$

Key proof ingredient

Definition
reverse lexicographic order $\succ$ defined by $x^\alpha \succ x^\beta$ if the *largest i* with $\alpha_i \neq \beta_i$ satisfies $\alpha_i < \beta_i$.

So $x_1^d \succ x_1^{d-1}x_2 \succ x_1^{d-2}x_2^2 \succ ... \succ x_2^d \succ x_1^{d-1}x_3 \succ x_1^{d-2}x_2x_3 \succ ... \succ x_2^{d-1}x_3 \succ x_1^{d-2}x_3^2 \succ ...$

Theorem [Fløystad, 1999]
If $s \geq 3$, char $K = 0$ and a subspace $F \subseteq K[x_1, ..., x_n]_d$ has $\text{gin}_\succ F = x_1^{d-1} \cdot \langle x_1, ..., x_s \rangle$, then $F = f \cdot \langle \ell_1, ..., \ell_s \rangle$ for some $f \in K[x_1, ..., x_n]_{d-1}$ and some linear forms $\ell_1, ..., \ell_s$.

Key proof ingredient

Definition

reverse lexicographic order $\succ$ defined by $x^\alpha \succ x^\beta$ if the *largest i* with $\alpha_i \neq \beta_i$ satisfies $\alpha_i < \beta_i$.

So $x_1^d \succ x_1^{d-1}x_2 \succ x_1^{d-2}x_2^2 \succ ... \succ x_2^d \succ x_1^{d-1}x_3 \succ x_1^{d-2}x_2x_3 \succ ... \succ x_2^{d-1}x_3 \succ x_1^{d-2}x_3^2 \succ ...$

Theorem [Fløystad, 1999]

If $s \geq 3$, char $K = 0$ and a subspace $F \subseteq K[x_1, ..., x_n]_d$ has $\text{gin}_\succ F = x_1^{d-1} \cdot \langle x_1, ..., x_s \rangle$, then $F = f \cdot \langle \ell_1, ..., \ell_s \rangle$ for some $f \in K[x_1, ..., x_n]_{d-1}$ and some linear forms $\ell_1, ..., \ell_s$.

We established a characteristic-*p* analogue of this, with p^e-th powers of linear forms.

Key proof ingredient

Definition
reverse lexicographic order $\succ$ defined by $x^\alpha \succ x^\beta$ if the *largest i* with $\alpha_i \neq \beta_i$ satisfies $\alpha_i < \beta_i$.

So $x_1^d \succ x_1^{d-1}x_2 \succ x_1^{d-2}x_2^2 \succ ... \succ x_2^d \succ x_1^{d-1}x_3 \succ x_1^{d-2}x_2x_3 \succ ... \succ x_2^{d-1}x_3 \succ x_1^{d-2}x_3^2 \succ ...$

Theorem [Fløystad, 1999]
If $s \geq 3$, char $K = 0$ and a subspace $F \subseteq K[x_1, ..., x_n]_d$ has $\text{gin}_\succ F = x_1^{d-1} \cdot \langle x_1, ..., x_s \rangle$, then $F = f \cdot \langle \ell_1, ..., \ell_s \rangle$ for some $f \in K[x_1, ..., x_n]_{d-1}$ and some linear forms $\ell_1, ..., \ell_s$.

We established a characteristic-p analogue of this, with p^e-th powers of linear forms.

Open problem: the case of symmetric matrices!

Hitting set generators (after Robert Andrews)

Definition

For a family of polynomials $S \subseteq K[x_1, \ldots, x_n]$, a *hitting set generator* is a polynomial map $g : K^m \to K^n$ such that $f \circ g \in K[y_1, \ldots, y_m] \setminus \{0\}$ for all $f \in S \setminus \{0\}$.

Hitting set generators (after Robert Andrews)

Definition
For a family of polynomials $S \subseteq K[x_1, ..., x_n]$, a *hitting set generator* is a polynomial map $g : K^m \to K^n$ such that $f \circ g \in K[y_1, ..., y_m] \setminus \{0\}$ for all $f \in S \setminus \{0\}$.

One wants m small compared to n and $\deg(g)$ small.

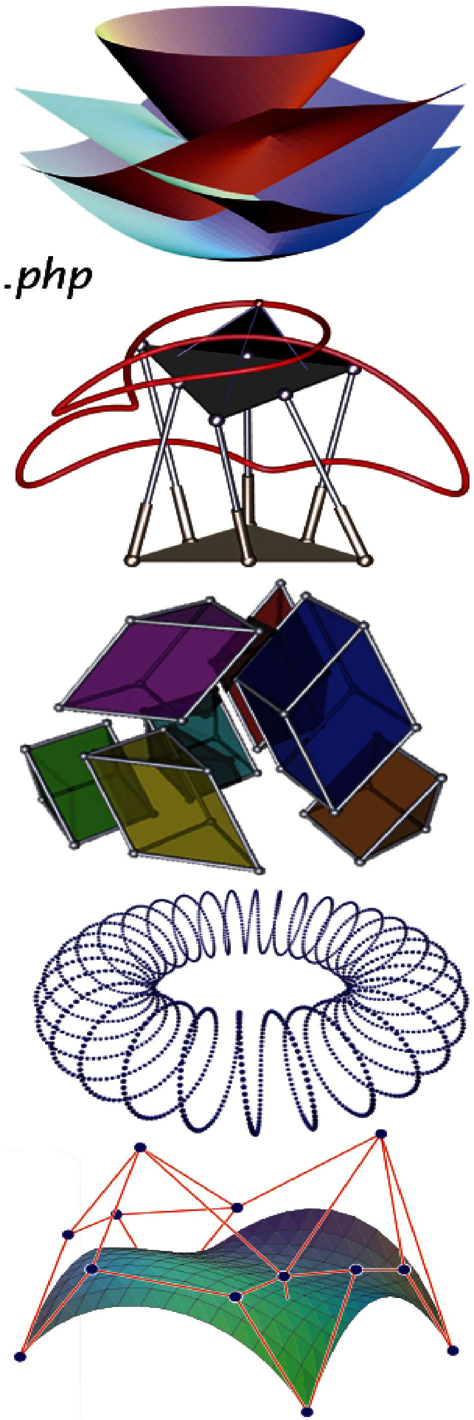
Hitting set generators (after Robert Andrews)

Definition
For a family of polynomials $S \subseteq K[x_1, \dots, x_n]$, a *hitting set generator* is a polynomial map $g : K^m \to K^n$ such that $f \circ g \in K[y_1, \dots, y_m] \setminus \{0\}$ for all $f \in S \setminus \{0\}$.

One wants m small compared to n and $\deg(g)$ small.

Observation [Robert Andrews]
For $S = \{\text{polynomials with} \leq t \text{ terms}\}$, choose r such that $(r+1)! \geq t$, Theorem 2 gives a degree-two hitting set generator $g : K^{\sqrt{n}\times r} \times K^{r\times\sqrt{n}} \to K^{\sqrt{n}\times\sqrt{n}} = K^n, (A, B) \mapsto AB$.

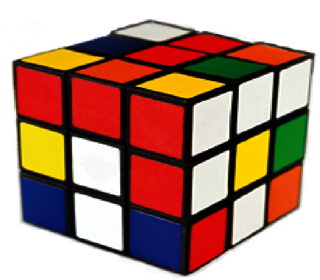
The resulting $m = c \cdot \sqrt{n} \cdot \log(t) / \log(\log(t))$ is near optimal.

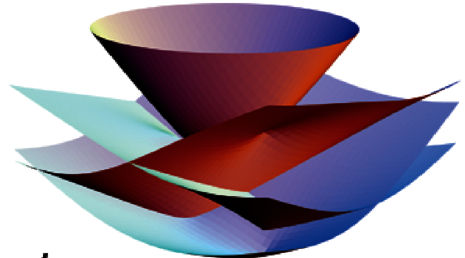


http://www.siam.org/journals/siaga.php

SIAM Journal on

Applied Algebra and Geometry

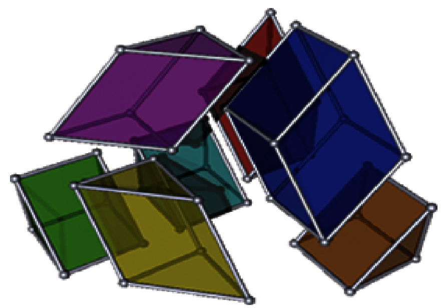


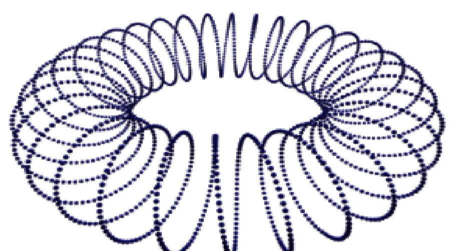


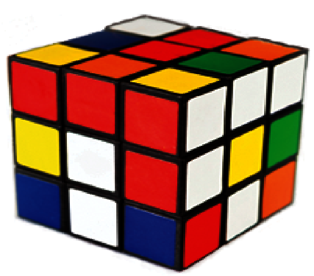
http://www.siam.org/journals/siaga.php

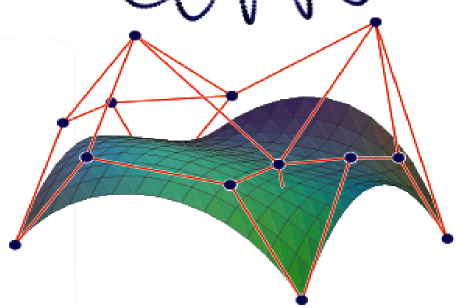
SIAM Journal on

Applied Algebra and Geometry









Thank you!