

Fast Decomposition of Sparse Polynomials

Mark Giesbrecht

Cheriton School of Computer Science
Faculty of Mathematics
University of Waterloo, Canada

Pascal Koiran

ENS de Lyon, CNRS
Université Claude Bernard Lyon 1, LIP
France

Saiyue Lyu

Department of Computer Science
University of British Columbia, Canada

Daniel S. Roche

Computer Science Department
United States Naval Academy, USA

ISSAC 2026 — Oldenburg, Germany
July 2026

Functional Decomposition

$$f(x) = x^{5 \cdot 2^{100}} + 15x^{2^{102} + 2^{47}} + 90x^{3 \cdot 2^{100} + 2^{48}} + 270x^{2^{101} + 3 \cdot 2^{47}} \\ + 405x^{2^{100} + 2^{49}} + 243x^{5 \cdot 2^{47}} + 1$$

$$\begin{aligned} \text{decompose}(f) &\Rightarrow g(h(x)) = g \circ h \\ &\Rightarrow \underbrace{(x^5 + 1)}_g \circ \underbrace{(x^{2^{100}} + 3x^{2^{47}})}_h. \end{aligned}$$

Dense versus sparse cost

Dense decomposition is essentially polynomial in $\deg f$. Here $\deg f = 5 \cdot 2^{100}$, while f has **7** non-zero terms.

Sparse complexity goal

Complexity polynomial in the sparse sizes of the input and output:

$$(\tau(f) + \tau(h) + \deg g + \log \deg f)^{O(1)}.$$

Sparse Decomposition Problem

Given sparse $f \in \mathbb{F}[x]$ and $n = rs = \deg f$, compute

$$f = g \circ h, \quad \deg g = r, \quad \deg h = s,$$

with h represented sparsely.

Structural bounds

Zannier's theorem gives, in characteristic $p = 0$ and $p > \deg f$

$$\deg g \leq 2\tau(f)(\tau(f) + 1),$$

and bounds $\tau(h)$ by a function depending only on $\tau(f)$.

Known explicit bounds (Dona, 2015)

$$\tau(h) \leq \left(2^{(2\tau(f))^{16(2\tau(f))\tau(f)}} \right)^{5 \left(2^{(2\tau(f))^{16(2\tau(f))\tau(f)}} \right)^2}$$

Our algorithms sensitive to $\tau(h)$, not this bound!

Our decomposition algorithm is output-sensitive in $\tau(h)$.

SparseDecomp: Cost Statement

The decomposable case

Let $f \in F[x]$ be sparse, $n = rs = \deg f$, and suppose

$$f = g \circ h, \quad \deg g = r, \quad \deg h = s,$$

with h sparse. Assume $\text{char } F = 0$, or $\text{char } F \nmid r$ with the p -adic root routine used in small characteristic.

$$O\left(\tau(f)\tau(h) + r(\tau(f) + \tau(h)) \log n + r \log^2 r\right) \text{ operations in } F$$

- $\tau(f)\tau(h)$ for the sparse modular root.
- $r(\tau(f) + \tau(h)) \log n$ for sparse evaluations.
- $r \log^2 r$ for interpolation of g .

Reversal Reduces Decomposition to a Root

Normalize f, g, h so that f and h are monic and $h(0) = 0$.

Define the reversals

$$\tilde{f}(x) = x^n f(1/x), \quad \tilde{h}(x) = x^s h(1/x).$$

If $f = g \circ h$, then

$$\tilde{f} \equiv \tilde{h}^r \pmod{x^s}$$

using only the top s coefficients of f .

Reduction used by SparseDecomp

- 1 Compute $\tilde{h} = \tilde{f}^{1/r} \bmod x^s$ with $\tilde{h}(0) = 1$.
- 2 Reverse $\tilde{h}$ to recover h .
- 3 Recover g from evaluations $g(h(\alpha)) = f(\alpha)$.

The root computation is performed term by term in sparse form.

SparseModRoot: Residual Equation

Suppose

$$v \equiv u^r \pmod{x^s}, \quad u(0) = v(0) = 1.$$

The logarithmic derivative gives

$$v'u - rvu' \equiv 0 \pmod{x^{s-1}}.$$

Let the current truncation be

$$u_{<m} = 1 + \cdots, \quad u = u_{<m} + u_m x^m + \cdots,$$

and set $R = v'u_{<m} - rvu'_{<m}$. Then

$$\text{ord } R = m - 1, \quad \text{tcoeff}(R) = rm \, u_m.$$

$$u_m = \frac{1}{rm} \text{tcoeff}(R)$$

Sparse update

The exponent m and coefficient u_m are read from the first non-zero term of the residual. Each loop appends one non-zero term of u .

Small Characteristic: Why SparseModRootP is Needed

Over $\mathbb{F}_p$, the update

$$u_m = (rm)^{-1} \text{tcoeff}(R)$$

is not valid when $p \mid m$.

Work in a short lift

Set

$$\ell = 1 + \lfloor \log_p(s-1) \rfloor, \quad p^\ell \geq s,$$

lift v to $\hat{v} \in (\mathbb{Z}/p^\ell\mathbb{Z})[x]$, and run the residual loop in the lifted ring.

If $m = p^k m_0$ with $p \nmid m_0$, then in the lift

$$\text{tcoeff}(R) = r p^k m_0 u_m.$$

The division by p^k is exact for the lifted root.

$$u_m \equiv r^{-1} \frac{\text{tcoeff}(R)/p^k}{m_0} \pmod{p^{\ell-k}}, \quad \text{then reduce mod } p.$$

SparseModRootP

Input: $v \in \mathbb{F}_p[x]$, $v(0) = 1$, and $r, s \in \mathbb{N}$ with $p \nmid r$

Output: $u \in \mathbb{F}_p[x]$, $\deg u < s$, such that $u^r \equiv v \pmod{x^s}$

$\ell \leftarrow 1 + \lfloor \log_p(s-1) \rfloor$

Lift v to $\hat{v} \in (\mathbb{Z}/p^\ell\mathbb{Z})[x]$ and reduce $\hat{v} \pmod{x^s}$

$\hat{d} \leftarrow \hat{v}'$; $u \leftarrow 1$; $R \leftarrow \hat{d}$

while $R \neq 0$ and $\text{ord } R < s-1$ **do**

$m \leftarrow \text{ord}(R) + 1$

$a \leftarrow r^{-1} \text{tcoeff}(R) \pmod{p^\ell}$

$k \leftarrow v_p(m)$; $m_0 \leftarrow m/p^k$

$a \leftarrow a/p^k$; // exact division

$u_m \leftarrow a m_0^{-1} \pmod{p^{\ell-k}}$

$u \leftarrow u + u_m x^m$

$R \leftarrow R + \hat{d} u_m x^m - r \hat{v} u_m x^{m-1}$

end

return $u \pmod{p}$ and $\pmod{x^s}$

Algorithm: SparseModRootP

$O(\tau(v)\tau(u))$ operations in $\mathbb{Z}/p^\ell\mathbb{Z}$, $\ell = 1 + \lfloor \log_p(s-1) \rfloor$.

SparseModRootP: Correctness and Cost

Correctness invariant

At the start of each iteration, u is the truncation of the unique lifted r th root of v up to the next non-zero term.

One iteration

The leading term of

$$R = \hat{v}'u - r\hat{v}u'$$

gives the next exponent m and the next coefficient u_m , including the exact p^k division when $m = p^k m_0$.

Sparse residual update

$$R \leftarrow R + \hat{d} u_m x^m - r\hat{v} m u_m x^{m-1}.$$

This is a sum of shifted copies of $\hat{v}$ and $\hat{d}$.

No dense power series is formed.

SparseDecomp

Input: sparse $f \in \mathbb{F}[x]$, $r, s \in \mathbb{N}$ with $n = rs = \deg f$
Output: $g, h \in \mathbb{F}[x]$ with $f = g \circ h$, or evidence against this r
 $a \leftarrow \text{coeff}(f, n)$; $f \leftarrow f/a$
Form $\tilde{f} \equiv x^n f(1/x) \bmod x^s$
 $u \leftarrow \text{SparseModRoot or SparseModRootP}(\tilde{f}, r, s)$
 $h \leftarrow x^s u(1/x)$; //reverse u
Choose $\alpha_0, \dots, \alpha_r \in \mathbb{S}$ until $h(\alpha_i)$ are distinct
for $i = 0$ **to** r **do**
 $y_i \leftarrow h(\alpha_i)$; $z_i \leftarrow f(\alpha_i)$
end
Interpolate g of degree $\leq r$ satisfying $g(y_i) = z_i$
Test $f(\beta) = g(h(\beta))$ at fresh random β 's
if a test fails **then**
 return "not decomposable with this r "
end
 $g \leftarrow a g$
return g, h

Algorithm: SparseDecomp

Interpolation and Verification of g

After the root step, h is known. The remaining step is dense interpolation in degree r .

Evaluation data

Choose $r + 1$ points such that the values $h(\alpha_i)$ are distinct:

$$y_i = h(\alpha_i), \quad z_i = f(\alpha_i) = g(y_i).$$

Interpolate the unique polynomial g of degree at most r satisfying $g(y_i) = z_i$.

Composition test

Check

$$f(\beta) = g(h(\beta))$$

at fresh random points. A failed test rejects the candidate right factor for the chosen r .

$$O\left(\tau(f)\tau(h) + r(\tau(f) + \tau(h)) \log n + r \log^2 r\right)$$

Example

Here $n = 5 \cdot 2^{100}$, $r = 5$, $s = 2^{100}$.

$$\begin{aligned} f(x) = & x^{5 \cdot 2^{100}} + 15x^{2^{102} + 2^{47}} + 90x^{3 \cdot 2^{100} + 2^{48}} \\ & + 270x^{2^{101} + 3 \cdot 2^{47}} + 405x^{2^{100} + 2^{49}} + 243x^{5 \cdot 2^{47}} + 1. \end{aligned}$$

Example

Here $n = 5 \cdot 2^{100}$, $r = 5$, $s = 2^{100}$.

$$\begin{aligned} f(x) = & x^{5 \cdot 2^{100}} + 15x^{2^{102} + 2^{47}} + 90x^{3 \cdot 2^{100} + 2^{48}} \\ & + 270x^{2^{101} + 3 \cdot 2^{47}} + 405x^{2^{100} + 2^{49}} + 243x^{5 \cdot 2^{47}} + 1. \end{aligned}$$

Let $d = s - 2^{47} = 2^{100} - 2^{47}$. Modulo x^s ,

$$\begin{aligned} \widetilde{f} &= x^n f(1/x) \\ &\equiv 1 + 15x^d \\ &\equiv (1 + 3x^d)^5. \end{aligned}$$

Example

Here $n = 5 \cdot 2^{100}$, $r = 5$, $s = 2^{100}$.

$$\begin{aligned} f(x) = & x^{5 \cdot 2^{100}} + 15x^{2^{102} + 2^{47}} + 90x^{3 \cdot 2^{100} + 2^{48}} \\ & + 270x^{2^{101} + 3 \cdot 2^{47}} + 405x^{2^{100} + 2^{49}} + 243x^{5 \cdot 2^{47}} + 1. \end{aligned}$$

Let $d = s - 2^{47} = 2^{100} - 2^{47}$. Modulo x^s ,

$$\begin{aligned} \tilde{f} &= x^n f(1/x) \\ &\equiv 1 + 15x^d \\ &\equiv (1 + 3x^d)^5. \end{aligned}$$

$$\text{SparseModRoot}(\tilde{f}, 5, s) = 1 + 3x^d,$$

$$h(x) = x^s u(1/x) = x^{2^{100}} + 3x^{2^{47}},$$

$$g(x) = x^5 + 1.$$

Decomposability $\Rightarrow$ Indecomposability



Indecomposability Problem

Root step for every r

For r prime to $\text{char } F$, the congruence

$$\tilde{h}^r \equiv \tilde{f} \pmod{x^s}, \quad \tilde{h}(0) = 1,$$

has a unique power-series solution.

If f is indecomposable, the recovered h may be very large (dense)

No proven sparsity cutoff

A rule such as “stop when $\tau(h) > C\tau(f)$ ” would need a concrete theorem bounding true right factors. The available Zannier bounds are not useful as stopping criteria.



1 striker shoots 1 ball at 1 goalie.
Does the goalie stop it?



1 striker shoots 100 balls at 100 goalies.
How many goalies stop a ball?



1 striker shoots 100 balls at 100 goalies.
How many goalies stop a ball?

On average: $\approx 100(1 - \frac{1}{e}) \approx \mathbf{63}$

Value set sizes

Goal: Given f , guess whether f is decomposable.

Definition: Value Set of $f \in F[x]$

The set of evaluations of f : $\{f(a) : a \in F\}$

Expected value set sizes

- For random f : $(1 - \frac{1}{e})\#F$
- For random *decomposable* f : ...



1 striker shoots 100 balls at 100 goalies.
Each goalie who makes a stop, returns 1 ball to the striker.
How many goalies stop a ball **in the second round**?



1 striker shoots 100 balls at 100 goalies.
Each goalie who makes a stop, returns 1 ball to the striker.
How many goalies stop a ball **in the second round**?

On average: $\approx 100(1 - e^{-63/100}) \approx \mathbf{47}$

Collision Counts Over $\mathbb{F}_q$

Sample distinct $a, b \in \mathbb{F}_q$ and compare $f(a)$ and $f(b)$.

Random monic polynomial

For a random monic dense polynomial f of degree at least 2,

$$\Pr[f(a) = f(b)] = \frac{1}{q}.$$

Random composition

If $f = g \circ h$ with random monic g, h of degrees at least 2, then a collision can occur first through h , or later through g :

$$\Pr[f(a) = f(b)] = \frac{1}{q} + \frac{q-1}{q} \cdot \frac{1}{q} = \frac{2q-1}{q^2}.$$

In this random dense model, decompositions give almost twice as many pair collisions.

What the Test Does Not Prove

The test gives statistical evidence, not a certificate.

Current limitations

- 1 The exact probability calculation is for **random dense** polynomials.
- 2 Pair collision events are not independent over a sample set.
- 3 Counterexamples exist!
For instance, if g or h is a *permutation polynomial*.

Use over $\mathbb{Q}[x]$?

One practical approach is to reduce modulo several small primes and apply the collision test over finite fields.

Maybe this works? We have no proof.

Conclusions: What we have

SparseModRoot and SparseModRootP

The congruence

$$\tilde{f} \equiv \tilde{h}^r \pmod{x^s}$$

is solved by a residual equation. The lifted version handles small characteristic when $\text{char } F \nmid r$.

SparseDecomp

Given a sparse decomposable f and the degree r of g , the algorithm reconstructs h from a sparse modular root and then interpolates g .

$$O\left(\tau(f)\tau(h) + r(\tau(f) + \tau(h)) \log n + r \log^2 r\right)$$

MonteCarloDecompTest

Given any $f \in F[x]$, this **heuristic** guesses whether f is decomposable using $O(\sqrt{\#F})$ random evaluations.

Conclusions: Open Questions

- Can the $O(\tau(f)\tau(h))$ root step be made quasi-linear?
- Is there a rigorous sparse, sub-degree test for indecomposability?
- Can permutation-polynomial cases be isolated, for example through Dickson-polynomial structure?
- Can $f = g \circ h$ be verified without expanding the composition?
- Can sparsity bounds be sharpened enough to justify early stopping?

Sparse decomposition is fast when decomposable.
Decomposability testing is still open!