Peter Paule 60 years young: cogito ergo summo

Joachim von zur Gathen
B-IT, Universität Bonn

18 May 2018

Peter Paule

- ISSAC 1996 Zürich: Peter explains GFF to me for *Modern Computer Algebra*, very patiently. “Cogito ergo summo”.
- Christmas cards, designed by his wife.
- 2002 Waterloo and Shakespeare at Stratford on Avon.
- 2011 Christmas salon

Peter Paule

- ISSAC 1996 Zürich: Peter explains GFF to me for *Modern Computer Algebra*, very patiently. “Cogito ergo summo”.
- Christmas cards, designed by his wife.
- 2002 Waterloo and Shakespeare at Stratford on Avon.
- 2011 Christmas salon

Peter Paule

- ISSAC 1996 Zürich: Peter explains GFF to me for *Modern Computer Algebra*, very patiently. “Cogito ergo summo”.
- Christmas cards, designed by his wife.
- 2002 Waterloo and Shakespeare at Stratford on Avon.
- 2011 Christmas salon

Peter Paule

- ISSAC 1996 Zürich: Peter explains GFF to me for *Modern Computer Algebra*, very patiently. “Cogito ergo summo”.
- Christmas cards, designed by his wife.
- 2002 Waterloo and Shakespeare at Stratford on Avon.
- 2011 Christmas salon

Peter Paule

- ISSAC 1996 Zürich: Peter explains GFF to me for *Modern Computer Algebra*, very patiently. “Cogito ergo summo”.
- Christmas cards, designed by his wife.
- 2002 Waterloo and Shakespeare at Stratford on Avon.
- 2011 Christmas salon

2002 Waterloo.

Peter and my daughter Rafaela on Mark Giesbrecht's deck.
Photo courtesy of Mark Giesbrecht.

From my talk on Alexander von Humboldt at Peter's 2011 salon:

- 1805-1828: report on his travel, 30 volumes, richly illustrated, at own expense. Teaching in Berlin, today "Humboldt Universität". Up to 1000 people in the audience.
- 1829: expedition to Russia, assessing silver mines in the Altai region.
- 1830-1859: high positions at the royal court in Berlin. Diplomatic missions.
- Eloquent, elegant. Network of leading scientists. Fundamental contributions to anatomy, history and prehistory, botany, geology, philology, and zoology.
  Goethe: "You cannot read in eight days in books what this man tells you in an hour".

Cogito ergo summo.

From my talk on Alexander von Humboldt at Peter's 2011 salon:

- 1805-1828: report on his travel, 30 volumes, richly illustrated, at own expense. Teaching in Berlin, today "Humboldt Universität". Up to 1000 people in the audience.
- 1829: expedition to Russia, assessing silver mines in the Altai region.
- 1830-1859: high positions at the royal court in Berlin. Diplomatic missions.
- Eloquent, elegant. Network of leading scientists. Fundamental contributions to anatomy, history and prehistory, botany, geology, philology, and zoology.
  Goethe: "You cannot read in eight days in books what this man tells you in an hour".

Cogito ergo summo.

Technical part: Combinatorics on polynomial equations—do they describe nice varieties?

Joint work with Guillermo Matera

- Combinatorics on polynomials
- Task
- Some results
- Methods
- Open questions

Combinatorics on polynomials

General question: given a class of polynomials over finite fields, how many elements does it contain? Equivalent: probability to be in that class.

Classical: (ir)reducible univariate and multivariate polynomials (Carlitz; Cohen; Wan; Gao & Lauder; Bodin; Hou & Mullen). Amenable to a (non-standard) variant of generatingfunctionology plus some extra work (vzG, Viola & Ziegler). This yields exact formulas, asymptotics, and explicit estimates.

Combinatorics on polynomials

General question: given a class of polynomials over finite fields, how many elements does it contain? Equivalent: probability to be in that class.

Classical: (ir)reducible univariate and multivariate polynomials (Carlitz; Cohen; Wan; Gao & Lauder; Bodin; Hou & Mullen). Amenable to a (non-standard) variant of generatingfunctionology plus some extra work (vzG, Viola & Ziegler). This yields exact formulas, asymptotics, and explicit estimates.

Combinatorics on polynomials

- Irreducibility and other properties for several multivariate polynomials: this talk. Approximate results.
- Previous work: curves in high-dimensional spaces. Approximate results.
  Model: Chow variety (Eisenbud & Harris; Cesaratto, vzG & Matera).

Combinatorics on polynomials

- Irreducibility and other properties for several multivariate polynomials: this talk. Approximate results.
- Previous work: curves in high-dimensional spaces. Approximate results.
  Model: Chow variety (Eisenbud & Harris; Cesaratto, vzG & Matera).

The task

An algebraic variety V is defined by a system of polynomial equations. A fair number of results in algebraic geometry only hold if the system or the variety satisfy certain conditions of being "nice":

- V is a set-theoretic complete intersection. Equivalently: The system is regular, so that no polynomial is a zero divisor modulo the previous ones.
- V is an ideal-theoretic complete intersection.
- V is absolutely irreducible.
- V is nonsingular.
- V is non-degenerate (not contained in a hyperplane).

Intuition: these five properties hold for most systems and varieties.

The task

An algebraic variety V is defined by a system of polynomial equations. A fair number of results in algebraic geometry only hold if the system or the variety satisfy certain conditions of being "nice":

- V is a set-theoretic complete intersection. Equivalently: The system is regular, so that no polynomial is a zero divisor modulo the previous ones.
- V is an ideal-theoretic complete intersection.
- V is absolutely irreducible.
- V is nonsingular.
- V is non-degenerate (not contained in a hyperplane).

Intuition: these five properties hold for most systems and varieties.

The task

An algebraic variety V is defined by a system of polynomial equations. A fair number of results in algebraic geometry only hold if the system or the variety satisfy certain conditions of being "nice":

- V is a set-theoretic complete intersection. Equivalently: The system is regular, so that no polynomial is a zero divisor modulo the previous ones.
- V is an ideal-theoretic complete intersection.
- V is absolutely irreducible.
- V is nonsingular.
- V is non-degenerate (not contained in a hyperplane).

Intuition: these five properties hold for most systems and varieties.

The task

An algebraic variety V is defined by a system of polynomial equations. A fair number of results in algebraic geometry only hold if the system or the variety satisfy certain conditions of being "nice":

- V is a set-theoretic complete intersection. Equivalently: The system is regular, so that no polynomial is a zero divisor modulo the previous ones.
- V is an ideal-theoretic complete intersection.
- V is absolutely irreducible.
- V is nonsingular.
- V is non-degenerate (not contained in a hyperplane).

Intuition: these five properties hold for most systems and varieties.

The task

An algebraic variety V is defined by a system of polynomial equations. A fair number of results in algebraic geometry only hold if the system or the variety satisfy certain conditions of being "nice":

- V is a set-theoretic complete intersection. Equivalently: The system is regular, so that no polynomial is a zero divisor modulo the previous ones.
- V is an ideal-theoretic complete intersection.
- V is absolutely irreducible.
- V is nonsingular.
- V is non-degenerate (not contained in a hyperplane).

Intuition: these five properties hold for most systems and varieties.

The task

An algebraic variety V is defined by a system of polynomial equations. A fair number of results in algebraic geometry only hold if the system or the variety satisfy certain conditions of being “nice”:

- V is a set-theoretic complete intersection. Equivalently: The system is regular, so that no polynomial is a zero divisor modulo the previous ones.
- V is an ideal-theoretic complete intersection.
- V is absolutely irreducible.
- V is nonsingular.
- V is non-degenerate (not contained in a hyperplane).

Intuition: these five properties hold for most systems and varieties.

The task

An algebraic variety V is defined by a system of polynomial equations. A fair number of results in algebraic geometry only hold if the system or the variety satisfy certain conditions of being “nice”:

- V is a set-theoretic complete intersection. Equivalently: The system is regular, so that no polynomial is a zero divisor modulo the previous ones.
- V is an ideal-theoretic complete intersection.
- V is absolutely irreducible.
- V is nonsingular.
- V is non-degenerate (not contained in a hyperplane).

Intuition: these five properties hold for most systems and varieties.

Results

Setting:

- field K with algebraic closure $\bar{K}$,
- projective varieties and homogeneous polynomials,
- $r =$ dimension = (number of variables) -1,
- $s =$ number of polynomials,
- $d = (d_1, \ldots, d_s)$ degree pattern,
- $f = (f_1, \ldots, f_s)$ system of homogeneous polynomials in $r + 1$ variables over K with $\deg f_i = d_i$ for all i,
- $\delta = d_1 \cdots d_s =$ Bézout number,
- $\sigma = d_1 + \cdots + d_s - s =$ "sum" of degrees,
- $V(f) \subseteq \mathbb{P}^r_{\bar{K}}$ projective variety defined by f over $\bar{K}$.

The set of all such f forms a multiprojective space over K.

Results

Setting:

- field K with algebraic closure $\bar{K}$,
- projective varieties and homogeneous polynomials,
- $r =$ dimension = (number of variables) -1,
- $s =$ number of polynomials,
- $d = (d_1, \ldots, d_s)$ degree pattern,
- $f = (f_1, \ldots, f_s)$ system of homogeneous polynomials in $r + 1$ variables over K with $\deg f_i = d_i$ for all i,
- $\delta = d_1 \cdots d_s =$ Bézout number,
- $\sigma = d_1 + \cdots + d_s - s =$ "sum" of degrees,
- $V(f) \subseteq \mathbb{P}^r_{\bar{K}}$ projective variety defined by f over $\bar{K}$.

The set of all such f forms a multiprojective space over K.

Results

Setting:

- field K with algebraic closure $\bar{K}$,
- projective varieties and homogeneous polynomials,
- $r =$ dimension = (number of variables) -1,
- $s =$ number of polynomials,
- $d = (d_1, \ldots, d_s)$ degree pattern,
- $f = (f_1, \ldots, f_s)$ system of homogeneous polynomials in $r+1$ variables over K with $\deg f_i = d_i$ for all i,
- $\delta = d_1 \cdots d_s =$ Bézout number,
- $\sigma = d_1 + \cdots + d_s - s =$ "sum" of degrees,
- $V(f) \subseteq \mathbb{P}^r_{\bar{K}}$ projective variety defined by f over $\bar{K}$.

The set of all such f forms a multiprojective space over K.

Results

Setting:

- field K with algebraic closure $\bar{K}$,
- projective varieties and homogeneous polynomials,
- $r =$ dimension = (number of variables) -1,
- $s =$ number of polynomials,
- $d = (d_1, \ldots, d_s)$ degree pattern,
- $f = (f_1, \ldots, f_s)$ system of homogeneous polynomials in $r+1$ variables over K with $\deg f_i = d_i$ for all i,
- $\delta = d_1 \cdots d_s =$ Bézout number,
- $\sigma = d_1 + \cdots + d_s - s =$ "sum" of degrees,
- $V(f) \subseteq \mathbb{P}^r_{\bar{K}}$ projective variety defined by f over $\bar{K}$.

The set of all such f forms a multiprojective space over K.

Results

Setting:

- field K with algebraic closure $\bar{K}$,
- projective varieties and homogeneous polynomials,
- $r =$ dimension = (number of variables) -1,
- $s =$ number of polynomials,
- $d = (d_1, \ldots, d_s)$ degree pattern,
- $f = (f_1, \ldots, f_s)$ system of homogeneous polynomials in $r + 1$ variables over K with $\deg f_i = d_i$ for all i,
- $\delta = d_1 \cdots d_s =$ Bézout number,
- $\sigma = d_1 + \cdots + d_s - s =$ "sum" of degrees,
- $V(f) \subseteq \mathbb{P}^r_{\bar{K}}$ projective variety defined by f over $\bar{K}$.

The set of all such f forms a multiprojective space over K.

Results

Setting:

- field K with algebraic closure $\bar{K}$,
- projective varieties and homogeneous polynomials,
- $r =$ dimension = (number of variables) -1,
- $s =$ number of polynomials,
- $d = (d_1, \ldots, d_s)$ degree pattern,
- $f = (f_1, \ldots, f_s)$ system of homogeneous polynomials in $r + 1$ variables over K with $\deg f_i = d_i$ for all i,
- $\delta = d_1 \cdots d_s =$ Bézout number,
- $\sigma = d_1 + \cdots + d_s - s =$ "sum" of degrees,
- $V(f) \subseteq \mathbb{P}^r_{\bar{K}}$ projective variety defined by f over $\bar{K}$.

The set of all such f forms a multiprojective space over K.

Results

Setting:

- field K with algebraic closure $\bar{K}$,
- projective varieties and homogeneous polynomials,
- $r =$ dimension = (number of variables) -1,
- $s =$ number of polynomials,
- $d = (d_1, \ldots, d_s)$ degree pattern,
- $f = (f_1, \ldots, f_s)$ system of homogeneous polynomials in $r + 1$ variables over K with $\deg f_i = d_i$ for all i,
- $\delta = d_1 \cdots d_s =$ Bézout number,
- $\sigma = d_1 + \cdots + d_s - s =$ "sum" of degrees,
- $V(f) \subseteq \mathbb{P}^r_{\bar{K}}$ projective variety defined by f over $\bar{K}$.

The set of all such f forms a multiprojective space over K.

Results

Setting:

- field K with algebraic closure $\bar{K}$,
- projective varieties and homogeneous polynomials,
- $r =$ dimension = (number of variables) -1,
- $s =$ number of polynomials,
- $d = (d_1, \ldots, d_s)$ degree pattern,
- $f = (f_1, \ldots, f_s)$ system of homogeneous polynomials in $r + 1$ variables over K with $\deg f_i = d_i$ for all i,
- $\delta = d_1 \cdots d_s =$ Bézout number,
- $\sigma = d_1 + \cdots + d_s - s =$ "sum" of degrees,
- $V(f) \subseteq \mathbb{P}^r_{\bar{K}}$ projective variety defined by f over $\bar{K}$.

The set of all such f forms a multiprojective space over K.

Results

Setting:

- field K with algebraic closure $\bar{K}$,
- projective varieties and homogeneous polynomials,
- $r =$ dimension = (number of variables) -1,
- $s =$ number of polynomials,
- $d = (d_1, \ldots, d_s)$ degree pattern,
- $f = (f_1, \ldots, f_s)$ system of homogeneous polynomials in $r + 1$ variables over K with $\deg f_i = d_i$ for all i,
- $\delta = d_1 \cdots d_s =$ Bézout number,
- $\sigma = d_1 + \cdots + d_s - s =$ "sum" of degrees,
- $V(f) \subseteq \mathbb{P}^r_{\bar{K}}$ projective variety defined by f over $\bar{K}$.

The set of all such f forms a multiprojective space over K.

Results

Setting:

- field K with algebraic closure $\bar{K}$,
- projective varieties and homogeneous polynomials,
- $r =$ dimension = (number of variables) -1,
- $s =$ number of polynomials,
- $d = (d_1, \ldots, d_s)$ degree pattern,
- $f = (f_1, \ldots, f_s)$ system of homogeneous polynomials in $r + 1$ variables over K with $\deg f_i = d_i$ for all i,
- $\delta = d_1 \cdots d_s =$ Bézout number,
- $\sigma = d_1 + \cdots + d_s - s =$ "sum" of degrees,
- $V(f) \subseteq \mathbb{P}^r_{\bar{K}}$ projective variety defined by f over $\bar{K}$.

The set of all such f forms a multiprojective space over K.

Results

Setting:

- field K with algebraic closure $\bar{K}$,
- projective varieties and homogeneous polynomials,
- $r =$ dimension = (number of variables) -1,
- $s =$ number of polynomials,
- $d = (d_1, \ldots, d_s)$ degree pattern,
- $f = (f_1, \ldots, f_s)$ system of homogeneous polynomials in $r + 1$ variables over K with $\deg f_i = d_i$ for all i,
- $\delta = d_1 \cdots d_s =$ Bézout number,
- $\sigma = d_1 + \cdots + d_s - s =$ "sum" of degrees,
- $V(f) \subseteq \mathbb{P}^r_{\bar{K}}$ projective variety defined by f over $\bar{K}$.

The set of all such f forms a multiprojective space over K.

Results

The first four properties hold for almost all systems, but the last one, non-degeneracy, does not.

For each of the first four properties "prop", we find a nonzero "genericity polynomial" P_{prop} in the coefficients of the systems f with explicitly bounded degree so that for all systems f we have

$$P_{\text{prop}}(f) \neq 0 \Longrightarrow V(f) \text{ has the property.}$$

When $K = \mathbb{F}_q$ is a finite field, then each property holds with a probability that tends rapidly to 1 with growing q.

In contrast, most systems describe a degenerate variety.

Results

The first four properties hold for almost all systems, but the last one, non-degeneracy, does not.

For each of the first four properties "prop", we find a nonzero "genericity polynomial" P_{prop} in the coefficients of the systems f with explicitly bounded degree so that for all systems f we have

$$P_{\text{prop}}(f) \neq 0 \Longrightarrow V(f) \text{ has the property.}$$

When $K = \mathbb{F}_q$ is a finite field, then each property holds with a probability that tends rapidly to 1 with growing q.

In contrast, most systems describe a degenerate variety.

Results

The first four properties hold for almost all systems, but the last one, non-degeneracy, does not.

For each of the first four properties "prop", we find a nonzero "genericity polynomial" P_{prop} in the coefficients of the systems f with explicitly bounded degree so that for all systems f we have

$$P_{\text{prop}}(f) \neq 0 \Longrightarrow V(f) \text{ has the property.}$$

When $K = \mathbb{F}_q$ is a finite field, then each property holds with a probability that tends rapidly to 1 with growing q.

In contrast, most systems describe a degenerate variety.

Results

The first four properties hold for almost all systems, but the last one, non-degeneracy, does not.

For each of the first four properties "prop", we find a nonzero "genericity polynomial" P_{prop} in the coefficients of the systems f with explicitly bounded degree so that for all systems f we have

$$P_{\text{prop}}(f) \neq 0 \Longrightarrow V(f) \text{ has the property.}$$

When $K = \mathbb{F}_q$ is a finite field, then each property holds with a probability that tends rapidly to 1 with growing q.

In contrast, most systems describe a degenerate variety.

Results

The first four properties hold for almost all systems, but the last one, non-degeneracy, does not.

For each of the first four properties "prop", we find a nonzero "genericity polynomial" P_{prop} in the coefficients of the systems f with explicitly bounded degree so that for all systems f we have

$$P_{\text{prop}}(f) \neq 0 \Longrightarrow V(f) \text{ has the property.}$$

When $K = \mathbb{F}_q$ is a finite field, then each property holds with a probability that tends rapidly to 1 with growing q.

In contrast, most systems describe a degenerate variety.

Template of results

For a property "prop", we state results of the following form.

Geometric theorem. There exists a nonzero multihomogeneous genericity polynomial P_{prop} in variables representing the coefficients of a system f with the following properties:

- For each f with $P_{\text{prop}}(f) \neq 0$, $V(f)$ has property "prop".
- The degree of P_{prop} in each of the s sets of variables is at most degBound.

Combinatorial corollary. For a finite field $\mathbb{F}_q$ with $q \geq s \cdot \text{degBound}/3$, the probability that $V(f)$ has property "prop" for a uniformly random system f over $\mathbb{F}_q$ satisfies

$$1 - \frac{s \cdot \text{degBound}}{q} \leq \text{probability} \leq 1.$$

Tool: multihomogeneous Weil bounds.

Template of results

For a property "prop", we state results of the following form.

Geometric theorem. There exists a nonzero multihomogeneous genericity polynomial P_{prop} in variables representing the coefficients of a system f with the following properties:

- For each f with $P_{\text{prop}}(f) \neq 0$, $V(f)$ has property "prop".
- The degree of P_{prop} in each of the s sets of variables is at most degBound.

Combinatorial corollary. For a finite field $\mathbb{F}_q$ with $q \geq s \cdot \text{degBound}/3$, the probability that $V(f)$ has property "prop" for a uniformly random system f over $\mathbb{F}_q$ satisfies

$$1 - \frac{s \cdot \text{degBound}}{q} \leq \text{probability} \leq 1.$$

Tool: multihomogeneous Weil bounds.

Template of results

For a property "prop", we state results of the following form.

Geometric theorem. There exists a nonzero multihomogeneous genericity polynomial P_{prop} in variables representing the coefficients of a system f with the following properties:

- For each f with $P_{\text{prop}}(f) \neq 0$, $V(f)$ has property "prop".
- The degree of P_{prop} in each of the s sets of variables is at most degBound.

Combinatorial corollary. For a finite field $\mathbb{F}_q$ with $q \geq s \cdot \text{degBound}/3$, the probability that $V(f)$ has property "prop" for a uniformly random system f over $\mathbb{F}_q$ satisfies

$$1 - \frac{s \cdot \text{degBound}}{q} \leq \text{probability} \leq 1.$$

Tool: multihomogeneous Weil bounds.

Template of results

For a property "prop", we state results of the following form.

Geometric theorem. There exists a nonzero multihomogeneous genericity polynomial P_{prop} in variables representing the coefficients of a system f with the following properties:

- For each f with $P_{\text{prop}}(f) \neq 0$, $V(f)$ has property "prop".
- The degree of P_{prop} in each of the s sets of variables is at most degBound.

Combinatorial corollary. For a finite field $\mathbb{F}_q$ with $q \geq s \cdot \text{degBound}/3$, the probability that $V(f)$ has property "prop" for a uniformly random system f over $\mathbb{F}_q$ satisfies

$$1 - \frac{s \cdot \text{degBound}}{q} \leq \text{probability} \leq 1.$$

Tool: multihomogeneous Weil bounds.

Template of results

Feature: degBound and s depend on the geometric system parameters like r, the degrees, and the property under consideration, but not on q.

The genericity polynomials are explicitly given and can be evaluated in polynomial time in the model of arithmetic circuits (aka straight-line programs).

Template of results

Feature: degBound and s depend on the geometric system parameters like r, the degrees, and the property under consideration, but not on q.

The genericity polynomials are explicitly given and can be evaluated in polynomial time in the model of arithmetic circuits (aka straight-line programs).

Complete intersection

Property: set-theoretic complete intersection. Thus $V(f)$ has dimension $r - s$, and (equivalently) the system f forms a regular sequence of $\overline{K}[X_0, \ldots, X_r]$.
Geometry: degBound $= \delta$.

Property: ideal-theoretic complete intersection. $V(f)$ is a set-theoretic complete intersection and the ideal generated by f in $\overline{K}[X_0, \ldots, X_r]$ is radical. In particular, $\dim V(f) = r - s$ and $\deg V(f) = \delta$.
Geometry:

$$\text{degBound} = 2\sigma\delta.$$

Combinatorics over $\mathbb{F}_q$:

$$1 - \frac{2s\sigma\delta}{q} \leq \text{probability} \leq 1.$$

Complete intersection

Property: set-theoretic complete intersection. Thus $V(f)$ has dimension $r - s$, and (equivalently) the system f forms a regular sequence of $\overline{K}[X_0, \ldots, X_r]$.
Geometry: degBound $= \delta$.

Property: ideal-theoretic complete intersection. $V(f)$ is a set-theoretic complete intersection and the ideal generated by f in $\overline{K}[X_0, \ldots, X_r]$ is radical. In particular, $\dim V(f) = r - s$ and $\deg V(f) = \delta$.
Geometry:

$$\text{degBound} = 2\sigma\delta.$$

Combinatorics over $\mathbb{F}_q$:

$$1 - \frac{2s\sigma\delta}{q} \leq \text{probability} \leq 1.$$

Complete intersection

Property: set-theoretic complete intersection. Thus $V(f)$ has dimension $r - s$, and (equivalently) the system f forms a regular sequence of $\overline{K}[X_0, \ldots, X_r]$.
Geometry: degBound $= \delta$.

Property: ideal-theoretic complete intersection. $V(f)$ is a set-theoretic complete intersection and the ideal generated by f in $\overline{K}[X_0, \ldots, X_r]$ is radical. In particular, $\dim V(f) = r - s$ and $\deg V(f) = \delta$.
Geometry:

$$\text{degBound} = 2\sigma\delta.$$

Combinatorics over $\mathbb{F}_q$:

$$1 - \frac{2s\sigma\delta}{q} \leq \text{probability} \leq 1.$$

Nonsingular complete intersection

Property: $V(f)$ is a nonsingular complete intersection of dimension $r - s$ and degree δ.

Geometry:

$$\text{degBound} = (\sigma + r)\sigma^{r-s}\delta.$$

Combinatorics over $\mathbb{F}_q$:

$$1 - \frac{s(\sigma + r)\sigma^{r-s}\delta}{q} \leq \text{probability} \leq 1.$$

Nonsingular complete intersection

Property: $V(f)$ is a nonsingular complete intersection of dimension $r - s$ and degree δ.

Geometry:

$$\text{degBound} = (\sigma + r)\sigma^{r-s}\delta.$$

Combinatorics over $\mathbb{F}_q$:

$$1 - \frac{s(\sigma + r)\sigma^{r-s}\delta}{q} \leq \text{probability} \leq 1.$$

Absolutely irreducible complete intersection

Property: $V(f)$ is an absolutely irreducible complete intersection of dimension $r - s$ and degree δ.

Geometry:

$$\text{degBound} = 3\sigma^2\delta.$$

Combinatorics over $\mathbb{F}_q$:

$$1 - \frac{3s\sigma^2\delta}{q} \leq \text{probability} \leq 1.$$

Absolutely irreducible complete intersection

Property: $V(f)$ is an absolutely irreducible complete intersection of dimension $r - s$ and degree δ.

Geometry:

$$\text{degBound} = 3\sigma^2\delta.$$

Combinatorics over $\mathbb{F}_q$:

$$1 - \frac{3s\sigma^2\delta}{q} \leq \text{probability} \leq 1.$$

Most varieties are degenerate

Fix integers $s, b \geq 2$ and consider all $d = (d_1, \ldots, d_s)$ with $d_1 \geq d_2 \geq \cdots \geq d_s \geq 1$, $d_1 \geq 2$, and Bézout number $\delta(d) = d_1 \cdots d_s = b$. These correspond to unordered factorizations of b, 1 being allowed as a factor.

Lemma. The number of all such d is at most $b^{\log_2 \log_2 b}$.

Notation:

$$
\begin{aligned}
D_i(d) &= \binom{r + d_i}{r} - 1 \quad \text{for } 1 \leq i \leq s, \\
D(d) &= (D_1(d), \ldots, D_s(d)), \\
|D(d)| &= D_1(d) + \cdots + D_s(d), \\
d^{(b)} &= (b, 1, \ldots, 1), \\
D^{(b)} &= D(b^{(d)}).
\end{aligned}
$$

Most varieties are degenerate

Fix integers $s, b \geq 2$ and consider all $d = (d_1, \ldots, d_s)$ with $d_1 \geq d_2 \geq \cdots \geq d_s \geq 1$, $d_1 \geq 2$, and Bézout number $\delta(d) = d_1 \cdots d_s = b$. These correspond to unordered factorizations of b, 1 being allowed as a factor.

Lemma. The number of all such d is at most $b^{\log_2 \log_2 b}$.

Notation:

$$D_i(d) = \binom{r + d_i}{r} - 1 \quad \text{for } 1 \leq i \leq s,$$

$$D(d) = (D_1(d), \ldots, D_s(d)),$$

$$|D(d)| = D_1(d) + \cdots + D_s(d),$$

$$d^{(b)} = (b, 1, \ldots, 1),$$

$$D^{(b)} = D(b^{(d)}).$$

Most varieties are degenerate

Fix integers $s, b \geq 2$ and consider all $d = (d_1, \ldots, d_s)$ with $d_1 \geq d_2 \geq \cdots \geq d_s \geq 1$, $d_1 \geq 2$, and Bézout number $\delta(d) = d_1 \cdots d_s = b$. These correspond to unordered factorizations of b, 1 being allowed as a factor.

Lemma. The number of all such d is at most $b^{\log_2 \log_2 b}$.

Notation:

$$
\begin{aligned}
D_i(d) &= \binom{r + d_i}{r} - 1 \quad \text{for } 1 \leq i \leq s, \\
D(d) &= (D_1(d), \ldots, D_s(d)), \\
|D(d)| &= D_1(d) + \cdots + D_s(d), \\
d^{(b)} &= (b, 1, \ldots, 1), \\
D^{(b)} &= D(b^{(d)}).
\end{aligned}
$$

Most varieties are degenerate

Lemma. For all $d \neq d^{(b)}$, we have $|D^{(b)}| \geq |D(b)| + g(b)$, where

$$g(b) = \binom{b+r}{r} - 2\binom{b/2+r}{r}.$$

Then $g(b) \geq 1$.

Geometry. $S^{(d)}$ = set of all f with degree pattern d, defining an absolutely irreducible complete intersection of dimension $r - s$ and degree b.
Then for any $d \neq d^{(b)}$, we have

$$\dim S^{d^{(b)}} \geq \dim S^d + g(b).$$

Most varieties are degenerate

Lemma. For all $d \neq d^{(b)}$, we have $|D^{(b)}| \geq |D(b)| + g(b)$, where

$$g(b) = \binom{b+r}{r} - 2\binom{b/2+r}{r}.$$

Then $g(b) \geq 1$.

Geometry. $S^{(d)} =$ set of all f with degree pattern d, defining an absolutely irreducible complete intersection of dimension $r - s$ and degree b.
Then for any $d \neq d^{(b)}$, we have

$$\dim S^{d^{(b)}} \geq \dim S^d + g(b).$$

Most varieties are degenerate

Combinatorics over $\mathbb{F}_q$.

$$p_r = \#\mathbb{P}^r(\mathbb{F}_q) = q^r + q^{r-1} + \cdots + 1.$$

The number of all f with degree pattern $d^{(b)}$ is $p_{D_b} \cdot p_r^{s-1}$.
$N^{(b)} =$ number of polynomial sequences over $\mathbb{F}_q$ defining an absolutely irreducible hypersurface of dimension $r - s$ and degree b within some $r - s + 1$-dimensional projective linear subspace, for any d with $b = \delta(d)$. Then

$$\left| \frac{N^{(b)}}{p_{D_b} p_r^{s-1}} - 1 \right| \leq \frac{14}{q^{r-s+1}} + \frac{b^{\log_2 \log_2 b}}{q^{g(b)}}.$$

One proof idea

Property: ideal-theoretic complete intersection. The polynomials in f form a regular sequence of $\overline{K}[X_0, \ldots, X_r]$ and the ideal generated by f in $\overline{K}[X_0, \ldots, X_r]$ is radical.

Geometry:

$$\text{degBound} = 2\sigma\delta.$$

General fact: each irreducible component of $V(f_1, \ldots, f_s)$ has codimension at most s. If $s = r + 1$, then "typically" $V(f_0, \ldots, f_r)$ is empty. If this is not the case, then the resultant of $(f_0, \ldots, f_r, J(f))$ vanishes, where

$$J(f_0, \ldots, f_r) = \det\left(\left(\frac{\partial f_i}{\partial x_j}\right)_{0 \le i,j \le r}\right)$$

is the determinant of the Jacobian.

One proof idea

Property: ideal-theoretic complete intersection. The polynomials in f form a regular sequence of $\overline{K}[X_0, \ldots, X_r]$ and the ideal generated by f in $\overline{K}[X_0, \ldots, X_r]$ is radical.
Geometry:

$$\text{degBound} = 2\sigma\delta.$$

General fact: each irreducible component of $V(f_1, \ldots, f_s)$ has codimension at most s. If $s = r + 1$, then "typically" $V(f_0, \ldots, f_r)$ is empty. If this is not the case, then the resultant of $(f_0, \ldots, f_r, J(f))$ vanishes, where

$$J(f_0, \ldots, f_r) = \det\big((\frac{\partial f_i}{\partial x_j})_{0 \le i,j \le r}\big)$$

is the determinant of the Jacobian.

One proof idea

Back to $f = (f_1, \ldots, f_s)$. Each f_i is a sum of terms

$$\text{coefficient} \cdot \text{ power product of } x_0, \ldots, x_r.$$

We consider $F = (F_1, \ldots, F_s)$, where each such coefficient is replaced by a variable. As genericity polynomial we take

$$P = \text{ multivariate resultant of } F_1, \ldots, F_s, J(F), x_{s+1}, \ldots, x_r.$$

The degrees of its arguments in the "coefficient variables" are $d_1, \ldots, d_s, \sigma, 0, \ldots, 0$. Therefore the degree of P in coeffs(F_i) is $d_1 \cdots d_{i-1} d_{i+1} \cdots d_s \sigma = \sigma\delta/d_i$ from $F_1, \ldots, F_s$, plus δ from $J(F)$. The total comes to $\sigma\delta/d_i + \delta \leq 2\sigma\delta$. See Cox, Little, O'Shea.

One proof idea

genericity. We take some system f with $P(f) \neq 0$. Then $V(f, J(f), x_{s+1}, \ldots, x_r)$ is empty. For $V' = V(f, J(f))$, the following hold:

$$\dim V' \leq r - s - 1 \Longrightarrow \dim V' = r - s - 1$$

$$\Longrightarrow \dim V(f) = r - s \Longrightarrow (f_1, \ldots, f_s) \text{ regular sequence.}$$

Also: the ideal generated by the $s \times s$ minors of $J(f)$ has codimension at least 1 in $V(f)$. Therefore: f generates a radical ideal in $\bar{K}[x_0, \ldots, x_r]$ and $V(f)$ is an ideal-theoretic complete intersection. See Eisenbud. $\square$

Open questions

- Affine varieties.
- More precise genericity: necessary and sufficient.
- Relation between this model and Chow model for varieties.
- Another “nice”: Gröbner basis in singly-exponential time.

Open questions

- Affine varieties.
- More precise genericity: necessary and sufficient.
- Relation between this model and Chow model for varieties.
- Another “nice”: Gröbner basis in singly-exponential time.

Open questions

- Affine varieties.
- More precise genericity: necessary and sufficient.
- Relation between this model and Chow model for varieties.
- Another “nice”: Gröbner basis in singly-exponential time.

Open questions

- Affine varieties.
- More precise genericity: necessary and sufficient.
- Relation between this model and Chow model for varieties.
- Another “nice”: Gröbner basis in singly-exponential time.

The end (of this talk)

Alles Gute zum Geburtstag, Peter!