Algorithms for Additive and Projective Polynomials

Mark Giesbrecht
with
Joachim von zur Gathen and Konstantin Ziegler

University of Waterloo

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

ORCCA
Ontario Research Centre for Computer Algebra

January 20, 2011

Polynomial Composition and Decomposition

Functional Composition

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

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

A (generally) non-distributive operation (but not always):

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

Polynomial Composition and Decomposition

Functional Composition

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

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

A (generally) non-distributive operation (but not always):

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

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 n.

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

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

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 n.

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

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

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

Tame decomposition (mathematically)

- 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 $f(x) = g(h(x))$.

Tame and Wild Decomposition

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

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

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

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

Wild decomposition (mathematically)

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

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

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

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

Wild decomposition (mathematically)

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

Algorithms for Polynomial Decomposition

Barton & Zippel (1982)

Based on factorization of bivariate polynomials

$$f = g \circ h \iff h(x) - h(y) \mid f(x) - f(y)$$

Works as long as you can factor. Potentially exponential time.

Algorithms for Polynomial Decomposition

Barton & Zippel (1982)

Based on factorization of bivariate polynomials

$$f = g \circ h \iff h(x) - h(y) \mid f(x) - f(y)$$

Works as long as you can factor. Potentially exponential time.

Kozen & Landau (1987)

First polynomial-time algorithm for *tame* case. Noticed that the high-order coefficients of f do not depend on (monic) g.

➜ find h, then g.

Algorithms for Polynomial Decomposition

Barton & Zippel (1982)

Based on factorization of bivariate polynomials

$$f = g \circ h \iff h(x) - h(y) \mid f(x) - f(y)$$

Works as long as you can factor. Potentially exponential time.

Giesbrecht & May (2004)

Except for a very special case (Dickson polynomials), easily handled, Barton & Zippel's algorithm *runs in polynomial time!*

Algorithms for Polynomial Decomposition

Barton & Zippel (1982)

Based on factorization of bivariate polynomials

$$f = g \circ h \iff h(x) - h(y) \mid f(x) - f(y)$$

Works as long as you can factor. Potentially exponential time.

Theorem: Fried (1970) – Schur's Conjecture

Let $f \in \mathbb{Q}[x]$ be indecomposable of degree $n > 1$.

- *If n is not an odd prime, then $(f(x) - f(y))/(x - y)$ is absolutely irreducible;*
- *If n is an odd prime, and it is not the case that $f(x) = \alpha D_n(a, x + b) + \beta$ for $\alpha, \beta, a, b \in \mathbb{Q}$, where $a = 0$ if $n = 3$, then $(f(x) - f(y))/(x - y)$ is absolutely irreducible.*

Indecomposability $\Rightarrow$ Dickson or Irreducible (G & May 2005)

Algorithms for Polynomial Decomposition

Barton & Zippel (1982)

Based on factorization of bivariate polynomials

$$f = g \circ h \iff h(x) - h(y) \mid f(x) - f(y)$$

Works as long as you can factor. Potentially exponential time.

Von zur Gathen (1988,1990)

Nearly linear time decomposition in tame case.

Algorithms for Wild Decomposition

Barton & Zippel (1982)

Based on factorization of bivariate polynomials

$$f = g \circ h \iff h(x) - h(y) \mid f(x) - f(y)$$

Works as long as you can factor. Really exponential time.

Algorithms for Wild Decomposition

Barton & Zippel (1982)

Based on factorization of bivariate polynomials

$$f = g \circ h \iff h(x) - h(y) \,|\, f(x) - f(y)$$

Works as long as you can factor. Really exponential time.

Zippel (1991): Polynomial decomposition via Galois theory

If $f = g \circ h$ then there exists a field L such that

$$\mathsf{F}(f(x)) \subsetneq L \subsetneq \mathsf{F}(x),$$

and $L = h(x)$ for some $h \in \mathsf{F}[x]$.

Find subfields by adapting Landau & Miller's (1985) algorithm to find subfields between $\mathbb{Q}$ and $\mathbb{Q}(\alpha)$ (for algebra algebraic α).

- Polynomial time, at least in principle

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.

The Geometry of Additive Polynomials

Denote the set of all additive polynomials over $\mathbb{F}_q$ as

$$\mathbb{F}_q[x;p] = \left\{ a_0 x + a_1 x^p + ... + a_n x^{p^n} \in \mathbb{F}_q[x] \right\}$$

The Geometry of Additive Polynomials

Denote the set of all additive polynomials over $\mathbb{F}_q$ as

$$\mathbb{F}_q[x;p] = \left\{ a_0 x + a_1 x^p + ... + a_n x^{p^n} \in \mathbb{F}_q[x] \right\}$$

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

Denote the set of all additive polynomials over $\mathbb{F}_q$ as

$$\mathbb{F}_q[x;p] = \left\{ a_0x + a_1x^p + ... + a_nx^{p^n} \in \mathbb{F}_q[x] \right\}$$

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

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

The Geometry of Additive Polynomials

Denote the set of all additive polynomials over $\mathbb{F}_q$ as

$$\mathbb{F}_q[x;p] = \left\{ a_0 x + a_1 x^p + \ldots + a_n x^{p^n} \in \mathbb{F}_q[x] \right\}$$

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

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

The Geometry of Additive Polynomials

Denote the set of all additive polynomials over $\mathbb{F}_q$ as
$$\mathbb{F}_q[x;p] = \left\{ a_0 x + a_1 x^p + \ldots + a_n x^{p^n} \in \mathbb{F}_q[x] \right\}$$

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

- f squarefree $\iff f' = a_0 \neq 0$
- Roots V_f of f form an $\mathbb{F}_p$-vector space of $\overline{\mathbb{F}}_q$ of dimension n.
- If W is any $\mathbb{F}_p$-subspace of V_f, and $h \in \overline{\mathbb{F}}_q[x]$ has roots exactly W (i.e., $h(W) = 0$)
  ➡ $h \in \overline{\mathbb{F}}_q[x;p]$ and $\exists g \in \overline{\mathbb{F}}_q[x;p]$ such that $f = g \circ h$.
- If W is also σ_q-invariant, then $h \in \mathbb{F}_q[x;p]$
  σ_q is known as the Frobenius automorphism

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 $f \in \mathbb{F}_q[x;p]$ of degree n, let's 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

Right Composition Factors as EigenVectors of σ_q

Given $f \in \mathbb{F}_q[x; p]$ of degree n, let's 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 $\mathbb{F}_p$

Right Composition Factors as EigenVectors of σ_q

Given $f \in \mathbb{F}_q[x;p]$ of degree n, let's 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:

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

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:

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

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:

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

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

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

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

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

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

$$\begin{pmatrix} \lambda & & \\ & \lambda & \\ & & \mu \end{pmatrix}, \quad \begin{pmatrix} \lambda & & \\ & \mu & \\ & & \nu \end{pmatrix}, \quad \begin{pmatrix} \lambda & \\ & \square \end{pmatrix}, \quad \begin{pmatrix} \square \end{pmatrix}$$

Right Composition Factors as EigenVectors of σ_q (3)

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

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

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

$$
\begin{array}{cccc}
\begin{pmatrix} \lambda & & \\ & \lambda & \\ & & \mu \end{pmatrix}, & \begin{pmatrix} \lambda & & \\ & \mu & \\ & & \nu \end{pmatrix}, & \begin{pmatrix} \lambda & \\ & \boxed{} \end{pmatrix}, & \begin{pmatrix} \boxed{} \end{pmatrix} \\
p+2 & 3 & 1 & 0
\end{array}
$$

Right Composition Factors as EigenVectors of σ_q (3)

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

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

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

$$\underset{p+2}{\begin{pmatrix} \lambda & & \\ & \lambda & \\ & & \mu \end{pmatrix}}, \quad \underset{3}{\begin{pmatrix} \lambda & & \\ & \mu & \\ & & \nu \end{pmatrix}}, \quad \underset{1}{\begin{pmatrix} \lambda & \\ & \boxed{} \end{pmatrix}}, \quad \underset{0}{\begin{pmatrix} \boxed{} \end{pmatrix}}$$

Right Composition Factors as EigenVectors of σ_q (3)

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

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

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

$$\underset{p+2}{\begin{pmatrix} \lambda & & \\ & \lambda & \\ & & \mu \end{pmatrix}}, \underset{3}{\begin{pmatrix} \lambda & & \\ & \mu & \\ & & \nu \end{pmatrix}}, \underset{1}{\begin{pmatrix} \lambda & \\ & \boxed{} \end{pmatrix}}, \underset{0}{\begin{pmatrix} \boxed{} \end{pmatrix}}$$

- 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:

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

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 Krüll 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 Things

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

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

The Centre of Things

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

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

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

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

The Centre of Things

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

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

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

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

A cool trick

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

The Centre of Things

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

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

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

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

A cool trick

Given any $f \in \mathbb{F}_q[x;p]$ we can find a left multiple in the center.
For example (again in $\mathbb{F}_{125}$):

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

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

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

The Centre of Things

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

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

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

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

A cool trick

Given any $f \in \mathbb{F}_q[x;p]$ we can find a left multiple in the center.
For example (again in $\mathbb{F}_{125}$):

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

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

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

The mclm can be found with $O(n^3 \log^2 q)$ operations in $\mathbb{F}_q$

The centre of things (2)

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

$$
\begin{aligned}
f &= x^{25} + (3\theta^2 + 4\theta + 2)x^5 + (3\theta^2 + 4\theta + 2)x \in \mathbb{F}_q[x;5] \\
f^* &= x^{125^2} + 4x^{125} + 3x \in \mathbb{F}_p[x;125] \\
&\mapsto y^2 + 4y + 3 = (y+1)(y+3) \\
f^* &= \underbrace{(x^{125} + x)}_{f_1} \circ \underbrace{(x^{125} + 3x)}_{f_2} = (x^{125} + 3x) \circ (x^{125} + x)
\end{aligned}
$$

$$
\left.
\begin{aligned}
\operatorname{gcrd}(f, f_1) &= x^5 + (\theta^2 + 2\theta)x \\
\operatorname{gcrd}(f, f_2) &= x^5 + 3\theta x
\end{aligned}
\right\} \text{ right composition factors of } f
$$

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

Theorem: (Giesbrecht 1992, 1998)

Given $f = \sum_{0 \leqslant i \leqslant n} a_i x^{p^i} \in \mathbb{F}_q[x]$, we 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).

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

Theorem: (Giesbrecht 1992, 1998)

Given $f = \sum_{0 \leqslant i \leqslant n} a_i x^{p^i} \in \mathbb{F}_q[x]$, we 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 Krüll-Schmidt and Jordan-Hölder like decompositions, which show structure of all decompositions

Central Multiples and Frobenius Automorphisms

Theorem: (von zur Gathen, Giesbrecht, and Ziegler 2010)

Let $f \in \mathbb{F}_q[x;p]$ be squarefree of degree p^n with roots V_f, and let $\sigma_q : V_f \to V_f$ be the Frobenius automorphism.
Let $f^* \in \mathbb{F}_p[x;q]$ be the minimal central left multiple of f.
$f^* = \sum_{0 \leqslant i \leqslant m} \alpha_i x^{q_i} \implies f^+ = \sum_{0 \leqslant i \leqslant m} \alpha_i y^i$ *is min poly of* σ_q.

Central Multiples and Frobenius Automorphisms

Theorem: (von zur Gathen, Giesbrecht, and Ziegler 2010)

Let $f \in \mathbb{F}_q[x;p]$ be squarefree of degree p^n with roots V_f, and let $\sigma_q : V_f \to V_f$ be the Frobenius automorphism.
Let $f^* \in \mathbb{F}_p[x;q]$ be the minimal central left multiple of f.
$f^* = \sum_{0 \leqslant i \leqslant m} \alpha_i x^{q_i} \implies f^+ = \sum_{0 \leqslant i \leqslant m} \alpha_i y^i$ *is min poly of* σ_q.

- We can find the minimal polynomial of σ_q quickly
- With a little more work we can compute the complete rational Jordan form of σ_q
  - We can count the number of eigenvectors/right factors of degree p quickly:
  - 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 $\mathbb{F}_q$.

Central Multiples and Frobenius Automorphisms

Theorem: (von zur Gathen, Giesbrecht, and Ziegler 2010)

Let $f \in \mathbb{F}_q[x;p]$ *be squarefree of degree* p^n *with roots* V_f*, and let* $\sigma_q : V_f \to V_f$ *be the Frobenius automorphism.*
Let $f^* \in \mathbb{F}_p[x;q]$ *be the minimal central left multiple of* f*.*
$f^* = \sum_{0 \leqslant i \leqslant m} \alpha_i x^{q_i} \implies f^+ = \sum_{0 \leqslant i \leqslant m} \alpha_i y^i$ *is min poly of* σ_q*.*

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

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

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

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

Projective Polynomials

Projective polynomials were defined by Abhyankar (1997) as a way of constructing polynomials with specific Galois groups.

$$\Psi_n^{(a,b)} = x^{(p^n-1)/(p-1)} + ax + b \in \mathbb{F}_q[x] \text{ for } b \neq 0$$

They have recently been shown to have numerous applications: strong Davenport pairs, difference sets, cryptographically secure sequences, construction of error-correcting codes...

Projective Polynomials

Projective polynomials were defined by Abhyankar (1997) as a way of constructing polynomials with specific Galois groups.

$$\Psi_n^{(a,b)} = x^{(p^n-1)/(p-1)} + ax + b \in \mathbb{F}_q[x] \text{ for } b \neq 0$$

They have recently been shown to have numerous applications: strong Davenport pairs, difference sets, cryptographically secure sequences, construction of error-correcting codes...

Bluher (2004) showed that for $n = 2$, $\Psi_2^{(a,b)}$ have either 0, 1, 2, or $p + 1$ roots in $\mathbb{F}_q$. This looks familiar!

Projective Polynomials

Projective polynomials were defined by Abhyankar (1997) as a way of constructing polynomials with specific Galois groups.

$$\Psi_n^{(a,b)} = x^{(p^n-1)/(p-1)} + ax + b \in \mathbb{F}_q[x] \text{ for } b \neq 0$$

They have recently been shown to have numerous applications: strong Davenport pairs, difference sets, cryptographically secure sequences, construction of error-correcting codes...

Bluher (2004) showed that for $n = 2$, $\Psi_2^{(a,b)}$ have either 0, 1, 2, or $p + 1$ roots in $\mathbb{F}_q$. This looks familiar!

Lemma

$\Psi_n^{(a,b)}$ *has a root* $c \in \mathbb{F}_q \iff x^{p^n} + ax^p + bx = g \circ (x^p - cx)$.

Projective Polynomials

Projective polynomials were defined by Abhyankar (1997) as a way of constructing polynomials with specific Galois groups.

$$\Psi_n^{(a,b)} = x^{(p^n-1)/(p-1)} + ax + b \in \mathbb{F}_q[x] \text{ for } b \neq 0$$

They have recently been shown to have numerous applications: strong Davenport pairs, difference sets, cryptographically secure sequences, construction of error-correcting codes...

Theorem

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

Inverse Problems

How many additive polynomials of degree n have each possible number of right factors?

Equivalently: how many projective polynomials have each possible number of roots?

Inverse Problems

How many additive polynomials of degree n have each possible number of right factors?

Equivalently: how many projective polynomials have each possible number of roots?

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

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

Inverse Problems

How many additive polynomials of degree n have each possible number of right factors?

Equivalently: how many projective polynomials have each possible number of roots?

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

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

We give an elementary proof and a way to efficiently enumerate all classes

Inverse Problems (2)

We now have a general method to give formulas for the number of additive polynomials with a prescribed number of right factors of degree p.

Inverse Problems (2)

We now have a general method to give formulas for the number of additive polynomials with a prescribed number of right factors of degree p.

Von zur Gathen & Giesbrecht (2011): for $f = x^{p^3} + a_2 x^{p^2} + a_1 x^p + a_0 x \in \mathbb{F}_q[x;p]$

Right factors of degree p	# additive polynomials of degree p^3 with that many right factors
0	$\frac{1}{3}\frac{(p^3-p)(q^3-1)}{p^3-1}$
1	?
2	?
3	$\frac{(p-2)(p-3)(q-1)^3}{(p-1)^2}$
$p+1$	?
$p+2$	$\frac{(q-1)^2(q-p)(p-2)}{(p^2-1)(p^2-p)}$
p^2+p+1	$\frac{(q-1)(q-p)(q-p^2)(p-1)}{(p^3-1)(p^3-p)(p^3-p^2)}$

Conjecture

Consider *any* polynomial $f \in \mathbb{F}_q[x]$ of degree p^2.

Conjecture: f can have either $0, 1, 2, p+1$ decompositions.

Verified in Sage for $p \leqslant 11$.

In fact, we think they all fall into very specific families.

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?