No short polynomials vanish on bounded-rank matrices

Jan Draisma (Bern/Eindhoven)
Konstanz, January 2022
joint with Thomas Kahle and Finn Wiersig

The setting

Definition

K field

$I \subseteq K[x_1, \dots, x_n]$ ideal

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

The setting

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

Example
$c(I) = 1$ iff I contains a monomial. Can be tested by Gröbner basis computations.

The setting

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

Example
$c(I) = 1$ iff I contains a monomial. Can be tested by Gröbner basis computations.

Remarks
- highly dependent on coordinates
- various questions: computational, theoretical
- various techniques: geometry, commutative algebra

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

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 $c(I_n) = 2$ but $x^n - yz^{n-1}$ is the lowest-degree binomial in I_n.

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

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 $c(I_n) = 2$ but $x^n - yz^{n-1}$ is the lowest-degree binomial in I_n.

Theorem [Jensen-Kahle-Kathän, 2017]

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

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

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 $c(I_n) = 2$ but $x^n - yz^{n-1}$ is the lowest-degree binomial in I_n.

Theorem [Jensen-Kahle-Kathän, 2017]
There exists an algorithm that, on input $I \subseteq \mathbb{Q}[x_1, \dots, x_n]$, decides whether $c(I) = 2$.

Outline:

- Rule out $c(I) = 1$, pass to $I \subseteq \mathbb{Q}[x_1^{\pm}, \dots, x_n^{\pm}]$.
- If $x^\alpha - a \cdot x^0 \in I$, then the tropical variety $T(I)$ of I is in the hyperplane $\perp \alpha$; find a basis $\alpha_1, \dots, \alpha_m \in \mathbb{Z}^n$ of $T(I)^\perp$.
- Look for binomials in $\mathbb{Q}[x^{\alpha_1}, \dots, x^{\alpha_m}] \cap I$ (Artinian case) via membership problem in commutative matrix semigroups.

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 $X := \{A \in K^{m \times n} \mid \operatorname{rk}(A) \leq r\}$ we have $c(X) = (r+1)!$

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

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 $c(X) = (r+1)!!$

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

Theorem 1 $\Rightarrow$ Theorem 2

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

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

Theorem 1 $\Rightarrow$ Theorem 2

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

• 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 all rank-$\leq r$ matrices.

Theorem 1 $\Rightarrow$ Theorem 2

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

- 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 all rank-$\leq r$ matrices.
- Expand $f(A, x_m) = \sum_{\alpha \in \mathbb{Z}^n_{\geq 0}} f_\alpha(A) x_m^\alpha$ where A stands for the first $m - 1$ rows and x_m for the last.

Theorem 1 $\Rightarrow$ Theorem 2

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

- 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 all rank-$\leq r$ matrices.
- Expand $f(A, x_m) = \sum_{\alpha \in \mathbb{Z}^n_{\geq 0}} f_\alpha(A) x_m^\alpha$ where A stands for the first $m - 1$ rows and x_m for the last.
- Each $f_\alpha \neq 0$ vanishes on rank-$\leq (r - 1)$ matrices A, hence has $\geq r!$ terms.

Theorem 1 $\Rightarrow$ Theorem 2

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

- 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 all rank-$\leq r$ matrices.
- Expand $f(A, x_m) = \sum_{\alpha \in \mathbb{Z}^n_{\geq 0}} f_\alpha(A) x_m^\alpha$ where A stands for the first $m-1$ rows and x_m for the last.
- Each $f_\alpha \neq 0$ vanishes on rank-$\leq (r-1)$ matrices A, hence has $\geq r!$ terms.
- If an $f_\alpha \neq 0$ vanishes on rank-$\leq r$ matrices, done.

Theorem 1 $\Rightarrow$ Theorem 2

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

- 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 all rank-$\leq r$ matrices.
- Expand $f(A, x_m) = \sum_{\alpha \in \mathbb{Z}^n_{\geq 0}} f_\alpha(A) x_m^\alpha$ where A stands for the first $m-1$ rows and x_m for the last.
- Each $f_\alpha \neq 0$ vanishes on rank-$\leq (r-1)$ matrices A, hence has $\geq r!$ terms.
- If an $f_\alpha \neq 0$ vanishes on 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.

□

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 $c(X) = r + 1$.

- Take some $d \in \mathbb{Z}_{\geq 0}$, look at degree-$d$ equations.

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

- Take some $d \in \mathbb{Z}_{\geq 0}$, look at degree-$d$ equations.
- For any $F \in \mathrm{Gr}(s, K[x_1, \ldots, x_n])_d$, the set $H(F) := \{X \in \mathrm{Gr}(r, K^n) \mid \exists [f] \in \mathbb{P}F : f|_X = 0\}$ is closed.

Proof of Theorem 1

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

• Take some $d \in \mathbb{Z}_{\geq 0}$, look at degree-$d$ equations.

• For any $F \in \mathrm{Gr}(s, K[x_1, \dots, x_n])_d$, the set
$H(F) := \{X \in \mathrm{Gr}(r, K^n) \mid \exists [f] \in \mathbb{P}F : f|_X = 0\}$ is closed.

• May assume that X is outside all $H(F)$ for all F *spanned by monomials* with $H(F) \subsetneq \mathrm{Gr}(r, K^n)$ (countable union).

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

- Take some $d \in \mathbb{Z}_{\geq 0}$, look at degree-$d$ equations.
- For any $F \in \mathrm{Gr}(s, K[x_1, \ldots, x_n])_d$, the set $H(F) := \{X \in \mathrm{Gr}(r, K^n) \mid \exists [f] \in \mathbb{P}F : f|_X = 0\}$ is closed.
- May assume that X is outside all $H(F)$ for all F *spanned by monomials* with $H(F) \subsetneq \mathrm{Gr}(r, K^n)$ (countable union).
- If then $X \in H(F)$ for a monomial F, then $F \in Z = \{E \in \mathrm{Gr}(s, K[x_1, \ldots, x_n]_d) \mid H(E) = \mathrm{Gr}(r, K^n)\}$, a closed set on which GL_n acts.

Proof of Theorem 1

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

• Take some $d \in \mathbb{Z}_{\geq 0}$, look at degree-$d$ equations.

• For any $F \in \mathrm{Gr}(s, K[x_1, \ldots, x_n])_d$, the set $H(F) := \{X \in \mathrm{Gr}(r, K^n) \mid \exists [f] \in \mathbb{P}F : f|_X = 0\}$ is closed.

• May assume that X is outside all $H(F)$ for all F *spanned by monomials* with $H(F) \subsetneq \mathrm{Gr}(r, K^n)$ (countable union).

• If then $X \in H(F)$ for a monomial F, then $F \in Z = \{E \in \mathrm{Gr}(s, K[x_1, \ldots, x_n]_d) \mid H(E) = \mathrm{Gr}(r, K^n)\}$, a closed set on which GL_n acts.

• By Borel's fixed point theorem, Z contains a point F' stable under B (upper triangular matrices).

Proof of Theorem 1, continued

- Then F' is spanned by s monomials, and preserved under the linear maps $x_i \mapsto x_i + cx_j$ with $j < i$.

Proof of Theorem 1, continued

- Then F' is spanned by s monomials, and preserved under the linear maps $x_i \mapsto x_i + cx_j$ with $j < i$.

- In characteristic zero, this means that if $x^\beta \in F'$ and $\beta_i > 0$ and $j < i$, then also $x^{\beta - e_i + e_j} \in F'$.

Proof of Theorem 1, continued

- Then F' is spanned by s monomials, and preserved under the linear maps $x_i \mapsto x_i + cx_j$ with $j < i$.

- In characteristic zero, this means that if $x^\beta \in F'$ and $\beta_i > 0$ and $j < i$, then also $x^{\beta - e_i + e_j} \in F'$.

- So if $\beta_i > 0$ for some $i > r$, then also $x^{\beta - e_i + e_1}, \ldots, x^{\beta - e_i + e_r}$ are in F', so $|F| = |F'| = s \geq r + 1$.

Proof of Theorem 1, continued

• Then F' is spanned by s monomials, and preserved under the linear maps $x_i \mapsto x_i + cx_j$ with $j < i$.

• In characteristic zero, this means that if $x^\beta \in F'$ and $\beta_i > 0$ and $j < i$, then also $x^{\beta - e_i + e_j} \in F'$.

• So if $\beta_i > 0$ for some $i > r$, then also $x^{\beta - e_i + e_1}, \ldots, x^{\beta - e_i + e_r}$ are in F', so $|F| = |F'| = s \geq r + 1$.

• Assume F' contains only monomials in $x_1, \ldots, x_r$. Then there are linear spaces on which no polynomial in F' vanishes, e.g. $K^r \times \{0\}^{n-r}$. Hence $F' \notin Z$, a contradiction.

Proof of Theorem 1, continued

- Then F' is spanned by s monomials, and preserved under the linear maps $x_i \mapsto x_i + cx_j$ with $j < i$.

- In characteristic zero, this means that if $x^\beta \in F'$ and $\beta_i > 0$ and $j < i$, then also $x^{\beta - e_i + e_j} \in F'$.

- So if $\beta_i > 0$ for some $i > r$, then also $x^{\beta - e_i + e_1}, \dots, x^{\beta - e_i + e_r}$ are in F', so $|F| = |F'| = s \geq r + 1$.

- Assume F' contains only monomials in $x_1, \dots, x_r$. Then there are linear spaces on which no polynomial in F' vanishes, e.g. $K^r \times \{0\}^{n-r}$. Hence $F' \notin Z$, a contradiction.

- A similar argument works in characteristic $p > 0$.

$\square$

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 $f \in I \subseteq K[x_1, ..., x_n]$, 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 $f \in I \subseteq K[x_1, \ldots, x_n]$, 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.

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.

Proof idea

Consider

$$Z = \{F \in \mathrm{Gr}(r+1, K[x_1, \ldots, x_n]_d) \mid \forall X \in \mathrm{Gr}(r, K^n) \exists [f] \in \mathbb{P}F : f|_X = 0\}$$

Proof idea

Consider

$$Z = \{F \in \mathrm{Gr}(r+1, K[x_1, \ldots, x_n]_d) \mid \\ \forall X \in \mathrm{Gr}(r, K^n) \exists [f] \in \mathbb{P}F : f|_X = 0\}$$

Seen before: if X is very general and $I(X)$ contains an $r+1$-term polynomial f, then the terms of f span an $F \in Z$.

Proof idea

Consider

$$Z = \{F \in \mathrm{Gr}(r+1, K[x_1, \dots, x_n]_d) \mid \\ \forall X \in \mathrm{Gr}(r, K^n) \exists [f] \in \mathbb{P}F : f|_X = 0\}$$

Seen before: if X is very general and $I(X)$ contains an $r+1$-term polynomial f, then the terms of f span an $F \in Z$.

Then for any $g \in \mathrm{GL}_n$, $F' := \mathrm{in}_< gF \in Z$ for any monomial order $<$ with $x_1 > \dots > x_n$; this is a B-stable point in $\overline{\mathrm{GL}_n \cdot F}$.

Proof idea

Consider

$$Z = \{F \in \mathrm{Gr}(r+1, K[x_1, ..., x_n]_d) \mid \forall X \in \mathrm{Gr}(r, K^n) \exists [f] \in \mathbb{P}F : f|_X = 0\}$$

Seen before: if X is very general and $I(X)$ contains an $r+1$-term polynomial f, then the terms of f span an $F \in Z$.

Then for any $g \in \mathrm{GL}_n$, $F' := \mathrm{in}_< gF \in Z$ for any monomial order $<$ with $x_1 > ... > x_n$; this is a B-stable point in $\overline{\mathrm{GL}_n \cdot F}$.

For $g \in GL_n$ sufficiently general, F' is constant, called $\mathrm{gin}_< F$, the *generic initial space* of F.

Proof idea

Consider

$$Z = \{F \in \mathrm{Gr}(r+1, K[x_1, \dots, x_n]_d) \mid \\ \forall X \in \mathrm{Gr}(r, K^n) \exists [f] \in \mathbb{P}F : f|_X = 0\}$$

Seen before: if X is very general and $I(X)$ contains an $r+1$-term polynomial f, then the terms of f span an $F \in Z$.

Then for any $g \in \mathrm{GL}_n$, $F' := \mathrm{in}_< gF \in Z$ for any monomial order $<$ with $x_1 > \dots > x_n$; this is a B-stable point in $\overline{\mathrm{GL}_n \cdot F}$.

For $g \in GL_n$ sufficiently general, F' is constant, called $\mathrm{gin}_< F$, the *generic initial space* of F.

Have seen: $\mathrm{gin}_< F$ is *not* contained in $K[x_1, \dots, x_r]$, and in characteristic zero, $\mathrm{gin}_< F = x_1^{d-1} \cdot \langle x_1, \dots, x_{r+1} \rangle$.

Proof idea

Definition

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

Proof idea

Definition

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

So $x_1^d > x_1^{d-1}x_2 > x_1^{d-2}x_2^2 > ... > x_2^d > x_1^{d-1}x_3 > x_1^{d-2}x_2x_3 > ... > x_2^{d-1}x_3 > x_1^{d-2}x_3^2 > ...$ for $> = >_{\text{revlex}}$

Proof idea

Definition

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

So $x_1^d > x_1^{d-1}x_2 > x_1^{d-2}x_2^2 > ... > x_2^d > x_1^{d-1}x_3 > x_1^{d-2}x_2x_3 > ... > x_2^{d-1}x_3 > x_1^{d-2}x_3^2 > ...$ for $> = >_{\text{revlex}}$

Theorem [Fløystad, 1999]

If $s \geq 3$, $\operatorname{char} K = 0$ and a subspace $F \subseteq K[x_1, ..., x_n]_d$ satisfies $\operatorname{gin}_{<_{\text{revlex}}} F = x_1^{d-1} \cdot \langle x_1, ..., x_s \rangle$, 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 $\ell_1, ..., \ell_s$.

Proof idea

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

So $x_1^d > x_1^{d-1}x_2 > x_1^{d-2}x_2^2 > ... > x_2^d > x_1^{d-1}x_3 > x_1^{d-2}x_2x_3 > ... > x_2^{d-1}x_3 > x_1^{d-2}x_3^2 > ...$ for $> = >_{\text{revlex}}$

Theorem [Fløystad, 1999]
If $s \geq 3$, $\operatorname{char} K = 0$ and a subspace $F \subseteq K[x_1, ..., x_n]_d$ satisfies $\operatorname{gin}_{<_{\text{revlex}}} F = x_1^{d-1} \cdot \langle x_1, ..., x_s \rangle$, 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 have proved a characteristic-p analogue of this, with p^e-th powers of linear forms.

Hitting set generators (after Robert Andrews)

Definition

For a family of nonzero 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 $f \in S$.

Definition

For a family of nonzero 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 $f \in S$.

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

Hitting set generators (after Robert Andrews)

Definition
For a family of nonzero 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 $f \in S$.

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.

Hitting set generators (after Robert Andrews)

Definition
For a family of nonzero 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 $f \in S$.

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.

Thank you!