Reconstruction algorithms for sums of affine powers

Specfun seminar - Paris 05-2018

Ignacio Garcia-Marco, Pascal Koiran, **Timothée Pecatte**

Contents

Motivation: algebraic complexity

Introduction

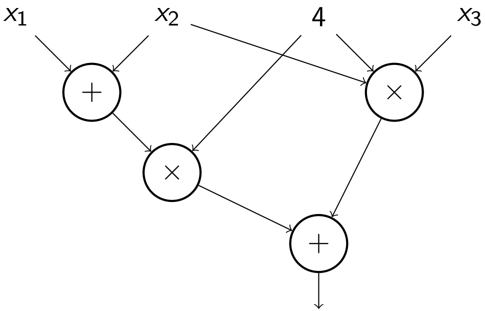
- Objects studied: families of polynomials over a field $\mathbb{F}$.

Introduction

- Objects studied: families of polynomials over a field $\mathbb{F}$.
- Meta-Question: is a polynomial f "hard" to compute ?

Introduction

- Objects studied: families of polynomials over a field $\mathbb{F}$.
- Meta-Question: is a polynomial f "hard" to compute ?
- Models: formula, straight-line programs, circuits, ...



- Objects studied: families of polynomials over a field $\mathbb{F}$.
- Meta-Question: is a polynomial f "hard" to compute ?
- Models: formula, straight-line programs, circuits, ...

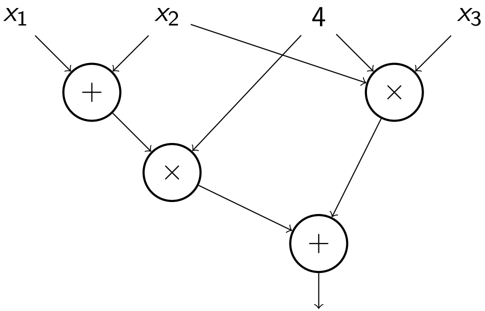


Figure: Circuit computing the polynomial $4(x_1 + x_2) + 4x_2x_3$.

- Objects studied: families of polynomials over a field $\mathbb{F}$.
- Meta-Question: is a polynomial f "hard" to compute ?
- Models: formula, straight-line programs, circuits, ...

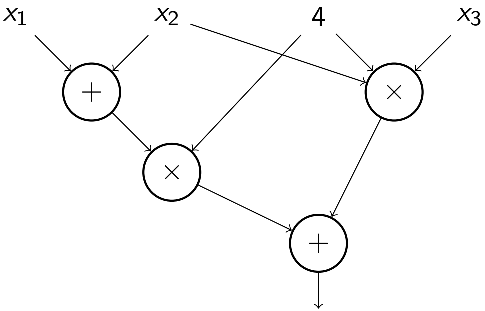


Figure: Circuit computing the polynomial $4(x_1 + x_2) + 4x_2x_3$.

- Hardness in the case of circuits: *depth* and *size*.

Complexity classes

Complexity classes

Definition (VP)

The class VP consists of all families of polynomials $\{f_n\}$ such that:

- arithmetic circuits of polynomial size compute f_n,
- the number of variables and the degree are $n^{O(1)}$.

Complexity classes

Definition (VP)

The class VP consists of all families of polynomials $\{f_n\}$ such that:

- arithmetic circuits of polynomial size compute f_n,
- the number of variables and the degree are $n^{O(1)}$.

Example

$$\mathrm{DET}_n(X) = \sum_{\sigma \in S_n} \mathrm{sgn}(\sigma) \prod_{i=1}^{n} x_{i,\sigma(i)}$$

Definition (VNP)

The class VNP consists of all families of polynomials $\{f_n\}$ such that there exists a family $\{g_n\}$ in VP with:

$$f_n(x_1,\dots,x_{k(n)}) = \sum_{w\in\{0,1\}^{p(n)}} g_{p(n)}\left(x_1,\dots,x_{k(n)},\quad w_1\dots,w_{p(n)}\right)$$

Definition (VNP)

The class VNP consists of all families of polynomials $\{f_n\}$ such that there exists a family $\{g_n\}$ in VP with:

$$f_n(x_1,\ldots,x_{k(n)}) = \sum_{w\in\{0,1\}^{p(n)}} g_{p(n)}\left(x_1,\ldots,x_{k(n)},\;\; w_1\ldots,w_{p(n)}\right)$$

Example

$$\mathrm{PERM}_n(X) = \sum_{\sigma\in S_n}\prod_{i=1}^{n} x_{i,\sigma(i)}$$

Definition (VNP)

The class VNP consists of all families of polynomials $\{f_n\}$ such that there exists a family $\{g_n\}$ in VP with:

$$f_n(x_1, \ldots, x_{k(n)}) = \sum_{w \in \{0,1\}^{p(n)}} g_{p(n)}\left(x_1, \ldots, x_{k(n)}, \quad w_1 \ldots, w_{p(n)}\right)$$

Example

$$\mathrm{PERM}_n(X) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} x_{i,\sigma(i)}$$

PERM is VNP-complete.

Models of interest

Let $\mathbb{F}$ be any characteristic zero field. We consider f an **univariate** polynomial with **coefficients in $\mathbb{F}$**, this is, $f \in \mathbb{F}[x]$.

Let $\mathbb{F}$ be any characteristic zero field. We consider f an **univariate** polynomial with **coefficients in $\mathbb{F}$**, this is, $f \in \mathbb{F}[x]$.

Model (Univariate $\Sigma \wedge \Sigma$)

$$\sum_{i=1}^{k} \alpha_i (x - a_i)^{e_i} \quad \text{with } \alpha_i, a_i \in \mathbb{F}$$

Let $\mathbb{F}$ be any characteristic zero field. We consider f an **univariate** polynomial with **coefficients in $\mathbb{F}$**, this is, $f \in \mathbb{F}[x]$.

Model (Univariate $\Sigma \wedge \Sigma$)

$$\sum_{i=1}^{k} \alpha_i (x - a_i)^{e_i} \quad \text{with } \alpha_i, a_i \in \mathbb{F}$$

A polynomial can be written in many ways in this model, for example $f = 10x^4 + 20x^2 + 2 \in \mathbb{R}[x]$ can be written as:

$$f = \; 10\,(x-0)^4 \; + \; 20\,(x-0)^2 \; + \; 2\,(x-0)^0 =$$

Sums of affine powers

Let $\mathbb{F}$ be any characteristic zero field. We consider f an **univariate** polynomial with **coefficients in $\mathbb{F}$**, this is, $f \in \mathbb{F}[x]$.

Model (Univariate $\Sigma \wedge \Sigma$)

$$\sum_{i=1}^{k} \alpha_i (x - a_i)^{e_i} \quad \text{with } \alpha_i, a_i \in \mathbb{F}$$

A polynomial can be written in many ways in this model, for example $f = 10x^4 + 20x^2 + 2 \in \mathbb{R}[x]$ can be written as:

$$\begin{aligned} f &= 10\,(x-0)^4 + 20\,(x-0)^2 + 2\,(x-0)^0 = \\ &= (x+1)^5 - (x-1)^5 \end{aligned}$$

Associated measure

For $f \in \mathbb{F}[x]$,

Definition

$$\mathrm{AffPow}_{\mathbb{K}}(f) := \min\left\{ k : f(x) = \sum_{i=1}^{k} \alpha_i (x - a_i)^{e_i} \quad \text{with } \alpha_i, a_i \in \mathbb{K} \right\}$$

Associated measure

For $f \in \mathbb{F}[x]$,

Definition

$$\mathrm{AffPow}_{\mathbb{K}}(f) := \min \left\{ k : f(x) = \sum_{i=1}^{k} \alpha_i (x - a_i)^{e_i} \quad \text{with } \alpha_i, a_i \in \mathbb{K} \right\}$$

Example:

For $f = 10x^4 + 20x^2 + 2$ we have that $f(x) = (x+1)^5 - (x-1)^5$, then $\mathrm{AffPow}_{\mathbb{R}}(f) \leq 2$

Associated measure

For $f \in \mathbb{F}[x]$,

Definition

$$\mathrm{AffPow}_{\mathbb{K}}(f) := \min \left\{ k : f(x) = \sum_{i=1}^{k} \alpha_i (x - a_i)^{e_i} \quad \text{with } \alpha_i, a_i \in \mathbb{K} \right\}$$

Example:

For $f = 10x^4 + 20x^2 + 2$ we have that $f(x) = (x+1)^5 - (x-1)^5$, then $\mathrm{AffPow}_{\mathbb{R}}(f) \leq 2$

In fact, $\mathrm{AffPow}_{\mathbb{R}}(f) = 2$.

Related models

Model (Sparsest shift)

$$f(x) = \sum_{i=1}^{s} \alpha_i (x-a)^{e_i}$$

$$f = 10\,(x-0)^4 + 20\,(x-0)^2 + 2\,(x-0)^0$$

Related models

Model (Sparsest shift)

$$f(x) = \sum_{i=1}^{s} \alpha_i (x-a)^{e_i}$$

$$f = 10\,(x-0)^4 + 20\,(x-0)^2 + 2\,(x-0)^0$$

Model (Waring decomposition)

$$f(x) = \sum_{i=1}^{s} \alpha_i (x-a_i)^d \text{ where } d = \deg(f)$$

$f = (x+1)^5 - (x-1)^5$ is not a Waring decomposition!

Goal: reconstruction algorithms

Problem

Given a polynomial $f \in \mathbb{F}[x]$, compute the exact value $s = \mathit{AffPow}_{\mathbb{F}}(f)$ and a decomposition with s terms.

$$f = \sum_{i=0}^{d} f_i x^i \longrightarrow \boxed{\textbf{Algorithm}} \longrightarrow \begin{array}{c} \mathrm{AffPow}(f) = s \\ f = \sum_{i=1}^{s} \alpha_i (x - a_i)^{e_i} \end{array}$$

Structural results

Structural results

Real polynomials

Uniqueness

Theorem (Koiran,Garcia-Marco'15)

Consider a polynomial identity of the form:

$$\sum_{i=1}^{k} \alpha_i (x - a_i)^{e_i} = 0$$

with $(a_i, e_i) \neq (a_j, e_j)$ *for all* $i \neq j$, *and* $\alpha_i \neq 0$.

Theorem (Koiran,Garcia-Marco'15)

Consider a polynomial identity of the form:

$$\sum_{i=1}^{k} \alpha_i (x - a_i)^{e_i} = 0$$

with $(a_i, e_i) \neq (a_j, e_j)$ *for all* $i \neq j$*, and* $\alpha_i \neq 0$*.*

If $d := \max(e_1, \ldots, e_k) \implies k \geq \lceil (d+3)/2 \rceil$*.*

Uniqueness

Theorem (Koiran,Garcia-Marco'15)

Consider a polynomial identity of the form:

$$\sum_{i=1}^{k} \alpha_i (x - a_i)^{e_i} = 0$$

with $(a_i, e_i) \neq (a_j, e_j)$ *for all* $i \neq j$, *and* $\alpha_i \neq 0$.

If $d := \max(e_1, \ldots, e_k) \Longrightarrow k \geq \lceil (d+3)/2 \rceil$.

Corollary

Let $f \in \mathbb{R}[x]$ *be a polynomial of the form* $f = \sum_{i=1}^{s} \alpha_i (x - a_i)^{e_i}$.

Uniqueness

Theorem (Koiran,Garcia-Marco'15)

Consider a polynomial identity of the form:

$$\sum_{i=1}^{k} \alpha_i (x - a_i)^{e_i} = 0$$

with $(a_i, e_i) \neq (a_j, e_j)$ *for all* $i \neq j$, *and* $\alpha_i \neq 0$.

If $d := \max(e_1, \ldots, e_k) \Longrightarrow k \geq \lceil (d+3)/2 \rceil$.

Corollary

Let $f \in \mathbb{R}[x]$ *be a polynomial of the form* $f = \sum_{i=1}^{s} \alpha_i (x - a_i)^{e_i}$.

Define $n_e := \#\{e_i : e_i \leq e\}$.
If $2n_e < \lceil (e+3)/2 \rceil$ *for all* $e \in \mathbb{N}$, *then* $AffPow_{\mathbb{R}}(f) = s$ *and the optimal representation of* f *is unique.*

Real polynomials

- Let $f = (x+1)^d - (x-1)^d + i(x+i)^d - i(x-i)^d \in \mathbb{R}[X]$. $\mathrm{AffPow}_{\mathbb{C}}(f) \leq 4$ but $\mathrm{AffPow}_{\mathbb{R}}(f) = \lfloor (d+1)/4 \rfloor$.

Real polynomials

- Let $f = (x+1)^d - (x-1)^d + i(x+i)^d - i(x-i)^d \in \mathbb{R}[X]$.
  $\mathrm{AffPow}_{\mathbb{C}}(f) \leq 4$ but $\mathrm{AffPow}_{\mathbb{R}}(f) = \lfloor (d+1)/4 \rfloor$.

- Orthogonality of Waring rank and sparsest shift:
  For $f \in \mathbb{R}[X]$,

$$\mathrm{Waring}_{\mathbb{R}}(f) + \mathrm{Sparsest}_{\mathbb{R}}(f) \geq \frac{d+3}{2}$$

  except if $f = \alpha(x-a)^d$.

Real polynomials

- Let $f = (x+1)^d - (x-1)^d + i(x+i)^d - i(x-i)^d \in \mathbb{R}[X]$.
  $\mathrm{AffPow}_{\mathbb{C}}(f) \leq 4$ but $\mathrm{AffPow}_{\mathbb{R}}(f) = \lfloor (d+1)/4 \rfloor$.

- Orthogonality of Waring rank and sparsest shift:
  For $f \in \mathbb{R}[X]$,

$$\mathrm{Waring}_{\mathbb{R}}(f) + \mathrm{Sparsest}_{\mathbb{R}}(f) \geq \frac{d+3}{2}$$

  except if $f = \alpha(x-a)^d$.

- $2\mathrm{Waring}_{\mathbb{R}}(f) \geq \mathrm{Waring}_{\mathbb{R}}(f) + \mathrm{AffPow}_{\mathbb{R}}(f) \geq \frac{d+3}{2}$,
  except if $\mathrm{Waring}_{\mathbb{R}}(f) = \mathrm{AffPow}_{\mathbb{R}}(f)$.

Structural results

Characteristic zero

Uniqueness

Proposition

Consider a polynomial identity of the form:

$$\sum_{i=1}^{k} \alpha_i (x - a_i)^{e_i} = 0$$

with $(a_i, e_i) \neq (a_j, e_j)$ *for all* $i \neq j$*, and* $\alpha_i \neq 0$*.*

Uniqueness

Proposition

Consider a polynomial identity of the form:

$$\sum_{i=1}^{k} \alpha_i (x - a_i)^{e_i} = 0$$

with $(a_i, e_i) \neq (a_j, e_j)$ *for all* $i \neq j$, *and* $\alpha_i \neq 0$.

If $d := \max(e_1, \ldots, e_k) \Longrightarrow k > \sqrt{2(d+1)}$.

Uniqueness

Proposition

Consider a polynomial identity of the form:

$$\sum_{i=1}^{k} \alpha_i (x - a_i)^{e_i} = 0$$

with $(a_i, e_i) \neq (a_j, e_j)$ *for all* $i \neq j$, *and* $\alpha_i \neq 0$.

If $d := \max(e_1, \ldots, e_k) \implies k > \sqrt{2(d+1)}$.

Corollary

Let $f \in \mathbb{F}[x]$ *be a polynomial of the form* $f = \sum_{i=1}^{s} \alpha_i (x - a_i)^{e_i}$.

Uniqueness

Proposition

Consider a polynomial identity of the form:

$$\sum_{i=1}^{k} \alpha_i (x - a_i)^{e_i} = 0$$

with $(a_i, e_i) \neq (a_j, e_j)$ *for all* $i \neq j$, *and* $\alpha_i \neq 0$.

If $d := \max(e_1, \ldots, e_k) \implies k > \sqrt{2(d+1)}$.

Corollary

Let $f \in \mathbb{F}[x]$ *be a polynomial of the form* $f = \sum_{i=1}^{s} \alpha_i (x - a_i)^{e_i}$.

If $2n_e \leq \sqrt{2(e+1)}$ *for all* $e \in \mathbb{N}$, *then* $AffPow_{\mathbb{F}}(f) = s$ *and the optimal representation of* f *is unique.*

An unexpected consequence

Proposition

Let $f \in \mathbb{F}[x]$ be a nonzero polynomial of degree d, then:

$$AffPow_{\mathbb{K}}(f) \leq \left\lceil \frac{d+1}{2} \right\rceil$$

An unexpected consequence

Proposition

Let $f \in \mathbb{F}[x]$ be a nonzero polynomial of degree d, then:

$$AffPow_{\mathbb{K}}(f) \leq \left\lceil \frac{d+1}{2} \right\rceil$$

Corollary

If $f = \sum_{i=1}^{s} \alpha_i (x - a_i)^{e_i} \in \mathbb{F}[x]$, with $s = AffPow_{\mathbb{K}}(f)$. Then,

$$e_i \leq d + \frac{(d+2)^2}{8}$$

An unexpected consequence

Proposition

Let $f \in \mathbb{F}[x]$ be a nonzero polynomial of degree d, then:

$$\mathit{AffPow}_{\mathbb{K}}(f) \leq \left\lceil \frac{d+1}{2} \right\rceil$$

Corollary

If $f = \sum_{i=1}^{s} \alpha_i (x - a_i)^{e_i} \in \mathbb{F}[x]$, with $s = \mathit{AffPow}_{\mathbb{K}}(f)$. Then,

$$e_i \leq d + \frac{(d+2)^2}{8}$$

Proposition

If f is a **generic** *polynomial, then $\mathit{AffPow}_{\mathbb{F}}(f) = \left\lceil \frac{d+1}{2} \right\rceil$*

Characteristic zero

- Let $f = (x+1)^d - dx^{d-1}$. $\mathrm{AffPow}_{\mathbb{C}}(f) = 2$ but $\mathrm{Waring}_{\mathbb{C}}(f) \geq d-1$ and $\mathrm{Sparsest}_{\mathbb{C}}(f) \geq (d+1)/2$.

Characteristic zero

- Let $f = (x+1)^d - dx^{d-1}$. $\mathrm{AffPow}_{\mathbb{C}}(f) = 2$ but $\mathrm{Waring}_{\mathbb{C}}(f) \geq d-1$ and $\mathrm{Sparsest}_{\mathbb{C}}(f) \geq (d+1)/2$.

- Orthogonality of Waring rank and sparsest shift:

$$\mathrm{Waring}_{\mathbb{C}}(f).\mathrm{Sparsest}_{\mathbb{C}}(f) \geq d+1$$

except if $f = \alpha(x-a)^d$.

Characteristic zero

- Let $f = (x+1)^d - dx^{d-1}$. $\mathrm{AffPow}_{\mathbb{C}}(f) = 2$ but $\mathrm{Waring}_{\mathbb{C}}(f) \geq d-1$ and $\mathrm{Sparsest}_{\mathbb{C}}(f) \geq (d+1)/2$.

- Orthogonality of Waring rank and sparsest shift:

$$\mathrm{Waring}_{\mathbb{C}}(f).\mathrm{Sparsest}_{\mathbb{C}}(f) \geq d+1$$

  except if $f = \alpha(x-a)^d$.

- This is tight for

$$f = \sum_{j=1}^{\sqrt{d}} (x+\xi^j)^d = \sqrt{d} \sum_{\substack{0 \leq i \leq d \\ i \equiv 0 \pmod{\sqrt{d}}}} \binom{d}{i} x^{d-i}$$

  where ξ is a $\sqrt{d}$-th primitive root of unity:
  $\mathrm{Waring}_{\mathbb{C}}(f) \leq \sqrt{d}$ and $\mathrm{Sparsest}_{\mathbb{C}}(f) \leq \lceil (d+1)/\sqrt{d} \rceil$.

The tool: Shifted Differential Equations

Shifted differential equations

Definition (SDE)

A SDE(k) is an order k differential equation

$$\sum_{i=0}^{k} P_i(x)\, g^{(i)}(x) = 0$$

where $P_i \in \mathbb{F}[x]$ is a polynomial of degree $\deg P_i \leq i$.

Shifted differential equations

Definition (SDE)

A SDE(k) is an order k differential equation

$$\sum_{i=0}^{k} P_i(x)\, g^{(i)}(x) = 0$$

where $P_i \in \mathbb{F}[x]$ is a polynomial of degree $\deg P_i \leq i$.

Remark

$$f \text{ satisfies an SDE}(k)$$
$$\Updownarrow$$
$$\left\{ x^j f^{(i)}(x) \;:\; 0 \leq i \leq k,\, 0 \leq j \leq i \right\} \text{ is } \mathbb{F}\text{-linearly dependent.}$$

An example

Let $f = x^d + x^{d-1}$. The polynomials:

$$\left.\begin{array}{rcrcr} f & = & x^d & + & x^{d-1} \\ f' & = & d\,x^{d-1} & + & (d-1)\,x^{d-2} \\ x\,f' & = & d\,x^d & + & (d-1)\,x^{d-1} \\ f'' & = & d(d-1)\,x^{d-2} & + & (d-1)(d-2)\,x^{d-3} \\ x\,f'' & = & d(d-1)\,x^{d-1} & + & (d-1)(d-2)\,x^{d-2} \\ x^2 f'' & = & d(d-1)\,x^d & + & (d-1)(d-2)\,x^{d-1} \end{array}\right\}$$

are linearly dependent.

An example

Let $f = x^d + x^{d-1}$. The polynomials:

$$\left.\begin{array}{rcrcr} f & = & x^d & + & x^{d-1} \\ f' & = & d\,x^{d-1} & + & (d-1)\,x^{d-2} \\ x\,f' & = & d\,x^d & + & (d-1)\,x^{d-1} \\ f'' & = & d(d-1)\,x^{d-2} & + & (d-1)(d-2)\,x^{d-3} \\ x\,f'' & = & d(d-1)\,x^{d-1} & + & (d-1)(d-2)\,x^{d-2} \\ x^2 f'' & = & d(d-1)\,x^d & + & (d-1)(d-2)\,x^{d-1} \end{array}\right\}$$

are linearly dependent. Indeed,

$$x^2 f'' - 2(d-1)x\,f' + d(d-1)f = 0,$$

An example

Let $f = x^d + x^{d-1}$. The polynomials:

$$\left.\begin{array}{rcrcr} f & = & x^d & + & x^{d-1} \\ f' & = & d\,x^{d-1} & + & (d-1)\,x^{d-2} \\ x\,f' & = & d\,x^d & + & (d-1)\,x^{d-1} \\ f'' & = & d(d-1)\,x^{d-2} & + & (d-1)(d-2)\,x^{d-3} \\ x\,f'' & = & d(d-1)\,x^{d-1} & + & (d-1)(d-2)\,x^{d-2} \\ x^2 f'' & = & d(d-1)\,x^d & + & (d-1)(d-2)\,x^{d-1} \end{array}\right\}$$

are linearly dependent. Indeed,

$$x^2 f'' - 2(d-1)x\,f' + d(d-1)f = 0,$$

so f satisfies the following SDE(2):

$$x^2 g'' - 2(d-1)xg' + d(d-1)g = 0.$$

Small SDEs

Proposition

If $f(x) = \sum_{i=1}^{s} \alpha_i (x - a_i)^{e_i}$*, then* f *satisfies an* $SDE(2s-1)$*, which is also satisfied by the* $(x - a_i)^{e_i}$*'s.*

Small SDEs

Proposition

If $f(x) = \sum_{i=1}^{s} \alpha_i (x - a_i)^{e_i}$, then f satisfies an SDE$(2s-1)$, which is also satisfied by the $(x - a_i)^{e_i}$'s.

Proof idea:
Define $C_k(f) = \dim \left\{ x^j f^{(i)}(x) \ : \ 0 \le j \le i \le k, \right\}$.

Proposition

If $f(x) = \sum_{i=1}^{s} \alpha_i (x - a_i)^{e_i}$, then f satisfies an SDE$(2s-1)$, which is also satisfied by the $(x - a_i)^{e_i}$'s.

Proof idea:
Define $C_k(f) = \dim \left\{ x^j f^{(i)}(x) \ : \ 0 \leq j \leq i \leq k, \right\}$.

For $f = (x - a)^e$, we have

$$\begin{aligned} \left\{ x^j f^{(i)}(x) \ : \ 0 \leq j \leq i \leq k \right\} &= \left\{ (x-a)^j f^{(i)}(x) \ : \ 0 \leq j \leq i \leq k \right\} \\ &\subseteq \left\{ (x-a)^d \ : \ e - k \leq d \leq e \right\} \end{aligned}$$

Small SDEs

Proposition

If $f(x) = \sum_{i=1}^{s} \alpha_i (x - a_i)^{e_i}$*, then* f *satisfies an* $SDE(2s-1)$*, which is also satisfied by the* $(x - a_i)^{e_i}$*'s.*

Proof idea:

Define $C_k(f) = \dim \left\{ x^j f^{(i)}(x) \ : \ 0 \le j \le i \le k, \right\}$.

For $f = (x-a)^e$, we have

$$\begin{aligned} \left\{ x^j f^{(i)}(x) \ : \ 0 \le j \le i \le k \right\} &= \left\{ (x-a)^j f^{(i)}(x) \ : \ 0 \le j \le i \le k \right\} \\ &\subseteq \left\{ (x-a)^d \ : \ e-k \le d \le e \right\} \end{aligned}$$

Therefore, $C_k(\,(x-a)^e\,) \le k+1$.

Proposition

If $f(x) = \sum_{i=1}^{s} \alpha_i (x - a_i)^{e_i}$, then f satisfies an SDE$(2s-1)$, which is also satisfied by the $(x - a_i)^{e_i}$'s.

Proof idea:

Define $C_k(f) = \dim \left\{ x^j f^{(i)}(x) \ : \ 0 \le j \le i \le k, \right\}$.

For $f = (x-a)^e$, we have

$$\left\{ x^j f^{(i)}(x) \ : \ 0 \le j \le i \le k \right\} = \left\{ (x-a)^j f^{(i)}(x) \ : \ 0 \le j \le i \le k \right\}$$
$$\subseteq \left\{ (x-a)^d \ : \ e-k \le d \le e \right\}$$

Therefore, $C_k(\,(x-a)^e\,) \le k+1$.

It is enough to have

$$s(k+1) < \frac{(k+1)(k+2)}{2}$$

Algorithms

The strategy

Input: $f = \sum_{i=0}^{d} f_i x^i$.

Decomposition wanted: $f(x) = \sum_{i=1}^{s} \alpha_i (x - a_i)^{e_i}$.

The strategy

Input: $f = \sum_{i=0}^{d} f_i x^i$.

Decomposition wanted: $f(x) = \sum_{i=1}^{s} \alpha_i (x - a_i)^{e_i}$.

1. **Find a "small" SDE satisfied by f.**
   Hope that the powers $(x - a_i)^{e_i}$ satisfy the same equation.

The strategy

Input: $f = \sum_{i=0}^{d} f_i x^i$.

Decomposition wanted: $f(x) = \sum_{i=1}^{s} \alpha_i (x - a_i)^{e_i}$.

1. **Find a "small" SDE satisfied by f.**
   Hope that the powers $(x - a_i)^{e_i}$ satisfy the same equation.

2. **Find the solutions of the SDE of the form $(x - a)^e$.**

The strategy

Input: $f = \sum_{i=0}^{d} f_i x^i$.

Decomposition wanted: $f(x) = \sum_{i=1}^{s} \alpha_i (x - a_i)^{e_i}$.

1. **Find a "small" SDE satisfied by f.**
   Hope that the powers $(x - a_i)^{e_i}$ satisfy the same equation.

2. **Find the solutions of the SDE of the form $(x - a)^e$.**

3. **Write f as a linear combination of these solutions**
   (and hope it is the good one)

Step 1

1. **Find a "small" SDE satisfied by f.**
   Hope that the powers $(x - a_i)^{e_i}$ satisfy the same equation.

1. **Find a "small" SDE satisfied by f.**
   Hope that the powers $(x - a_i)^{e_i}$ satisfy the same equation.

Proposition

If $f(x) = \sum_{i=1}^{s} \alpha_i (x - a_i)^{e_i}$, then f satisfies an SDE$(2s-1)$, which is also satisfied by the $(x - a_i)^{e_i}$'s.

Step 1

1. **Find a "small" SDE satisfied by f.**
   Hope that the powers $(x-a_i)^{e_i}$ satisfy the same equation.

Proposition

If $f(x) = \sum_{i=1}^{s} \alpha_i (x-a_i)^{e_i}$, then f satisfies an SDE$(2s-1)$, which is also satisfied by the $(x-a_i)^{e_i}$'s.

So, there is a SDE fulfilling our wishes.

1. **Find a "small" SDE satisfied by f.**
   Hope that the powers $(x - a_i)^{e_i}$ satisfy the same equation.

Proposition

If $f(x) = \sum_{i=1}^{s} \alpha_i (x - a_i)^{e_i}$, then f satisfies an SDE$(2s-1)$, which is also satisfied by the $(x - a_i)^{e_i}$'s.

So, there is a SDE fulfilling our wishes.

Issue:

What if we do not find the 'good' SDE?

2. **Find the solutions of the SDE of the form** $(x-a)^e$.

Step 2

2. **Find the solutions of the SDE of the form** $(x - a)^e$.

$$\sum_{i=0}^{k} P_i(x) g^{(i)}(x) \equiv 0 \tag{1}$$

2. **Find the solutions of the SDE of the form $(x-a)^e$.**

$$\sum_{i=0}^{k} P_i(x) g^{(i)}(x) \equiv 0 \tag{1}$$

For a given $e \in \mathbb{N}$, plug $g = (x-a)^e$ in (1) to obtain:

$$\begin{cases} Q_0(a) = 0 \\ \quad \vdots \\ Q_e(a) = 0 \end{cases} \iff a \in \mathrm{Zeros}(Q_0 \wedge Q_1 \wedge \cdots \wedge Q_e)$$

2. **Find the solutions of the SDE of the form** $(x-a)^e$.

$$\sum_{i=0}^{k} P_i(x) g^{(i)}(x) \equiv 0 \tag{1}$$

For a given $e \in \mathbb{N}$, plug $g = (x-a)^e$ in (1) to obtain:

$$\begin{cases} Q_0(a) = 0 \\ \quad \vdots \\ Q_e(a) = 0 \end{cases} \iff a \in \mathrm{Zeros}(Q_0 \wedge Q_1 \wedge \cdots \wedge Q_e)$$

Some issues:

- How large should e be ?

2. **Find the solutions of the SDE of the form** $(x-a)^e$.

$$\sum_{i=0}^{k} P_i(x) g^{(i)}(x) \equiv 0 \tag{1}$$

For a given $e \in \mathbb{N}$, plug $g = (x-a)^e$ in (1) to obtain:

$$\begin{cases} Q_0(a) = 0 \\ \quad \vdots \\ Q_e(a) = 0 \end{cases} \iff a \in \mathrm{Zeros}(Q_0 \wedge Q_1 \wedge \cdots \wedge Q_e)$$

Some issues:

- How large should e be ? $\Rightarrow$ **solved by the unexpected corollary**

Step 2

❷ **Find the solutions of the SDE of the form** $(x-a)^e$.

$$\sum_{i=0}^{k} P_i(x) g^{(i)}(x) \equiv 0 \tag{1}$$

For a given $e \in \mathbb{N}$, plug $g = (x-a)^e$ in (1) to obtain:

$$\begin{cases} Q_0(a) = 0 \\ \quad \vdots \\ Q_e(a) = 0 \end{cases} \iff a \in \mathrm{Zeros}(Q_0 \wedge Q_1 \wedge \cdots \wedge Q_e)$$

Some issues:

- How large should e be ? $\Rightarrow$ **solved by the unexpected corollary**
- We may obtain some "false positives".

3. **Write f as a linear combination of these solutions**
   (and hope it is the good one)

3. **Write f as a linear combination of these solutions**
   (and hope it is the good one)

We just have to solve a linear system.

Step 3

3. **Write f as a linear combination of these solutions**
   (and hope it is the good one)

We just have to solve a linear system.
If step 1 is good, we know that there is at least one solution.

Step 3

3. **Write f as a linear combination of these solutions**
   (and hope it is the good one)

We just have to solve a linear system.
If step 1 is good, we know that there is at least one solution.

Some issues:

- What if there are several solutions?

3. **Write f as a linear combination of these solutions** (and hope it is the good one)

We just have to solve a linear system.
If step 1 is good, we know that there is at least one solution.

Some issues:

- What if there are several solutions?
- How do we find the "shortest one"?

Distinct nodes

Large exponents

The key lemma

Lemma

Let $f \in \mathbb{F}[x]$ be written as

$$f = \sum_{i=1}^{s} \alpha_i (x - a_i)^{e_i},$$

where the $a_i \in \mathbb{F}$ are **all distinct**. *Whenever f satisfies a SDE(k), if*

$$e_i \text{ is big}$$

then $(x - a_i)^{e_i}$ satisfies the same SDE.

The key lemma

Lemma

Let $f \in \mathbb{F}[x]$ be written as

$$f = \sum_{i=1}^{s} \alpha_i (x - a_i)^{e_i},$$

where the $a_i \in \mathbb{F}$ are **all distinct**. *Whenever f satisfies a SDE(k), if*

$$e_i \geq ks + \binom{s}{2}$$

then $(x - a_i)^{e_i}$ satisfies the same SDE.

An algorithm for large exponents

$$f = \sum_{i=1}^{s} \alpha_i (x - a_i)^{e_i} \quad \text{with distinct } a_i, \quad e_i > \frac{5s^2}{2}$$

An algorithm for large exponents

$$f = \sum_{i=1}^{s} \alpha_i (x - a_i)^{e_i} \quad \text{with distinct } a_i, \quad e_i > \frac{5s^2}{2}$$

a) $\{(x - a_i)^{e_i} \mid 1 \leq i \leq s\}$ is linearly independent,

An algorithm for large exponents

$$f = \sum_{i=1}^{s} \alpha_i (x - a_i)^{e_i} \quad \text{with distinct } a_i, \quad e_i > \frac{5s^2}{2}$$

a) $\{(x - a_i)^{e_i} \mid 1 \leq i \leq s\}$ is linearly independent,

b) $\mathrm{AffPow}_{\mathbb{F}}(f) = s$ and the decomposition is unique,

An algorithm for large exponents

$$f = \sum_{i=1}^{s} \alpha_i (x - a_i)^{e_i} \quad \text{with distinct } a_i, \quad e_i > \frac{5s^2}{2}$$

a) $\{(x - a_i)^{e_i} \mid 1 \leq i \leq s\}$ is linearly independent,

b) $\mathrm{AffPow}_{\mathbb{F}}(f) = s$ and the decomposition is unique,

c) f does not satisfy any $\mathrm{SDE}(r)$ with $r < s$,

An algorithm for large exponents

$$f = \sum_{i=1}^{s} \alpha_i (x - a_i)^{e_i} \quad \text{with distinct } a_i, \quad e_i > \frac{5s^2}{2}$$

a) $\{(x - a_i)^{e_i} \mid 1 \leq i \leq s\}$ is linearly independent,

b) $\mathrm{AffPow}_{\mathbb{F}}(f) = s$ and the decomposition is unique,

c) f does not satisfy any SDE(r) with $r < s$,

d) If f satisfies a SDE(k) with $k \leq 2s - 1$, then so does $(x - a_i)^{e_i}$,

$$f = \sum_{i=1}^{s} \alpha_i (x - a_i)^{e_i} \quad \text{with distinct } a_i, \quad e_i > \frac{5s^2}{2}$$

a) $\{(x - a_i)^{e_i} \mid 1 \leq i \leq s\}$ is linearly independent,

b) $\mathrm{AffPow}_{\mathbb{F}}(f) = s$ and the decomposition is unique,

c) f does not satisfy any SDE(r) with $r < s$,

d) If f satisfies a SDE(k) with $k \leq 2s - 1$, then so does $(x - a_i)^{e_i}$,

e) We have $e_i \leq \deg(f) + (s^2/2)$.

The algorithm

Step 1. Take r the minimum value such that f satisfies a SDE(r) and compute explictly one of these SDE.

The algorithm

Step 1. Take r the minimum value such that f satisfies a SDE(r) and compute explictly one of these SDE.

Step 2. Compute $B = \{(x - b_i)^{d_i} \,|\, 1 \leq i \leq r\}$,
the set of all solutions of the SDE of the form $(x - b)^e$ with $(r + 1)^2/2 \leq e \leq \deg(f) + (r^2/2)$.

The algorithm

Step 1. Take r the minimum value such that f satisfies a SDE(r) and compute explictly one of these SDE.

Step 2. Compute $B = \{(x - b_i)^{d_i} \mid 1 \leq i \leq r\}$,
the set of all solutions of the SDE of the form $(x - b)^e$ with $(r+1)^2/2 \leq e \leq \deg(f) + (r^2/2)$.

Step 3. Determine $\alpha_1, \ldots, \alpha_r$ such that $f = \sum_{i=1}^{r} \alpha_i (x - b_i)^{d_i}$ and outputs the expression.

Step 1. Take r the minimum value such that f satisfies a SDE(r) and compute explictly one of these SDE.

Step 2. Compute $B = \{(x - b_i)^{d_i} \mid 1 \leq i \leq r\}$,
the set of all solutions of the SDE of the form $(x - b)^e$ with $(r + 1)^2/2 \leq e \leq \deg(f) + (r^2/2)$.

Step 3. Determine $\alpha_1, \ldots, \alpha_r$ such that $f = \sum_{i=1}^{r} \alpha_i (x - b_i)^{d_i}$ and outputs the expression.

Lemma

We have $|B| \leq r$ and B is $\mathbb{F}$-linearly independent.

Distinct nodes

Large and small exponents

Weaken the hypothesis

Theorem

Let $f(x) = \sum_{i=1}^{s} \alpha_i (x - a_i)^{e_i}$ *with*

- $a_i \in \mathbb{F}$ *all distinct*
- $n_k \leq (3k/4)^{1/3} - 1$

Then $\mathit{AffPow}(f) = s$ *and there is an polynomial time algorithm for the reconstruction problem.*

Weaken the hypothesis

Theorem

Let $f(x) = \sum_{i=1}^{s} \alpha_i (x - a_i)^{e_i}$ *with*

- $a_i \in \mathbb{F}$ *all distinct*
- $n_k \leq (3k/4)^{1/3} - 1$

Then $AffPow(f) = s$ *and there is an polynomial time algorithm for the reconstruction problem.*

Idea: if there is a **gap** in the exponents sequence, taking the "right" derivative of f make large exponents "appear".

Weaken the hypothesis

Theorem

Let $f(x) = \sum_{i=1}^{s} \alpha_i (x - a_i)^{e_i}$ *with*

- $a_i \in \mathbb{F}$ *all distinct*
- $n_k \leq (3k/4)^{1/3} - 1$

Then $\mathit{AffPow}(f) = s$ *and there is an polynomial time algorithm for the reconstruction problem.*

Idea: if there is a **gap** in the exponents sequence, taking the "right" derivative of f make large exponents "appear".

- Find a SDE(t) satisfied by f.

Weaken the hypothesis

Theorem

Let $f(x) = \sum_{i=1}^{s} \alpha_i (x - a_i)^{e_i}$ *with*

- $a_i \in \mathbb{F}$ *all distinct*
- $n_k \leq (3k/4)^{1/3} - 1$

Then $\mathit{AffPow}(f) = s$ *and there is an polynomial time algorithm for the reconstruction problem.*

Idea: if there is a **gap** in the exponents sequence, taking the "right" derivative of f make large exponents "appear".

- Find a SDE(t) satisfied by f.
- Compute the set of large exponents solutions

Weaken the hypothesis

Theorem

Let $f(x) = \sum_{i=1}^{s} \alpha_i (x - a_i)^{e_i}$ *with*

- $a_i \in \mathbb{F}$ *all distinct*
- $n_k \leq (3k/4)^{1/3} - 1$

Then $\mathit{AffPow}(f) = s$ *and there is an polynomial time algorithm for the reconstruction problem.*

Idea: if there is a **gap** in the exponents sequence, taking the "right" derivative of f make large exponents "appear".

- Find a SDE(t) satisfied by f.
- Compute the set of large exponents solutions
- Reconstruct coefficients of large exponents using the right derivative.

Weaken the hypothesis

Theorem

Let $f(x) = \sum_{i=1}^{s} \alpha_i (x - a_i)^{e_i}$ *with*

- $a_i \in \mathbb{F}$ *all distinct*
- $n_k \leq (3k/4)^{1/3} - 1$

Then AffPow$(f) = s$ *and there is an polynomial time algorithm for the reconstruction problem.*

Idea: if there is a **gap** in the exponents sequence, taking the "right" derivative of f make large exponents "appear".

- Find a SDE(t) satisfied by f.
- Compute the set of large exponents solutions
- Reconstruct coefficients of large exponents using the right derivative.
- Substract them and go on until 0 is found.

The algorithm

Step 1. We take t the minimum value such that f satisfies a SDE(t) and compute explicitly one of these SDE.

The algorithm

Step 1. We take t the minimum value such that f satisfies a SDE(t) and compute explicitly one of these SDE.

Step 2. Consider $B := \{(x - b_i)^{d_i} \mid 1 \leq i \leq l\}$, the set of all the solutions of the SDE of the form $(x - b)^e$, assume that $d_1 \geq d_2 \geq \cdots \geq d_l$.

Step 1. We take t the minimum value such that f satisfies a SDE(t) and compute explicitly one of these SDE.

Step 2. Consider $B := \{(x - b_i)^{d_i} \mid 1 \leq i \leq l\}$, the set of all the solutions of the SDE of the form $(x - b)^e$, assume that $d_1 \geq d_2 \geq \cdots \geq d_l$.

Step 3. We take $r \in \{1, \ldots, l\}$ such that $d_r - d_{r+1} > r^2/2$ and $d_{r+1} < \deg(f)$.

The algorithm

Step 1. We take t the minimum value such that f satisfies a SDE(t) and compute explicitly one of these SDE.

Step 2. Consider $B := \{(x - b_i)^{d_i} \mid 1 \le i \le l\}$, the set of all the solutions of the SDE of the form $(x - b)^e$, assume that $d_1 \ge d_2 \ge \cdots \ge d_l$.

Step 3. We take $r \in \{1, \ldots, l\}$ such that $d_r - d_{r+1} > r^2/2$ and $d_{r+1} < \deg(f)$.

Step 4. We set $j := d_{r+1} + 1$ and write $f^{(j)}$ as $f^{(j)} = \sum_{i=1}^{r} \beta_i \cdot \frac{d_i!}{(d_i-j)!}(x - b_i)^{d_i-j}$ with $\beta_1, \ldots, \beta_r \in \mathbb{F}$.

The algorithm

Step 1. We take t the minimum value such that f satisfies a SDE(t) and compute explicitly one of these SDE.

Step 2. Consider $B := \{(x-b_i)^{d_i} \mid 1 \leq i \leq l\}$, the set of all the solutions of the SDE of the form $(x-b)^e$, assume that $d_1 \geq d_2 \geq \cdots \geq d_l$.

Step 3. We take $r \in \{1, \ldots, l\}$ such that $d_r - d_{r+1} > r^2/2$ and $d_{r+1} < \deg(f)$.

Step 4. We set $j := d_{r+1} + 1$ and write $f^{(j)}$ as $f^{(j)} = \sum_{i=1}^{r} \beta_i \cdot \frac{d_i!}{(d_i-j)!}(x-b_i)^{d_i-j}$ with $\beta_1, \ldots, \beta_r \in \mathbb{F}$.

Step 5. We set $\widetilde{f} := \sum_{i=1}^{r} \beta_i (x-b_i)^{d_i}$ and $h := f - \widetilde{f}$.

Towards repeated nodes.

Small intervals

Let $\delta \in \mathbb{N}$. We aim now at reconstructing expressions of the form

$$f = \sum_{i=1}^{s} \alpha_i (x - a_i)^{e_i}$$

such that whenever $a_i = a_j$, then $|e_i - e_j| \leq \delta$.

Let $\delta \in \mathbb{N}$. We aim now at reconstructing expressions of the form

$$f = \sum_{i=1}^{s} \alpha_i (x - a_i)^{e_i}$$

such that whenever $a_i = a_j$, then $|e_i - e_j| \leq \delta$.

We **rewrite** f as

$$f = \sum_{i=1}^{t} Q_i(x)(x - a_i)^{e_i},$$

where

- Q_i is a polynomial of degree $\leq \delta$, and
- $a_i \neq a_j$ when $i \neq j$.

Repeated nodes: the key lemma

Lemma

Let $\delta \in \mathbb{N}$ and let $f \in \mathbb{F}[x]$ be written as

$$f = \sum_{i=1}^{t} Q_i(x)\,(x - a_i)^{e_i},$$

with distinct $a_i \in \mathbb{F}$ and $\deg(Q_i) \leq \delta$.

Lemma

Let $\delta \in \mathbb{N}$ and let $f \in \mathbb{F}[x]$ be written as

$$f = \sum_{i=1}^{t} Q_i(x)\,(x - a_i)^{e_i},$$

with distinct $a_i \in \mathbb{F}$ and $\deg(Q_i) \leq \delta$.

If f satisfies a $SDE(k)$ and

$$e_i \geq t(k + \delta) + \binom{t}{2},$$

then $Q_i(x)\,(x - a_i)^{e_i}$ satisfies the same SDE.

The algorithm

Let

$$f = \sum_{i=1}^{t} Q_i(x)\,(x - a_i)^{e_i},$$

with $\deg(Q_i) \leq \delta$ and $e_i \geq \frac{t^2(t+1)}{2} + 2t^2(\delta+1)^2.$

Let

$$f = \sum_{i=1}^{t} Q_i(x)\,(x-a_i)^{e_i},$$

with $\deg(Q_i) \leq \delta$ and $e_i \geq \frac{t^2(t+1)}{2} + 2t^2(\delta+1)^2$.

Then, one can compute the **optimal** expression of f as follows:

Step 1. Take r the minimum value such that f satisfies a SDE(r)

The algorithm

Let

$$f = \sum_{i=1}^{t} Q_i(x)\,(x - a_i)^{e_i},$$

with $\deg(Q_i) \leq \delta$ and $e_i \geq \frac{t^2(t+1)}{2} + 2t^2(\delta+1)^2.$

Then, one can compute the **optimal** expression of f as follows:

Step 1. Take r the minimum value such that f satisfies a SDE(r)

Step 2. Compute the set $B = \{g_1, \ldots, g_p\}$ of solutions of the SDE of the form

$$g(x) = R(x)(x - c)^e,$$

with $e < d + \frac{d^2}{8}$, where $\deg(R) \leq \delta$.

Let

$$f = \sum_{i=1}^{t} Q_i(x)\,(x-a_i)^{e_i},$$

with $\deg(Q_i) \leq \delta$ and $e_i \geq \frac{t^2(t+1)}{2} + 2t^2(\delta+1)^2$.

Then, one can compute the **optimal** expression of f as follows:

Step 1. Take r the minimum value such that f satisfies a SDE(r)

Step 2. Compute the set $B = \{g_1, \ldots, g_p\}$ of solutions of the SDE of the form

$$g(x) = R(x)(x-c)^e,$$

with $e < d + \frac{d^2}{8}$, where $\deg(R) \leq \delta$.

Step 3. Write $f = \sum_{i=1}^{p} \lambda_i g_i$ with $\lambda_i \in \mathbb{F}$ and output the expression.

Multivariate reconstruction

Multivariate model

Model (Multivariate AffPow)

$$\sum_{i=1}^{k} \alpha_i \ell_i^{e_i} \quad \text{with } \alpha_i \in \mathbb{F}, \deg(\ell_i) = 1$$

Multivariate model

Model (Multivariate AffPow)

$$\sum_{i=1}^{k} \alpha_i \ell_i^{e_i} \quad \text{with } \alpha_i \in \mathbb{F}, \deg(\ell_i) = 1$$

We will design algorithms in the "black box" setting:

Multivariate model

Model (Multivariate AffPow)

$$\sum_{i=1}^{k} \alpha_i \ell_i^{e_i} \quad \text{with } \alpha_i \in \mathbb{F}, \deg(\ell_i) = 1$$

We will design algorithms in the "black box" setting: they have access to the input polynomial only through an oracle so that for any point $a \in \mathbb{F}^n$, we can obtain $f(a)$ in a single step by querying this oracle. We will use:

- Change of basis

Multivariate model

Model (Multivariate AffPow)

$$\sum_{i=1}^{k} \alpha_i \ell_i^{e_i} \quad \text{with } \alpha_i \in \mathbb{F}, \deg(\ell_i) = 1$$

We will design algorithms in the "black box" setting: they have access to the input polynomial only through an oracle so that for any point $a \in \mathbb{F}^n$, we can obtain $f(a)$ in a single step by querying this oracle. We will use:

- Change of basis
- Solving linear systems

Multivariate model

Model (Multivariate AffPow)

$$\sum_{i=1}^{k} \alpha_i \ell_i^{e_i} \quad \text{with } \alpha_i \in \mathbb{F}, \deg(\ell_i) = 1$$

We will design algorithms in the "black box" setting: they have access to the input polynomial only through an oracle so that for any point $a \in \mathbb{F}^n$, we can obtain $f(a)$ in a single step by querying this oracle. We will use:

- Change of basis
- Solving linear systems
- Factorization

Multivariate model

Model (Multivariate AffPow)

$$\sum_{i=1}^{k} \alpha_i \ell_i^{e_i} \quad \text{with } \alpha_i \in \mathbb{F}, \deg(\ell_i) = 1$$

We will design algorithms in the "black box" setting: they have access to the input polynomial only through an oracle so that for any point $a \in \mathbb{F}^n$, we can obtain $f(a)$ in a single step by querying this oracle. We will use:

- Change of basis
- Solving linear systems
- Factorization
- PIT

Multivariate model

Model (Multivariate AffPow)

$$\sum_{i=1}^{k} \alpha_i \ell_i^{e_i} \quad \text{with } \alpha_i \in \mathbb{F}, \deg(\ell_i) = 1$$

We will design algorithms in the "black box" setting: they have access to the input polynomial only through an oracle so that for any point $a \in \mathbb{F}^n$, we can obtain $f(a)$ in a single step by querying this oracle. We will use:

- Change of basis
- Solving linear systems
- Factorization
- PIT
- Derivatives

Multivariate model

Model (Multivariate AffPow)

$$\sum_{i=1}^{k} \alpha_i \ell_i^{e_i} \quad \text{with } \alpha_i \in \mathbb{F}, \deg(\ell_i) = 1$$

We will design algorithms in the "black box" setting: they have access to the input polynomial only through an oracle so that for any point $a \in \mathbb{F}^n$, we can obtain $f(a)$ in a single step by querying this oracle. We will use:

- Change of basis
- Solving linear systems
- Factorization
- PIT
- Derivatives
- Homogeneous components

Essential variables

$$f(x_1, x_2, x_3) = x_1^3 + x_1^2 x_2 - 2x_1^2 x_3 - 2x_1 x_2 x_3 + x_1 x_3^2 + x_2 x_3^2$$

Essential variables

$$\begin{aligned} f(x_1, x_2, x_3) &= x_1^3 + x_1^2 x_2 - 2x_1^2 x_3 - 2x_1 x_2 x_3 + x_1 x_3^2 + x_2 x_3^2 \\ &= (x_2 + x_3)(x_1 - x_3)^2 + (x_1 - x_3)^3 \end{aligned}$$

Essential variables

$$
\begin{aligned}
f(x_1, x_2, x_3) &= x_1^3 + x_1^2 x_2 - 2x_1^2 x_3 - 2x_1 x_2 x_3 + x_1 x_3^2 + x_2 x_3^2 \\
&= (x_2 + x_3)(x_1 - x_3)^2 + (x_1 - x_3)^3 \\
g(y_1, y_2) &= f(z_1, y_1 + y_2 - z_1, z_1 - y_2) = y_1 y_2^2 + y_2^3
\end{aligned}
$$

Essential variables

$$f(x_1, x_2, x_3) = x_1^3 + x_1^2 x_2 - 2x_1^2 x_3 - 2x_1 x_2 x_3 + x_1 x_3^2 + x_2 x_3^2$$
$$= (x_2 + x_3)(x_1 - x_3)^2 + (x_1 - x_3)^3$$
$$g(y_1, y_2) = f(z_1, y_1 + y_2 - z_1, z_1 - y_2) = y_1 y_2^2 + y_2^3$$

Proposition (Carlini)

For a polynomial $f \in \mathbb{F}[X]$, we have

$$EssVar(f) = \dim_{\mathbb{F}} \left\langle \frac{\partial f}{\partial x_i} \,\middle|\, 1 \leq i \leq n \right\rangle$$

Essential variables

$$
\begin{aligned}
f(x_1, x_2, x_3) &= x_1^3 + x_1^2 x_2 - 2x_1^2 x_3 - 2x_1 x_2 x_3 + x_1 x_3^2 + x_2 x_3^2 \\
&= (x_2 + x_3)(x_1 - x_3)^2 + (x_1 - x_3)^3 \\
g(y_1, y_2) &= f(z_1, y_1 + y_2 - z_1, z_1 - y_2) = y_1 y_2^2 + y_2^3
\end{aligned}
$$

Proposition (Carlini)

For a polynomial $f \in \mathbb{F}[X]$, we have

$$
EssVar(f) = \dim_{\mathbb{F}} \left\langle \frac{\partial f}{\partial x_i} \,|\, 1 \leq i \leq n \right\rangle
$$

Eliminating redundant variables can be done with a randomized polynomial time algorithm [Kayal] $\Rightarrow$ we will assume that f is *regular*.

Essential variables

$$
\begin{aligned}
f(x_1, x_2, x_3) &= x_1^3 + x_1^2 x_2 - 2x_1^2 x_3 - 2x_1 x_2 x_3 + x_1 x_3^2 + x_2 x_3^2 \\
&= (x_2 + x_3)(x_1 - x_3)^2 + (x_1 - x_3)^3 \\
g(y_1, y_2) &= f(z_1, y_1 + y_2 - z_1, z_1 - y_2) = y_1 y_2^2 + y_2^3
\end{aligned}
$$

Proposition (Carlini)

For a polynomial $f \in \mathbb{F}[X]$, we have

$$
EssVar(f) = \dim_{\mathbb{F}} \left\langle \frac{\partial f}{\partial x_i} \,\middle|\, 1 \leq i \leq n \right\rangle
$$

Eliminating redundant variables can be done with a randomized polynomial time algorithm [Kayal] $\Rightarrow$ we will assume that f is *regular*.

$$
\mathrm{EssVar}(f) \leq \mathrm{AffPow}(f)
$$

From reconstruction to polynomial equivalence

Take f such that $\mathrm{EssVar}(f) = \mathrm{AffPow}(f)$, i.e. $f = \sum_{i=1}^{n} \ell_i^{e_i}$.

From reconstruction to polynomial equivalence

Take f such that $\mathrm{EssVar}(f) = \mathrm{AffPow}(f)$, i.e. $f = \sum_{i=1}^{n} \ell_i^{e_i}$.
Set

$$A = \begin{pmatrix} [\ell_1] \\ \vdots \\ [\ell_n] \end{pmatrix}, \qquad b = \begin{pmatrix} \ell_1(0) \\ \vdots \\ \ell_n(0) \end{pmatrix}$$

so that

From reconstruction to polynomial equivalence

Take f such that $\mathrm{EssVar}(f) = \mathrm{AffPow}(f)$, i.e. $f = \sum_{i=1}^n \ell_i^{e_i}$.
Set

$$A = \begin{pmatrix} [\ell_1] \\ \vdots \\ [\ell_n] \end{pmatrix}, \qquad b = \begin{pmatrix} \ell_1(0) \\ \vdots \\ \ell_n(0) \end{pmatrix}$$

so that

$$f(X) = g(A \cdot X + b) \quad \text{with} \quad g = \sum_{i=1}^n x_i^{e_i}$$

From reconstruction to polynomial equivalence

Take f such that $\mathrm{EssVar}(f) = \mathrm{AffPow}(f)$, i.e. $f = \sum_{i=1}^{n} \ell_i^{e_i}$.
Set

$$A = \begin{pmatrix} [\ell_1] \\ \vdots \\ [\ell_n] \end{pmatrix}, \qquad b = \begin{pmatrix} \ell_1(0) \\ \vdots \\ \ell_n(0) \end{pmatrix}$$

so that

$$f(X) = g(A \cdot X + b) \quad \text{with} \quad g = \sum_{i=1}^{n} x_i^{e_i}$$

Definition (Polynomial equivalence)

$$f \sim g \text{ if } f(X) = g(A \cdot X) \text{ with } A \in \mathrm{GL}_n(\mathbb{F})$$

$$f \equiv g \text{ if } f(X) = g(A \cdot X + c) \text{ with } A \in \mathrm{GL}_n(\mathbb{F}), c \in \mathbb{F}^n$$

From reconstruction to polynomial equivalence

Take f such that $\mathrm{EssVar}(f) = \mathrm{AffPow}(f)$, i.e. $f = \sum_{i=1}^{n} \ell_i^{e_i}$.
Set

$$A = \begin{pmatrix} [\ell_1] \\ \vdots \\ [\ell_n] \end{pmatrix}, \qquad b = \begin{pmatrix} \ell_1(0) \\ \vdots \\ \ell_n(0) \end{pmatrix}$$

so that

$$f(X) = g(A \cdot X + b) \quad \text{with} \quad g = \sum_{i=1}^{n} x_i^{e_i}$$

Definition (Polynomial equivalence)

$$f \sim g \textit{ if } f(X) = g(A \cdot X) \textit{ with } A \in \mathrm{GL}_n(\mathbb{F})$$

$$f \equiv g \textit{ if } f(X) = g(A \cdot X + c) \textit{ with } A \in \mathrm{GL}_n(\mathbb{F}), c \in \mathbb{F}^n$$

$$\mathrm{AffPow}(f) = \mathrm{EssVar}(f) \Leftrightarrow f \equiv g \text{ with } g = \sum_{i=1}^{n} x_i^{e_i} \text{ for some } (e_i) \in \mathbb{N}^n$$

The Hessian matrix

$$H_f(X) = \begin{pmatrix} \frac{\partial^2 f}{\partial x_1 \partial x_1} & \cdots & \frac{\partial^2 f}{\partial x_1 \partial x_n} \\ \vdots & \ddots & \vdots \\ \frac{\partial^2 f}{\partial x_n \partial x_1} & \cdots & \frac{\partial^2 f}{\partial x_n \partial x_n} \end{pmatrix}$$

The Hessian matrix

$$H_f(X) = \begin{pmatrix} \frac{\partial^2 f}{\partial x_1 \partial x_1} & \cdots & \frac{\partial^2 f}{\partial x_1 \partial x_n} \\ \vdots & \ddots & \vdots \\ \frac{\partial^2 f}{\partial x_n \partial x_1} & \cdots & \frac{\partial^2 f}{\partial x_n \partial x_n} \end{pmatrix}$$

Lemma (Kayal)

Let $g \in \mathbb{F}[X]$ be an n-variate polynomial. Let $A \in \mathcal{M}_n(\mathbb{F})$ be a linear transformation, and let $b \in \mathbb{F}^n$. Let $f(X) = g(A \cdot X + b)$. Then,

$$H_f(X) = A^T \cdot H_g(A \cdot X + b) \cdot A.$$

The Hessian matrix

$$H_f(X) = \begin{pmatrix} \frac{\partial^2 f}{\partial x_1 \partial x_1} & \cdots & \frac{\partial^2 f}{\partial x_1 \partial x_n} \\ \vdots & \ddots & \vdots \\ \frac{\partial^2 f}{\partial x_n \partial x_1} & \cdots & \frac{\partial^2 f}{\partial x_n \partial x_n} \end{pmatrix}$$

Lemma (Kayal)

Let $g \in \mathbb{F}[X]$ be an n-variate polynomial. Let $A \in \mathcal{M}_n(\mathbb{F})$ be a linear transformation, and let $b \in \mathbb{F}^n$. Let $f(X) = g(A \cdot X + b)$. Then,

$$H_f(X) = A^T \cdot H_g(A \cdot X + b) \cdot A.$$

In particular,

$$\det(H_f(X)) = \det(A)^2 \det(H_g(A \cdot X + b)).$$

Algorithm overview

When $g = \sum_{i=1}^{n} x_i^{e_i}$, we have

$$\frac{\partial^2 g}{\partial x_i \cdot \partial x_j} = \begin{cases} 0 & \text{if } i \neq j, \\ e_i(e_i - 1)x_i^{e_i - 2} & \text{if } i = j \end{cases}$$

Algorithm overview

When $g = \sum_{i=1}^{n} x_i^{e_i}$, we have

$$\frac{\partial^2 g}{\partial x_i \cdot \partial x_j} = \begin{cases} 0 & \text{if } i \neq j, \\ e_i(e_i - 1)x_i^{e_i - 2} & \text{if } i = j \end{cases}$$

$$\det(H_g(X)) = \prod_{i=1}^{n} e_i(e_i - 1)x_i^{e_i - 2}.$$

Algorithm overview

When $g = \sum_{i=1}^{n} x_i^{e_i}$, we have

$$\frac{\partial^2 g}{\partial x_i \cdot \partial x_j} = \begin{cases} 0 & \text{if } i \neq j, \\ e_i(e_i - 1)x_i^{e_i - 2} & \text{if } i = j \end{cases}$$

$$\det(H_g(X)) = \prod_{i=1}^{n} e_i(e_i - 1)x_i^{e_i - 2}.$$

Lemma

Let f be a regular polynomial such that $f(X) = \sum_{i=1}^{n} \ell_i(X)^{e_i}$ where $\ell_1(X), \ldots, \ell_n(X)$ are affine forms and $e_i \geq 2$. Then we have

$$\det(H_f(X)) = c \cdot \prod_{i=1}^{n} \ell_i(X)^{e_i - 2}$$

where $c \in \mathbb{F}$ is a nonzero constant.

Quadratic polynomials

Proposition (Folklore)

Let $\mathbb{F}$ be an algebraically closed field of characteristic different from 2 and let $f, g \in \mathbb{F}[X]$ be homogeneous quadratic polynomials. Then,

$$f \sim g \iff EssVar(f) = EssVar(g).$$

Quadratic polynomials

Proposition (Folklore)

Let $\mathbb{F}$ be an algebraically closed field of characteristic different from 2 and let $f, g \in \mathbb{F}[X]$ be homogeneous quadratic polynomials. Then,

$$f \sim g \iff \mathit{EssVar}(f) = \mathit{EssVar}(g).$$

Theorem

Let $\mathbb{F}$ be an algebraically closed field of characteristic different from 2 and let $f \in \mathbb{F}[X]$ be a polynomial of degree at most 2. Then, there exists a unique $r \in [\![0, n]\!]$ such that

i) $f \equiv \sum_{i=1}^{r} x_i^2$,

ii) $f \equiv \sum_{i=1}^{r} x_i^2 + c$ *with* $c \in \mathbb{F} \setminus \{0\}$, *or*

iii) $f \equiv \sum_{i=1}^{r-1} x_i^2 + x_r$.

Moreover, only one of these three scenarios can hold and $r = \mathit{EssVar}(f)$.

Linear term

If $g = \sum_{i=1}^{n-1} x_i^{e_i} + x_n = h + x_n$ and $f = g(A \cdot X + b)$, then

Linear term

If $g = \sum_{i=1}^{n-1} x_i^{e_i} + x_n = h + x_n$ and $f = g(A \cdot X + b)$, then

$$H_f(X) = (B^T \; \ell^T) \cdot \begin{pmatrix} H_h(A \cdot X + b) & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} B \\ \ell \end{pmatrix} \quad \text{with } A = \begin{pmatrix} B \\ \ell \end{pmatrix}$$

Linear term

If $g = \sum_{i=1}^{n-1} x_i^{e_i} + x_n = h + x_n$ and $f = g(A \cdot X + b)$, then

$$H_f(X) = (B^T \; \ell^T) \cdot \begin{pmatrix} H_h(A \cdot X + b) & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} B \\ \ell \end{pmatrix} \quad \text{with } A = \begin{pmatrix} B \\ \ell \end{pmatrix}$$

$$[H_f(X)]_{k,k} = ([B]_k)^T \cdot H_h(A \cdot X + b) \cdot [B]_k$$

Linear term

If $g = \sum_{i=1}^{n-1} x_i^{e_i} + x_n = h + x_n$ and $f = g(A \cdot X + b)$, then

$$H_f(X) = (B^T \; \ell^T) \cdot \begin{pmatrix} H_h(A \cdot X + b) & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} B \\ \ell \end{pmatrix} \quad \text{with } A = \begin{pmatrix} B \\ \ell \end{pmatrix}$$

$$[H_f(X)]_{k,k} = ([B]_k)^T \cdot H_h(A \cdot X + b) \cdot [B]_k$$

Lemma

Let f be a regular polynomial such that $f(X) = \sum_{i=1}^{n-1} \ell_i(X)^{e_i} + \ell_n(X)$ where $\ell_1, \ldots, \ell_n$ are affine forms. Then there exists an integer $k \in [\![1, n]\!]$ and a nonzero constant c such that

$$\det([H_f(X)]_{k,k}) = c \cdot \prod_{i=1}^{n-1} \ell_i(X)^{e_i - 2}$$

Wrapping up

Theorem

There exists a polynomial-time randomized algorithm that receives as input a blackbox access to a regular polynomial $f \in \mathbb{F}[X]$ *and finds an optimal decomposition of* f *in the Affine Powers model if* $\mathit{AffPow}(f) = n$*, or rejects otherwise.*

Wrapping up

Theorem

There exists a polynomial-time randomized algorithm that receives as input a blackbox access to a regular polynomial $f \in \mathbb{F}[X]$ and finds an optimal decomposition of f in the Affine Powers model if $\mathit{AffPow}(f) = n$, or rejects otherwise.

- Compute blackbox access to $D(X) = \det(H_g(X))$.

Wrapping up

Theorem

There exists a polynomial-time randomized algorithm that receives as input a blackbox access to a regular polynomial $f \in \mathbb{F}[X]$ and finds an optimal decomposition of f in the Affine Powers model if $\mathit{AffPow}(f) = n$, or rejects otherwise.

- Compute blackbox access to $D(X) = \det(H_g(X))$.
- If $D \neq 0$: write $D = c \cdot \prod_{i=1}^{t} \ell_i^{m_i}$ with $t \leq n$.

Wrapping up

Theorem

There exists a polynomial-time randomized algorithm that receives as input a blackbox access to a regular polynomial $f \in \mathbb{F}[X]$ and finds an optimal decomposition of f in the Affine Powers model if $\mathit{AffPow}(f) = n$, or rejects otherwise.

- Compute blackbox access to $D(X) = \det(H_g(X))$.
- If $D \neq 0$: write $D = c \cdot \prod_{i=1}^{t} \ell_i^{m_i}$ with $t \leq n$.
- Build the matrices A and b corresponding to the ℓ_i's, and find a solution X_0 of $A \cdot X = -b$.

Wrapping up

Theorem

There exists a polynomial-time randomized algorithm that receives as input a blackbox access to a regular polynomial $f \in \mathbb{F}[X]$ and finds an optimal decomposition of f in the Affine Powers model if $AffPow(f) = n$, or rejects otherwise.

- Compute blackbox access to $D(X) = \det(H_g(X))$.
- If $D \neq 0$: write $D = c \cdot \prod_{i=1}^{t} \ell_i^{m_i}$ with $t \leq n$.
- Build the matrices A and b corresponding to the ℓ_i's, and find a solution X_0 of $A \cdot X = -b$.
- Set $h(X) = g(X + X_0)$, and write $h = \sum_{i=1}^{t} \alpha_i [\ell_i]^{m_i+2} + [h]_{\leq 2}$.

Wrapping up

Theorem

There exists a polynomial-time randomized algorithm that receives as input a blackbox access to a regular polynomial $f \in \mathbb{F}[X]$ and finds an optimal decomposition of f in the Affine Powers model if $AffPow(f) = n$, or rejects otherwise.

- Compute blackbox access to $D(X) = \det(H_g(X))$.
- If $D \neq 0$: write $D = c \cdot \prod_{i=1}^{t} \ell_i^{m_i}$ with $t \leq n$.
- Build the matrices A and b corresponding to the ℓ_i's, and find a solution X_0 of $A \cdot X = -b$.
- Set $h(X) = g(X + X_0)$, and write $h = \sum_{i=1}^{t} \alpha_i [\ell_i]^{m_i+2} + [h]_{\leq 2}$.
- Express $[h]_{\leq 2} = \sum_{i=1}^{r} \beta_i t_i^{e_i}$ with $t + r = n$, and output the optimal expression.

Theorem

There exists a polynomial-time randomized algorithm that receives as input a blackbox access to a regular polynomial $f \in \mathbb{F}[X]$ and finds an optimal decomposition of f in the Affine Powers model if $\mathit{AffPow}(f) = n$, or rejects otherwise.

- Compute blackbox access to $D(X) = \det(H_g(X))$.
- If $D \neq 0$: write $D = c \cdot \prod_{i=1}^{t} \ell_i^{m_i}$ with $t \leq n$.
- Build the matrices A and b corresponding to the ℓ_i's, and find a solution X_0 of $A \cdot X = -b$.
- Set $h(X) = g(X + X_0)$, and write $h = \sum_{i=1}^{t} \alpha_i [\ell_i]^{m_i+2} + [h]_{\leq 2}$.
- Express $[h]_{\leq 2} = \sum_{i=1}^{r} \beta_i t_i^{e_i}$ with $t + r = n$, and output the optimal expression.
- If $D = 0$, repeat previous procedure with $\det([H_f(X)]_{k,k})$ for all k.

Uniqueness

For $s \in \mathbb{N}^*$, denote by $E_n := \{\underline{e} = (e_1, \ldots, e_n) \in (\mathbb{N}^*)^n \mid e_1 \geq \cdots \geq e_n\}$.

Uniqueness

For $s \in \mathbb{N}^*$, denote by $E_n := \{\underline{e} = (e_1, \ldots, e_n) \in (\mathbb{N}^*)^n \mid e_1 \geq \cdots \geq e_n\}$. For each sequence $\underline{e} \in E_n$, we consider the associated polynomial $p_{\underline{e}} := \sum_{i=1}^{n} x_i^{e_i}$.

Uniqueness

For $s \in \mathbb{N}^*$, denote by $E_n := \{\underline{e} = (e_1, \ldots, e_n) \in (\mathbb{N}^*)^n \mid e_1 \geq \cdots \geq e_n\}$.
For each sequence $\underline{e} \in E_n$, we consider the associated polynomial $p_{\underline{e}} := \sum_{i=1}^n x_i^{e_i}$.

Proposition

Let $f \in \mathbb{F}[X]$ be a regular polynomial. If $AffPow_{\mathbb{F}}(f) = n$, then there exists a unique $\underline{e} = (e_1, \ldots, e_n) \in E_n$ with $e_{n-1} > 1$ such that $f \equiv p_{\underline{e}}$.

For $s \in \mathbb{N}^*$, denote by $E_n := \{\underline{e} = (e_1, \dots, e_n) \in (\mathbb{N}^*)^n \mid e_1 \geq \cdots \geq e_n\}$.
For each sequence $\underline{e} \in E_n$, we consider the associated polynomial $p_{\underline{e}} := \sum_{i=1}^n x_i^{e_i}$.

Proposition

Let $f \in \mathbb{F}[X]$ be a regular polynomial. If $AffPow_{\mathbb{F}}(f) = n$, then there exists a unique $\underline{e} = (e_1, \dots, e_n) \in E_n$ with $e_{n-1} > 1$ such that $f \equiv p_{\underline{e}}$.

Proposition

Let $f \in \mathbb{F}[X]$ be a regular polynomial. If

$$f = \sum_{i=1}^{n} \alpha_i \ell_i^{e_i} = \sum_{i=1}^{n} \beta_i t_i^{d_i}$$

with ℓ_i, t_i linear forms and $\underline{e} = (e_1, \dots, e_n), \underline{d} = (d_1, \dots, d_n) \in E_n$, then, $e_i = d_i$ for all i, and there exists a permutation $\sigma \in \mathfrak{S}_n$ such that $\alpha_i \ell_i^{e_i} = \beta_{\sigma(i)} t_{\sigma(i)}^{d_{\sigma(i)}}$ if $e_i \geq 3$.

Repeated affine forms.

Univariate decompositions

Test if $f \equiv g$ with $g = \sum_{i=1}^{n} \sum_{j=1}^{t_i} \alpha_{i,j}\, x_i^{e_{i,j}}$.

Univariate decompositions

Test if $f \equiv g$ with $g = \sum_{i=1}^{n} \sum_{j=1}^{t_i} \alpha_{i,j}\, x_i^{e_{i,j}}$.

$f = \sum_{i=1}^{n} g_i(\ell_i(X))$ with $g_i(x) = \sum_{j=1}^{t_i} \alpha_{i,j}\, x^{e_{i,j}}$ and ℓ_i an affine form.

Univariate decompositions

Test if $f \equiv g$ with $g = \sum_{i=1}^{n} \sum_{j=1}^{t_i} \alpha_{i,j}\, x_i^{e_{i,j}}$.

$f = \sum_{i=1}^{n} g_i(\ell_i(X))$ with $g_i(x) = \sum_{j=1}^{t_i} \alpha_{i,j}\, x^{e_{i,j}}$ and ℓ_i an affine form.

Problem (Univariate decomposition)

Given $f \in \mathbb{F}[X]$, is $f \equiv g$ with $g = \sum_{i=1}^{n} g_i(x_i)$?

Univariate decompositions

Test if $f \equiv g$ with $g = \sum_{i=1}^{n} \sum_{j=1}^{t_i} \alpha_{i,j} \, x_i^{e_{i,j}}$.
$f = \sum_{i=1}^{n} g_i(\ell_i(X))$ with $g_i(x) = \sum_{j=1}^{t_i} \alpha_{i,j} \, x^{e_{i,j}}$ and ℓ_i an affine form.

Problem (Univariate decomposition)

Given $f \in \mathbb{F}[X]$, is $f \equiv g$ with $g = \sum_{i=1}^{n} g_i(x_i)$?

Theorem (Theorem C.2,Kayal)

Given an n-variate polynomial $f(X) \in \mathbb{F}[X]$, there exists an algorithm that finds a decomposition of f as

$$f(A \cdot X) = p(x_1, \ldots, x_t) + q(x_{t+1}, \ldots, x_n),$$

with A invertible, if it exists, in randomized polynomial time provided $\det(H_f)$ is a regular polynomial, i.e. it has n essential variables.

Univariate decompositions

Test if $f \equiv g$ with $g = \sum_{i=1}^{n} \sum_{j=1}^{t_i} \alpha_{i,j}\, x_i^{e_{i,j}}$.

$f = \sum_{i=1}^{n} g_i(\ell_i(X))$ with $g_i(x) = \sum_{j=1}^{t_i} \alpha_{i,j}\, x^{e_{i,j}}$ and ℓ_i an affine form.

Problem (Univariate decomposition)

Given $f \in \mathbb{F}[X]$, is $f \equiv g$ with $g = \sum_{i=1}^{n} g_i(x_i)$?

Theorem (Theorem C.2,Kayal)

Given an n-variate polynomial $f(X) \in \mathbb{F}[X]$, there exists an algorithm that finds a decomposition of f as

$$f(A \cdot X) = p(x_1, \ldots, x_t) + q(x_{t+1}, \ldots, x_n),$$

with A invertible, if it exists, in randomized polynomial time provided $\det(H_f)$ is a regular polynomial, i.e. it has n essential variables.

If f has a univariate decomposition, does taking an optimal decomposition for each g_i yield an optimal decomposition of f ?

The algorithm idea

Proposition

Let $f \in \mathbb{F}[X]$*, and let the* g_i*'s be univariate polynomials sorted by decreasing degree. Let* $d_i := \deg(g_i)$ *and* $k := \max\{i : d_i \geq 3\}$*. Let* $\ell_1, \ldots, \ell_n$ *be linear forms such that* $f = \sum_{i=1}^{n} g_i(\ell_i)$*. Then,*

The algorithm idea

Proposition

Let $f \in \mathbb{F}[X]$*, and let the* g_i*'s be univariate polynomials sorted by decreasing degree. Let* $d_i := \deg(g_i)$ *and* $k := \max\{i : d_i \geq 3\}$*. Let* $\ell_1, \ldots, \ell_n$ *be linear forms such that* $f = \sum_{i=1}^{n} g_i(\ell_i)$*. Then,*

$$\det(H_f(X)) = c \cdot \prod_{i=1}^{k} \prod_{j=1}^{d_i - 2} (\ell_i - \alpha_{i,j}),$$

where $c \in \mathbb{F}$*, and* $\alpha_{i,j}$ *are the roots of* $g_i''(x)$ *for* $1 \leq i \leq k$*.*

The algorithm idea

Proposition

Let $f \in \mathbb{F}[X]$, and let the g_i's be univariate polynomials sorted by decreasing degree. Let $d_i := \deg(g_i)$ and $k := \max\{i : d_i \geq 3\}$. Let $\ell_1, \ldots, \ell_n$ be linear forms such that $f = \sum_{i=1}^{n} g_i(\ell_i)$. Then,

$$\det(H_f(X)) = c \cdot \prod_{i=1}^{k} \prod_{j=1}^{d_i-2} (\ell_i - \alpha_{i,j}),$$

where $c \in \mathbb{F}$, and $\alpha_{i,j}$ are the roots of $g_i''(x)$ for $1 \leq i \leq k$.

Moreover, if $\ell_1, \ldots, \ell_n$ are linearly independent, for any solution $X_0 \in \mathbb{F}^n$ to the system $B \cdot X_0 = (\alpha_{1,1}, \ldots, \alpha_{k,1})^T$, where B is the $k \times n$ matrix whose rows are the coefficients of the $\ell_1, \ldots, \ell_k$, we have that

The algorithm idea

Proposition

Let $f \in \mathbb{F}[X]$, and let the g_i's be univariate polynomials sorted by decreasing degree. Let $d_i := \deg(g_i)$ and $k := \max\{i : d_i \geq 3\}$. Let $\ell_1, \ldots, \ell_n$ be linear forms such that $f = \sum_{i=1}^{n} g_i(\ell_i)$. Then,

$$\det(H_f(X)) = c \cdot \prod_{i=1}^{k} \prod_{j=1}^{d_i - 2} (\ell_i - \alpha_{i,j}),$$

where $c \in \mathbb{F}$, and $\alpha_{i,j}$ are the roots of $g_i''(x)$ for $1 \leq i \leq k$.

Moreover, if $\ell_1, \ldots, \ell_n$ are linearly independent, for any solution $X_0 \in \mathbb{F}^n$ to the system $B \cdot X_0 = (\alpha_{1,1}, \ldots, \alpha_{k,1})^T$, where B is the $k \times n$ matrix whose rows are the coefficients of the $\ell_1, \ldots, \ell_k$, we have that

(a) $[f(X + X_0)]_{\geq 3} = \sum_{i=1}^{k} h_i(\ell_i)$ for some unique $h_i \in \mathbb{F}[x]$, and

(b) $\mathrm{EssVar}([f(X + X_0)]_2) = |\{i \,|\, \deg(g_i) = 2\}|$.

The bivariate case

If $f = f_1(x_1) + f_2(x_2)$, set $s_i := \mathrm{AffPow}(f_i)$ and write

$$f_i = \sum_{j=1}^{s_i} \alpha_{i,j}(x_i + a_{i,j})^{e_{i,j}}.$$

If $f = f_1(x_1) + f_2(x_2)$, set $s_i := \mathrm{AffPow}(f_i)$ and write

$$f_i = \sum_{j=1}^{s_i} \alpha_{i,j}(x_i + a_{i,j})^{e_{i,j}}.$$

If $e_{1,1} \leq 1$ and $e_{2,1} \leq 1$, define $\mathrm{UnivAffPow}(f) := s_1 + s_2 - 1$, and otherwise $\mathrm{UnivAffPow}(f) := s_1 + s_2$.

The bivariate case

If $f = f_1(x_1) + f_2(x_2)$, set $s_i := \mathrm{AffPow}(f_i)$ and write

$$f_i = \sum_{j=1}^{s_i} \alpha_{i,j}(x_i + a_{i,j})^{e_{i,j}}.$$

If $e_{1,1} \leq 1$ and $e_{2,1} \leq 1$, define $\mathrm{UnivAffPow}(f) := s_1 + s_2 - 1$, and otherwise $\mathrm{UnivAffPow}(f) := s_1 + s_2$.

Proposition

Let $f_1 \in \mathbb{F}[x_1], f_2 \in \mathbb{F}[x_2]$, then $\mathrm{AffPow}(f_1 + f_2) = \mathrm{UnivAffPow}(f_1 + f_2)$.

The bivariate case

If $f = f_1(x_1) + f_2(x_2)$, set $s_i := \mathrm{AffPow}(f_i)$ and write

$$f_i = \sum_{j=1}^{s_i} \alpha_{i,j}(x_i + a_{i,j})^{e_{i,j}}.$$

If $e_{1,1} \leq 1$ and $e_{2,1} \leq 1$, define $\mathrm{UnivAffPow}(f) := s_1 + s_2 - 1$, and otherwise $\mathrm{UnivAffPow}(f) := s_1 + s_2$.

Proposition

Let $f_1 \in \mathbb{F}[x_1], f_2 \in \mathbb{F}[x_2]$, then $\mathit{AffPow}(f_1 + f_2) = \mathit{UnivAffPow}(f_1 + f_2)$.

Lemma

Let $s, d \in \mathbb{Z}^+$ and $b_1, \ldots, b_s$ different nonzero elements of $\mathbb{F}$. If

$$\lambda_1 x_1^d + \lambda_2 x_2^d = \sum_{i=1}^{s} \gamma_i (x_1 + b_i x_2)^d,$$

with $\lambda_1, \lambda_2 \in \mathbb{F}$ and $\gamma_i \in \mathbb{F}$ not all zero, then $s \geq d$.

Allowing more affine forms.

Previous algorithm fails

Base case: $f \equiv g$ with $g = \sum_{i=1}^{n} x_i^{e_i} + \ell^e = h + \ell^e$.

Previous algorithm fails

Base case: $f \equiv g$ with $g = \sum_{i=1}^{n} x_i^{e_i} + \ell^e = h + \ell^e$. We have $H_g = H_h + H_{\ell^e}$ and $H_{\ell^e} = e^{\underline{2}}\, \ell^{e-2} \beta\beta^T$, where $e^{\underline{i}} := e \cdots (e-i+1)$.

Previous algorithm fails

Base case: $f \equiv g$ with $g = \sum_{i=1}^{n} x_i^{e_i} + \ell^e = h + \ell^e$. We have $H_g = H_h + H_{\ell^e}$ and $H_{\ell^e} = e^{\underline{2}}\ \ell^{e-2}\beta\beta^T$, where $e^{\underline{i}} := e \cdots (e-i+1)$.

Lemma (Folklore)

Let $A \in \mathcal{M}_n(\mathbb{F})$ and $u, v \in \mathbb{F}^n$ two column vectors. Then,

$$\det(A + uv^T) = \det(A) + v^T \operatorname{adj}(A) u,$$

where $\operatorname{adj}(A)$ denotes the adjugate matrix of A.

Previous algorithm fails

Base case: $f \equiv g$ with $g = \sum_{i=1}^{n} x_i^{e_i} + \ell^e = h + \ell^e$. We have $H_g = H_h + H_{\ell^e}$ and $H_{\ell^e} = e^{\underline{2}}\, \ell^{e-2} \beta \beta^T$, where $e^{\underline{i}} := e \cdots (e - i + 1)$.

Lemma (Folklore)

Let $A \in \mathcal{M}_n(\mathbb{F})$ and $u, v \in \mathbb{F}^n$ two column vectors. Then,

$$\det(A + uv^T) = \det(A) + v^T \operatorname{adj}(A) u,$$

where $\operatorname{adj}(A)$ denotes the adjugate matrix of A.

$$\det(H_g) = \det(H_h) + e^{\underline{2}}\, \ell^{e-2} \beta^T \operatorname{adj}(H_h) \beta$$

Previous algorithm fails

Base case: $f \equiv g$ with $g = \sum_{i=1}^{n} x_i^{e_i} + \ell^e = h + \ell^e$. We have $H_g = H_h + H_{\ell^e}$ and $H_{\ell^e} = e^{\underline{2}}\, \ell^{e-2} \beta\beta^T$, where $e^{\underline{i}} := e \cdots (e-i+1)$.

Lemma (Folklore)

Let $A \in \mathcal{M}_n(\mathbb{F})$ and $u, v \in \mathbb{F}^n$ two column vectors. Then,

$$\det(A + uv^T) = \det(A) + v^T \operatorname{adj}(A) u,$$

where $\operatorname{adj}(A)$ denotes the adjugate matrix of A.

$$\det(H_g) = \det(H_h) + e^{\underline{2}}\, \ell^{e-2} \beta^T \operatorname{adj}(H_h) \beta$$

$$\det(H_f) = \det(A)^2 \left(\prod_{i=1}^{n} e_i^{\underline{2}}\, \ell_i(X)^{e_i-2} + e^{\underline{2}}\, \ell(A \cdot X + b)^{e-2} P(X) \right)$$

with $P(X) = \sum_{i=1}^{n} \beta_i^2 \left(\prod_{j \neq i} e_j^{\underline{2}}\, \ell_j(X)^{e_i-2} \right) \in \mathbb{F}[X]$.

Higher order Hessian

Definition (Symmetric 4-th order Hessian)

$$\forall a \leq b, i \leq j, \quad (\overline{H}_f)_{(a,b),(i,j)} = \frac{\partial^4 f}{\partial x_a \partial x_b \partial x_i \partial x_j}$$

Higher order Hessian

Definition (Symmetric 4-th order Hessian)

$$\forall a \leq b, i \leq j, \quad (\overline{H}_f)_{(a,b),(i,j)} = \frac{\partial^4 f}{\partial x_a \partial x_b \partial x_i \partial x_j}$$

Proposition

Let $n \in \mathbb{N}^*$, $m := \binom{n+1}{2}$ and $f = \sum_{i=1}^{m} \ell_i^{e_i}$, with $\ell_i = \sum_{j=1}^{n} b_{i,j} x_j + b_{i,0}$ affine forms and $e_i \geq 4$ for all i. Let U be the square $m \times m$ matrix with entries $U_{(i,j),k} := b_{k,i}\, b_{k,j}$ for all $1 \leq k \leq m$, $1 \leq i \leq j \leq n$. If $\det(U) \neq 0$*, there exists $c \neq 0$ such that*

$$\det(\overline{H}_f(X)) = c \cdot \prod_{i=1}^{m} \ell_i^{e_i - 4},$$

Proof

By linearity of the symmetric 4-th order Hessian, we have

$$\overline{H}_f(X) = \sum_{k=1}^{m} \overline{H}_{\ell_k}(X) = \sum_{k=1}^{m} e_k^4 \, \ell_k^{e_k - 4}(u_k \cdot u_k^T) = U \cdot D \cdot U^T,$$

where $D = \mathrm{Diag}(e_1^4 \, \ell_1^{e_1 - 4}, \ldots, e_m^4 \, \ell_m^{e_m - 4})$, and u_k is the column vector whose (i, j)-th entry is $b_{k,i} b_{k,j}$ with $1 \leq i \leq j \leq n$. Thus,

$$\det(\overline{H}_f(X)) = \det(U)^2 \prod_{k=1}^{m} e_k^4 \, \ell_k^{e_k - 4}.$$

Lemma

Let $n \in \mathbb{N}^*$ *and* $m := \binom{n+1}{2}$*, and consider the set of variables* $\mathcal{V} := \{y_{(k,l),i} \mid 1 \le k \le l \le n,\ 1 \le i \le n\}$*. Let* U *be the* $m \times m$ *square matrix with entries* $U_{(i,j),(k,l)} := y_{(k,l),i}\, y_{(k,l),j}$*, where* $1 \le i \le j \le n$*,* $1 \le k \le l \le n$*. Then,* $\det(U) \in \mathbb{Z}[\mathcal{V}]$ *is a nonzero polynomial of degree* $2m$*.*

Lemma

Let $n \in \mathbb{N}^*$ and $m := \binom{n+1}{2}$, and consider the set of variables $\mathcal{V} := \{y_{(k,l),i} \,|\, 1 \leq k \leq l \leq n,\ 1 \leq i \leq n\}$. Let U be the $m \times m$ square matrix with entries $U_{(i,j),(k,l)} := y_{(k,l),i}\, y_{(k,l),j}$, where $1 \leq i \leq j \leq n$, $1 \leq k \leq l \leq n$. Then, $\det(U) \in \mathbb{Z}[\mathcal{V}]$ is a nonzero polynomial of degree $2m$.

Proof.

Consider $\tilde{U}$ given by: $y_{(k,l),i} \mapsto 1$ if $i \in \{k, l\}$; or $y_{(k,l),i} \mapsto 0$ otherwise.

Lemma

Let $n \in \mathbb{N}^*$ and $m := \binom{n+1}{2}$, and consider the set of variables $\mathcal{V} := \{y_{(k,l),i} \,|\, 1 \le k \le l \le n,\ 1 \le i \le n\}$. Let U be the $m \times m$ square matrix with entries $U_{(i,j),(k,l)} := y_{(k,l),i}\, y_{(k,l),j}$, where $1 \le i \le j \le n$, $1 \le k \le l \le n$. Then, $\det(U) \in \mathbb{Z}[\mathcal{V}]$ is a nonzero polynomial of degree $2m$.

Proof.

Consider $\tilde{U}$ given by: $y_{(k,l),i} \mapsto 1$ if $i \in \{k, l\}$; or $y_{(k,l),i} \mapsto 0$ otherwise.

Theorem

Let $n \ge 2$ and $m := \binom{n+1}{2}$. Let $\ell_i = \sum_{j=1}^{n} b_{i,j} x_j + b_{i,0}$: $1 \le i \le m$ whose coefficients $b_{i,j}$ are taken uniformly at random from a finite set S and take $f := \sum_{i=1}^{m} \ell_i^{e_i} \in \mathbb{F}[X]$ with $e_i \ge 4$ for all i. Then, $\det(\overline{H}_f(X)) \neq 0$ with probability at least $1 - \frac{2m}{|S|}$.

Conclusion

Open questions I

- How can one handle with repeated nodes?

Open questions I

- How can one handle with repeated nodes?
- Can we improve our algorithms for $\mathbb{F} = \mathbb{R}$?
  - We have better structural results but we do not know how to derive algorithms from them.

Open questions I

- How can one handle with repeated nodes?
- Can we improve our algorithms for $\mathbb{F} = \mathbb{R}$?
  - We have better structural results but we do not know how to derive algorithms from them.
- Can we bound the bit size of an optimal decomposition by a polynomial function of the size of f?
  - Does Algorithm *Distinct Nodes* run in polynomial time?

Open questions II

A **generic** polynomial f of degree d has $\mathrm{AffPow}(f) = \left\lceil \frac{d+1}{2} \right\rceil$.

- For each $d \in \mathbb{N}$, can you provide a polynomial f_d of degree d and $\mathrm{AffPow}(f_d) = \left\lceil \frac{d+1}{2} \right\rceil$?

Open questions II

A **generic** polynomial f of degree d has $\mathrm{AffPow}(f) = \lceil \frac{d+1}{2} \rceil$.

- For each $d \in \mathbb{N}$, can you provide a polynomial f_d of degree d and $\mathrm{AffPow}(f_d) = \lceil \frac{d+1}{2} \rceil$?

Best answers known:

Theorem (Kayal, Koiran, Pecatte & Saha (2015))

For every $k \in \mathbb{N}$ and $a_1, a_2 \in \mathbb{F}$, the polynomial $f = [(x - a_1)(x - a_2)]^k$ of degree $d = 2k$ satisfies that

$$AffPow(f) \geq \sqrt{d}/2$$

Open questions II

A **generic** polynomial f of degree d has $\text{AffPow}(f) = \lceil \frac{d+1}{2} \rceil$.

- For each $d \in \mathbb{N}$, can you provide a polynomial f_d of degree d and $\text{AffPow}(f_d) = \lceil \frac{d+1}{2} \rceil$?

Best answers known:

Theorem (Kayal, Koiran, Pecatte & Saha (2015))

For every $k \in \mathbb{N}$ and $a_1, a_2 \in \mathbb{F}$, the polynomial $f = [(x - a_1)(x - a_2)]^k$ of degree $d = 2k$ satisfies that

$$AffPow(f) \geq \sqrt{d}/2$$

Theorem

When $\mathbb{F} = \mathbb{R}$, we provide polynomials f of degree d such that $AffPow(f) \geq d/4$.

Open questions III

- Can we remove the hypothesis $e_i \geq 4$ in the algorithm that reconstruct upto $\binom{n+1}{2}$ affine terms?

Open questions III

- Can we remove the hypothesis $e_i \geq 4$ in the algorithm that reconstruct upto $\binom{n+1}{2}$ affine terms?
- Can we design algorithms for more repeated affine form?

Open questions III

- Can we remove the hypothesis $e_i \geq 4$ in the algorithm that reconstruct upto $\binom{n+1}{2}$ affine terms?
- Can we design algorithms for more repeated affine form?
- We proved that $\mathrm{UnivAffPow}(f) = \mathrm{AffPow}(f)$ for bivariate polynomials. What about the general case?

Thank you for your attention!