24 Years of Decomposing (Polynomials)

Mark Giesbrecht

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

May 29, 2010

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:

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

Decomposition

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

$$f = x^4 - 2x^3 + 8x^2 - 7x + 5$$
$$g = x^2 + 3x - 5 \quad h = x^2 - x - 2$$

➡ $f = g \circ h$

Ritt (1922) describes all decompositions and "ambiguities".
Generally normalize f, g, h to monic and *original*: $h(0) = 0$

Algorithms for 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. Potentially exponential time

Kozen & Landau (1987)

First polynomial-time algorithm. Notice that the high-order coefficients of f do not depend on (monic) g.

➜ find h, then g.

Works if characteristic p does not divided $\deg h$ (the "tame" case).

von zur Gathen (1988,1990)

Kozen & Landau's equation solving can be recast as Newton iteration. Nearly linear time decomposition in tame case.

Wild Decomposition in Toronto (1987-1992)

Bi-Decomposition

Let F be a field of characteristic p.

$f \in \mathsf{F}[x]$, monic of degree n and r, s with $rs = n$.

Seek monic $g, h \in \mathsf{F}[x]$, $\deg g = r$, $\deg h = s$ and $h(0) = 0$.

Wild Bi-Decomposition: $p \mid r$

Wild decompositions harder to understand and compute

- Ritt's (1922) classification theorems don't hold
- The mathematics becomes incomplete (and impenetrable)
- Decomposition no longer unique
- Fast algorithms no longer work

Wild Decomposition in Toronto (1987-1992)

Bi-Decomposition

Let F be a field of characteristic p.

$f \in \mathsf{F}[x]$, monic of degree n and r, s with $rs = n$.

Seek monic $g, h \in \mathsf{F}[x]$, $\deg g = r$, $\deg h = s$ and $h(0) = 0$.

Wild Bi-Decomposition: $p \mid r$

Wild decompositions harder to understand and compute

- Ritt's (1922) classification theorems don't hold
- The mathematics becomes incomplete (and impenetrable)
- Decomposition no longer unique
- Fast algorithms no longer work
- Basically things are much harder (von zur Gathen 1990b)

Wild Decomposition in Toronto (1987-1992)

Bi-Decomposition

Let F be a field of characteristic p.

$f \in \mathsf{F}[x]$, monic of degree n and r, s with $rs = n$.

Seek monic $g, h \in \mathsf{F}[x]$, $\deg g = r$, $\deg h = s$ and $h(0) = 0$.

Wild Bi-Decomposition: $p \mid r$

Wild decompositions harder to understand and compute

- Ritt's (1922) classification theorems don't hold
- The mathematics becomes incomplete (and impenetrable)
- Decomposition no longer unique
- Fast algorithms no longer work
- Basically things are much harder (von zur Gathen 1990b)

Joachim's perfect topic for an unsuspecting Masters student...

How bad can it be?

How bad can it be?

Really bad

Last refuge of the flailing grad student: show there are too many decompositions to ever compute in polynomial time

How bad can it be?

Really bad

Last refuge of the flailing grad student: show there are too many decompositions to ever compute in polynomial time

Theorem: (G 1988)

Let F *be a field of characteristic* p*. For sufficiently large* n*, there exist polynomials in* $\mathsf{K}[x]$ *of degree* n *with more than* $n^{\log n/(2\log p)}$ *inequivalent decompositions, where* K *is a field extension of* F *degree* $O(n\log n)$*.*

Example

$$f = \sum_{0\le i\le m} a_i x^{p^i} \quad \text{for even } m \text{ and } a_0 \neq 0$$

has at least $p^{m^2/2}$ right composition factors of degree $p^{m/2}$, over its splitting field (of degree $O(mp^m)$).

Additive Polynomials

The "really wild" polynomial $\sum a_i x^{p^i}$ is an example of an additive or linearized polynomial. These polynomials satisfy

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

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, and more general "skew polynomials" were defined explicitly by Ore (1933,1934) and are employed in

- Error correcting codes
- HFE cryptosystems
- Finding simpler and closed form solutions of linear difference and differential equations.

Perhaps there is enough other structure to compute decompositions?

The Additive Years

Standing on the shoulder's of Ore (1933, 1934):

Theorem: (G 1992, 1998)

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

Main idea

- 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 (a polynomial-time one was given by Friedl & Ronyai (1987))
- Build very explicit Krüll-Schmidt and Jordan-Hölder like decompositions, which show structure of all decompositions

The Approximate Years

I moved to London (Ontario) in 1998 and things got fuzzy.

Approximate Decomposition

Given $f \in \mathbb{R}[x]$, does there exist a "small" perturbation $\Delta f \in \mathbb{R}[x]$ such that $f + \Delta f = g \circ h$ for some $g, h \in \mathbb{R}[x]$.

The Approximate Years

I moved to London (Ontario) in 1998 and things got fuzzy.

Approximate Decomposition

Given $f \in \mathbb{R}[x]$, does there exist a "small" perturbation $\Delta f \in \mathbb{R}[x]$ such that $f + \Delta f = g \circ h$ for some $g, h \in \mathbb{R}[x]$.

Iterative Method: Corless, G, Jeffrey and Watt (1999)

If there exists a "small" Δf, then we can (hopefully) find it.

Used an iterative scheme (sort of two coupled Newton iterations)

The Approximate Years

I moved to London (Ontario) in 1998 and things got fuzzy.

Approximate Decomposition

Given $f \in \mathbb{R}[x]$, does there exist a "small" perturbation $\Delta f \in \mathbb{R}[x]$ such that $f + \Delta f = g \circ h$ for some $g, h \in \mathbb{R}[x]$.

Structured Matrix Perturbations: G & May (2005)

Reduction to finding a nearby rank-reduced matrix.

- Back to Barton & Zippel (1985):
  $f(x) = g(h(x))$ if and only if $h(x) - h(y) \mid f(x) - f(y)$
- Unless $f(x)$ is "special" (has a Dickson factor) $f(x)$ indecomposable implies $(f(x) - f(y))/(x - y)$ abs. irreducible
- Ruppert (1998) shows that this is a linear condition. I.e., there is a matrix R_f such that irreducibility is a rank condition

The Approximate Years

I moved to London (Ontario) in 1998 and things got fuzzy.

Approximate Decomposition

Given $f \in \mathbb{R}[x]$, does there exist a “small” perturbation $\Delta f \in \mathbb{R}[x]$ such that $f + \Delta f = g \circ h$ for some $g, h \in \mathbb{R}[x]$.

Structured Matrix Perturbations: G & May (2005)

Two outcomes:

- reduced decomposition to finding a nearby (structured) rank deficient matrix (a well-studied numerical problem)
- show that Barton & Zippel’s (1985) algorithm runs in polynomial time, except when it has Dickson factors, which is easily handled.

The Sparse Years

From 2007–2009 I decomposed sparsely

With Dan Roche (ISSAC'2008, JSC 2010), showed that given

$$f = \sum_{0 \le i \le t} a_i x^{e_i} \in \mathbb{Z}[x]$$

(as a list of coefficients and exponents) can determine if

$$f = g \circ h$$

for some $h \in \mathbb{Z}[x]$, and produce h

Cost is (conjecturally) polynomial in the sparse representation of the input and the output $(t, \log \|f\|_\infty, \log \|g\|_\infty, \log \|h\|_\infty)$

- if $g = x^m$ (perfect powers) then conjecture free and Las Vegas
- recent work with Pascal Koiran may remove conjectures

In 2008 I met Joachim in a bar in Linz

"I have a few questions about your Master's thesis"

Counting Collisions

Von zur Gathen (2009 a,b,c,d) makes great progress towards studying the wild case and estimating *collisions*:

Definition: Compositional Collision

A k-collision of a polynomial $f \in \mathsf{F}[x]$ is a set of k distinct and "inequivalent" pairs $(g_1, h_1), ..., (g_k, h_k)$, with $f = g_i \circ h_i$

Counting Collisions

Von zur Gathen (2009 a,b,c,d) makes great progress towards studying the wild case and estimating *collisions*:

Definition: Compositional Collision

A k-collision of a polynomial $f \in \mathsf{F}[x]$ is a set of k distinct and "inequivalent" pairs $(g_1, h_1), ..., (g_k, h_k)$, with $f = g_i \circ h_i$

Degree p^2 collisions (von zur Gathen, G, Ziegler, 2010)

What is the largest collision we can construct for $\deg f = p^2$?

Reduces to Bluher (2004): The number of roots of a polynomial $x^{p+1} + ax + b \in \mathbb{F}_q[x]$ (q a power of p) for $b \neq 0$ is in $\{0, 1, 2, p + 1\}$.

- Can construct polynomials with $\{0, 1, 2, p + 1\}$ collisions.

  Give a collection of families we conjecture is complete.

Is that all there is?

Counting Collisions of Additive Polynomials

We more completely understand the additive case
(von zur Gathen, G, Ziegler 2010)

Theorem

Given $f = a_0x + a_1x^p + x^{p^2} \in \mathbb{F}_q[x]$ *(q a power of p), the number of distinct right composition factors of* f *of degree* p *is in* $\{0, 1, 2, p+1\}$.

Counting Collisions of Additive Polynomials

We more completely understand the additive case
(von zur Gathen, G, Ziegler 2010)

Theorem

Given $f = a_0 x + a_1 x^p + x^{p^2} \in \mathbb{F}_q[x]$ *(q a power of p), the number of distinct right composition factors of f of degree p is in* $\{0, 1, 2, p+1\}$.

Sketch

Roots of f an $\mathbb{F}_p$-subspace of $\overline{\mathbb{F}_q}$ of dim 2

- Want $\sigma : a \mapsto a^q$ invariant subspaces of dim 1

Can find rational Jordan form of σ in time $(\log p)^{O(1)}$.

$$\begin{array}{cccc} \begin{pmatrix} \gamma & 0 \\ 1 & \delta \end{pmatrix} & \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix} & \begin{pmatrix} \alpha & 1 \\ 0 & \alpha \end{pmatrix} & \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} \\ 0 & 1 & 2 & p+1 \end{array}$$

Counting Collisions of Additive Polynomials

We more completely understand the additive case
(von zur Gathen, G, Ziegler 2010)

Theorem

Given $f = a_0 x + a_1 x^p + x^{p^2} \in \mathbb{F}_q[x]$ *(q a power of p), the number of distinct right composition factors of f of degree p is in* $\{0, 1, 2, p+1\}$.

We can even say exactly how many additive polynomials have each number of collisions.

Collision size	# additive polynomials with that collision
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	$\frac{(q-1)(q-p)}{p(p^2-1)}$

Counting Collisions of Additive Polynomials (2)

Efficient Algorithms

Given $f = a_0 x + a_1 x^p + \cdots + a_m x^{p^m} \in \mathbb{F}_q[x]$, we can compute

$$\#\left\{(g, h) : \ f = g \circ h \ \ g, h \in \mathbb{F}_q[x], \deg h = p\right\}$$

in time polynomial in m and $\log q$.

Roots of Projective Polynomials

Abhyankar (1998) defines projective polynomials as

$$\Psi = a_0 + a_1 x^{\varphi_p(1)} + a_2 x^{\varphi_p(2)} + \cdots + a_m x^{\varphi_p(m)} \in \mathbb{F}_q[x]$$

where $\phi_p(i) = (p^i - 1)/(p - 1)$.

Projective polynomials arise naturally in many situations:

construction of strong Davenport pairs, difference sets, algebraic combinatorics, m-sequences, coding theory, ...

Counting Collisions of Additive Polynomials (2)

Efficient Algorithms

Given $f = a_0x + a_1x^p + \cdots + a_mx^{p^m} \in \mathbb{F}_q[x]$, we can compute

$$\#\left\{(g,h) :\ f = g \circ h \ \ g,h \in \mathbb{F}_q[x],\ \deg h = p\right\}$$

in time polynomial in m and $\log q$.

Roots of Projective Polynomials

Abhyankar (1998) defines projective polynomials as

$$\Psi = a_0 + a_1x^{\varphi_p(1)} + a_2x^{\varphi_p(2)} + \cdots + a_mx^{\varphi_p(m)} \in \mathbb{F}_q[x]$$

where $\phi_p(i) = (p^i - 1)/(p-1)$.

We can

- compute the number of roots of a projective $\Psi \in \mathbb{F}_q[x]$;
- construct projective $\Psi \in \mathbb{F}_q[x]$ with prescribed # of roots;

in time polynomial in $m = \log \deg \Psi$ and $\log q$.

Decomposing in the future

- Quantify and compute the number and structure of wild collisions of degree p^2, p^3 and beyond
- Bluher-like classification for projective polynomials of arbitrary degree.
- Determining solvability of Galois (monodromy) groups and find subfields of function fields (via an adapted Landau-Miller-like algorithm)
- Rational function decomposition
- Sparse polynomial decomposition

Happy Birthday Joachim!