Polynomial equivalence problem for sums of affine powers

ISSAC 2018

Ignacio Garcia-Marco[1], Pascal Koiran[2], **Timothée Pecatte**[2]

[1] Universidad de la Laguna, [2] LIP, École Normale Supérieure de Lyon

Models of interest

Classical models: the Waring model

Model (Waring decomposition)

$$\sum_{i=1}^{k} \alpha_i (x - a_i)^d \qquad \text{with } \alpha_i, a_i \in \mathbb{F}, e_i \in \mathbb{N}, \text{ and } d = \deg(f)$$

Classical models: the Waring model

Model (Waring decomposition)

$$\sum_{i=1}^{k} \alpha_i (x - a_i)^d \qquad \text{with } \alpha_i, a_i \in \mathbb{F}, e_i \in \mathbb{N}, \text{ and } d = \deg(f)$$

Reconstruction problem: Given f, one wants an **optimal** expression of f in this model (with the minimum value of k possible).

Classical models: the Waring model

Model (Waring decomposition)

$$\sum_{i=1}^{k} \alpha_i (x - a_i)^d \qquad \text{with } \alpha_i, a_i \in \mathbb{F}, e_i \in \mathbb{N}, \text{ and } d = \deg(f)$$

Reconstruction problem: Given f, one wants an **optimal** expression of f in this model (with the minimum value of k possible).

Solution: Sylvester (1851)

Classical models: the Waring model

Model (Waring decomposition)

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

Reconstruction problem: Given f, one wants an **optimal** expression of f in this model (with the minimum value of k possible).

Solution: Sylvester (1851)

Lots of partial solutions for the multivariate version: Auslander, Hirschowitz, Boij, Carlini, Geramita, Oeding, Landsberg, Sturmfels, ...

Classical models: the Sparsest Shift model

Model (Sparsest shift)

$$\sum_{i=1}^{k} \alpha_i (x - a)^{e_i} \qquad \text{with } \alpha_i, a \in \mathbb{F}, e_i \in \mathbb{N}.$$

Classical models: the Sparsest Shift model

Model (Sparsest shift)

$$\sum_{i=1}^{k} \alpha_i (x - a)^{e_i} \qquad \text{with } \alpha_i, a \in \mathbb{F}, e_i \in \mathbb{N}.$$

Reconstruction problem: Given f, one wants an **optimal** expression of f in this model.

Classical models: the Sparsest Shift model

Model (Sparsest shift)

$$\sum_{i=1}^{k} \alpha_i (x - a)^{e_i} \qquad \text{with } \alpha_i, a \in \mathbb{F}, e_i \in \mathbb{N}.$$

Reconstruction problem: Given f, one wants an **optimal** expression of f in this model.

Solution: Borodin-Tiwari (1991), Giesbrecht-Roche (2010)

Classical models: the Sparsest Shift model

Model (Sparsest shift)

$$\sum_{i=1}^{k} \alpha_i (x - a)^{e_i} \qquad \text{with } \alpha_i, a \in \mathbb{F}, e_i \in \mathbb{N}.$$

Reconstruction problem: Given f, one wants an **optimal** expression of f in this model.

Solution: Borodin-Tiwari (1991), Giesbrecht-Roche (2010)

For the multivariate version: Grigoriev-Karpinski (1993), Giesbrecht-Kaltofen-Lee (2003).

Sums of affine powers

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

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

Sums of affine powers

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

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

We now consider f an **multivariate** polynomial with **coefficients in** $\mathbb{F}$, this is, $f \in \mathbb{F}[X]$.

Sums of affine powers

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

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

We now consider f an **multivariate** polynomial with **coefficients in** $\mathbb{F}$, this is, $f \in \mathbb{F}[X]$.

Model (Multivariate $\Sigma \wedge \Sigma$)

$$\sum_{i=1}^{k} \alpha_i (a_{i,1} x_1 + \ldots + a_{i,n} x_n + a_{i,0})^{e_i}$$

Sums of affine powers

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

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

We now consider f an **multivariate** polynomial with **coefficients in** $\mathbb{F}$, this is, $f \in \mathbb{F}[X]$.

Model (Multivariate $\Sigma \wedge \Sigma$)

$$\sum_{i=1}^{k} \ell_i^{e_i} \qquad \text{with } \ell_i \in \mathbb{F}[X], \deg(\ell_i) \leq 1$$

Goal: reconstruction algorithms

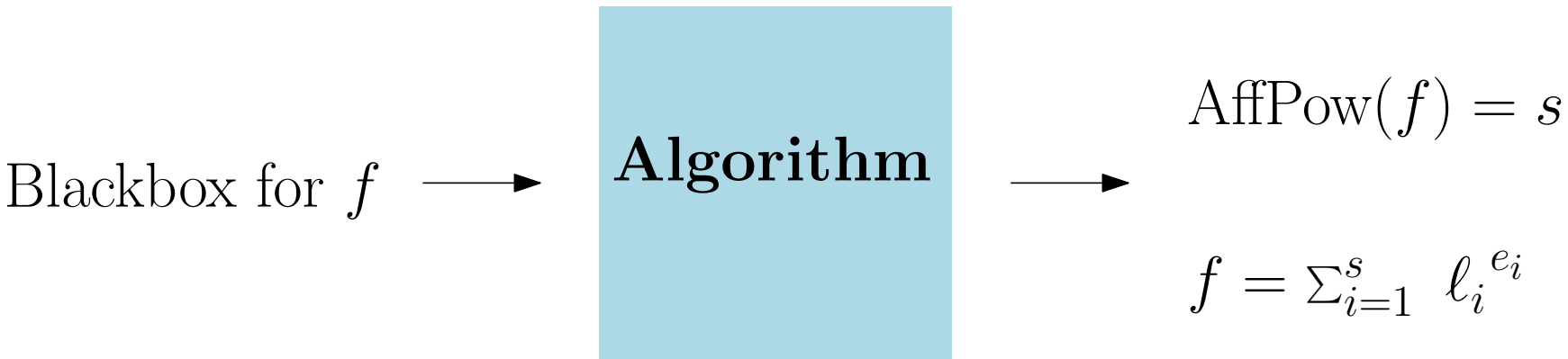
Problem

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

Goal: reconstruction algorithms

Problem

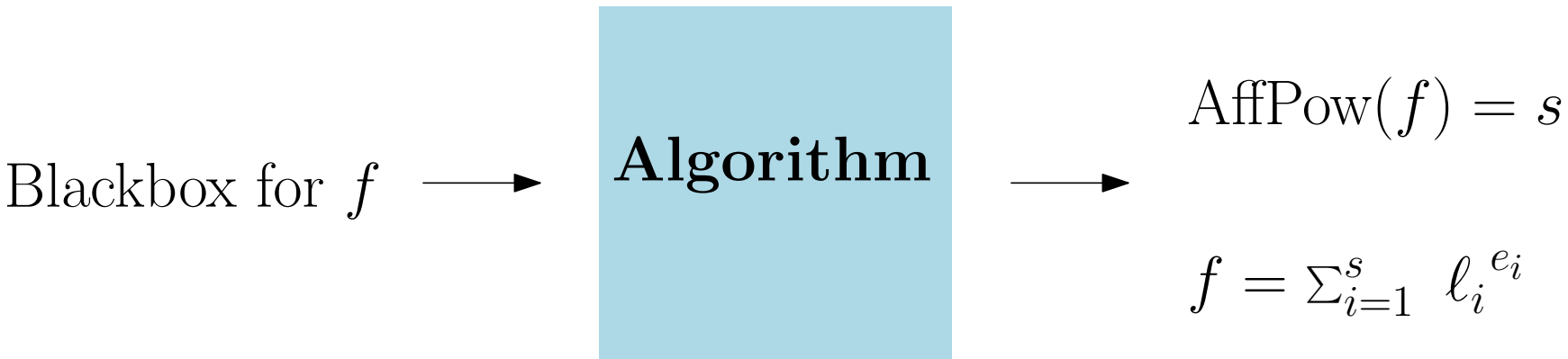
Given a polynomial $f \in \mathbb{F}[X]$, compute the exact value $s = \mathit{AffPow}_{\mathbb{F}}(f)$ and a decomposition with s terms.



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.

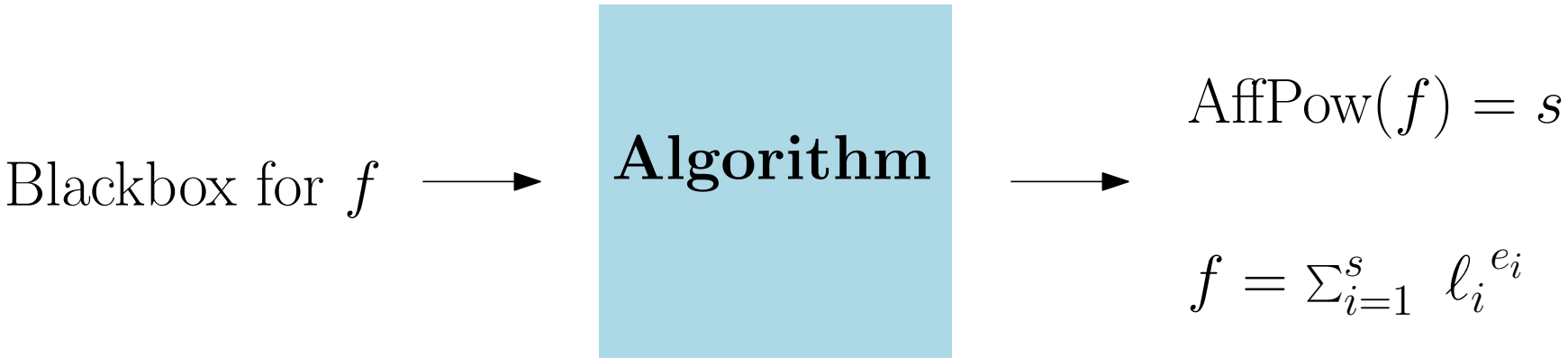


- Change of basis

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.

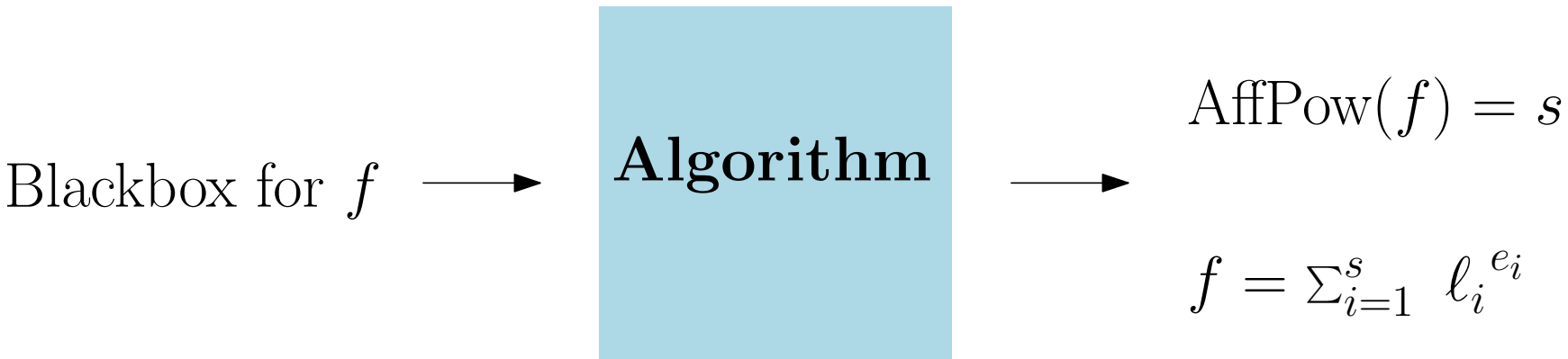


- Change of basis
- Solving linear systems

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.

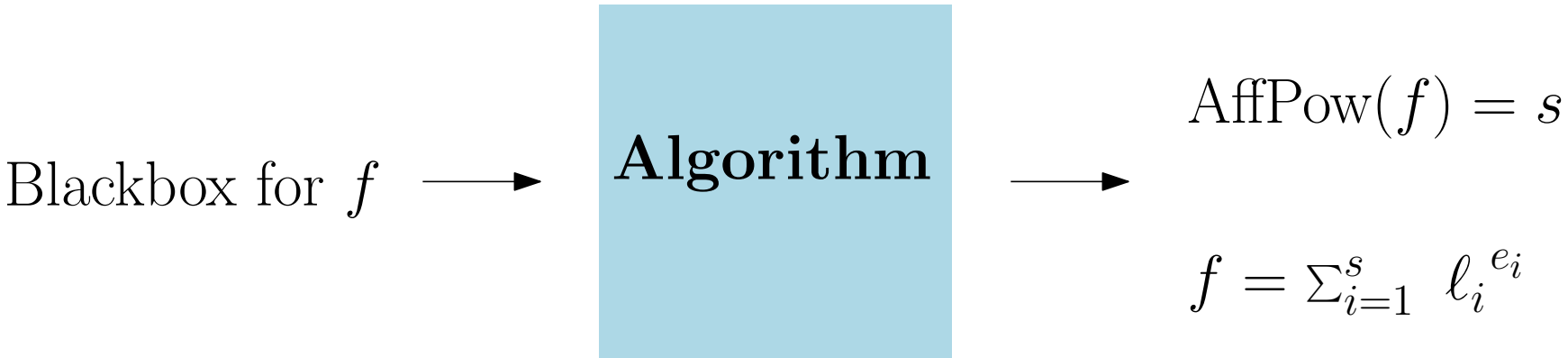


- Change of basis
- Solving linear systems
- Factorization

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.

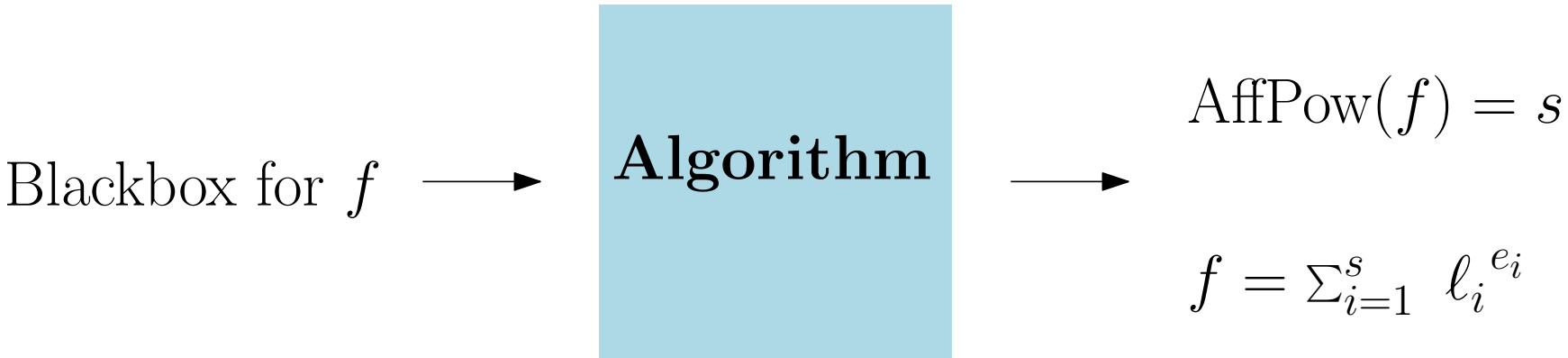


- Change of basis
- Solving linear systems
- Factorization
- PIT

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.

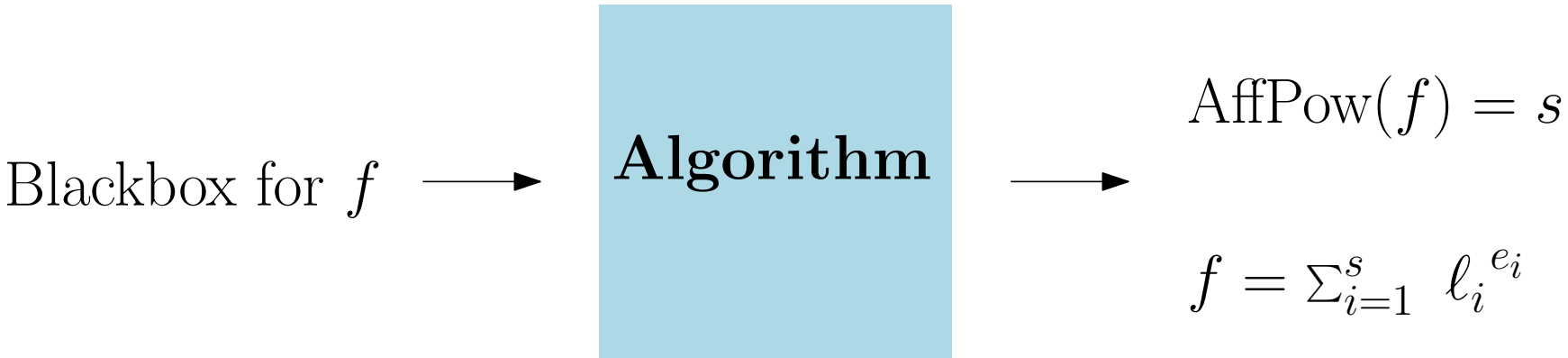


- Change of basis
- Solving linear systems
- Factorization
- PIT
- Derivatives

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.



- 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

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

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

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

Proposition (Carlini)

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

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

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

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

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

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

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 $\mathsf{EssVar}(f) = \mathsf{AffPow}(f)$, 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)

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

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

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)

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

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

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

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,

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

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 $AffPow(f) = n$, 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 $AffPow(f) = n$, 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 $AffPow(f) = n$, 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 $\mathit{AffPow}(f) = n$, 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 $h = \sum_{i=1}^{t} \alpha_i [\ell_i]^{m_i+2} + [h]_{\leq 2}$.

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.

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 $A \cdot X = -b$.
- 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 $\mathrm{AffPow}_{\mathbb{F}}(f) = n$, then there exists a unique $\underline{e} = (e_1, \ldots, e_n) \in E_n$ with $e_{n-1} > 1$ such that $f \equiv p_{\underline{e}}$.

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 $\mathrm{AffPow}_{\mathbb{F}}(f) = n$, then there exists a unique $\underline{e} = (e_1, \ldots, e_n) \in E_n$ with $e_{n-1} > 1$ such that $f \equiv p_{\underline{e}}$.

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 $\underline{e} = (e_1, \ldots, e_n), \underline{d} = (d_1, \ldots, d_n) \in E_n$, 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 $g = \sum_{i=1}^{n} x_i^{e_i}$.

Univariate decompositions

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

Univariate decompositions

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

$f = \sum_{i=1}^{n} g_i(\ell_i(X))$ 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 $g = \sum_{i=1}^{n} \left(\sum_{j=1}^{t_i} \alpha_{i,j}\, x_i^{e_{i,j}} \right)$.

$f = \sum_{i=1}^{n} g_i(\ell_i(X))$ 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 $g = \sum_{i=1}^{n} \left(\sum_{j=1}^{t_i} \alpha_{i,j} \, x_i^{e_{i,j}} \right)$.
$f = \sum_{i=1}^{n} g_i(\ell_i(X))$ 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 (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.

The bivariate case

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

The bivariate case

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

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

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

The bivariate case

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

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

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 $\mathit{AffPow}(f_1 + f_2) = \mathit{UnivAffPow}(f_1 + f_2)$.

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 $f(X) = \sum_{i=1}^{m} \ell_i(X)^{e_i}$, where $l_1, \ldots, l_n$ are affine forms and $e_i \geq 4$. Then we have

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

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 $f(X) = \sum_{i=1}^{m} \ell_i(X)^{e_i}$, where $l_1, \ldots, l_n$ are affine forms and $e_i \geq 4$. Then we have

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

with $c \neq 0$ as long as $det(U) \neq 0$, where U is the square $m \times m$ matrix with entries $U_{(i,j),k} := b_{k,i}\, b_{k,j}$ for all $1 \leq k \leq m$, $1 \leq i \leq j \leq n$.

Probabilistic analysis

Theorem

Let $n \geq 2$ *and* $m := \binom{n+1}{2}$. *Let* ℓ_i *whose coefficients 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* $e_i \geq 4$ *for all* i. *Then,* $\det(\overline{H}_f(X)) \neq 0$ *with probability at least* $1 - \frac{2m}{|S|}$.

Probabilistic analysis

Theorem

Let $n \geq 2$ *and* $m := \binom{n+1}{2}$. *Let* ℓ_i *whose coefficients 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* $e_i \geq 4$ *for all* i. *Then,* $\det(\overline{H}_f(X)) \neq 0$ *with probability at least* $1 - \frac{2m}{|S|}$.

Proof.

See the coefficients of the ℓ_i's as variables and show that the corresponding polynomial $\det(U)$ is non-zero.

Probabilistic analysis

Theorem

Let $n \geq 2$ and $m := \binom{n+1}{2}$. Let ℓ_i whose coefficients 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 $e_i \geq 4$ for all i. Then, $\det(\overline{H}_f(X)) \neq 0$ with probability at least $1 - \frac{2m}{|S|}$.

Proof.

See the coefficients of the ℓ_i's as variables and show that the corresponding polynomial $\det(U)$ is non-zero.

Theorem

There exists a polynomial time algorithm for finding an optimal expression of a polynomial f with high probability when $\mathit{AffPow}(f) \leq m = \binom{n+1}{2}$, the affine forms in optimal expression of f are chosen at random from a finite set and all the exponents involved are ≥ 5.

Conclusion & Perspectives

Open questions

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

Open questions

- 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 forms?

Open questions

- 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 forms?
- We proved that $\mathrm{UnivAffPow}(f) = \mathrm{AffPow}(f)$ for bivariate polynomials. What about the general case?

Open questions

- 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 forms?
- We proved that $\mathrm{UnivAffPow}(f) = \mathrm{AffPow}(f)$ for bivariate polynomials. What about the general case?

Thank you for your attention!