Algorithms and Statistics for Additive Polynomials

Mark Giesbrecht
with
Joachim von zur Gathen and Konstantin Ziegler

Symbolic Computation Group
Cheriton School of Computer Science
University of Waterloo
Waterloo, Ontario, Canada

November 28, 2013

Polynomial Composition and Decomposition

Functional Composition

Let $g, h \in \mathsf{F}[x]$, for a field F.

Compose g, h as functions $f(x) = g(h(x)) = g \circ h$

Generally non-distributive operation (not always, as we'll see!):

$$g(h_1(x) + h_2(x)) \neq g(h_1(x)) + g(h_2(x))$$

Polynomial Composition and Decomposition

Functional Composition

Let $g, h \in \mathsf{F}[x]$, for a field F.

Compose g, h as functions $f(x) = g(h(x)) = g \circ h$

Generally non-distributive operation (not always, as we'll see!):

$$g(h_1(x) + h_2(x)) \neq g(h_1(x)) + g(h_2(x))$$

Decomposition

Given $f \in \mathsf{F}[x]$, can it be decomposed?

Do there exist $g, h \in \mathsf{F}[x]$ such that $f = g \circ h$?

$f = x^4 - 2x^3 + 8x^2 - 7x + 5$

$g = x^2 + 3x - 5 \quad h = x^2 - x - 2$

➡ $f = g \circ h$

Tame and Wild Decomposition

Let F be a field of characteristic p and $f \in \mathsf{F}[x]$ monic of degree d.

Normalize f, g, h to monic and *original*: $h(0) = 0$

- f is *tame* if $p \nmid d$
- f is *wild* if $p \mid d$

Traditionally this describes the ramification of $\mathsf{F}(x)$ over $\mathsf{F}(f(x))$.

Tame and Wild Decomposition

Let F be a field of characteristic p and $f \in \mathsf{F}[x]$ monic of degree d.

Normalize f, g, h to monic and *original*: $h(0) = 0$

- f is *tame* if $p \nmid d$
- f is *wild* if $p \mid d$

Traditionally this describes the ramification of $\mathsf{F}(x)$ over $\mathsf{F}(f(x))$.

Tame decomposition

- Ritt (1922) describes all tame decompositions and "ambiguities".
- For a fixed s, there are either 0 or 1 monic $h \in \mathsf{F}[x]$ of degree s with $h(0) = 0$ such that $f(x) = g(h(x))$.
- See von zur Gathen (2013) for complete decompositions.

Tame and Wild Decomposition

Let F be a field of characteristic p and $f \in \mathsf{F}[x]$ monic of degree d.

Normalize f, g, h to monic and *original*: $h(0) = 0$

- f is *tame* if $p \nmid d$
- f is *wild* if $p \mid d$

Traditionally this describes the ramification of $\mathsf{F}(x)$ over $\mathsf{F}(f(x))$.

Wild decomposition

- Life is much more difficult
- (G, 1988) For a finite field F of characteristic p, there are $f \in \mathsf{F}[x]$ of degree d with $> \mathbf{d}^{\boldsymbol{\lambda} \log \mathbf{d}}$ monic, original, $h \in \mathsf{F}[x]$ of degree $s \approx \sqrt{s}$ such that $f(x) = g(h(x))$, where $\lambda = (6 \log p)^{-1}$.

Tame and Wild Decomposition

Let F be a field of characteristic p and $f \in \mathsf{F}[x]$ monic of degree d.

Normalize f, g, h to monic and *original*: $h(0) = 0$

- f is *tame* if $p \nmid d$
- f is *wild* if $p \mid d$

Traditionally this describes the ramification of $\mathsf{F}(x)$ over $\mathsf{F}(f(x))$.

Wild decomposition

- On the bright side, there are at most $(d-1)/(s-1)$ *indecomposable* monic, orginal $h \in \mathsf{F}[x]$ of degree s such that $f(x) = g(h(x))$. (Von zur Gathen, G, Ziegler, 2010)

Additive Polynomials

Additive or linearized polynomials are those such that

$$f(x+y) = f(x) + f(y)$$

Non-linear additive polynomials only exist in $\mathsf{F}[x]$ if F has prime characteristic p, and have the form

$$f = a_0 x + a_1 x^p + a_2 x^{p^2} + \cdots + a_n x^{p^n} \in \mathsf{F}[x].$$

Additive Polynomials

Additive or linearized polynomials are those such that

$$f(x+y) = f(x) + f(y)$$

Non-linear additive polynomials only exist in $\mathsf{F}[x]$ if F has prime characteristic p, and have the form

$$f = a_0 x + a_1 x^p + a_2 x^{p^2} + \cdots + a_n x^{p^n} \in \mathsf{F}[x].$$

Example

Let $\mathbb{F}_{125} = \mathbb{F}_5[\theta]/(\theta^3 + \theta + 1)$.

$$f = x^{25} + (3\theta^2 + 4\theta + 2)x^5 + (3\theta^2 + 4\theta + 2)x$$

is an additive polynomial, and

$$\begin{aligned} f &= (x^5 + (\theta^2 + \theta + 4)x) \circ (x^5 + 3\theta x) \\ &= (x^5 + (2\theta^2 + 4\theta + 2)x) \circ (x^5 + (\theta^2 + 2\theta)x) \end{aligned}$$

Ore's Legacy

In 1932-4, Oystein Ore wrote four seminal papers for finite fields, differential algebra, and computer algebra

1. O. Ore, *Formale Theorie der linearen Differentialgleichungen*, J. reine angew. Math., v. 168, pp. 233-252, 1932.
2. O. Ore, *Theory of Non-Commutative Polynomials*, "Annals of Mathematics", v. 34, no. 22, pp. 480–508, 1933.
3. O. Ore, *On a Special Class of Polynomials*, Trans. Amer. Math. Soc., v. 35, pp. 559-584, 1933.
4. O. Ore, *Contributions to the Theory of Finite Fields*, Trans. Amer. Math. Soc., v. 36, pp. 243-274, 1934.

[1,2] form the basis for modern computational theory of LODEs (Ore_algebra,OreTools)

[3,4] have had great influence on theory of finite fields

Ore Polynomials in Computational Algebra

Additive polynomials are employed in

- Error correcting codes
- HFE and other cryptosystems
- Mathematical constructions in algebraic function fields
- General fun and parlour tricks.

Despite their large (exponential) degrees we will see that we can compute very efficiently with them.

Ore Polynomials and Additive Polynomials

Let $q = p^e$ for prime p and integer e.

$\mathbb{F}_q$ the finite field with q elements.

- Additive polynomials over $\mathbb{F}_q$:

$$\mathbb{F}_q[x; p] = \left\{ \sum_{0 \leqslant i \leqslant n} a_i x^{p^i} \in \mathbb{F}_q[x] \right\}$$

Ring under usual polynomial addition ($+$) and functional composition($\circ$), with $x^p \circ ax = a^p x^p$.

Ore Polynomials and Additive Polynomials

Let $q = p^e$ for prime p and integer e.

$\mathbb{F}_q$ the finite field with q elements.

- Additive polynomials over $\mathbb{F}_q$:

$$\mathbb{F}_q[x; p] = \left\{ \sum_{0 \leqslant i \leqslant n} a_i x^{p^i} \in \mathbb{F}_q[x] \right\}$$

  Ring under usual polynomial addition $(+)$ and functional composition$(\circ)$, with $x^p \circ ax = a^p x^p$.

- Ore polynomials over $\mathbb{F}_q$:

$$\mathbb{F}_q[x; \sigma_p] = \left\{ \sum_{0 \leqslant i \leqslant n} a_i x^{i} \in \mathbb{F}_q[x] \right\}$$

  Ring under usual polynomial addition $(+)$ and multiplication
  - $xa = \sigma_p(a)x$
  - $\sigma_p(a) = a^p$ is the Frobenius automorphism of $\mathbb{F}_q/\mathbb{F}_p$

Ore Polynomials and Additive Polynomials

Let $q = p^e$ for prime p and integer e.
$\mathbb{F}_q$ the finite field with q elements.

- Additive polynomials over $\mathbb{F}_q$:

$$\mathbb{F}_q[x;p] = \left\{ \sum_{0 \leqslant i \leqslant n} a_i x^{p^i} \in \mathbb{F}_q[x] \right\}$$

  Ring under usual polynomial addition $(+)$ and functional composition$(\circ)$, with $x^p \circ ax = a^p x^p$.

- Ore polynomials over $\mathbb{F}_q$:

$$\mathbb{F}_q[x;\sigma_p] = \left\{ \sum_{0 \leqslant i \leqslant n} a_i x^i \in \mathbb{F}_q[x] \right\}$$

  Ring under usual polynomial addition $(+)$ and multiplication
  - $xa = \sigma_p(a)x$
  - $\sigma_p(a) = a^p$ is the Frobenius automorphism of $\mathbb{F}_q/\mathbb{F}_p$

The Geometry of Additive Polynomials

Assume $f \in \mathbb{F}_q[x;p]$ squarefree of degree p^n

The Geometry of Additive Polynomials

Assume $f \in \mathbb{F}_q[x;p]$ squarefree of degree p^n

- f squarefree $\iff$ $f' = a_0 \neq 0$

The Geometry of Additive Polynomials

Assume $f \in \mathbb{F}_q[x;p]$ squarefree of degree p^n

- f squarefree $\iff$ $f' = a_0 \neq 0$
- Roots $V_f \subseteq \overline{\mathbb{F}}_q$ of f form $\mathbb{F}_p$-vector space of dimension n.

The Geometry of Additive Polynomials

Assume $f \in \mathbb{F}_q[x;p]$ squarefree of degree p^n

- f squarefree $\iff$ $f' = a_0 \neq 0$
- Roots $V_f \subseteq \overline{\mathbb{F}}_q$ of f form $\mathbb{F}_p$-vector space of dimension n.
- If W an $\mathbb{F}_p$-subspace of V_f, and
  $h \in \overline{\mathbb{F}}_q[x]$ has roots exactly W
  then $h \in \overline{\mathbb{F}}_q[x;p]$ and $\exists g \in \overline{\mathbb{F}}_q[x;p]$ such that $f = g \circ h$.

The Geometry of Additive Polynomials

Assume $f \in \mathbb{F}_q[x;p]$ squarefree of degree p^n

- f squarefree $\iff$ $f' = a_0 \neq 0$
- Roots $V_f \subseteq \overline{\mathbb{F}}_q$ of f form $\mathbb{F}_p$-vector space of dimension n.
- If W an $\mathbb{F}_p$-subspace of V_f, and
  $h \in \overline{\mathbb{F}}_q[x]$ has roots exactly W
  then $h \in \overline{\mathbb{F}}_q[x;p]$ and $\exists g \in \overline{\mathbb{F}}_q[x;p]$ such that $f = g \circ h$.

Decomposing additive polynomials $\equiv$ finding subspaces of V_f

The Geometry of Additive Polynomials

Assume $f \in \mathbb{F}_q[x;p]$ squarefree of degree p^n

- f squarefree $\iff$ $f' = a_0 \neq 0$
- Roots $V_f \subseteq \overline{\mathbb{F}}_q$ of f form $\mathbb{F}_p$-vector space of dimension n.
- If W an $\mathbb{F}_p$-subspace of V_f, and
  $h \in \overline{\mathbb{F}}_q[x]$ has roots exactly W
  then $h \in \overline{\mathbb{F}}_q[x;p]$ and $\exists g \in \overline{\mathbb{F}}_q[x;p]$ such that $f = g \circ h$.

Decomposing additive polynomials $\equiv$ finding subspaces of V_f

- Let $\sigma_q(a) = a^q$, the q-Frobenius automorphism.

  If W is also σ_q-invariant, then $h \in \mathbb{F}_q[x;p]$

Decomposing additive polynomial over $\mathbb{F}_q[x]$
$\equiv$ finding σ_q-invariant subspace of V_f

The Geometry of Additive Polynomials (2)

Example

Again let $\mathbb{F}_{125} = \mathbb{F}_5[\theta]/(\theta^3 + \theta + 1)$, and

$$f = x^{25} + (3\theta^2 + 4\theta + 2)x^5 + (3\theta^2 + 4\theta + 2)x$$

Then

$$\mu = \text{RootOf}\left(x^4 + (\theta^2 + 3\theta + 4)x^2 + (3\theta^2 + 4\theta)x + (4\theta^2 + \theta)\right)$$
$$\nu = \text{RootOf}\left(x^4 + (4\theta^2 + 2\theta + 1)x^2 + (4\theta^2 + 2\theta)x + (4\theta^2 + \theta)\right)$$

$$V_f = \{\alpha\mu + \beta\nu : \alpha, \beta \in \mathbb{F}_p\} \subseteq \mathbb{F}_{5^{12}}$$

$$\sigma_q = \begin{pmatrix} 3 & 3 \\ 2 & 3 \end{pmatrix} \quad \text{(after some ugly calculations)}$$

Probably not the best way to work with additive polynomials...

Right Composition Factors as Eigenvectors of σ_q

Given $f \in \mathbb{F}_q[x;p]$, find

$$\#\Big\{h = x^p + ax \in \mathbb{F}_q[x;p] : \exists g \in \mathbb{F}_q[x;p] \text{ with } f = g \circ h\Big\}$$

The number of right composition factors of f degree p

Right Composition Factors as Eigenvectors of σ_q

Given $f \in \mathbb{F}_q[x;p]$, find

$$\#\Big\{h = x^p + ax \in \mathbb{F}_q[x;p] : \exists g \in \mathbb{F}_q[x;p] \text{ with } f = g \circ h\Big\}$$

The number of right composition factors of f degree p

$=$ number of 1-dimensional σ_q-invariant subspaces of V_f

$=$ number of eigenvectors of σ_q

Remember, $\sigma_q : V_f \to V_f$ is a $\mathbb{F}_p$-linear map

➡ σ_q acts like an $n \times n$ matrix over $\mathbb{F}_p$

Right Composition Factors as Eigenvectors of σ_q

Given $f \in \mathbb{F}_q[x;p]$, find

$$\#\left\{h = x^p + ax \in \mathbb{F}_q[x;p] : \exists g \in \mathbb{F}_q[x;p] \text{ with } f = g \circ h\right\}$$

The number of right composition factors of f degree p

$=$ number of 1-dimensional σ_q-invariant subspaces of V_f

$=$ number of eigenvectors of σ_q

Remember, $\sigma_q : V_f \to V_f$ is a $\mathbb{F}_p$-linear map

➡ σ_q acts like an $n \times n$ matrix over $\mathbb{F}_p$

New questions:

- How many eigenvectors can an $n \times n$ matrix over $\mathbb{F}_q$ have?
- How can we compute this?

Right Composition Factors as Eigenvectors of σ_q (2)

How many eigenvectors can a matrix have?
Look at the (rational) Jordan form in $\mathbb{F}_p^{n\times n}$

Example: degree p^2 ($n = 2$): the number of ways of decomposing

$$\begin{aligned} f &= x^{p^2} + a_1 x^p + a_0 x \\ &= (x^p + b_0 x) \circ (x^p + c_0 x) \end{aligned}$$

Put σ_q in rational Jordan form; there are only four possibilities:

$$\sigma_q \sim \begin{pmatrix} 0 & \alpha \\ 1 & \beta \end{pmatrix} \quad \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}, \quad \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}, \quad \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix},$$

Here $\lambda, \mu, \alpha, \beta \in \mathbb{F}_p^*$, $\lambda \neq \mu$ and $y^2 - \beta y - \alpha \in \mathbb{F}_p[y]$ is irreducible.

Right Composition Factors as Eigenvectors of σ_q (2)

How many eigenvectors can a matrix have?
Look at the (rational) Jordan form in $\mathbb{F}_p^{n\times n}$

Example: degree p^2 ($n = 2$): the number of ways of decomposing

$$\begin{aligned} f &= x^{p^2} + a_1 x^p + a_0 x \\ &= (x^p + b_0 x) \circ (x^p + c_0 x) \end{aligned}$$

Put σ_q in rational Jordan form; there are only four possibilities:

$$\sigma_q \sim \begin{pmatrix} 0 & \alpha \\ 1 & \beta \end{pmatrix} \quad \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}, \quad \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}, \quad \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix},$$

0

Here $\lambda, \mu, \alpha, \beta \in \mathbb{F}_p^*$, $\lambda \neq \mu$ and $y^2 - \beta y - \alpha \in \mathbb{F}_p[y]$ is irreducible.

Right Composition Factors as Eigenvectors of σ_q (2)

How many eigenvectors can a matrix have?
Look at the (rational) Jordan form in $\mathbb{F}_p^{n\times n}$

Example: degree p^2 ($n = 2$): the number of ways of decomposing

$$\begin{aligned} f &= x^{p^2} + a_1 x^p + a_0 x \\ &= (x^p + b_0 x) \circ (x^p + c_0 x) \end{aligned}$$

Put σ_q in rational Jordan form; there are only four possibilities:

$$\sigma_q \sim \underset{0}{\begin{pmatrix} 0 & \alpha \\ 1 & \beta \end{pmatrix}} \quad \underset{1}{\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}}, \quad \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}, \quad \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix},$$

Here $\lambda, \mu, \alpha, \beta \in \mathbb{F}_p^*$, $\lambda \neq \mu$ and $y^2 - \beta y - \alpha \in \mathbb{F}_p[y]$ is irreducible.

Right Composition Factors as Eigenvectors of σ_q (2)

How many eigenvectors can a matrix have?
Look at the (rational) Jordan form in $\mathbb{F}_p^{n\times n}$

Example: degree p^2 ($n = 2$): the number of ways of decomposing

$$\begin{aligned} f &= x^{p^2} + a_1 x^p + a_0 x \\ &= (x^p + b_0 x) \circ (x^p + c_0 x) \end{aligned}$$

Put σ_q in rational Jordan form; there are only four possibilities:

$$\sigma_q \sim \underset{0}{\begin{pmatrix} 0 & \alpha \\ 1 & \beta \end{pmatrix}} \quad \underset{1}{\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}}, \quad \underset{2}{\begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}}, \quad \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix},$$

Here $\lambda, \mu, \alpha, \beta \in \mathbb{F}_p^*$, $\lambda \neq \mu$ and $y^2 - \beta y - \alpha \in \mathbb{F}_p[y]$ is irreducible.

Right Composition Factors as Eigenvectors of σ_q (2)

How many eigenvectors can a matrix have?
Look at the (rational) Jordan form in $\mathbb{F}_p^{n\times n}$

Example: degree p^2 ($n = 2$): the number of ways of decomposing

$$\begin{aligned} f &= x^{p^2} + a_1 x^p + a_0 x \\ &= (x^p + b_0 x) \circ (x^p + c_0 x) \end{aligned}$$

Put σ_q in rational Jordan form; there are only four possibilities:

$$\sigma_q \sim \underset{0}{\begin{pmatrix} 0 & \alpha \\ 1 & \beta \end{pmatrix}} \quad \underset{1}{\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}}, \quad \underset{2}{\begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}}, \quad \underset{p+1}{\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}},$$

Here $\lambda, \mu, \alpha, \beta \in \mathbb{F}_p^*$, $\lambda \neq \mu$ and $y^2 - \beta y - \alpha \in \mathbb{F}_p[y]$ is irreducible.

An $f \in \mathbb{F}_q[x;\sigma]$ of degree p^2 can have only $0, 1, 2$, or $p+1$ right composition factors of degree p.

Right Composition Factors as Eigenvectors of σ_q (3)

Example: degree p^3 ($n = 3$): the number of ways of decomposing

$$f = x^{p^3} + a_2 x^{p^2} + a_1 x^p + a_0 x$$
$$= (x^{p^2} + b_1 x^p + b_0 x) \circ (x^p + c_0 x)$$

$$\sigma_q \sim \quad \begin{pmatrix} \lambda & & \\ & \lambda & \\ & & \lambda \end{pmatrix}, \quad \begin{pmatrix} \lambda & 1 & \\ & \lambda & \\ & & \lambda \end{pmatrix}, \quad \begin{pmatrix} \lambda & 1 & \\ & \lambda & 1 \\ & & \lambda \end{pmatrix}, \quad \begin{pmatrix} \lambda & 1 & \\ & \lambda & \\ & & \mu \end{pmatrix}$$

$$\begin{pmatrix} \lambda & & \\ & \lambda & \\ & & \mu \end{pmatrix}, \quad \begin{pmatrix} \lambda & & \\ & \mu & \\ & & \nu \end{pmatrix}, \quad \left(\lambda \; \square \right), \quad \left(\square \right)$$

Right Composition Factors as Eigenvectors of σ_q (3)

Example: degree p^3 ($n = 3$): the number of ways of decomposing

$$f = x^{p^3} + a_2 x^{p^2} + a_1 x^p + a_0 x$$
$$= (x^{p^2} + b_1 x^p + b_0 x) \circ (x^p + c_0 x)$$

$$\sigma_q \sim \quad \begin{pmatrix} \lambda & & \\ & \lambda & \\ & & \lambda \end{pmatrix}, \quad \begin{pmatrix} \lambda & 1 & \\ & \lambda & \\ & & \lambda \end{pmatrix}, \quad \begin{pmatrix} \lambda & 1 & \\ & \lambda & 1 \\ & & \lambda \end{pmatrix}, \quad \begin{pmatrix} \lambda & 1 & \\ & \lambda & \\ & & \mu \end{pmatrix}$$

$$\begin{pmatrix} \lambda & & \\ & \lambda & \\ & & \mu \end{pmatrix}, \quad \begin{pmatrix} \lambda & & \\ & \mu & \\ & & \nu \end{pmatrix}, \quad \left(\lambda \; \square\right), \quad \left(\square\right)$$

$p + 2$ 3 1 0

Right Composition Factors as Eigenvectors of σ_q (3)

Example: degree p^3 ($n = 3$): the number of ways of decomposing

$$f = x^{p^3} + a_2 x^{p^2} + a_1 x^p + a_0 x$$
$$= (x^{p^2} + b_1 x^p + b_0 x) \circ (x^p + c_0 x)$$

$\sigma_q \sim$

$\begin{pmatrix} \lambda & & \\ & \lambda & \\ & & \lambda \end{pmatrix}$, $p^2 + p + 1$ $\quad$ $\begin{pmatrix} \lambda & 1 & \\ & \lambda & \\ & & \lambda \end{pmatrix}$, $p + 1$ $\quad$ $\begin{pmatrix} \lambda & 1 & \\ & \lambda & 1 \\ & & \lambda \end{pmatrix}$, 1 $\quad$ $\begin{pmatrix} \lambda & 1 & \\ & \lambda & \\ & & \mu \end{pmatrix}$, 2

$\begin{pmatrix} \lambda & & \\ & \lambda & \\ & & \mu \end{pmatrix}$, $p + 2$ $\quad$ $\begin{pmatrix} \lambda & & \\ & \mu & \\ & & \nu \end{pmatrix}$, 3 $\quad$ $\left(\begin{array}{cc|c} \lambda & & \\ & \square & \end{array}\right)$, 1 $\quad$ $\left(\begin{array}{c|c} \square & \end{array}\right)$, 0

Right Composition Factors as Eigenvectors of σ_q (3)

Example: degree p^3 ($n = 3$): the number of ways of decomposing

$$f = x^{p^3} + a_2 x^{p^2} + a_1 x^p + a_0 x$$
$$= (x^{p^2} + b_1 x^p + b_0 x) \circ (x^p + c_0 x)$$

$\sigma_q \sim$

$\begin{pmatrix} \lambda & & \\ & \lambda & \\ & & \lambda \end{pmatrix}$, $p^2 + p + 1$ $\quad$ $\begin{pmatrix} \lambda & 1 & \\ & \lambda & \\ & & \lambda \end{pmatrix}$, $p + 1$ $\quad$ $\begin{pmatrix} \lambda & 1 & \\ & \lambda & 1 \\ & & \lambda \end{pmatrix}$, 1 $\quad$ $\begin{pmatrix} \lambda & 1 & \\ & \lambda & \\ & & \mu \end{pmatrix}$, 2

$\begin{pmatrix} \lambda & & \\ & \lambda & \\ & & \mu \end{pmatrix}$, $p + 2$ $\quad$ $\begin{pmatrix} \lambda & & \\ & \mu & \\ & & \nu \end{pmatrix}$, 3 $\quad$ $\left(\lambda \begin{array}{|c|}\hline \\ \hline \end{array}\right)$, 1 $\quad$ $\left(\begin{array}{|c|}\hline \\ \hline \end{array}\right)$, 0

➡ An $f \in \mathbb{F}_q[x; \sigma]$ of degree p^3 can have only

$$0, 1, 2, 3, p + 1, p + 2, \text{or } p^2 + p + 1$$

right composition factors of degree p.

General categorization of number of composition factors

How many composition factors of degree p can an additive polynomial of degree p^n have? S_n is the set of possible numbers:

$$
\begin{aligned}
S_0 &= \{0\} \\
S_1 &= \{0, 1\} \\
S_2 &= \{0, 1, 2, p+1\} \\
S_3 &= \{0, 1, 2, 3, p+1, p+2, p^2+p+1\} \\
S_4 &= \{0, 1, 2, 3, 4, 2p+2, p^2+p+2, p^3+p^2+p+1\} \\
\vdots &\quad \vdots
\end{aligned}
$$

In general $\#S_n = \sum_{0 \leqslant k \leqslant n} P(k)$, where $P(k)$ is the number of additive partitions of k.

Efficient Counting of Composition Factors

Roots of $f \in \mathbb{F}_q[x;p]$ of degree p^n may be in an extension field of high degree ($O(p^{O(n^2)})$).

➡ Can't really compute directly with V_f.

Want algorithms which take time poly in $n \log p$ (not p^n)

Efficient Counting of Composition Factors

Roots of $f \in \mathbb{F}_q[x;p]$ of degree p^n may be in an extension field of high degree ($O(p^{O(n^2)})$).

➡ Can't really compute directly with V_f.

Want algorithms which take time poly in $n \log p$ (not p^n)

Look at the ring structure of $\mathbb{F}_q[x;p]$

$\mathbb{F}_q[x;p]$ is a (non-commutative) ring under the $+$ and $\circ$

Efficient Counting of Composition Factors

Roots of $f \in \mathbb{F}_q[x;p]$ of degree p^n may be in an extension field of high degree ($O(p^{O(n^2)})$).

➡ Can't really compute directly with V_f.

Want algorithms which take time poly in $n \log p$ (not p^n)

Look at the ring structure of $\mathbb{F}_q[x;p]$

$\mathbb{F}_q[x;p]$ is a (non-commutative) ring under the $+$ and $\circ$

- Left (and right) Euclidean ring: LCLM and GCRD operations.
- No unique factorization (but Jordan-Hölder and Krull-Schmidt give a lot of structure to factorizations)
- Fast algorithms for $+$, $\circ$, lclm and gcrd (time $O(n^3 \log^2 q)$).

Efficient Counting of Composition Factors

Roots of $f \in \mathbb{F}_q[x;p]$ of degree p^n may be in an extension field of high degree ($O(p^{O(n^2)})$).

➡ Can't really compute directly with V_f.

Want algorithms which take time poly in $n \log p$ (not p^n)

Example ($\mathbb{F}_{125}[x;5]$ again – a left Euclidean ring)

$$
\begin{aligned}
f &= x^{25} + (3\theta^2 + 4\theta + 2)x^5 + (3\theta^2 + 4\theta + 2)x \\
g &= x^{25} + (3\theta^2 + \theta + 3)x^5 + (4\theta^2 + 2\theta + 2)x \\
f + g &= 2x^{25} + (3\theta^2 + 2\theta + 3)x^5 + (4\theta^2 + 3\theta + 2)x \\
f \circ g &= x^{625} + (4\theta^2 + 2)x^{125} + \cdots + (2\theta^2 + 3\theta + 1)x \\
\mathrm{lclm}(f,g) &= x^{125} + (\theta^2 + 3\theta + 1)x^{25} + (2\theta^2 + 3)x^5 + (2\theta^2 + 2\theta + 3)x \\
\mathrm{gcrd}(f,g) &= x^5 + 3\theta x
\end{aligned}
$$

The Centre of It All

The centre of $\mathbb{F}_q[x;p]$ is also very useful:

$$\text{centre}(\mathbb{F}_q[x;p]) = \mathbb{F}_p[x;q] = \left\{ \sum \alpha_i x^{q^i} \in \mathbb{F}_p[x] \right\}$$

The Centre of It All

The centre of $\mathbb{F}_q[x;p]$ is also very useful:

$$\operatorname{centre}(\mathbb{F}_q[x;p]) = \mathbb{F}_p[x;q] = \left\{ \sum \alpha_i x^{q^i} \in \mathbb{F}_p[x] \right\}$$

$$\cong \mathbb{F}_p[y] \quad \text{the usual (commutative) polynomials!}$$

$$\sum_{0 \leqslant i \leqslant n} \alpha_i x^{q^i} \mapsto \sum_{0 \leqslant i \leqslant n} \alpha_i y^i \qquad \text{for } a_0, \ldots, a_n \in \mathbb{F}_p$$

The Centre of It All

The centre of $\mathbb{F}_q[x;p]$ is also very useful:

$$\begin{aligned}\operatorname{centre}(\mathbb{F}_q[x;p]) = \mathbb{F}_p[x;q] &= \left\{\sum \alpha_i x^{q^i} \in \mathbb{F}_p[x]\right\} \\ &\cong \mathbb{F}_p[y] \quad \text{the usual (commutative) polynomials!}\end{aligned}$$

$$\sum_{0\leqslant i\leqslant n} \alpha_i x^{q^i} \mapsto \sum_{0\leqslant i\leqslant n} \alpha_i y^i \qquad \text{for } a_0, \ldots, a_n \in \mathbb{F}_p$$

A cool trick

Given any $f \in \mathbb{F}_q[x;p]$ we can find a left multiple in the center with $O(n^3 \log^2 q)$ operations in $\mathbb{F}_q$.

The Centre of It All

The centre of $\mathbb{F}_q[x;p]$ is also very useful:

$$\operatorname{centre}(\mathbb{F}_q[x;p]) = \mathbb{F}_p[x;q] = \left\{ \sum \alpha_i x^{q^i} \in \mathbb{F}_p[x] \right\}$$

$$\cong \mathbb{F}_p[y] \quad \text{the usual (commutative) polynomials!}$$

$$\sum_{0 \leqslant i \leqslant n} \alpha_i x^{q^i} \mapsto \sum_{0 \leqslant i \leqslant n} \alpha_i y^i \qquad \text{for } a_0, \ldots, a_n \in \mathbb{F}_p$$

A cool trick

Given any $f \in \mathbb{F}_q[x;p]$ we can find a left multiple in the center with $O(n^3 \log^2 q)$ operations in $\mathbb{F}_q$.

$$f = x^{25} + (3\theta^2 + 4\theta + 2)x^5 + (3\theta^2 + 4\theta + 2)x \in \mathbb{F}_q[x;5]$$

$$f^* = x^{125^2} + 4x^{125} + 3x \in \mathbb{F}_p[x;125]$$

f^* is the minimal central left multiple (mclm) of f

The Centre of It All (2)

Basis of the factoring algorithm in G (1992, 1998):
Factor the minimal central left multiple and take GCRDs:

$$f = x^{25} + (3\theta^2 + 4\theta + 2)x^5 + (3\theta^2 + 4\theta + 2)x \in \mathbb{F}_q[x;5]$$

$$f^* = x^{125^2} + 4x^{125} + 3x \in \mathbb{F}_p[x;125]$$

$$\mapsto y^2 + 4y + 3 = (y+1)(y+3)$$

$$f^* = \underbrace{(x^{125} + x)}_{f_1} \circ \underbrace{(x^{125} + 3x)}_{f_2} = (x^{125} + 3x) \circ (x^{125} + x)$$

$$\left.\begin{array}{r} \gcd(f, f_1) = x^5 + (\theta^2 + 2\theta)x \\ \gcd(f, f_2) = x^5 + 3\theta x \end{array}\right\} \text{ right composition factors of } f$$

Can't completely decompose with this technique...

Decomposition in $\mathbb{F}_q[x;p]$

Theorem (G 1992, 1998)

Given $f = \sum_{0 \leqslant i \leqslant n} a_i x^{p^i} \in \mathbb{F}_q[x]$, can find $g, h \in \mathbb{F}_q[x]$, if they exist, such that $f = g \circ h$. Requires expected time $O(n^4 \log^2 q)$ operations in $\mathbb{F}_q$ (Las Vegas).

Decomposition in $\mathbb{F}_q[x;p]$

Theorem (G 1992, 1998)

Given $f = \sum_{0 \leqslant i \leqslant n} a_i x^{p^i} \in \mathbb{F}_q[x]$, can find $g, h \in \mathbb{F}_q[x]$, if they exist, such that $f = g \circ h$. Requires expected time $O(n^4 \log^2 q)$ operations in $\mathbb{F}_q$ (Las Vegas).

Hardest when minimal central left multiple is irreducible in $\mathbb{F}_p[y]$.

- Construct a finite algebra $\mathcal{A}$ from f, called the *eigenring*; show that zero-divisors in $\mathcal{A}$ yields composition factors of f.
- Show how to find zero divisors in a finite algebra quickly.
- Build very explicit Krull-Schmidt and Jordan-Hölder like decompositions, which show structure of all decompositions

Enter the Eigenring

Decompose an algebra over $\mathbb{F}_q$ associated with f.

Definitions

- Idealizer: $\mathcal{I}_f \subseteq \mathsf{R}$ largest subring in which $\mathsf{R}f$ a two-sided ideal

$$\mathcal{I}_f = \{u \in \mathsf{R} \ : \ fu \in \mathsf{R}f\}$$

- Eigenring: $\mathsf{E}_f = \mathcal{I}_f/\mathsf{R}f$ an associative algebra over $\mathbb{F}_q$

Theorems

- E_f has zero divisors $uv = 0$ iff f is decomposable.
- Zero divisors "split" f: $\gcrd(f, v) \neq 1$.
- E_f has orthogonal idempotents $v^2 = 1, w^2 = 1$ with $v + w = 1$ iff $f = \mathrm{lclm}(f_1, f_2)$, with $\gcrd(f_1, f_2) = 1$
- Can find eigenring with $\tilde{O}(n^3)$ operations in $\mathbb{F}_q$

Detour: Decomposing Associative Algebras over $\mathbb{F}_q$

Describe associative algebra $\mathcal{A}$ by a $\mathbb{F}_q$-basis $\mathfrak{a}_1, \ldots, \mathfrak{a}_\ell \in \mathbb{F}_q^{m \times m}$

- $\mathcal{A} = \langle \mathfrak{a}_1, \ldots, \mathfrak{a}_\ell \rangle \subseteq \mathbb{F}_q^{m \times m}$

How do we

- Find zero-divisors or certify there are none
- If $\mathcal{A}$ semisimple, decompose $\mathcal{A} = \mathcal{A}_1 \oplus \cdots \oplus \mathcal{A}_r$, for $\mathcal{A}_i$ simple
- If $\mathcal{A}$ is simple, find the explicit isomorphism with $\mathbb{F}_{q^\eta}^{s \times s}$

Friedl & Rónyai (1985) show how to do all this in polynomial time (up to factoring polynomials in $\mathbb{F}_p[x]$)

G & Eberly (2000, 2004): "nearly optimal" $O(m^3 \log m + m^2 \ell)$ operations in $\mathbb{F}_q$

- Las Vegas for semisimple algebras over $\mathbb{F}_q$
- Monte Carlo for general algebras over $\mathbb{F}_q$

Detour: Decomposing Associative Algebras over $\mathbb{F}_q$

Density Theorems

Let $\mathcal{A} = \langle \mathfrak{a}_1, \ldots, \mathfrak{a}_\ell \rangle \subseteq \mathbb{F}_q^{n \times n}$ be an associative algebra over $\mathbb{F}_q$, $\mathfrak{a}$ randomly chosen from $\mathcal{A}$, and $f = \mathrm{minpoly}(\mathfrak{a}) \in \mathbb{F}_q[x]$.

- For *any* $\mathcal{A}$ over $\mathbb{F}_q$ with zero divisors,

$$\mathrm{Prob}\Big\{ f \text{ reducible} \Big\} \geqslant 1/9$$

- If $f = f_1 f_2$ then $f_1(a) f_2(a) = 0$, so $f_1(a), f_2(a)$ zero divisors
- When $\mathcal{A}$ is a field, $\mathrm{Prob}\{\deg f = n\} \geqslant 1/4$.

Central Multiples and Frobenius Automorphisms

Theorem (von zur Gathen, G, and Ziegler 2010)

- $f \in \mathbb{F}_q[x;p]$ *squarefree of degree* p^n *with roots* V_f
- $\sigma_q : V_f \to V_f$ *the Frobenius automorphism.*
- $f^* \in \mathbb{F}_p[x;q]$ *be the minimal central left multiple of* f.

$f^* = \sum_{0 \leqslant i \leqslant n} \alpha_i x^{q_i}$ ➡ $f^+ = \sum_{0 \leqslant i \leqslant n} \alpha_i y^i$ *is min poly of* σ_q.

Central Multiples and Frobenius Automorphisms

Theorem (von zur Gathen, G, and Ziegler 2010)

- $f \in \mathbb{F}_q[x;p]$ *squarefree of degree* p^n *with roots* V_f
- $\sigma_q : V_f \to V_f$ *the Frobenius automorphism.*
- $f^* \in \mathbb{F}_p[x;q]$ *be the minimal central left multiple of* f*.*

$f^* = \sum_{0 \leqslant i \leqslant n} \alpha_i x^{q_i}$ ➡ $f^+ = \sum_{0 \leqslant i \leqslant n} \alpha_i y^i$ *is min poly of* σ_q*.*

- ➡ Can find the minimal polynomial of σ_q quickly
- ➡ Can compute the complete rational Jordan form of σ_q
- ➡ Given $f \in \mathbb{F}_q[x;p]$ of degree p^n, we can compute the number of right composition factors of degree p with $O(n^3 \log^2 q)$ operations in $\mathbb{F}_q$.

Back to our example in $\mathbb{F}_{125}[x;5]$

$$
\begin{aligned}
f &= x^{25} + (3\theta^2 + 4\theta + 2)x^5 + (3\theta^2 + 4\theta + 2)x \in \mathbb{F}_q[x;5] \\
f^* &= x^{125^2} + 4x^{125} + 3x \in \mathbb{F}_p[x;125] \\
&= (x^{125} - 4x) \circ (x^{125} - 2x)
\end{aligned}
$$

So $\sigma_q \sim \begin{pmatrix} 4 & 0 \\ 0 & 2 \end{pmatrix}$ and $\begin{cases} \sigma_q \text{ has two eigenvectors} \\ f \text{ has two right factors of degree } 5 \\ h_1 = x^5 + \theta^2 x + 2\theta x,\ h_2 = x^5 + 3\theta x \end{cases}$

Subadditive/Projective Polynomials

Subadditive polynomials: Cohen (1990), Abhyankar (1997):

$$\Psi = \sum_{0 \leqslant i \leqslant n} a_i x^{(p^i-1)/(p-1)} \in \mathbb{F}_q[x] \text{ for } b \neq 0$$

Numerous applications: strong Davenport pairs, difference sets, cryptographically secure sequences, error-correcting codes...

Bluher (2004) showed that $x^{p+1} + ax + b$ has either 0, 1, 2, or $p+1$ roots in $\mathbb{F}_q$. This looks familiar!

Subadditive/Projective Polynomials

Subadditive polynomials: Cohen (1990), Abhyankar (1997):

$$\Psi = \sum_{0 \leqslant i \leqslant n} a_i x^{(p^i-1)/(p-1)} \in \mathbb{F}_q[x] \text{ for } b \neq 0$$

Numerous applications: strong Davenport pairs, difference sets, cryptographically secure sequences, error-correcting codes...

Bluher (2004) showed that $x^{p+1} + ax + b$ has either 0, 1, 2, or $p + 1$ roots in $\mathbb{F}_q$. This looks familiar!

Lemma

Ψ has a root $c \in \mathbb{F}_q$ $\iff$ $\sum a_i x^{p^i} = g \circ (x^p - cx)$ *for* $g \in \mathbb{F}_q[x; p]$

Subadditive/Projective Polynomials

Subadditive polynomials: Cohen (1990), Abhyankar (1997):

$$\Psi = \sum_{0 \leqslant i \leqslant n} a_i x^{(p^i-1)/(p-1)} \in \mathbb{F}_q[x] \text{ for } b \neq 0$$

Numerous applications: strong Davenport pairs, difference sets, cryptographically secure sequences, error-correcting codes...

Bluher (2004) showed that $x^{p+1} + ax + b$ has either 0, 1, 2, or $p + 1$ roots in $\mathbb{F}_q$. This looks familiar!

Lemma

Ψ has a root $c \in \mathbb{F}_q$ $\iff$ $\sum a_i x^{p^i} = g \circ (x^p - cx)$ for $g \in \mathbb{F}_q[x; p]$

Theorem

We can compute the number of roots in $\mathbb{F}_q$ of a subadditive $\Psi \in \mathbb{F}_q[x]$ with $O(n^3 \log^2 q)$ operations in $\mathbb{F}_q$ (even though $\deg \Psi \approx p^{n-1}$).

Inverse Problem – degree p^2 case

- For each possible number of right components, how many additive polynomials of degree n have that many right components?
- Equivalently: how many subadditive polynomials in $\mathbb{F}_q[x]$ have each possible number of roots in $\mathbb{F}_q$?

Inverse Problem – degree p^2 case

- For each possible number of right components, how many additive polynomials of degree n have that many right components?
- Equivalently: how many subadditive polynomials in $\mathbb{F}_q[x]$ have each possible number of roots in $\mathbb{F}_q$?

Bluher (2004): For $f = x^{p^2} + a_1 x^p + a_0 x \in \mathbb{F}_q[x;p]$ $(a_0 \neq 0)$

Right components of degree p	# additive polynomials of degree p^2 with that many right components
0	$\frac{p^2-p}{2} \cdot \frac{q^2-1}{p-1}$
1	$(p-1) \cdot \frac{q^2-q}{p^2-p}$
2	$\frac{(p-1)(p-2)}{2} \cdot \frac{(q-1)^2}{(p-1)^2}$
$p+1$	$(p-1) \cdot \frac{(q-1)(q-p)}{p(p-1)^2(p+1)}$

Inverse Problem – degree p^2 case

- For each possible number of right components, how many additive polynomials of degree n have that many right components?
- Equivalently: how many subadditive polynomials in $\mathbb{F}_q[x]$ have each possible number of roots in $\mathbb{F}_q$?

Bluher (2004): For $f = x^{p^2} + a_1 x^p + a_0 x \in \mathbb{F}_q[x;p]$ $(a_0 \neq 0)$

Right components of degree p	# additive polynomials of degree p^2 with that many right components
0	$\frac{p^2-p}{2} \cdot \frac{q^2-1}{p-1}$
1	$(p-1) \cdot \frac{q^2-q}{p^2-p}$
2	$\frac{(p-1)(p-2)}{2} \cdot \frac{(q-1)^2}{(p-1)^2}$
$p+1$	$(p-1) \cdot \frac{(q-1)(q-p)}{p(p-1)^2(p+1)}$

Get an elementary proof, algorithm for enumeration

Inverse Problem – the degree p^3 case

Von zur Gathen & G (2011): degree p^3 in $\mathbb{F}_q[x;p]$

Right components of degree p	Number of $f \in \mathbb{F}_q[x;p]$ of degree p^3 with specified number of right components
0	$\frac{p^3-p}{3} \cdot \frac{q^3-1}{p^3-1}$
1	$(p-1) \cdot \frac{p^2-p}{2} \cdot \frac{q-1}{p-1} \cdot \frac{q^2-1}{p^2-1} + (p-1) \cdot \frac{q^3-q^2}{p^3-p^2}$
2	$(p-1)(p-2) \cdot \frac{q^2-q}{p^2-p} \cdot \frac{q-1}{p-1}$
3	$\frac{(p-1)(p-2)(p-3)}{6} \cdot \frac{(q-1)^3}{(p-1)^3}$
$p+1$	$(p-1) \cdot \frac{q^2-q}{p^2-p} \cdot \frac{q-p}{p-1} \cdot \frac{1}{p^2}$
$p+2$	$(p-1)(p-2) \cdot \frac{q-1}{p-1} \cdot \frac{(q-1)(q-p)}{p(p-1)^2(p+1)}$
p^2+p+1	$(p-1) \cdot \frac{(q-1)(q-p)(q-p^2)}{(p^3-1)(p^3-p)(p^3-p^2)}$

Indecomposable Additive Polynomials

Indecomposable additive polynomials $f \in \mathbb{F}_q[x;p]$

- σ_q has a single, irreducible Jordan block
- $f^* \in \mathbb{F}_p[y]$ is irreducible of degree n

$$\text{Let} \quad N_p(n) = \sum_{k|n} \mu(n/k) p^k \quad = \quad \begin{cases} \text{\# irreducibles in } \mathbb{F}_p[y] \\ \text{of degree } d \end{cases}$$

Number of indecomposable additive polynomials is then

$$\frac{q^n - 1}{p^n - 1} \cdot N_p(n) \approx \frac{q^n}{n}$$

- Gives a very compact proof of a theorem of Odoni (1999)
- A random additive polynomial of degree p^n in $\mathbb{F}_q[x;p]$ will be indecomposable with probability about $1/n$
- Randomized polynomial-time algorithm for generating.

Maximizing collisions

For $f \in \mathbb{F}_q[x;r]$ of degree p^n, the number of distinct right components of degree p is at most $(p^n - 1)/(p-1)$.

Goal: Generate $f \in \mathbb{F}_q[x;r]$ with this maximal number

- Let $V_f \subseteq \overline{\mathbb{F}}_q$ and $\sigma_q : V_f \to V_f$
- Components maximized when $\sigma = c \cdot \mathrm{Id}$ for some $c \in \mathbb{F}_p$
- Happens when $\mathrm{minpoly}(\sigma) = y - c$

Maximizing collisions

For $f \in \mathbb{F}_q[x;r]$ of degree p^n, the number of distinct right components of degree p is at most $(p^n-1)/(p-1)$.

Goal: Generate $f \in \mathbb{F}_q[x;r]$ with this maximal number

- Let $V_f \subseteq \overline{\mathbb{F}}_q$ and $\sigma_q : V_f \to V_f$
- Components maximized when $\sigma = c \cdot \mathrm{Id}$ for some $c \in \mathbb{F}_p$
- Happens when $\mathrm{minpoly}(\sigma) = y - c$

Algorithm:

- Find right components of $x^q - cx$ of degree p^n
  - all have $(p^n-1)/(p-1)$ distinct right components of degree p
- Cost is $O(n^4)$ operations in $\mathbb{F}_q$

How many maximal collisions?

Count the number of n-dimensional subspaces of V_{f^*} :

$$S(q,p,n) = \frac{(q-1)(q-p)\cdots(q-p^{n-1})}{(p^n-1)(p^n-p)\cdots(p^n-p^{n-1})}$$

assuming $p^{n-1} < q$.

There are $p-1$ non-zero values for $c \in \mathsf{F}_p$ in $f^* = x^q - cx$

Total number of "maximal collision polynomials" is thus:

$$(p-1)\cdot S(q,p,n)$$

Open Questions

- Inverse theory for number of right factors of degree p of any polynomial in $\mathbb{F}_q[x;p]$
- Automatically generate inverse formulas
- Compute number of right factors of any given degree of a polynomial in $\mathbb{F}_q[x;\sigma]$
- Resolve conjecture: how many decompositions possible for a general polynomial?