Counting reducible and singular bivariate polynomials

Joachim von zur Gathen
Bonn

Four "accidents" can happen to a bivariate (or multivariate) polynomial over a field:

- a nontrivial factor,
- a square factor,
- a factor over an extension field,
- a singular root, where all partial derivatives also vanish.

We have a ground field F. The accidents may occur at two places:

- in F ("rational"),
- in an algebraic closure of F ("absolute").

Four “accidents” can happen to a bivariate (or multivariate) polynomial over a field:

- a nontrivial factor,
- a square factor,
- a factor over an extension field,
- a singular root, where all partial derivatives also vanish.

We have a ground field F. The accidents may occur at two places:

- in F (“rational”),
- in an algebraic closure of F (“absolute”).

Four "accidents" can happen to a bivariate (or multivariate) polynomial over a field:

- a nontrivial factor,
- a square factor,
- a factor over an extension field,
- a singular root, where all partial derivatives also vanish.

We have a ground field F. The accidents may occur at two places:

- in F ("rational"),
- in an algebraic closure of F ("absolute").

Four "accidents" can happen to a bivariate (or multivariate) polynomial over a field:

- a nontrivial factor,
- a square factor,
- a factor over an extension field,
- a singular root, where all partial derivatives also vanish.

We have a ground field F. The accidents may occur at two places:

- in F ("rational"),
- in an algebraic closure of F ("absolute").

Overview

Introduction

Reducible polynomials

Squareful polynomials

Relatively irreducible polynomials

Singular Polynomials

Overview

Introduction

Reducible polynomials

Squareful polynomials

Relatively irreducible polynomials

Singular Polynomials

Overview

Introduction

Reducible polynomials

Squareful polynomials

Relatively irreducible polynomials

Singular Polynomials

Overview

Introduction

Reducible polynomials

Squareful polynomials

Relatively irreducible polynomials

Singular Polynomials

Overview

Introduction

Reducible polynomials

Squareful polynomials

Relatively irreducible polynomials

Singular Polynomials

Taxonomy of views on polynomials over finite fields

1 variable   2 variables ≥ 2 variables

Taxonomy of views on polynomials over finite fields

~~1 variable~~ 2 variables ≥ 2 variables

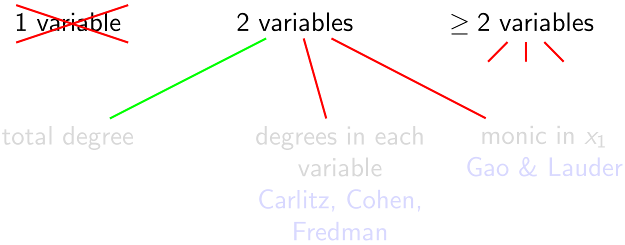
Taxonomy of views on polynomials over finite fields

~~1 variable~~ | 2 variables | $\geq$ 2 variables

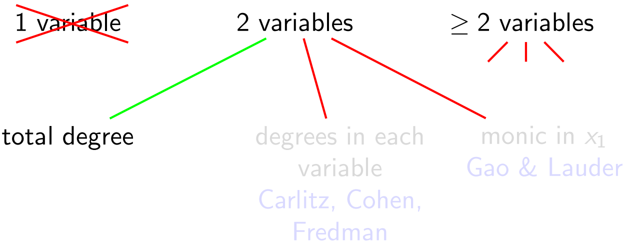
Taxonomy of views on polynomials over finite fields

~~1 variable~~ 2 variables ≥ 2 variables

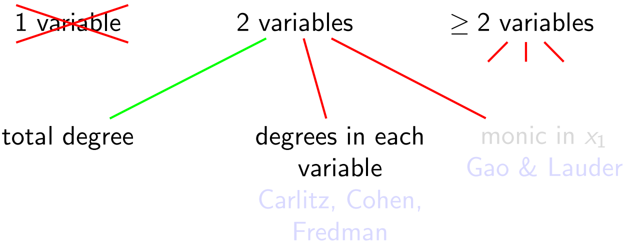
Taxonomy of views on polynomials over finite fields



Taxonomy of views on polynomials over finite fields



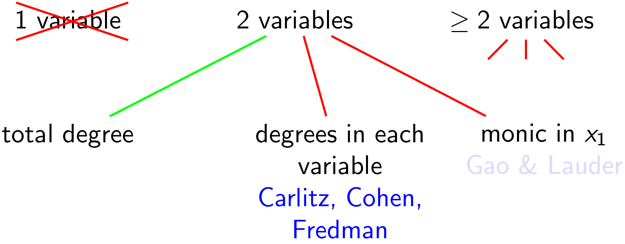
Taxonomy of views on polynomials over finite fields



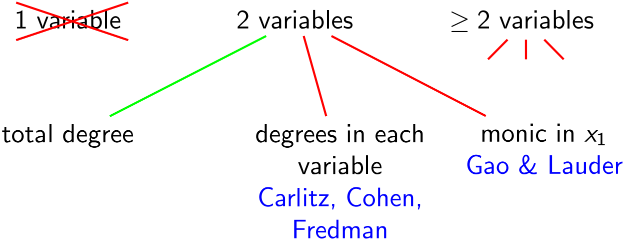
Taxonomy of views on polynomials over finite fields

- ~~1 variable~~
- 2 variables
  - total degree
  - degrees in each variable
    Carlitz, Cohen, Fredman
  - monic in x_1
    Gao & Lauder
- ≥ 2 variables

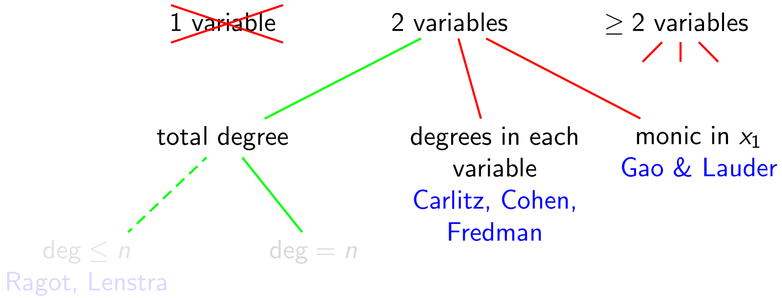
Taxonomy of views on polynomials over finite fields



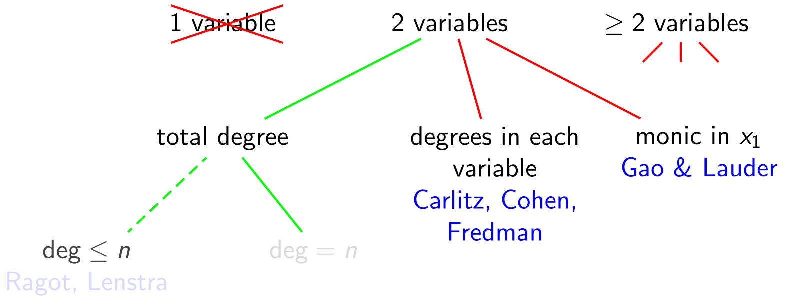
Taxonomy of views on polynomials over finite fields



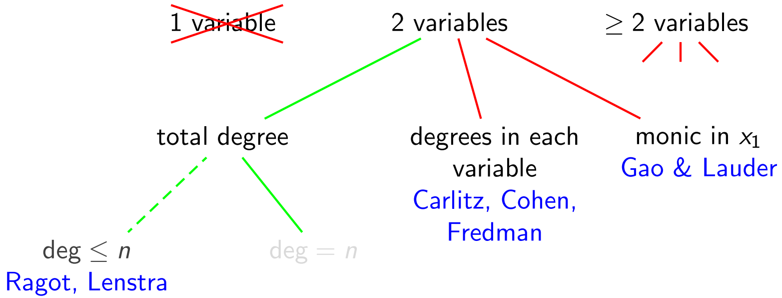
Taxonomy of views on polynomials over finite fields



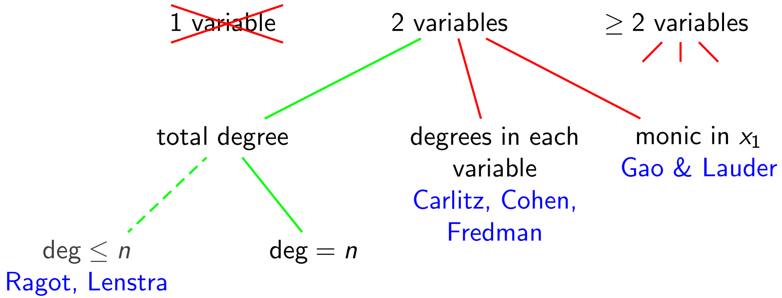
Taxonomy of views on polynomials over finite fields



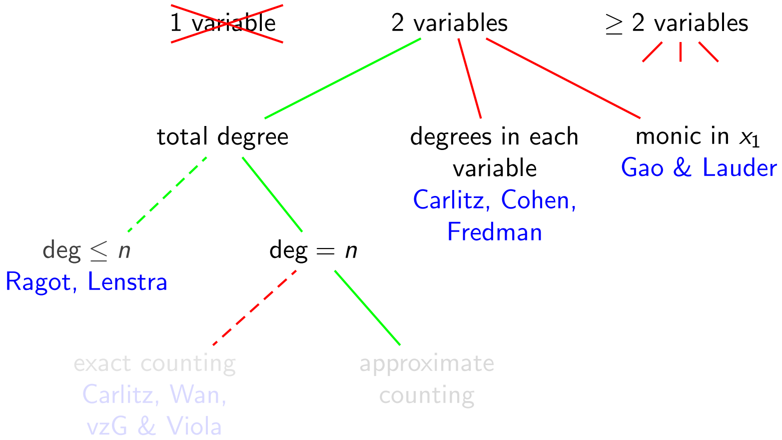
Taxonomy of views on polynomials over finite fields



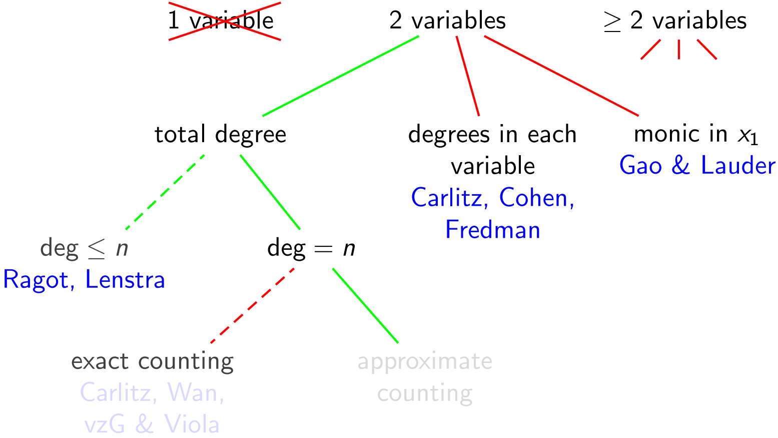
Taxonomy of views on polynomials over finite fields



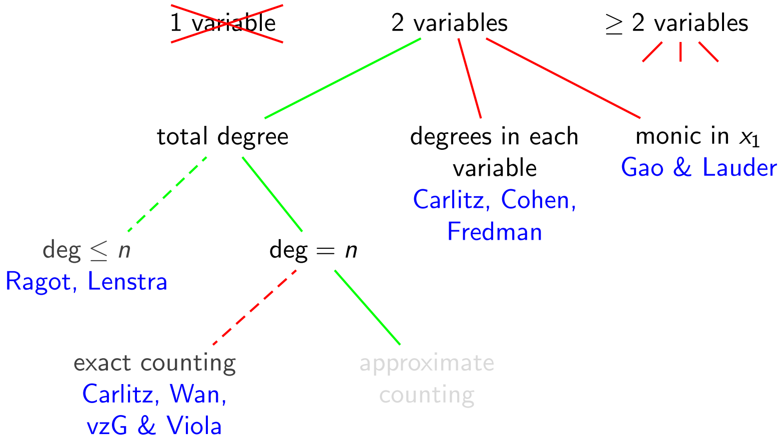
Taxonomy of views on polynomials over finite fields



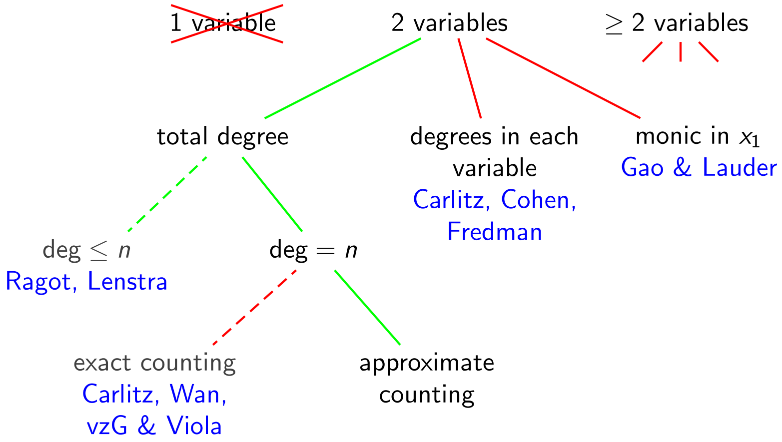
Taxonomy of views on polynomials over finite fields



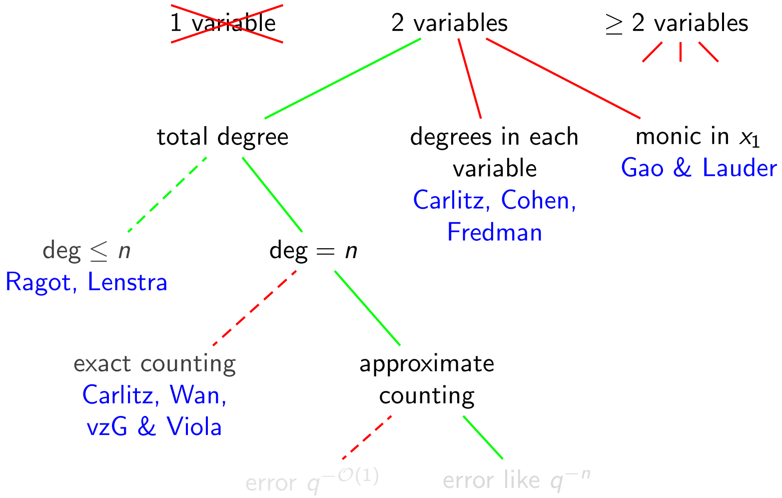
Taxonomy of views on polynomials over finite fields



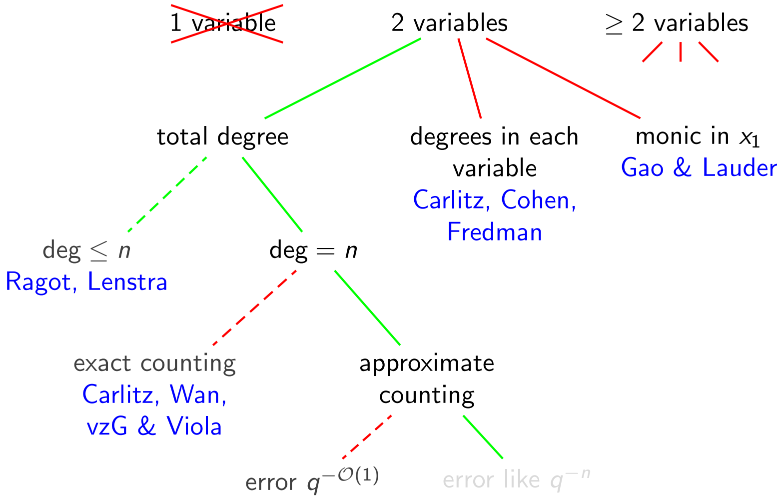
Taxonomy of views on polynomials over finite fields



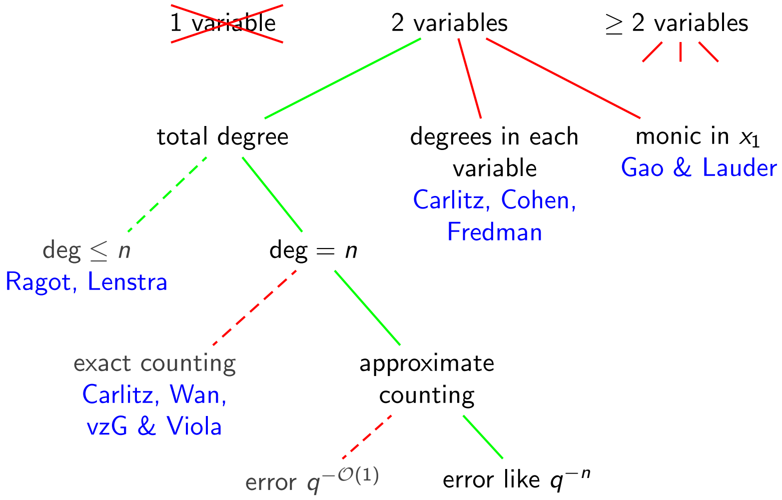
Taxonomy of views on polynomials over finite fields



Taxonomy of views on polynomials over finite fields



Taxonomy of views on polynomials over finite fields



Notation:

- $B_n(F) \subseteq F[x, y]$: bivariate polynomials with total degree $\leq n$.
- Certain natural sets $A_n(F) \subseteq B_n(F)$.

Two different languages: geometric and combinatorial.

- Geometry: $B_n(F)$ affine space over F, $A_n(F)$ union of images of polynomial maps, thus (reducible) subvariety. Geometric goal: determine the codimension of $A_n(F)$ = codimension of irreducible components of maximal dimension.
- Combinatorial goal: $F = \mathbb{F}_q$ for a prime power q, find functions $\alpha_n(q)$ and $\beta_n(q)$ so that

$$\left| \frac{\#A_n(\mathbb{F}_q)}{\#B_n(\mathbb{F}_q)} - \alpha_n(q) \right| \leq \alpha_n(q) \cdot \beta_n(q),$$

with $\beta_n(q)$ tending to zero as q and n grow.

Notation:

- $B_n(F) \subseteq F[x, y]$: bivariate polynomials with total degree $\leq n$.
- Certain natural sets $A_n(F) \subseteq B_n(F)$.

Two different languages: geometric and combinatorial.

- Geometry: $B_n(F)$ affine space over F, $A_n(F)$ union of images of polynomial maps, thus (reducible) subvariety. Geometric goal: determine the codimension of $A_n(F)$ = codimension of irreducible components of maximal dimension.
- Combinatorial goal: $F = \mathbb{F}_q$ for a prime power q, find functions $\alpha_n(q)$ and $\beta_n(q)$ so that

$$\left| \frac{\#A_n(\mathbb{F}_q)}{\#B_n(\mathbb{F}_q)} - \alpha_n(q) \right| \leq \alpha_n(q) \cdot \beta_n(q),$$

with $\beta_n(q)$ tending to zero as q and n grow.

Notation:

- $B_n(F) \subseteq F[x, y]$: bivariate polynomials with total degree $\leq n$.
- Certain natural sets $A_n(F) \subseteq B_n(F)$.

Two different languages: geometric and combinatorial.

- Geometry: $B_n(F)$ affine space over F, $A_n(F)$ union of images of polynomial maps, thus (reducible) subvariety. Geometric goal: determine the codimension of $A_n(F)$ = codimension of irreducible components of maximal dimension.
- Combinatorial goal: $F = \mathbb{F}_q$ for a prime power q, find functions $\alpha_n(q)$ and $\beta_n(q)$ so that

$$\left| \frac{\#A_n(\mathbb{F}_q)}{\#B_n(\mathbb{F}_q)} - \alpha_n(q) \right| \leq \alpha_n(q) \cdot \beta_n(q),$$

with $\beta_n(q)$ tending to zero as q and n grow.

Notation:

- $B_n(F) \subseteq F[x, y]$: bivariate polynomials with total degree $\leq n$.
- Certain natural sets $A_n(F) \subseteq B_n(F)$.

Two different languages: geometric and combinatorial.

- Geometry: $B_n(F)$ affine space over F, $A_n(F)$ union of images of polynomial maps, thus (reducible) subvariety. Geometric goal: determine the codimension of $A_n(F)$ = codimension of irreducible components of maximal dimension.
- Combinatorial goal: $F = \mathbb{F}_q$ for a prime power q, find functions $\alpha_n(q)$ and $\beta_n(q)$ so that

$$\left| \frac{\#A_n(\mathbb{F}_q)}{\#B_n(\mathbb{F}_q)} - \alpha_n(q) \right| \leq \alpha_n(q) \cdot \beta_n(q),$$

  with $\beta_n(q)$ tending to zero as q and n grow.

Thus a random element of $B_n(\mathbb{F}_q)$ is in $A_n(\mathbb{F}_q)$ with probability about $\alpha_n(q)$.

- Best results: $\beta_n(q)$ goes to zero like q^{-n}.
- Simpler results: $\alpha_n(q) = q^{-m}$ with $\beta_n(q) = O(q^{-1})$.
- Weil bounds: $\beta_n(q) = n^{O(1)} q^{-1/2}$.

Thus a random element of $B_n(\mathbb{F}_q)$ is in $A_n(\mathbb{F}_q)$ with probability about $\alpha_n(q)$.

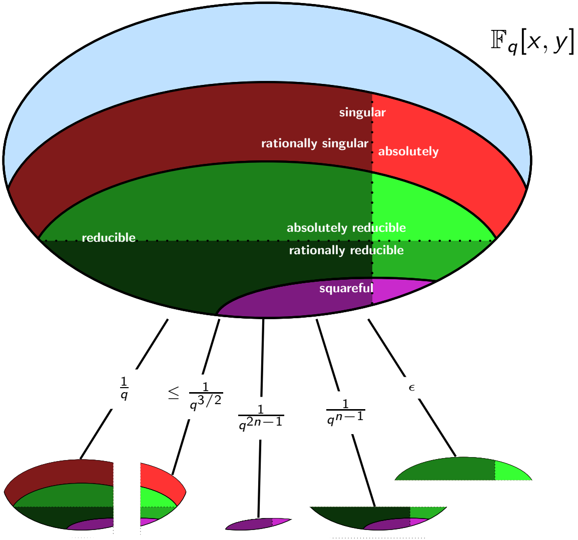
- Best results: $\beta_n(q)$ goes to zero like q^{-n}.
- Simpler results: $\alpha_n(q) = q^{-m}$ with $\beta_n(q) = O(q^{-1})$.
- Weil bounds: $\beta_n(q) = n^{O(1)} q^{-1/2}$.

Thus a random element of $B_n(\mathbb{F}_q)$ is in $A_n(\mathbb{F}_q)$ with probability about $\alpha_n(q)$.

- Best results: $\beta_n(q)$ goes to zero like q^{-n}.
- Simpler results: $\alpha_n(q) = q^{-m}$ with $\beta_n(q) = \mathrm{O}(q^{-1})$.
- Weil bounds: $\beta_n(q) = n^{\mathrm{O}(1)} q^{-1/2}$.

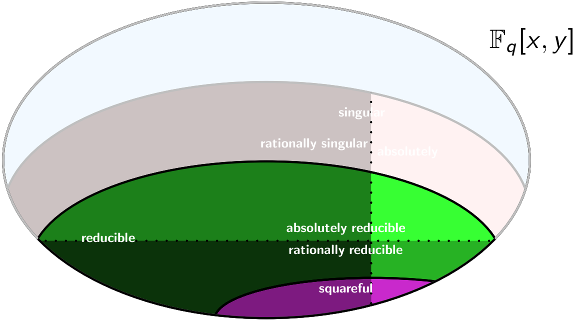
Thus a random element of $B_n(\mathbb{F}_q)$ is in $A_n(\mathbb{F}_q)$ with probability about $\alpha_n(q)$.

- Best results: $\beta_n(q)$ goes to zero like q^{-n}.
- Simpler results: $\alpha_n(q) = q^{-m}$ with $\beta_n(q) = O(q^{-1})$.
- Weil bounds: $\beta_n(q)= n^{O(1)}q^{-1/2}$.



$\mathbb{F}_q[x, y]$
singular
rationally singular
absolutely
reducible
absolutely reducible
rationally reducible
squareful
$\frac{1}{q}$
$\leq \frac{1}{q^{3/2}}$
$\frac{1}{q^{2n-1}}$
$\frac{1}{q^{n-1}}$
ϵ

Reducible polynomials



n	all	reducibles
1	$q^3 - q$	0
2	$q^6 - q^3$	$(q^5 + q^4 - q^2 - q)/2$
3	$q^{10} - q^6$	$(3q^8 + 2q^7 - 2q^6 - 3q^5 - q^4 + 2q^3 - q)/3$
4	$q^{15} - q^{10}$	$(4q^{12} + 6q^{11} - 2q^{10} - 5q^9 - 7q^8 + 6q^6 - 2q^4 - q^3$ $+q^2)/4$
5	$q^{21} - q^{15}$	$(5q^{17} + 5q^{16} + 5q^{15} - 10q^{13} - 15q^{12} - 6q^{11}$ $+11q^{10} + 10q^9 - 5q^7 - q^6 + q^5 + q^3 - q)/5$
6	$q^{28} - q^{21}$	$(6q^{23} + 6q^{22} + 6q^{20} + 3q^{19} - 3q^{18} - 21q^{17}$ $-23q^{16} - 10q^{15} + 18q^{14} + 32q^{13} + 10q^{12} - 15q^{11}$ $-12q^{10} + 3q^8 - q^7 + 2q^5 - 3q^3 + q^2 + q)/6$

The numbers of reducible polynomials of degrees up to 6

Theorem

Consider polynomials of degree $n \geq 2$.

1. $\{reducibles\}$ *is a subvariety of codimension* $n-1$ *in* $\{all\}$.
2. *Let* $\rho_n(q) = (q+1)q^{-n}$. *Then for* $n \geq 3$

$$\left|\frac{\#\{reducibles\}}{\#\{all\}} - \rho_n(q)\right| \leq \rho_n(q) \cdot 2q^{-n+3},$$

$$\text{at degree 2:} \quad \frac{\#\{reducibles\}}{\#\{all\}} = \frac{\rho_2(q)}{2}.$$

3. *For* $n \geq 6$, *we have*

$$\left|\frac{\#\{reducibles\}}{\#\{all\}} - q^{-n+1}\right| \leq 2q^{-n}.$$

For $1 \leq k < n$: multiplication map

$$\mu_{k,n}\colon \begin{array}{rcl} \{\text{degree } k\} \times \{\text{degree } n-k\} & \longrightarrow & \{\text{degree } n\}, \\ (g,h) & \longmapsto & g \cdot h, \end{array}$$

$$\{\text{reducibles}\} = \bigcup_{1 \leq k \leq n/2} \operatorname{im} \mu_{k,n}.$$

Multiplication by units gives fiber dimension ≥ 1
$\Longrightarrow$ Zariski closure of im $\mu_{k,n}$ is a proper irreducible subvariety
$\Longrightarrow$ complement (= irreducible polynomials) is dense.

g, h irreducible
$\Longrightarrow$ fiber dimension $= 1$.
$\Longrightarrow$ generic fiber dimension is 1,
$b_n = \dim\{\text{polynomials of degree } n\}$.

$$\dim \operatorname{im} \mu_{k,n} = b_k + b_{n-k} - 1 = b_n - k(n-k).$$

Maximum at $k = 1$: $b_n - n + 1$. Hence codim $= n - 1$.

For $1 \leq k < n$: multiplication map

$$\mu_{k,n}\colon \begin{array}{ccc} \{\text{degree } k\} \times \{\text{degree } n-k\} & \longrightarrow & \{\text{degree } n\}, \\ (g,h) & \longmapsto & g \cdot h, \end{array}$$

$$\{\text{reducibles}\} = \bigcup_{1 \leq k \leq n/2} \operatorname{im} \mu_{k,n}.$$

Multiplication by units gives fiber dimension ≥ 1
$\Longrightarrow$ Zariski closure of im $\mu_{k,n}$ is a proper irreducible subvariety
$\Longrightarrow$ complement (= irreducible polynomials) is dense.

g, h irreducible
$\Longrightarrow$ fiber dimension $= 1$.
$\Longrightarrow$ generic fiber dimension is 1,
$b_n = \dim\{\text{polynomials of degree } n\}$.

$$\dim \operatorname{im} \mu_{k,n} = b_k + b_{n-k} - 1 = b_n - k(n-k).$$

Maximum at $k = 1$: $b_n - n + 1$. Hence codim $= n - 1$.

For $1 \leq k < n$: multiplication map

$$\mu_{k,n}\colon \begin{array}{ccc} \{\text{degree } k\} \times \{\text{degree } n-k\} & \longrightarrow & \{\text{degree } n\}, \\ (g,h) & \longmapsto & g \cdot h, \end{array}$$

$$\{\text{reducibles}\} = \bigcup_{1 \leq k \leq n/2} \operatorname{im} \mu_{k,n}.$$

Multiplication by units gives fiber dimension ≥ 1
$\Longrightarrow$ Zariski closure of im $\mu_{k,n}$ is a proper irreducible subvariety
$\Longrightarrow$ complement ($=$ irreducible polynomials) is dense.

g, h irreducible
$\Longrightarrow$ fiber dimension $= 1$.
$\Longrightarrow$ generic fiber dimension is 1,
$b_n = \dim\{\text{polynomials of degree } n\}$.

$$\dim \operatorname{im} \mu_{k,n} = b_k + b_{n-k} - 1 = b_n - k(n-k).$$

Maximum at $k = 1$: $b_n - n + 1$. Hence codim $= n - 1$.

For $1 \leq k < n$: multiplication map

$$\mu_{k,n}\colon \quad \begin{array}{rcl} \{\text{degree } k\} \times \{\text{degree } n-k\} & \longrightarrow & \{\text{degree } n\}, \\ (g, h) & \longmapsto & g \cdot h, \end{array}$$

$$\{\text{reducibles}\} = \bigcup_{1 \leq k \leq n/2} \operatorname{im} \mu_{k,n}.$$

Multiplication by units gives fiber dimension ≥ 1
$\Longrightarrow$ Zariski closure of im $\mu_{k,n}$ is a proper irreducible subvariety
$\Longrightarrow$ complement ($=$ irreducible polynomials) is dense.

g, h irreducible
$\Longrightarrow$ fiber dimension $= 1$.
$\Longrightarrow$ generic fiber dimension is 1,
$b_n = \dim\{\text{polynomials of degree } n\}$.

$$\dim \operatorname{im} \mu_{k,n} = b_k + b_{n-k} - 1 = b_n - k(n-k).$$

Maximum at $k = 1$: $b_n - n + 1$. Hence codim $= n - 1$.

For $1 \leq k < n$: multiplication map

$$\mu_{k,n}\colon \begin{array}{rcl} \{\text{degree } k\} \times \{\text{degree } \; n-k\} & \longrightarrow & \{\text{degree } n\}, \\ (g,h) & \longmapsto & g \cdot h, \end{array}$$

$$\{\text{reducibles}\} = \bigcup_{1 \leq k \leq n/2} \operatorname{im} \mu_{k,n}.$$

Multiplication by units gives fiber dimension ≥ 1
$\Longrightarrow$ Zariski closure of im $\mu_{k,n}$ is a proper irreducible subvariety
$\Longrightarrow$ complement ($=$ irreducible polynomials) is dense.

g, h irreducible
$\Longrightarrow$ fiber dimension $= 1$.
$\Longrightarrow$ generic fiber dimension is 1,
$b_n = \dim\{\text{polynomials of degree } n\}$.

$$\dim \operatorname{im} \mu_{k,n} = b_k + b_{n-k} - 1 = b_n - k(n-k).$$

Maximum at $k = 1$: $b_n - n + 1$. Hence codim $= n - 1$.

For $1 \leq k < n$: multiplication map

$$\mu_{k,n}: \begin{array}{rcl} \{\text{degree } k\} \times \{\text{degree } \ n-k\} & \longrightarrow & \{\text{degree } n\}, \\ (g,h) & \longmapsto & g \cdot h, \end{array}$$

$$\{\text{reducibles}\} = \bigcup_{1 \leq k \leq n/2} \operatorname{im} \mu_{k,n}.$$

Multiplication by units gives fiber dimension ≥ 1
$\Longrightarrow$ Zariski closure of im $\mu_{k,n}$ is a proper irreducible subvariety
$\Longrightarrow$ complement ($=$ irreducible polynomials) is dense.

g, h irreducible
$\Longrightarrow$ fiber dimension $= 1$.
$\Longrightarrow$ generic fiber dimension is 1,
$b_n = \dim\{\text{polynomials of degree } n\}$.

$$\dim \operatorname{im} \mu_{k,n} = b_k + b_{n-k} - 1 = b_n - k(n-k).$$

Maximum at $k = 1$: $b_n - n + 1$. Hence codim $= n - 1$.

Let $n \geq 3$. Each fiber of $\mu_{k,n}$ has at least $q-1$ elements.

$$\begin{aligned}
\#\,\mathrm{im}\,\mu_{k,n} &\leq \frac{1}{q-1} \cdot \#\{\text{degree } k\} \cdot \#\{\text{degree } n-k\} \\
&< \frac{q^{b_k}(1-q^{-k-1}) \cdot q^{b_{n-k}}}{q-1} \\
&= \frac{\rho_n(q) \cdot \{\text{all}\} \cdot q^{n-1-k(n-k)}(1-q^{-k-1})}{(1-q^{-2})(1-q^{-n-1})}.
\end{aligned}$$

- Some calculation gives the upper bound for $q \geq 3$.
- More calculation for $q = 2$ and $n \geq 8$.
- Even more for $q = 2$ and $n \neq 6$.
- One more for $q = 2$ and $n = 6$.

Let $n \geq 3$. Each fiber of $\mu_{k,n}$ has at least $q-1$ elements.

$$\begin{aligned}
\#\operatorname{im}\mu_{k,n} &\leq \frac{1}{q-1}\cdot\#\{\text{degree } k\}\cdot\#\{\text{degree } n-k\}\\
&< \frac{q^{b_k}(1-q^{-k-1})\cdot q^{b_{n-k}}}{q-1}\\
&= \frac{\rho_n(q)\cdot\{\text{all}\}\cdot q^{n-1-k(n-k)}(1-q^{-k-1})}{(1-q^{-2})(1-q^{-n-1})}.
\end{aligned}$$

- Some calculation gives the upper bound for $q \geq 3$.
- More calculation for $q = 2$ and $n \geq 8$.
- Even more for $q = 2$ and $n \neq 6$.
- One more for $q = 2$ and $n = 6$.

Let $n \geq 3$. Each fiber of $\mu_{k,n}$ has at least $q-1$ elements.

$$
\begin{aligned}
\# \operatorname{im} \mu_{k,n} &\leq \frac{1}{q-1} \cdot \#\{\text{degree } k\} \cdot \#\{\text{degree } n-k\} \\
&< \frac{q^{b_k}(1-q^{-k-1}) \cdot q^{b_{n-k}}}{q-1} \\
&= \frac{\rho_n(q) \cdot \{\text{all}\} \cdot q^{n-1-k(n-k)}(1-q^{-k-1})}{(1-q^{-2})(1-q^{-n-1})}.
\end{aligned}
$$

- Some calculation gives the upper bound for $q \geq 3$.
- More calculation for $q = 2$ and $n \geq 8$.
- Even more for $q = 2$ and $n \neq 6$.
- One more for $q = 2$ and $n = 6$.

Let $n \geq 3$. Each fiber of $\mu_{k,n}$ has at least $q-1$ elements.

$$\begin{aligned}\#\operatorname{im}\mu_{k,n} &\leq \frac{1}{q-1}\cdot\#\{\text{degree } k\}\cdot\#\{\text{degree } n-k\}\\ &< \frac{q^{b_k}(1-q^{-k-1})\cdot q^{b_{n-k}}}{q-1}\\ &= \frac{\rho_n(q)\cdot\{\text{all}\}\cdot q^{n-1-k(n-k)}(1-q^{-k-1})}{(1-q^{-2})(1-q^{-n-1})}.\end{aligned}$$

- Some calculation gives the upper bound for $q \geq 3$.
- More calculation for $q = 2$ and $n \geq 8$.
- Even more for $q = 2$ and $n \neq 6$.
- One more for $q = 2$ and $n = 6$.

Let $n \geq 3$. Each fiber of $\mu_{k,n}$ has at least $q-1$ elements.

$$\begin{aligned}
\#\operatorname{im}\mu_{k,n} &\leq \frac{1}{q-1}\cdot\#\{\text{degree } k\}\cdot\#\{\text{degree } n-k\} \\
&< \frac{q^{b_k}(1-q^{-k-1})\cdot q^{b_{n-k}}}{q-1} \\
&= \frac{\rho_n(q)\cdot\{\text{all}\}\cdot q^{n-1-k(n-k)}(1-q^{-k-1})}{(1-q^{-2})(1-q^{-n-1})}.
\end{aligned}$$

- Some calculation gives the upper bound for $q \geq 3$.
- More calculation for $q = 2$ and $n \geq 8$.
- Even more for $q = 2$ and $n \neq 6$.
- One more for $q = 2$ and $n = 6$.

Corollary

We have for $n \geq 2$

$$\#\{\textit{irreducibles}\} \geq q^{b_n} \cdot (1 - (q+2)q^{-n}).$$

Lower bound: g, h irreducible, $k < n/2$,
$\Longrightarrow$ fiber size is $q - 1$,
$\Longrightarrow$ lower bound on reducibles.

Corollary

We have for $n \geq 2$

$$\#\{\textit{irreducibles}\} \geq q^{b_n} \cdot (1 - (q+2)q^{-n}).$$

Lower bound: g, h irreducible, $k < n/2$,

$\Longrightarrow$ fiber size is $q - 1$,

$\Longrightarrow$ lower bound on reducibles.

Corollary

We have for $n \geq 2$

$$\#\{\textit{irreducibles}\} \geq q^{b_n} \cdot (1 - (q+2)q^{-n}).$$

Lower bound: g, h irreducible, $k < n/2$,
$\implies$ fiber size is $q - 1$,
$\implies$ lower bound on reducibles.

Corollary

We have for $n \geq 2$

$$\#\{irreducibles\} \geq q^{b_n} \cdot (1 - (q+2)q^{-n}).$$

Lower bound: g, h irreducible, $k < n/2$,
$\Longrightarrow$ fiber size is $q - 1$,
$\Longrightarrow$ lower bound on reducibles.

Previous work:

- Carlitz 1963:

$$\text{fraction of irreducibles} - 1 = O((q-1)q^{-n-1}).$$

"As the referee pointed out, [it] can be proved by a crude counting argument" that

$$1 - \frac{q^{-n+4}}{(q-1)^3} \leq \text{fraction of irreducibles} \leq 1.$$

- Carlitz 1965, Cohen 1968, 1970: fraction of irreducibles is $1 - q^{-m} + O(nq^{-(m+n+1)})$ among polynomials of degrees $m \leq n$ in x, y, respectively.
- Corresponding results for multivariate polynomials.

Previous work:

- Carlitz 1963:

$$\text{fraction of irreducibles} - 1 = O((q-1)q^{-n-1}).$$

"As the referee pointed out, [it] can be proved by a crude counting argument" that

$$1 - \frac{q^{-n+4}}{(q-1)^3} \leq \text{fraction of irreducibles} \leq 1.$$

- Carlitz 1965, Cohen 1968, 1970: fraction of irreducibles is $1 - q^{-m} + O(nq^{-(m+n+1)})$ among polynomials of degrees $m \leq n$ in x, y, respectively.
- Corresponding results for multivariate polynomials.

Previous work:

- Carlitz 1963:

$$\text{fraction of irreducibles} - 1 = O((q-1)q^{-n-1}).$$

"As the referee pointed out, [it] can be proved by a crude counting argument" that

$$1 - \frac{q^{-n+4}}{(q-1)^3} \leq \text{fraction of irreducibles} \leq 1.$$

- Carlitz 1965, Cohen 1968, 1970: fraction of irreducibles is $1 - q^{-m} + O(nq^{-(m+n+1)})$ among polynomials of degrees $m \leq n$ in x, y, respectively.
- Corresponding results for multivariate polynomials.

Previous work:

- Carlitz 1963:

$$\text{fraction of irreducibles} - 1 = O((q-1)q^{-n-1}).$$

  "As the referee pointed out, [it] can be proved by a crude counting argument" that

$$1 - \frac{q^{-n+4}}{(q-1)^3} \leq \text{fraction of irreducibles} \leq 1.$$

- Carlitz 1965, Cohen 1968, 1970: fraction of irreducibles is $1 - q^{-m} + O(nq^{-(m+n+1)})$ among polynomials of degrees $m \leq n$ in x, y, respectively.
- Corresponding results for multivariate polynomials.

Previous work:

- Carlitz 1963:

$$\text{fraction of irreducibles} - 1 = O((q-1)q^{-n-1}).$$

"As the referee pointed out, [it] can be proved by a crude counting argument" that

$$1 - \frac{q^{-n+4}}{(q-1)^3} \leq \text{fraction of irreducibles} \leq 1.$$

- Carlitz 1965, Cohen 1968, 1970: fraction of irreducibles is $1 - q^{-m} + O(nq^{-(m+n+1)})$ among polynomials of degrees $m \leq n$ in x, y, respectively.
- Corresponding results for multivariate polynomials.

- Cohen 1968 comes to “a fairly long, complicated argument, which we shall omit”, and warns the interested reader that “the derivation of the above results is increasingly complicated. Each further computation, using this method, would require considerable calculation.”
- Ragot 1997 shows:

$$q^{-n+1}(1-\frac{5}{q}) \leq \text{fraction of reducibles} \leq q^{-n+1}(1+\frac{6}{q}).$$

- Gao & Lauder 2002, for polynomials monic in x.
- Bodin 2007: relative error bound of $\frac{1}{n}$ for large enough n.

- Cohen 1968 comes to "a fairly long, complicated argument, which we shall omit", and warns the interested reader that "the derivation of the above results is increasingly complicated. Each further computation, using this method, would require considerable calculation."
- Ragot 1997 shows:

$$q^{-n+1}(1-\frac{5}{q}) \leq \text{fraction of reducibles} \leq q^{-n+1}(1+\frac{6}{q}).$$

- Gao & Lauder 2002, for polynomials monic in x.
- Bodin 2007: relative error bound of $\frac{1}{n}$ for large enough n.

- Cohen 1968 comes to "a fairly long, complicated argument, which we shall omit", and warns the interested reader that "the derivation of the above results is increasingly complicated. Each further computation, using this method, would require considerable calculation."
- Ragot 1997 shows:

$$q^{-n+1}(1 - \frac{5}{q}) \leq \text{fraction of reducibles} \leq q^{-n+1}(1 + \frac{6}{q}).$$

- Gao & Lauder 2002, for polynomials monic in x.
- Bodin 2007: relative error bound of $\frac{1}{n}$ for large enough n.

“Self-reducibility”:

Upper bound on reducibles

$\Longrightarrow$ lower bound on irreducibles

$\Longrightarrow$ lower bound on reducibles, by induction

“Self-reducibility”:
Upper bound on reducibles

$\Longrightarrow$ lower bound on irreducibles
$\Longrightarrow$ lower bound on reducibles, by induction

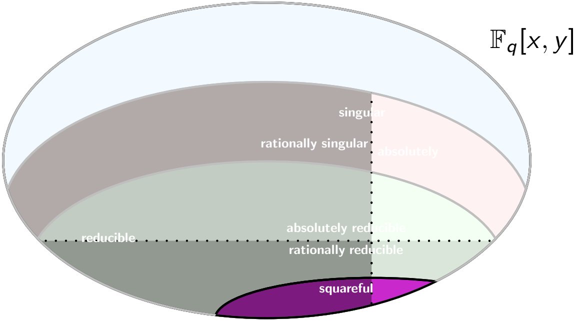
“Self-reducibility”:
Upper bound on reducibles

$\Longrightarrow$ lower bound on irreducibles
$\Longrightarrow$ lower bound on reducibles, by induction

“Self-reducibility”:
Upper bound on reducibles

$\Longrightarrow$ lower bound on irreducibles
$\Longrightarrow$ lower bound on reducibles, by induction

Squareful polynomials



n	squareful polynomials
1	0
2	$q^3 - q$
3	$q^5 + q^4 - q^3 - q^2$
4	$q^8 + q^7 + q^6 - 2q^5 - 2q^4 + q^2$
5	$q^{12} + q^{11} - q^7 - 2q^6 - q^5 + q^4 + q^3$
6	$q^{17} + q^{16} - q^{12} + q^{10} - q^9 - 4q^8 - q^7 + 2q^6 + 3q^5 - q^3$

The number of squareful polynomials of degrees up to 6.

Theorem

Let $n \geq 1$*.*

1. *For* $n \geq 2$, $\{squareful\}$ *is a subvariety of codimension* $2n-1$*.*
2. *Let*

$$\eta_n(q) = \frac{(q+1)q^{-2n}(1-q^{-n+1})}{1-q^{-n-1}}.$$

Then

$$|\text{fraction of squareful} - \eta_n(q)| \leq \eta_n(q) \cdot 3q^{-2n+6},$$

and for $n \leq 3$

$$\text{fraction of squareful} = \eta_n(q).$$

Cohen 1970: fraction of r-power-free polynomials is $1 - q^{-rm} + O(q^{-nm})$ among polynomials of degrees at most $m \leq n$ in x, y, respectively.

Theorem

Let $n \geq 1$.

1. *For $n \geq 2$, $\{squareful\}$ is a subvariety of codimension $2n-1$.*
2. *Let*

$$\eta_n(q) = \frac{(q+1)q^{-2n}(1-q^{-n+1})}{1-q^{-n-1}}.$$

Then

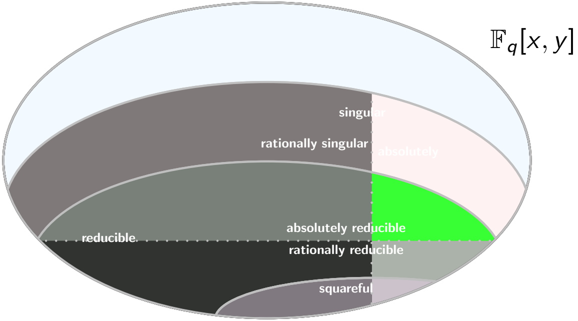
$$|\textit{fraction of squareful} - \eta_n(q)| \leq \eta_n(q) \cdot 3q^{-2n+6},$$

and for $n \leq 3$

$$\textit{fraction of squareful} = \eta_n(q).$$

Cohen 1970: fraction of r-power-free polynomials is $1 - q^{-rm} + O(q^{-nm})$ among polynomials of degrees at most $m \leq n$ in x, y, respectively.

Relatively irreducible polynomials



An irreducible bivariate polynomial is *relatively irreducible* if it is not absolutely irreducible. Then it is the product of all conjugates of an irreducible polynomial over some extension field.

Application: algorithms for curves: point finding, estimating the size. Huang & Ierardi, 1993; von zur Gathen, Shparlinski & Karpinski, 1993, 1996; von zur Gathen & Shparlinski 1995, 1998; Matera & Cafure 2006.

An irreducible bivariate polynomial is *relatively irreducible* if it is not absolutely irreducible. Then it is the product of all conjugates of an irreducible polynomial over some extension field.
Application: algorithms for curves: point finding, estimating the size.
Huang & Ierardi, 1993; von zur Gathen, Shparlinski & Karpinski, 1993, 1996; von zur Gathen & Shparlinski 1995, 1998; Matera & Cafure 2006.

n	relatively irreducibles
2	$(q^5 - q^4 - q^2 + q)/2$
3	$(q^7 - q^6 + q^4 - 2q^3 + q)/3$
4	$(2q^{11} - 2q^{10} + q^9 - q^8 - 2q^6 + 2q^4 + q^3 - q^2)/4$
5	$(q^{11} - q^{10} + q^6 - q^5 - q^3 + q)/5$
6	$(3q^{19} - 3q^{18} + 3q^{17} - q^{16} - 2q^{15} - 2q^{13} + 2q^{12}$
	$-3q^{11} + 3q^8 + q^7 - 2q^5 + 3q^3 - q^2 - q)/6$

The numbers of relatively irreducible polynomials of degrees up to 6.

Theorem

Let $n \geq 2$, let $l \geq 2$ be the smallest prime divisor of n,

$$\varepsilon_n(q) = \frac{q^{-n^2(l-1)/2l}(1-q^{-1})}{l(1-q^{-l})(1-q^{-n-1})},$$

$$\delta_n(q) = \begin{cases} 2q^{-2n+2} & \text{if } n \text{ is prime,} \\ 2q^{-n+l+1} & \text{otherwise.} \end{cases}$$

Then

1. $\left| \text{fraction of rel irred} - \varepsilon_n(q) \right| \leq \varepsilon_n(q) \cdot \delta_n(q)$.
2. $\varepsilon_n(q) \leq q^{-n^2/4}/2$.
3. *If n is prime, then* $\varepsilon_n(q) \leq q^{-n(n-1)/2}/n$ *and*

$$\#\{\text{rel irred}\} = (q-1)(q^{2n} + q^n - q^2 - q)/n.$$

Theorem

Let $n \geq 2$, let $l \geq 2$ be the smallest prime divisor of n,

$$\varepsilon_n(q) = \frac{q^{-n^2(l-1)/2l}(1-q^{-1})}{l(1-q^{-l})(1-q^{-n-1})},$$

$$\delta_n(q) = \begin{cases} 2q^{-2n+2} & \text{if } n \text{ is prime,} \\ 2q^{-n+l+1} & \text{otherwise.} \end{cases}$$

Then

1. $\left| \textit{fraction of rel irred} - \varepsilon_n(q) \right| \leq \varepsilon_n(q) \cdot \delta_n(q)$.
2. $\varepsilon_n(q) \leq q^{-n^2/4}/2$.
3. *If n is prime, then $\varepsilon_n(q) \leq q^{-n(n-1)/2}/n$ and*

$$\#\{\textit{rel irred}\} = (q-1)(q^{2n} + q^n - q^2 - q)/n.$$

Theorem

Let $n \geq 2$, let $l \geq 2$ be the smallest prime divisor of n,

$$\varepsilon_n(q) = \frac{q^{-n^2(l-1)/2l}(1-q^{-1})}{l(1-q^{-l})(1-q^{-n-1})},$$

$$\delta_n(q) = \begin{cases} 2q^{-2n+2} & \textit{if } n \textit{ is prime,} \\ 2q^{-n+l+1} & \textit{otherwise.} \end{cases}$$

Then

1. $\left| \textit{fraction of rel irred} - \varepsilon_n(q) \right| \leq \varepsilon_n(q) \cdot \delta_n(q).$
2. $\varepsilon_n(q) \leq q^{-n^2/4}/2.$
3. *If n is prime, then $\varepsilon_n(q) \leq q^{-n(n-1)/2}/n$ and*

$$\#\{\textit{rel irred}\} = (q-1)(q^{2n} + q^n - q^2 - q)/n.$$

Theorem

Let $n \geq 2$, let $l \geq 2$ be the smallest prime divisor of n,

$$\varepsilon_n(q) = \frac{q^{-n^2(l-1)/2l}(1-q^{-1})}{l(1-q^{-l})(1-q^{-n-1})},$$

$$\delta_n(q) = \begin{cases} 2q^{-2n+2} & \textit{if } n \textit{ is prime,} \\ 2q^{-n+l+1} & \textit{otherwise.} \end{cases}$$

Then

1. $\left| \textit{fraction of rel irred} - \varepsilon_n(q) \right| \leq \varepsilon_n(q) \cdot \delta_n(q).$
2. $\varepsilon_n(q) \leq q^{-n^2/4}/2.$
3. *If n is prime, then $\varepsilon_n(q) \leq q^{-n(n-1)/2}/n$ and*

$$\#\{\textit{rel irred}\} = (q-1)(q^{2n} + q^n - q^2 - q)/n.$$

Singular polynomials

$f \in F[x,y], P = (u,v) \in F^2:$

$$f(P) = 0 \iff P \text{ is on the curve } V(f) \subseteq F^2$$
$$\iff f \in m_p = (x-u, y-v) \subseteq F[x,y]$$

maximal ideal.

$$f(P) = \frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = 0 \iff P \text{ is singular on } V(f)$$
$$\iff f \text{ is singular at } P$$
$$\iff f \in s_p = m_p^2.$$

Quotient ring

$$F[x, y]/s_P = F + (x - u)F + (y - v)F$$

is a 3-dimensional vector space over F.

$$\operatorname{codim}_{F[x,y]} s_P = 3.$$

Affine Hilbert function of s_P:

$$\text{codim } s_P = 3$$

at degree n for n large enough.

Ragot 1997, 1999:

$$\text{fraction of singular} = 1 - (1 - q^{-3})^{q^2} \qquad (1)$$

for $n > 4q - 2$.
Similar result for multivariate polynomials.

Theorem
(Lenstra 2006): (1) $\iff n \geq 3q - 2$.

Affine Hilbert function of s_P:

$$\text{codim } s_P = 3$$

at degree n for n large enough.

Ragot 1997, 1999:

$$\text{fraction of singular} = 1 - (1 - q^{-3})^{q^2} \quad (1)$$

for $n > 4q - 2$.
Similar result for multivariate polynomials.

Theorem
(Lenstra 2006): (1) $\iff n \geq 3q - 2$.

Affine Hilbert function of s_P:

$$\operatorname{codim}\, s_P = 3$$

at degree n for n large enough.

Ragot 1997, 1999:

$$\text{fraction of singular} = 1 - (1 - q^{-3})^{q^2} \qquad (1)$$

for $n > 4q - 2$.
Similar result for multivariate polynomials.

Theorem
(Lenstra 2006): (1) $\Longleftrightarrow n \geq 3q - 2$.

Affine Hilbert function of s_P:

$$\operatorname{codim} s_P = 3$$

at degree n for n large enough.

Ragot 1997, 1999:

$$\text{fraction of singular} = 1 - (1 - q^{-3})^{q^2} \tag{1}$$

for $n > 4q - 2$.
Similar result for multivariate polynomials.

Theorem

(Lenstra 2006): (1) $\iff n \geq 3q - 2$.

$R = \mathbb{F}_q[x, y]$:

$P \in \mathbb{F}_q^2$, random polynomial:

$$\text{prob(singular at } P) = q^{-3}$$
$$\text{prob(nonsingular at } P) = 1 - q^{-3}$$

$R = \mathbb{F}_q[x, y]$:

$P \in \mathbb{F}_q^2$, random polynomial: 

$$\text{prob(singular at } P) = q^{-3}$$
$$\text{prob(nonsingular at } P) = 1 - q^{-3}$$

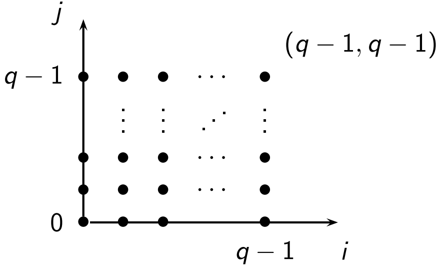
$\prod_{P \in \mathbb{F}_q^2} R/s_P$, random polynomial:  $\times \quad \cdots \quad \times$ 

$$\text{prob(nonsingular at all } P) = (1 - q^{-3})^{q^2}$$

Independence: Chinese Remainder Theorem

$$
\begin{aligned}
\prod_{P \in \mathbb{F}_q^2} R/m_P &= \prod_{u,v \in \mathbb{F}_q} R/(x-u, y-v) \\
&= R/\prod_{u,v \in \mathbb{F}_q} (x-u, y-v) \\
&= R/(x^q - x, y^q - y)
\end{aligned}
$$

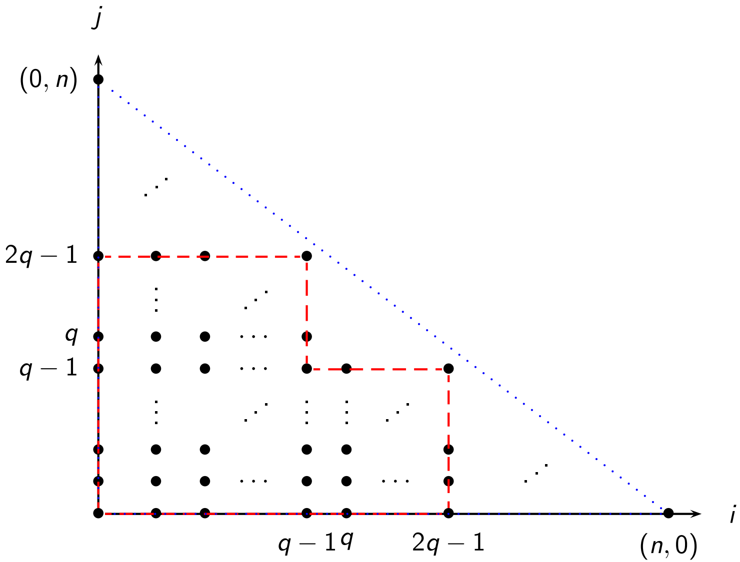
Monomial $x^i y^j \leftrightarrow (i,j)$:



Representatives for $R/(x^q - x, y^q - y)$

Representation of

$$\begin{aligned}\prod_{P\in\mathbb{F}_q^2} R/s_P &= \prod_{P\in\mathbb{F}_q^2} R/m_P^2 \\ &= R/(\prod_{P\in\mathbb{F}_q^2} m_P^2) = R/(x^q - x, y^q - y)^2 \\ &= R/((x^q - x)^2, (x^q - x)(y^q - y), (y^q - y)^2).\end{aligned}$$



j
(0, n)
2q − 1
q
q − 1
i
q − 1
q
2q − 1
(n, 0)

$$\begin{aligned}
\text{(1) holds} \quad &\Leftrightarrow \quad \text{degree } n \to R/(x^q - x, y^q - y)^2 \text{ surjective} \\
&\Leftrightarrow \quad n \geq 3q - 2. \quad \square
\end{aligned}$$

Small n?

$$\begin{aligned} 1-(1-q^{-3})^{q^2} &= \binom{q^2}{1}q^{-3} - \binom{q^2}{2}q^{-6} + - \cdots \\ &\approx q^{-1} - \frac{1}{2}q^{-2} + - \cdots \end{aligned}$$

Theorem

1. *$\{singular\}$ is an irreducible subvariety with codimension* 1*.*
2. *For $q, n \geq 3$, we have*

$$q^{-1} - \frac{1}{2}q^{-2} \leq \textit{fraction of singular} \leq q^{-1}.$$

Theorem

The fraction τ of absolutely singular and rationally nonsingular polynomials satisfies

$$\tau < 13n^{13}q^{-3/2}.$$

Conjecture

$|\tau - q^{-2}| = O(q^{-3})$.

Current work

- Exact counting, generating functions (alas, nowhere convergent), multivariate polynomials (with Alfredo Viola).
- Estimates for curves in higher dimensional spaces (with Guillermo Matera).
- Decomposable polynomials.

Thank you!