The number of decomposable univariate polynomials

Joachim von zur Gathen
Bonn

Overview

- Counting problems for polynomials
- (De)composition: tame vs. wild
- Collisions of compositions: distinct-degree
  Normal form for Ritt's Second Theorem
- Collisions of compositions: equal-degree
  Decomposition method
- Number of decomposables

Overview

- Counting problems for polynomials
- (De)composition: tame vs. wild
- Collisions of compositions: distinct-degree
  Normal form for Ritt's Second Theorem
- Collisions of compositions: equal-degree
  Decomposition method
- Number of decomposables

Overview

- Counting problems for polynomials
- (De)composition: tame vs. wild
- Collisions of compositions: distinct-degree
  Normal form for Ritt's Second Theorem
- Collisions of compositions: equal-degree
  Decomposition method
- Number of decomposables

Overview

- Counting problems for polynomials
- (De)composition: tame vs. wild
- Collisions of compositions: distinct-degree
  Normal form for Ritt's Second Theorem
- Collisions of compositions: equal-degree
  Decomposition method
- Number of decomposables

Overview

- Counting problems for polynomials
- (De)composition: tame vs. wild
- Collisions of compositions: distinct-degree
  Normal form for Ritt's Second Theorem
- Collisions of compositions: equal-degree
  Decomposition method
- Number of decomposables

Counting problems for polynomials

- Prime Number Theorem: random integer $m \leq x$:
  prob (m is prime) $\approx \frac{1}{\ln x}$.
- random $f \in \mathbb{F}_q[x]$ of degree n:
  prob (f irreducible) $\approx \frac{1}{n}$.
- random $f \in \mathbb{F}_q[x_1, \ldots, x_r]$ of degree n, for $r \geq 2$:
  prob (f irreducible) ≈ 1.
  error term $\longleftrightarrow$ reducible polynomials $\approx \rho_{r,n}$
- Second order approximation:
  reducibles $\approx \rho_{r,n} \cdot (1 +$ error term).

Counting problems for polynomials

- Prime Number Theorem: random integer $m \leq x$:
  prob (m is prime) $\approx \frac{1}{\ln x}$.
- random $f \in \mathbb{F}_q[x]$ of degree n:
  prob (f irreducible) $\approx \frac{1}{n}$.
- random $f \in \mathbb{F}_q[x_1, \ldots, x_r]$ of degree n, for $r \geq 2$:
  prob (f irreducible) ≈ 1.
  error term $\longleftrightarrow$ reducible polynomials $\approx \rho_{r,n}$
- Second order approximation:
  reducibles $\approx \rho_{r,n} \cdot (1 +$ error term$)$.

Counting problems for polynomials

- Prime Number Theorem: random integer $m \leq x$:
  prob (m is prime) $\approx \frac{1}{\ln x}$.
- random $f \in \mathbb{F}_q[x]$ of degree n:
  prob (f irreducible) $\approx \frac{1}{n}$.
- random $f \in \mathbb{F}_q[x_1, \ldots, x_r]$ of degree n, for $r \geq 2$:
  prob (f irreducible) ≈ 1.
  error term $\longleftrightarrow$ reducible polynomials $\approx \rho_{r,n}$
- Second order approximation:
  reducibles $\approx \rho_{r,n} \cdot (1 +$ error term$)$.

Counting problems for polynomials

- Prime Number Theorem: random integer $m \leq x$:
  prob (m is prime) $\approx \frac{1}{\ln x}$.
- random $f \in \mathbb{F}_q[x]$ of degree n:
  prob (f irreducible) $\approx \frac{1}{n}$.
- random $f \in \mathbb{F}_q[x_1, \ldots, x_r]$ of degree n, for $r \geq 2$:
  prob (f irreducible) ≈ 1.
  error term $\longleftrightarrow$ reducible polynomials $\approx \rho_{r,n}$
- Second order approximation:
  reducibles $\approx \rho_{r,n} \cdot (1 +$ error term$)$.

Counting problems for polynomials

- Prime Number Theorem: random integer $m \leq x$:
  prob (m is prime) $\approx \frac{1}{\ln x}$.
- random $f \in \mathbb{F}_q[x]$ of degree n:
  prob (f irreducible) $\approx \frac{1}{n}$.
- random $f \in \mathbb{F}_q[x_1, \ldots, x_r]$ of degree n, for $r \geq 2$:
  prob (f irreducible) ≈ 1.
  error term $\longleftrightarrow$ reducible polynomials $\approx \rho_{r,n}$
- Second order approximation:
  reducibles $\approx \rho_{r,n} \cdot (1 +$ error term).

Counting problems for polynomials

- Prime Number Theorem: random integer $m \leq x$:
  prob (m is prime) $\approx \frac{1}{\ln x}$.
- random $f \in \mathbb{F}_q[x]$ of degree n:
  prob (f irreducible) $\approx \frac{1}{n}$.
- random $f \in \mathbb{F}_q[x_1, \ldots, x_r]$ of degree n, for $r \geq 2$:
  prob (f irreducible) ≈ 1.
  error term $\longleftrightarrow$ reducible polynomials $\approx \rho_{r,n}$
- Second order approximation:
  reducibles $\approx \rho_{r,n} \cdot (1 +$ error term).

- Similarly: squareful, relatively irreducible, singular, decomposable multivariate polynomials.

Carlitz; S. Cohen; Gao & Lauder; Wan; Ragot; Hou & Mullen; Bodin, Dèbes & Najib; von zur Gathen, also with Viola & Ziegler and with Giesbrecht & Ziegler.

- Similarly: squareful, relatively irreducible, singular, decomposable multivariate polynomials.

Carlitz; S. Cohen; Gao & Lauder; Wan; Ragot; Hou & Mullen; Bodin, Dèbes & Najib; von zur Gathen, also with Viola & Ziegler and with Giesbrecht & Ziegler.

(De)composition

F a field of characteristic $p \geq 0$, $g, h \in F[x]$ of degree at least 2: $f = g \circ h = g(h) \in F[x]$ is their *composition*, and (g, h) a *decomposition* of f.

- $h(0) = 0$: h *original.*
- W.l.o.g.: h monic original.

Fundamental dichotomy: tame vs. wild.

- (g, h) *tame decomposition* of $f = g \circ h \Longleftrightarrow p \nmid \deg g$.
- f *tame polynomial* $\Longleftrightarrow p \nmid \deg f$.
- Otherwise: *wild.*

(De)composition

F a field of characteristic $p \geq 0$, $g, h \in F[x]$ of degree at least 2: $f = g \circ h = g(h) \in F[x]$ is their *composition*, and (g, h) a *decomposition* of f.

- $h(0) = 0$: h *original*.
- W.l.o.g.: h monic original.

Fundamental dichotomy: tame vs. wild.

- (g, h) *tame decomposition* of $f = g \circ h \iff p \nmid \deg g$.
- f *tame polynomial* $\iff p \nmid \deg f$.
- Otherwise: *wild*.

(De)composition

F a field of characteristic $p \geq 0$, $g, h \in F[x]$ of degree at least 2: $f = g \circ h = g(h) \in F[x]$ is their *composition*, and (g, h) a *decomposition* of f.

- $h(0) = 0$: h *original*.
- W.l.o.g.: h monic original.

Fundamental dichotomy: tame vs. wild.

- (g, h) *tame decomposition* of $f = g \circ h \iff p \nmid \deg g$.
- f *tame polynomial* $\iff p \nmid \deg f$.
- Otherwise: *wild*.

$$
\begin{aligned}
P_n &= \{\text{polynomials in } F[x] \text{ of degree } n\},\\
P_n^0 &= \{f \in P_n \colon f \text{ monic original}\},\\
E &= \{e \in \mathbb{N} \colon e \mid n, 1 < e < n\},\\
e \in E : \gamma_{n,e} &: P_e \times P_{n/e}^0 \to P_n,\\
&\quad (g,h) \mapsto g \circ h,\\
D_{n,e} &= \operatorname{im} \gamma_{n,e},\\
\# D_{n,e} &\le q^{e+n/e}(1 - q^{-1}),\\
D_n &= \bigcup_{e \in E} D_{n,e}.
\end{aligned}
$$

- Biggest contribution?

$$\ell = \text{smallest prime factor of } n.$$

$$
\begin{aligned}
P_n &= \{\text{polynomials in } F[x] \text{ of degree } n\}, \\
P_n^0 &= \{f \in P_n \colon f \text{ monic original}\}, \\
E &= \{e \in \mathbb{N} \colon e \mid n, 1 < e < n\}, \\
e \in E : \gamma_{n,e} &: P_e \times P_{n/e}^0 \to P_n, \\
&\quad (g, h) \mapsto g \circ h, \\
D_{n,e} &= \operatorname{im} \gamma_{n,e}, \\
\# D_{n,e} &\leq q^{e+n/e}(1 - q^{-1}), \\
D_n &= \bigcup_{e \in E} D_{n,e}.
\end{aligned}
$$

- Biggest contribution?

$$\ell = \text{smallest prime factor of } n.$$

Four tasks

$$\alpha_n = \begin{cases} q^{\ell+n/\ell}(1-q^{-1}) & \text{if } n = \ell^2, \\ 2q^{\ell+n/\ell}(1-q^{-1}) & \text{otherwise.} \end{cases}$$

We assume $n \neq \ell, \ell^2$.

- $\#D_{n,\ell} \geq \alpha_n(1/2-\epsilon)$,
- $\#D_{n,n/\ell} \geq \alpha_n(1/2-\epsilon)$,
- $t = \#(D_{n,\ell} \cap D_{n,n/\ell}) \leq \alpha_n \cdot \epsilon$,
- contribution of all $e \neq \ell, n/\ell$ is $\leq \alpha_n \cdot \epsilon$.

Then

$$\begin{aligned}\alpha_n(1-3\epsilon) &\leq \#D_{n,\ell} + \#D_{n,n/\ell} - t \\ &= \#(D_{n,\ell} \cup D_{n,n/\ell}) \leq \#D_n \leq \sum_{e\in E} \#D_{n,e} \leq \alpha_n(1+\epsilon).\end{aligned}$$

Four tasks

$$\alpha_n = \begin{cases} q^{\ell+n/\ell}(1-q^{-1}) & \text{if } n = \ell^2, \\ 2q^{\ell+n/\ell}(1-q^{-1}) & \text{otherwise.} \end{cases}$$

We assume $n \neq \ell, \ell^2$.

- $\#D_{n,\ell} \geq \alpha_n(1/2-\epsilon)$,
- $\#D_{n,n/\ell} \geq \alpha_n(1/2-\epsilon)$,
- $t = \#(D_{n,\ell} \cap D_{n,n/\ell}) \leq \alpha_n \cdot \epsilon$,
- contribution of all $e \neq \ell, n/\ell$ is $\leq \alpha_n \cdot \epsilon$.

Then

$$\begin{aligned} \alpha_n(1-3\epsilon) &\leq \#D_{n,\ell} + \#D_{n,n/\ell} - t \\ &= \#(D_{n,\ell} \cup D_{n,n/\ell}) \leq \#D_n \leq \sum_{e \in E} \#D_{n,e} \leq \alpha_n(1+\epsilon). \end{aligned}$$

The fourth task

Bounding the minor contributions:

$$u(e) = e + \frac{n}{e}.$$

- Several case distinctions: now only the "main" case: n has at least three prime factors.
- Consider $u(e) = e + n/e$ as a function of a real variable e:

$$\frac{\partial^2 u}{\partial e^2}(e) = \frac{2n}{e^3} > 0,$$

u is convex,

max u on $[a, b]$ is $u(a)$ or $u(b)$,

$u(e) \leq u(\ell_2)$ for $e \in E \smallsetminus \{\ell, n/\ell\} = E_2$,

where ℓ_2 is the second largest divisor of n.

The fourth task

Bounding the minor contributions:

$$u(e) = e + \frac{n}{e}.$$

- Several case distinctions: now only the "main" case: n has at least three prime factors.
- Consider $u(e) = e + n/e$ as a function of a real variable e:

$$\frac{\partial^2 u}{\partial e^2}(e) = \frac{2n}{e^3} > 0,$$

u is convex,

max u on $[a, b]$ is $u(a)$ or $u(b)$,

$u(e) \leq u(\ell_2)$ for $e \in E \setminus \{\ell, n/\ell\} = E_2$,

where ℓ_2 is the second largest divisor of n.

The fourth task

Bounding the minor contributions:

$$u(e) = e + \frac{n}{e}.$$

- Several case distinctions: now only the "main" case: n has at least three prime factors.
- Consider $u(e) = e + n/e$ as a function of a real variable e:

$$\frac{\partial^2 u}{\partial e^2}(e) = \frac{2n}{e^3} > 0,$$

u is convex,

max u on $[a, b]$ is $u(a)$ or $u(b)$,

$u(e) \leq u(\ell_2)$ for $e \in E \setminus \{\ell, n/\ell\} = E_2$,

where ℓ_2 is the second largest divisor of n.

The fourth task

Bounding the minor contributions:

$$u(e) = e + \frac{n}{e}.$$

- Several case distinctions: now only the "main" case: n has at least three prime factors.
- Consider $u(e) = e + n/e$ as a function of a real variable e:

$$\frac{\partial^2 u}{\partial e^2}(e) = \frac{2n}{e^3} > 0,$$

u is convex,

max u on $[a, b]$ is $u(a)$ or $u(b)$,

$u(e) \leq u(\ell_2)$ for $e \in E \setminus \{\ell, n/\ell\} = E_2,$

where ℓ_2 is the second largest divisor of n.

$$c = u(\ell) - u(\ell_2) > 0,$$

$$\begin{aligned}
\sum_{e \in E_2} \#D_{n,e} &\leq \sum_{e \in E_2} q^{u(e)}(1 - q^{-1}) \\
&= \alpha_n \cdot \sum_{e \in E_2} q^{u(e) - u(\ell_2) + u(\ell_2) - u(\ell)} \\
&= \alpha_n \cdot q^{-c} \cdot \sum_{e \in E_2} q^{u(e) - u(\ell_2)} \\
&< \alpha_n \cdot q^{-c} \cdot \frac{2}{1 - q^{-1}} = \alpha_n \cdot \varepsilon.
\end{aligned}$$

$$
\begin{aligned}
c &= u(\ell) - u(\ell_2) > 0, \\
\sum_{e \in E_2} \#D_{n,e} &\leq \sum_{e \in E_2} q^{u(e)}(1 - q^{-1}) \\
&= \alpha_n \cdot \sum_{e \in E_2} q^{u(e)-u(\ell_2)+u(\ell_2)-u(\ell)} \\
&= \alpha_n \cdot q^{-c} \cdot \sum_{e \in E_2} q^{u(e)-u(\ell_2)} \\
&< \alpha_n \cdot q^{-c} \cdot \frac{2}{1 - q^{-1}} = \alpha_n \cdot \varepsilon.
\end{aligned}
$$

Third task: distinct-degree collisions

$f = g \circ h = g^* \circ h^*$ (equal degree/distinct-degree)

$m = n/\ell$: $D_{n,\ell} \cap D_{n,m} \leftrightarrow$ distinct-degree collisions

Fundamental tool: Ritt's Second Theorem.
Beardon & Ng 2000: "difficult to use".
New: normal form for Ritt's Second Theorem.
Possibly "easy to use".

Third task: distinct-degree collisions

$$f = g \circ h = g^* \circ h^* \quad \text{(equal degree/distinct-degree)}$$

$$m = n/\ell\colon D_{n,\ell} \cap D_{n,m} \leftrightarrow \text{ distinct-degree collisions}$$

Fundamental tool: Ritt's Second Theorem.
Beardon & Ng 2000: "difficult to use".
New: normal form for Ritt's Second Theorem.
Possibly "easy to use".

First and second tasks: equal-degree collisions

$\#D_{n,\ell}$ and $\#D_{n,n/\ell}$ are large.

$$f = g \circ h = g^* \circ h^*,$$

$$\deg g = \deg g^*.$$

None if $p \nmid \deg g$.
So assume that $p \mid \deg g$.

Algorithm

Given f, returns all pairs (g, h) with $f = g \circ h$. It works for most but not all f.
Number: $\sigma(f)$.

The composition thus maps $\sigma(f)$ pairs (g, h) to one f.
Task: bound on $\sigma(f)$ "on average".

First and second tasks: equal-degree collisions

$\#D_{n,\ell}$ and $\#D_{n,n/\ell}$ are large.

$$f = g \circ h = g^* \circ h^*,$$

$$\deg g = \deg g^*.$$

None if $p \nmid \deg g$.
So assume that $p \mid \deg g$.

Algorithm

Given f, returns all pairs (g, h) with $f = g \circ h$. It works for most but not all f.
Number: $\sigma(f)$.

The composition thus maps $\sigma(f)$ pairs (g, h) to one f.
Task: bound on $\sigma(f)$ "on average".

First and second tasks: equal-degree collisions

$\#D_{n,\ell}$ and $\#D_{n,n/\ell}$ are large.

$$f = g \circ h = g^* \circ h^*,$$
$$\deg g = \deg g^*.$$

None if $p \nmid \deg g$.
So assume that $p \mid \deg g$.

Algorithm

Given f, returns all pairs (g, h) with $f = g \circ h$. It works for most but not all f.
Number: $\sigma(f)$.

The composition thus maps $\sigma(f)$ pairs (g, h) to one f.
Task: bound on $\sigma(f)$ "on average".

First and second tasks: equal-degree collisions

$\#D_{n,\ell}$ and $\#D_{n,n/\ell}$ are large.

$$f = g \circ h = g^* \circ h^*,$$

$$\deg g = \deg g^*.$$

None if $p \nmid \deg g$.
So assume that $p \mid \deg g$.

Algorithm

Given f, returns all pairs (g, h) with $f = g \circ h$. It works for most but not all f.
Number: $\sigma(f)$.

The composition thus maps $\sigma(f)$ pairs (g, h) to one f.
Task: bound on $\sigma(f)$ "on average".

Write

$$g = x^k + g_\kappa x^\kappa + \cdots,$$
$$h = x^m + h_{m-1}x^{m-1} + h_{m-2}x^{m-2} + \cdots,$$
$$g_\kappa, h_{m-1} \neq 0, p \mid k, p \nmid \kappa, n = km = \deg f,$$
$$f = g \circ h = f_n x^n + f_{n-1}x^{n-1} + \cdots$$
$$g, h \notin F[x^p].$$

Tool: coefficient comparison.
Example: $k = p$.
$g \circ h = h^p + g_\kappa h^\kappa + \cdots$
First phase: κ, γ_κ and h.
Second phase: rest of g.

Write

$$
\begin{aligned}
&g = x^k + g_\kappa x^\kappa + \cdots, \\
&h = x^m + h_{m-1}x^{m-1} + h_{m-2}x^{m-2} + \cdots, \\
&g_\kappa, h_{m-1} \neq 0, p \mid k, p \nmid \kappa, n = km = \deg f, \\
&f = g \circ h = f_n x^n + f_{n-1}x^{n-1} + \cdots \\
&g, h \notin F[x^p].
\end{aligned}
$$

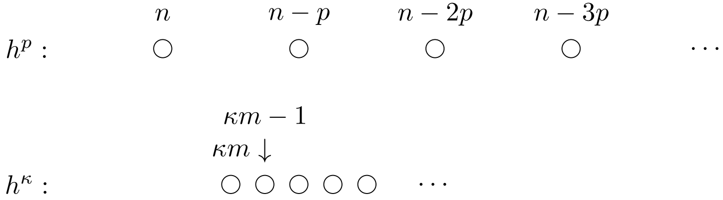
Tool: coefficient comparison.
Example: $k = p$.
$g \circ h = h^p + g_\kappa h^\kappa + \cdots$
First phase: κ, γ_κ and h.
Second phase: rest of g.

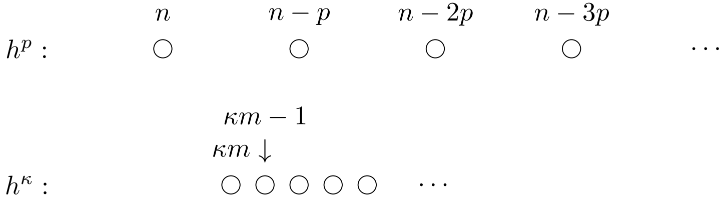
Write

$$
\begin{aligned}
&g = x^k + g_\kappa x^\kappa + \cdots , \\
&h = x^m + h_{m-1} x^{m-1} + h_{m-2} x^{m-2} + \cdots , \\
&g_\kappa, h_{m-1} \neq 0, p \mid k, p \nmid \kappa, n = km = \deg f, \\
&f = g \circ h = f_n x^n + f_{n-1} x^{n-1} + \cdots \\
&g, h \notin F[x^p].
\end{aligned}
$$

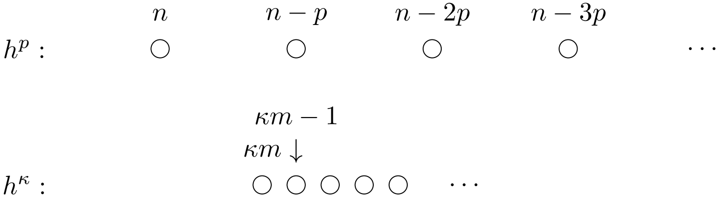
Tool: coefficient comparison.
Example: $k = p$.
$g \circ h = h^p + g_\kappa h^\kappa + \cdots$
First phase: κ, γ_κ and h.
Second phase: rest of g.

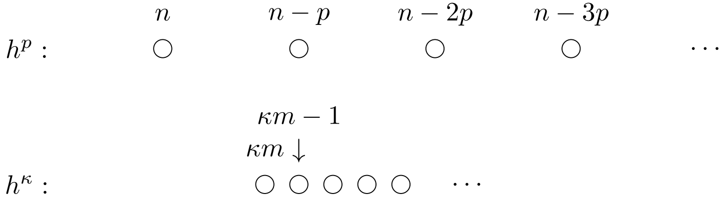

$h^p :$
n
$n - p$
$n - 2p$
$n - 3p$
$\cdots$


$h^p :$
n
$n-p$
$n-2p$
$n-3p$
$\cdots$
$h^\kappa :$
$\kappa m - 1$
$\kappa m \downarrow$
$\cdots$



Case 1: $\kappa m \geq n-p+2$. Solve for g_κ, then h_{m-1}, h_{m-2}, $\ldots$.

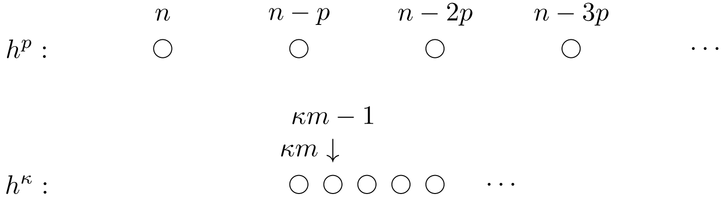

$h^p :$
n
$n-p$
$n-2p$
$n-3p$
$\cdots$
$h^\kappa :$
$\kappa m - 1$
$\kappa m \downarrow$
$\cdots$

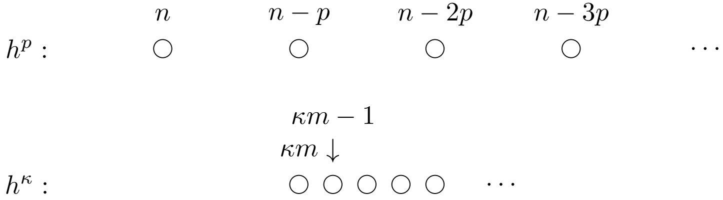


Case 2: $\kappa m = n - p + 1$. Solve for g_κ. Then

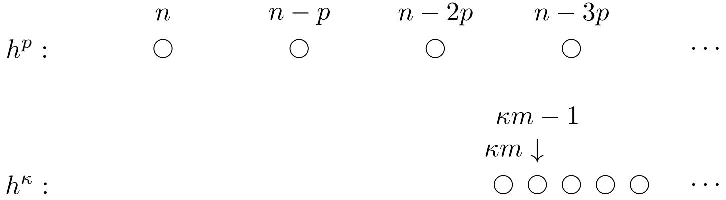
$$h^p_{m-1} + \kappa g_\kappa h_{m-1} = f_{n-p}. \tag{1}$$

Solve for h_{m-1} and continue with h_{m-2}, h_{m-3}, $\ldots$.

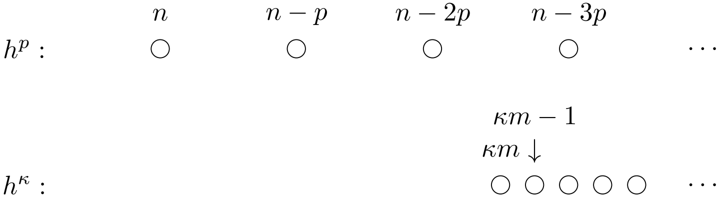

h^p :
n
$n-p$
$n-2p$
$n-3p$
$\cdots$
$\kappa m - 1$
$\kappa m \downarrow$
h^κ :
$\cdots$



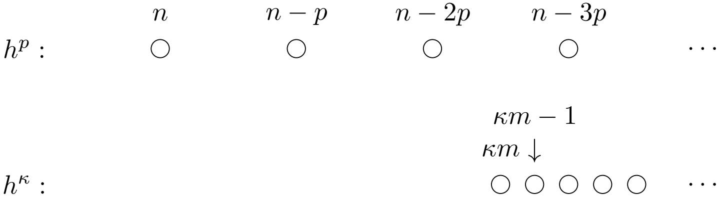
Case 3: $\kappa m = n - p$. Solve two equations (2) for g_κ and h_{m-1}. Then h_{m-2}, h_{m-3}, $\ldots$.



h^p :
n
$n-p$
$n-2p$
$n-3p$
$\cdots$
$\kappa m - 1$
$\kappa m \downarrow$
h^κ :
$\cdots$



Case 4: $\kappa m < n - p$. Determine h_{m-1}, h_{m-2}, ..., h_i via top row, then g_κ, then h_{i-1}, h_{i-2}, ... via bottom row. A collision is possible and leads to an equation of type (1).



Case 4: $\kappa m < n - p$. Determine h_{m-1}, h_{m-2}, ..., h_i via top row, then g_κ, then h_{i-1}, h_{i-2}, ... via bottom row. A collision is possible and leads to an equation of type (1).

Given f and h, solve for g: easy via Taylor expansion.

- Equation (1): write s for h_{m-i}.

$$s^p + \kappa g_\kappa s = c. \tag{1}$$

The left hand side is $\mathbb{F}_p$-linear. Kernel:

$$s^p + \kappa g_k s = 0,$$
$$s \neq 0 \colon s^{p-1} = -\kappa g_\kappa.$$

We allow only those g for which no such $s \neq 0$ exists. Then (1) has a unique solution.

- Equation (1): write s for h_{m-i}.

$$s^p + \kappa g_\kappa s = c. \tag{1}$$

The left hand side is $\mathbb{F}_p$-linear. Kernel:

$$s^p + \kappa g_k s = 0,$$
$$s \neq 0\colon s^{p-1} = -\kappa g_\kappa.$$

We allow only those g for which no such $s \neq 0$ exists. Then (1) has a unique solution.

- Equation (1): write s for h_{m-i}.

$$s^p + \kappa g_\kappa s = c. \tag{1}$$

The left hand side is $\mathbb{F}_p$-linear. Kernel:

$$s^p + \kappa g_k s = 0,$$
$$s \neq 0\colon\ s^{p-1} = -\kappa g_\kappa.$$

We allow only those g for which no such $s \neq 0$ exists. Then (1) has a unique solution.

- Equation (2):

$$\kappa m = n - p = km - p,$$
$$\kappa = k - \frac{p}{m}, m = p, \kappa = k - 1 \equiv -1 \mod p.$$

$s = h_{m-1}$:

$$f_{\kappa m} = s^p + g_\kappa,$$
$$f_{\kappa m-1} = \kappa g_\kappa s = -(f_{\kappa m} - s^p)s = s^{p+1} - f_{\kappa m} s. \quad (2)$$

Bluher (2004) has determined exactly the solution statistics of this equation:

It has $0, 1, 2$ or $p + 1$ solutions s.

For $i \in I = \{0, 1, 2, p+1\}$, let

$$c_i = q^{-1} \#\{(f_{\kappa m}, f_{\kappa m-1}) \text{ with } i \text{ solutions}\}.$$

Bluher determines the c_i exactly. For large p, we have

$$\begin{aligned} c_0 &\approx \frac{q}{2}, \\ c_1 &\approx \frac{q}{p} \approx 0, \\ c_2 &\approx \frac{q}{2}, \\ c_{p+1} &= \lfloor \frac{q}{p^3 - p} \rfloor \approx 0. \end{aligned}$$

For $i \in I = \{0, 1, 2, p+1\}$, let

$$c_i = q^{-1} \#\{(f_{\kappa m}, f_{\kappa m-1}) \text{ with } i \text{ solutions}\}.$$

Bluher determines the c_i exactly. For large p, we have

$$\begin{aligned} c_0 &\approx \frac{q}{2}, \\ c_1 &\approx \frac{q}{p} \approx 0, \\ c_2 &\approx \frac{q}{2}, \\ c_{p+1} &= \lfloor \frac{q}{p^3 - p} \rfloor \approx 0. \end{aligned}$$

Analysis of the algorithm:

- correctness,
- cost: $\mathcal{O}^{\sim}(n(m + \log q))$,
- number $\sigma(f)$ of outputs.

Open question:

Efficient general algorithm for decomposition.

Analysis of the algorithm:

- correctness,
- cost: $\mathcal{O}^{\sim}(n(m + \log q))$,
- number $\sigma(f)$ of outputs.

Open question:

Efficient general algorithm for decomposition.

Analysis of the algorithm:

- correctness,
- cost: $\mathcal{O}^{\sim}(n(m + \log q))$,
- number $\sigma(f)$ of outputs.

Open question:

Efficient general algorithm for decomposition.

Analysis of the algorithm:

- correctness,
- cost: $\mathcal{O}^{\sim}(n(m + \log q))$,
- number $\sigma(f)$ of outputs.

Open question:

Efficient general algorithm for decomposition.

Analysis of the algorithm:

- correctness,
- cost: $\mathcal{O}^{\sim}(n(m + \log q))$,
- number $\sigma(f)$ of outputs.

Open question:

Efficient general algorithm for decomposition.

Counting result of the algorithm

The number of decomposable polynomials $g \circ h$ is at least

$$q^{k+m}(1 - q^{-1}) \cdot (1 - 2\epsilon) = \alpha_n \cdot \left(\frac{1}{2} - \epsilon\right),$$

with three values of ϵ, which depend on the arithmetic of $k = \deg g$ and $m = \deg h$.

The final analysis

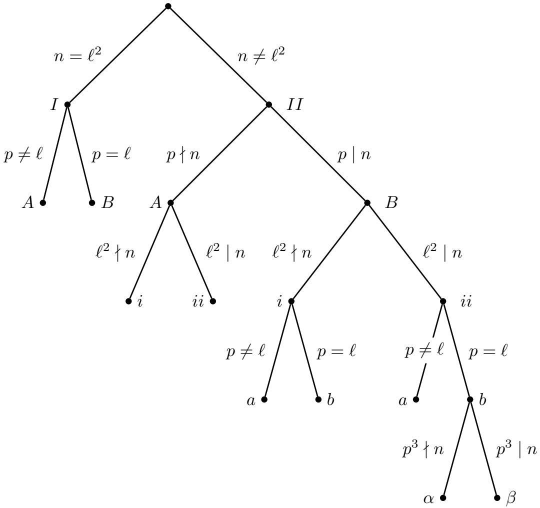


Figure: The tree of case distinctions for estimating $\#D_n$.

Main Theorem:

Let $\mathbb{F}_q$ be a finite field with q elements and characteristic p, let ℓ be the smallest prime divisor of the composite integer $n \geq 2$, D_n the set of decomposable polynomials in $\mathbb{F}_q[x]$ of degree n, and

$$\alpha_n = \begin{cases} 2q^{\ell+n/\ell}(1-q^{-1}) & \text{if } n \neq \ell^2, \\ q^{2\ell}(1-q^{-1}) & \text{if } n = \ell^2. \end{cases}$$

Then the following hold.

- $\alpha_n/2 \leq \#D_n \leq \alpha_n(1+q^{-n/3\ell^2})$.
- If $\ell \neq p$ or $p^2 \nmid n$ or $p^3 \mid n$, then $\#D_n \geq \alpha_n(1-2q^{-1})$.
- If $p \nmid n$, then $|\#D_n - \alpha_n| \leq \alpha_n \cdot q^{-n/3\ell^2}$.

Asymptotic result

Let $\nu_{q,n} = \#D_n/\alpha_n$ over $\mathbb{F}_q$, n be a composite integer and ℓ its smallest prime divisor. Then

$$\limsup_{q\to\infty} \nu_{q,n} = 1,$$

$$\liminf_{q\to\infty} \nu_{q,n} \begin{cases} \geq \frac{1}{2}(1+\frac{1}{\ell+1}) \geq \frac{2}{3} & \text{if } n = \ell^2, \\ \geq \frac{1}{4}(3+\frac{1}{\ell+1}) \geq \frac{5}{6} & \text{if } \ell^2 \parallel n \text{ and } n \neq \ell^2, \\ = 1 & \text{otherwise,} \end{cases}$$

$$\lim_{\substack{q\to\infty \\ \gcd(q,n)=1}} \nu_{q,n} = 1.$$

Open questions

- Tighten gap for $p = \ell$ and $p^2 \| n$.
- Simplify proof.

Thank you!