Efficient Integer-Linear Decomposition of Multivariate Polynomials

Hui Huang

Symbolic Computation Group
University of Waterloo

Joint work with Mark Giesbrecht, George Labahn and Eugene Zima

Outline

- Bivariate polynomials

- Multivariate polynomials

Outline

- Bivariate polynomials

- Multivariate polynomials

Notation. R, a UFD with $\mathrm{char}(\mathsf{R}) = 0$.

Bivariate integer-linear decomposition

Definition.

Bivariate integer-linear decomposition

Definition. $p \in R[x, y]$ irreducible, is integer-linear over R if

$$p = P(\lambda x + \mu y)$$

- $P(z) \in R[z]$ irreducible;
- $(\lambda, \mu) \in \mathbb{Z}^2$.

Bivariate integer-linear decomposition

Definition. $p \in R[x, y]$ irreducible, is integer-linear over R if

$$p = P(\lambda x + \mu y)$$

- $P(z) \in R[z]$ irreducible;
- $(\lambda, \mu) \in \mathbb{Z}^2$.

Example. $p = 4x - 6y + 2$

$$p = P(4x - 6y)$$

with $P(z) = z + 2$.

Bivariate integer-linear decomposition

Definition. $p \in R[x, y]$ irreducible, is integer-linear over R if

$$p = P(\lambda x + \mu y)$$

- $P(z) \in R[z]$ irreducible;
- $(\lambda, \mu) \in \mathbb{Z}^2$.

Example. $p = 4x - 6y + 2$

$$p = P(\boxed{4x - 6y})$$

with $P(z) = z + 2$.

Bivariate integer-linear decomposition

Definition. $p \in R[x, y]$ irreducible, is integer-linear over R if

$$p = P(\lambda x + \mu y)$$

- $P(z) \in R[z]$ irreducible;
- $(\lambda, \mu) \in \mathbb{Z}^2$.

Example. $p = 4x - 6y + 2$

$$p = P(-2x + 3y)$$

with $P(z) = -2z + 2$.

Bivariate integer-linear decomposition

Definition. $p \in R[x, y]$ irreducible, is integer-linear over R if

$$p = P(\lambda x + \mu y)$$

- $P(z) \in R[z]$ irreducible;
- $(\lambda, \mu) \in \mathbb{Z}^2$ coprime, $\mu \geq 0$.

Example. $p = 4x - 6y + 2$

$$p = P(-2x + 3y)$$

with $P(z) = -2z + 2$.

Bivariate integer-linear decomposition

Definition. $p \in R[x,y]$ irreducible, is integer-linear over R if

$$p = P(\lambda x + \mu y)$$

- $P(z) \in R[z]$ irreducible;
- $\boxed{(\lambda, \mu)} \in \mathbb{Z}^2$ coprime, $\mu \geq 0$.

integer-linear type

Example. $p = 4x - 6y + 2$

$$p = P(-2x + 3y)$$

with $P(z) = -2z + 2$.

Bivariate integer-linear decomposition

Definition. $p \in R[x, y]$ ~~irreducible,~~ is integer-linear over R if

$$p = \prod_{i=1}^{m} P_i(\lambda_i x + \mu_i y)^{e_i}$$

- $P_i(z) \in R[z]$ irreducible; $e_i \in \mathbb{Z}^+$;
- $\boxed{(\lambda_i, \mu_i)} \in \mathbb{Z}^2$ coprime, $\mu_i \geq 0$.

integer-linear types

Example. $p = (4x - 6y + 2)(3x + 6y + 1)((x + 2y)^2 + 1)$

$$p = P_1(-2x + 3y) \cdot P_2(x + 2y) \cdot P_3(x + 2y)$$

with $P_1(z) = -2z + 2$, $P_2(z) = 3z + 1$, $P_3(z) = z^2 + 1$.

Bivariate integer-linear decomposition

Definition. $p \in R[x, y]$ is integer-linear over R if

$$p = \prod_{i=1}^{m} P_i(\lambda_i x + \mu_i y)^{e_i}$$

- $P_i(z) \in R[z]$ irreducible; $e_i \in \mathbb{Z}^+$;
- $\boxed{(\lambda_i, \mu_i)} \in \mathbb{Z}^2$ coprime, $\mu_i \geq 0$.

integer-linear types

Example. $p = (4x - 6y + 2)(3x + 6y + 1)((x + 2y)^2 + 1)$

$$p = P_1(-2x + 3y) \cdot P_2(x + 2y) \cdot P_3(x + 2y)$$

with $P_1(z) = -2z + 2$, $P_2(z) = 3z + 1$, $P_3(z) = z^2 + 1$.

Bivariate integer-linear decomposition

Definition. $p \in R[x, y]$ is integer-linear over R if

$$p = \prod_{i=1}^{m} P_i(\lambda_i x + \mu_i y)^{e_i}$$

- $P_i(z) \in R[z]$ irreducible; $e_i \in \mathbb{Z}^+$;
- $\boxed{(\lambda_i, \mu_i)} \in \mathbb{Z}^2$ coprime, $\mu_i \geq 0$.

integer-linear types

Example. $p = (4x - 6y + 2)(3x + 6y + 1)((x + 2y)^2 + 1)$

$$p = P_1(-2x + 3y) \cdot \boxed{P_2(x + 2y) \cdot P_3(x + 2y)}$$

with $P_1(z) = -2z + 2$, $P_2(z) = 3z + 1$, $P_3(z) = z^2 + 1$.

Bivariate integer-linear decomposition

Definition. $p \in R[x,y]$ is integer-linear over R if

$$p = \prod_{i=1}^{m} P_i(\lambda_i x + \mu_i y)^{e_i}$$

- $P_i(z) \in R[z]$ irreducible; $e_i \in \mathbb{Z}^+$;
- $\boxed{(\lambda_i, \mu_i)} \in \mathbb{Z}^2$ coprime, $\mu_i \geq 0$.

integer-linear types

Example. $p = (4x - 6y + 2)(3x + 6y + 1)((x + 2y)^2 + 1)$

$$p = P_1(-2x + 3y) \cdot P_2(x + 2y)$$

with $P_1(z) = -2z + 2$, $P_2(z) = (3z + 1)(z^2 + 1)$.

Bivariate integer-linear decomposition

Definition. $p \in R[x, y]$ is integer-linear over R if

$$p = \prod_{i=1}^{m} P_i(\lambda_i x + \mu_i y)$$

- $P_i(z) \in R[z]$ ~~irreducible~~; $e_i \in \mathbb{Z}^+$;
- $\boxed{(\lambda_i, \mu_i)} \in \mathbb{Z}^2$ coprime, $\mu_i \geq 0$, distinct.

integer-linear types

Example. $p = (4x - 6y + 2)(3x + 6y + 1)((x + 2y)^2 + 1)$

$$p = P_1(-2x + 3y) \cdot P_2(x + 2y)$$

with $P_1(z) = -2z + 2$, $P_2(z) = (3z + 1)(z^2 + 1)$.

Bivariate integer-linear decomposition

Definition. $p \in R[x, y]$ is integer-linear over R if

$$p = \prod_{i=1}^{m} P_i(\lambda_i x + \mu_i y)$$

- $P_i(z) \in R[z]$;
- $\boxed{(\lambda_i, \mu_i)} \in \mathbb{Z}^2$ coprime, $\mu_i \geq 0$, distinct.

integer-linear types

Example. $p = (4x - 6y + 2)(3x + 6y + 1)((x + 2y)^2 + 1)$

$$p = P_1(-2x + 3y) \cdot P_2(x + 2y)$$

with $P_1(z) = -2z + 2$, $P_2(z) = (3z + 1)(z^2 + 1)$

Bivariate integer-linear decomposition

Definition. $p \in R[x, y]$ is integer-linear over R if

$$p = \prod_{i=1}^{m} P_i(\lambda_i x + \mu_i y)$$

- $P_i(z) \in R[z]$;
- $\boxed{(\lambda_i, \mu_i)} \in \mathbb{Z}^2$ coprime, $\mu_i \geq 0$, distinct.

integer-linear types

Example. $p = (4x - 6y + 2)(3x + 6y + 1)((x + 2y)^2 + 1)(3xy + 3)$

$$p = P_1(-2x + 3y) \cdot P_2(x + 2y) \cdot P_0(x, y)$$

with $P_1(z) = -2z + 2$, $P_2(z) = (3z + 1)(z^2 + 1)$, $P_0(x, y) = 3xy + 3$.

Bivariate integer-linear decomposition

Definition. $p \in R[x, y]$ is integer-linear over R if

$$p = \prod_{i=1}^{m} P_i(\lambda_i x + \mu_i y)$$

- $P_i(z) \in R[z]$;
- $\boxed{(\lambda_i, \mu_i)} \in \mathbb{Z}^2$ coprime, $\mu_i \geq 0$, distinct.

integer-linear types

Example. $p = (4x - 6y + 2)(3x + 6y + 1)((x + 2y)^2 + 1)(3xy + 3)$

$$p = (-6) \cdot P_1(-2x + 3y) \cdot P_2(x + 2y) \cdot P_0(x, y)$$

with $P_1(z) = z - 1$, $P_2(z) = (3z + 1)(z^2 + 1)$, $P_0(x, y) = xy + 1$.

Bivariate integer-linear decomposition

Definition. $p \in R[x,y]$ admits *the* integer-linear decomposition

$$p = c \cdot P_0(x,y) \cdot \prod_{i=1}^{m} P_i(\lambda_i x + \mu_i y)$$

- $c \in R$; $P_0 \in R[x,y]$ primitive and merely having non-integer-linear factors except for constants;
- $P_i(z) \in R[z]$ non-constant and primitive;
- $\boxed{(\lambda_i, \mu_i)} \in \mathbb{Z}^2$ coprime, $\mu_i \geq 0$, distinct.

integer-linear types

Example. $p = (4x - 6y + 2)(3x + 6y + 1)((x + 2y)^2 + 1)(3xy + 3)$

$$p = (-6) \cdot P_1(-2x + 3y) \cdot P_2(x + 2y) \cdot P_0(x,y)$$

with $P_1(z) = z - 1$, $P_2(z) = (3z + 1)(z^2 + 1)$, $P_0(x,y) = xy + 1$.

Applications

- Integer-linearity
  - Ore-Sato theorem (Ore1930, Sato1990)
  - Wilf-Zeilberger's conjecture (Abramov&Petkovšek2001, Abramov&Petkovšek2002, Chen&Koutschan2019)
  - Applicability of Zeilberger's algorithm (Abramov2003, Chen,Hou,H.,Labahn&Wang2019)

Applications

- Integer-linearity
  - Ore-Sato theorem (Ore1930, Sato1990)
  - Wilf-Zeilberger's conjecture (Abramov&Petkovšek2001, Abramov&Petkovšek2002, Chen&Koutschan2019)
  - Applicability of Zeilberger's algorithm (Abramov2003, Chen,Hou,H.,Labahn&Wang2019)
- Integer-linear decomposition
  - Ore-Sato decomposition (Payne1997)
  - Creative telescoping algorithm (Le2003, GHLZ2019)

Previous work

Goal. Given $p \in R[x, y]$, find $p = cP_0(x, y) \prod_{i=1}^{m} P_i(\lambda_i x + \mu_i y)$.

Previous work

Goal. Given $p \in R[x, y]$, find $p = cP_0(x, y) \prod_{i=1}^{m} P_i(\lambda_i x + \mu_i y)$.

- Abramov-Le (2002)

$$r = \lambda_i / \mu_i \quad \Longleftrightarrow \quad \mathrm{cont}_x(p(x, y - rx)) \notin R$$

Previous work

Goal. Given $p \in R[x, y]$, find $p = cP_0(x, y) \prod_{i=1}^{m} P_i(\lambda_i x + \mu_i y)$.

- Abramov-Le (2002)

$$r = \lambda_i / \mu_i \quad \Longleftrightarrow \quad \mathrm{cont}_x(p(x, y - rx)) \notin R$$

  - Find candidates for the (λ_i, μ_i) via resultant
  - Compute $P_i(z) = \mathrm{prim}_z \left(\mathrm{cont}_x \left(p(x, \frac{1}{\mu_i}(z - \lambda_i x)) \right) \right)$

Previous work

Goal. Given $p \in R[x, y]$, find $p = cP_0(x, y) \prod_{i=1}^{m} P_i(\lambda_i x + \mu_i y)$.

- Abramov-Le (2002)

$$r = \lambda_i / \mu_i \quad \Longleftrightarrow \quad \mathrm{cont}_x(p(x, y - rx)) \notin R$$

  - Find candidates for the (λ_i, μ_i) via resultant
  - Compute $P_i(z) = \mathrm{prim}_z \left(\mathrm{cont}_x \left(p(x, \frac{1}{\mu_i}(z - \lambda_i x)) \right) \right)$

- Li-Zhang (2013)

$$p = P(\lambda x + \mu y) \quad \Longleftrightarrow \quad p = \sum_{k=1}^{d} c_k \overset{\text{kth homogeneous component}}{\boxed{(\lambda x + \mu y)^k}}$$

Previous work

Goal. Given $p \in R[x,y]$, find $p = cP_0(x,y)\prod_{i=1}^{m} P_i(\lambda_i x + \mu_i y)$.

- Abramov-Le (2002)

$$r = \lambda_i/\mu_i \quad \Longleftrightarrow \quad \mathrm{cont}_x(p(x, y - rx)) \notin R$$

  - Find candidates for the (λ_i, μ_i) via resultant
  - Compute $P_i(z) = \mathrm{prim}_z\left(\mathrm{cont}_x\left(p(x, \frac{1}{\mu_i}(z - \lambda_i x))\right)\right)$

- Li-Zhang (2013)

kth homogeneous component

$$p = P(\lambda x + \mu y) \quad \Longleftrightarrow \quad p = \sum_{k=1}^{d} c_k \boxed{(\lambda x + \mu y)^k}$$

  - Full factorization of p
  - Check integer-linearity of each irreducible factor
  - Group factors of the same type

Key observation

Given $p \in R[x, y]$ primitive w.r.t. y, want

$$p = P_0(x, y) \cdot \prod_{i=1}^{m} P_i(\lambda_i x + \mu_i y), \quad \mu_i > 0.$$

Key observation

Given $p \in R[x, y]$ primitive w.r.t. y, want

$$p = P_0(x, y) \cdot \prod_{i=1}^{m} P_i(\lambda_i x + \mu_i y), \quad \mu_i > 0.$$

- Squarefree part of leading homogeneous component

$$\tilde{P}_0(x, y) \cdot \prod_{i=1}^{m} (\lambda_i x + \mu_i y)$$

Key observation

Given $p \in \mathsf{R}[x, y]$ primitive w.r.t. y, want

$$p = P_0(x, y) \cdot \prod_{i=1}^{m} P_i(\lambda_i x + \mu_i y), \quad \mu_i > 0.$$

- Squarefree part of leading homogeneous component

$$\tilde{P}_0(x, y) \cdot \prod_{i=1}^{m} (\lambda_i x + \mu_i y) \quad \Longleftrightarrow \quad \tilde{P}_0(1, z) \cdot \prod_{i=1}^{m} (\lambda_i + \mu_i z)$$

Key observation

Given $p \in R[x,y]$ primitive w.r.t. y, want

$$p = P_0(x,y) \cdot \prod_{i=1}^{m} P_i(\lambda_i x + \mu_i y), \quad \mu_i > 0.$$

- Squarefree part of leading homogeneous component

$$\tilde{P}_0(x,y) \cdot \prod_{i=1}^{m} (\lambda_i x + \mu_i y) \quad \Longleftrightarrow \quad \tilde{P}_0(1,z) \cdot \prod_{i=1}^{m} \underbrace{\boxed{(\lambda_i + \mu_i z)}}_{z = -\lambda_i/\mu_i}$$

Key observation

Given $p \in R[x, y]$ primitive w.r.t. y, want

$$p = P_0(x, y) \cdot \prod_{i=1}^{m} P_i(\lambda_i x + \mu_i y), \quad \mu_i > 0.$$

- Squarefree part of leading homogeneous component

$$\tilde{P}_0(x, y) \cdot \prod_{i=1}^{m} (\lambda_i x + \mu_i y) \quad \Longleftrightarrow \quad \tilde{P}_0(1, z) \cdot \prod_{i=1}^{m} \underbrace{\boxed{(\lambda_i + \mu_i z)}}_{z = -\lambda_i/\mu_i}$$

- Require: R admits effective rational root finding

Key observation

Given $p \in R[x, y]$ primitive w.r.t. y, want

$$p = P_0(x, y) \cdot \prod_{i=1}^{m} P_i(\lambda_i x + \mu_i y), \quad \mu_i > 0.$$

- Squarefree part of leading homogeneous component

$$\tilde{P}_0(x, y) \cdot \prod_{i=1}^{m} (\lambda_i x + \mu_i y) \quad \Longleftrightarrow \quad \tilde{P}_0(1, z) \cdot \prod_{i=1}^{m} \underbrace{\boxed{(\lambda_i + \mu_i z)}}_{z = -\lambda_i/\mu_i}$$

- Require: R admits effective rational root finding

  e.g., $\mathbb{Z}$, $\mathbb{Z}[x_1, \ldots, x_n]$, $\mathbb{Q}(\alpha)$ with α an algebraic number

Algorithm BivariateILD

Input. $p \in R[x, y]$ and R admits effective rational root finding.

Output. The integer-linear decomposition of p.

Algorithm BivariateILD

Input. $p \in R[x, y]$ and R admits effective rational root finding.

Output. The integer-linear decomposition of p.

```
1 If $p \in R$, return $p$; else $c = \mathrm{cont}_{x,y}(p)$ and $P_0 = p/c$.
2 If $\mathrm{cont}_x(P_0)$ or $\mathrm{cont}_y(P_0) \neq 1$, update $P_m(\lambda_m x + \mu_m y)$ and $P_0$.
3 If $P_0 = 1$, return $c \prod_{i=1}^{m} P_i(\lambda_i x + \mu_i y)$.
```

Algorithm BivariateILD

Input. $p \in R[x, y]$ and R admits effective rational root finding.

Output. The integer-linear decomposition of p.

```
1 If $p \in R$, return $p$; else $c = \mathrm{cont}_{x,y}(p)$ and $P_0 = p/c$.
2 If $\mathrm{cont}_x(P_0)$ or $\mathrm{cont}_y(P_0) \neq 1$, update $P_m(\lambda_m x + \mu_m y)$ and $P_0$.
3 If $P_0 = 1$, return $c \prod_{i=1}^{m} P_i(\lambda_i x + \mu_i y)$.
4 Compute the leading homogeneous component $\tilde{g}$ of $P_0$.
```

Algorithm BivariateILD

Input. $p \in R[x, y]$ and R admits effective rational root finding.

Output. The integer-linear decomposition of p.

```
1 If $p \in R$, return $p$; else $c = \mathrm{cont}_{x,y}(p)$ and $P_0 = p/c$.
2 If $\mathrm{cont}_x(P_0)$ or $\mathrm{cont}_y(P_0) \neq 1$, update $P_m(\lambda_m x + \mu_m y)$ and $P_0$.
3 If $P_0 = 1$, return $c \prod_{i=1}^{m} P_i(\lambda_i x + \mu_i y)$.
4 Compute the leading homogeneous component $\tilde{g}$ of $P_0$.
5 Find all nonzero rational roots $\{-\lambda/\mu\}$ of $\tilde{g}(1, z)$.
```

Algorithm BivariateILD

Input. $p \in R[x, y]$ and R admits effective rational root finding.

Output. The integer-linear decomposition of p.

```
1 If $p \in R$, return $p$; else $c = \mathrm{cont}_{x,y}(p)$ and $P_0 = p/c$.
2 If $\mathrm{cont}_x(P_0)$ or $\mathrm{cont}_y(P_0) \neq 1$, update $P_m(\lambda_m x + \mu_m y)$ and $P_0$.
3 If $P_0 = 1$, return $c \prod_{i=1}^{m} P_i(\lambda_i x + \mu_i y)$.
4 Compute the leading homogeneous component $\tilde{g}$ of $P_0$.
5 Find all nonzero rational roots $\{-\lambda/\mu\}$ of $\tilde{g}(1, z)$.
6 For each $-\lambda/\mu$, if $\mathrm{cont}_x(P_0(\mu x, z - \lambda x)) \notin R$, update
      $P_m(\lambda_m x + \mu_m y)$   and   $P_0 = P_0/P_m(\lambda x + \mu y)$.
```

Algorithm BivariateILD

Input. $p \in R[x, y]$ and R admits effective rational root finding.

Output. The integer-linear decomposition of p.

```
1 If $p \in R$, return $p$; else $c = \mathrm{cont}_{x,y}(p)$ and $P_0 = p/c$.
2 If $\mathrm{cont}_x(P_0)$ or $\mathrm{cont}_y(P_0) \neq 1$, update $P_m(\lambda_m x + \mu_m y)$ and $P_0$.
3 If $P_0 = 1$, return $c \prod_{i=1}^{m} P_i(\lambda_i x + \mu_i y)$.
4 Compute the leading homogeneous component $\tilde{g}$ of $P_0$.
5 Find all nonzero rational roots $\{-\lambda/\mu\}$ of $\tilde{g}(1, z)$.
6 For each $-\lambda/\mu$, if $\mathrm{cont}_x(P_0(\mu x, z - \lambda x)) \notin R$, update
      $P_m(\lambda_m x + \mu_m y)$ and $P_0 = P_0/P_m(\lambda x + \mu y)$.
7 return $c P_0 \prod_{i=1}^{m} P_i(\lambda_i x + \mu_i y)$.
```

Complexity over $\mathbb{Z}$ (word operations)

Given $p \in \mathbb{Z}[x, y]$ with $\deg_{x,y}(p) = d$ and $\|p\|_\infty = \beta$.

BivariateILD	Abramov-Le	Li-Zhang
$O^\sim(d^3 \log \beta)$	$O^\sim(d^4 + d^3 \log \beta)$	$O^\sim(d^7 \log \beta)$

Recall

- word length of nonzero $a \in \mathbb{Z}$: $O(\log |a|)$;
- max-norm of $p = \sum_{i,j \geq 0} p_{ij} x^i y^j \in \mathbb{Z}[x, y]$: $\|p\|_\infty = \max_{i,j \geq 0} |p_{ij}|$.

Multivariate integer-linear decomposition

Definition. $p \in R[x_1, \ldots, x_n]$ admits *the* integer-linear decomposition

$$p = c \cdot P_0(x_1, \ldots, x_n) \cdot \prod_{i=1}^{m} P_i(\lambda_{i1}x_1 + \cdots + \lambda_{in}x_n)$$

with

- $c \in R$;
- $P_0 \in R[x_1, \ldots, x_n]$ primitive and merely having non-integer-linear factors except for constants;
- $P_i(z) \in R[z]$ non-constant and primitive;
- $(\lambda_{i1}, \ldots, \lambda_{in}) \in \mathbb{Z}^n$ distinct integer-linear types.

Multivariate integer-linear decomposition

Definition. $p \in R[x_1, \ldots, x_n]$ admits *the* integer-linear decomposition

$$p = c \cdot P_0(x_1, \ldots, x_n) \cdot \prod_{i=1}^{m} P_i(\lambda_{i1}x_1 + \cdots + \lambda_{in}x_n)$$

with

- $c \in R$;
- $P_0 \in R[x_1, \ldots, x_n]$ primitive and merely having non-integer-linear factors except for constants;
- $P_i(z) \in R[z]$ non-constant and primitive;
- $\boxed{(\lambda_{i1}, \ldots, \lambda_{in})} \in \mathbb{Z}^n$ distinct integer-linear types.

$\gcd(\lambda_{i1}, \ldots, \lambda_{in}) = 1$ and $\lambda_{in} \geq 0$

Multivariate integer-linear decomposition

Definition. $p \in R[x_1, \ldots, x_n]$ admits *the* integer-linear decomposition

$$p = c \cdot P_0(x_1, \ldots, x_n) \cdot \prod_{i=1}^{m} P_i(\lambda_{i1} x_1 + \cdots + \lambda_{in} x_n)$$

with

- $c \in R$;
- $P_0 \in R[x_1, \ldots, x_n]$ primitive and merely having non-integer-linear factors except for constants;
- $P_i(z) \in R[z]$ non-constant and primitive;
- $\boxed{(\lambda_{i1}, \ldots, \lambda_{in})} \in \mathbb{Z}^n$ distinct integer-linear types.

$\gcd(\lambda_{i1}, \ldots, \lambda_{in}) = 1$ and $\lambda_{in} \geq 0$

$$\boxed{p \text{ is integer-linear over } R \iff P_0 = 1}$$

An appealing idea

Given $p \in \mathsf{R}[x_1, \ldots, x_n]$ primitive w.r.t. x_n, want

$$p = P_0(x_1, \ldots, x_n) \cdot \prod_{i=1}^{m} P_i(\lambda_{i1} x_1 + \cdots + \lambda_{in} x_n), \quad \lambda_{in} > 0.$$

An appealing idea

Given $p \in R[x_1, \dots, x_n]$ primitive w.r.t. x_n, want

$$p = P_0(x_1, \dots, x_n) \cdot \prod_{i=1}^{m} P_i(\lambda_{i1} x_1 + \cdots + \lambda_{in} x_n), \quad \lambda_{in} > 0.$$

- Squarefree part of leading homogeneous component

$$\tilde{P}_0(x_1, \dots, x_n) \cdot \prod_{i=1}^{m} (\lambda_{i1} x_1 + \cdots + \lambda_{in} x_n)$$

An appealing idea

Given $p \in R[x_1, \ldots, x_n]$ primitive w.r.t. x_n, want

$$p = P_0(x_1, \ldots, x_n) \cdot \prod_{i=1}^{m} P_i(\lambda_{i1} x_1 + \cdots + \lambda_{in} x_n), \quad \lambda_{in} > 0.$$

- Squarefree part of leading homogeneous component

$$\tilde{P}_0(x_1, \ldots, x_n) \cdot \prod_{i=1}^{m} \boxed{(\lambda_{i1} x_1 + \cdots + \lambda_{in} x_n)}$$

An appealing idea

Given $p \in R[x_1, \dots, x_n]$ primitive w.r.t. x_n, want

$$p = P_0(x_1, \dots, x_n) \cdot \prod_{i=1}^{m} P_i(\lambda_{i1} x_1 + \cdots + \lambda_{in} x_n), \quad \lambda_{in} > 0.$$

- Squarefree part of leading homogeneous component

$$\tilde{P}_0(x_1, \dots, x_n) \cdot \prod_{i=1}^{m} \boxed{(\lambda_{i1} x_1 + \cdots + \lambda_{in} x_n)}$$

- Compute $P_i(z)$ from $\operatorname{cont}_{x_1, \dots, x_{n-1}}$ of

$$p(\lambda_{in} x_1, \dots, \lambda_{in} x_{n-1}, z - \lambda_{i1} x_1 - \cdots - \lambda_{i,n-1} x_{n-1})$$

An appealing idea

Given $p \in R[x_1, \ldots, x_n]$ primitive w.r.t. x_n, want

$$p = P_0(x_1, \ldots, x_n) \cdot \prod_{i=1}^{m} P_i(\lambda_{i1} x_1 + \cdots + \lambda_{in} x_n), \quad \lambda_{in} > 0.$$

- Squarefree part of leading homogeneous component

$$\tilde{P}_0(x_1, \ldots, x_n) \cdot \prod_{i=1}^{m} \boxed{(\lambda_{i1} x_1 + \cdots + \lambda_{in} x_n)}$$

- Compute $P_i(z)$ from $\operatorname{cont}_{x_1, \ldots, x_{n-1}}$ of

$$p(\lambda_{in} x_1, \ldots, \lambda_{in} x_{n-1}, z - \lambda_{i1} x_1 - \cdots - \lambda_{i,n-1} x_{n-1})$$

Inefficient in high dimension!!!

A proposition by Abramov-Petkovšek (2002)

Let $p \in R[x_1, \ldots, x_n]$. Then

$$p = P(\lambda_1 x_1 + \cdots + \lambda_n x_n)$$

$$\Updownarrow$$

$$p = P_{ij}(\alpha_{ij} x_i + \beta_{ij} x_j) \quad \text{for any } 1 \leq i < j \leq n$$

where

- $P(z) \in R[z]$, $\lambda_i \in \mathbb{Z}$;
- $P_{ij}(z) \in R[x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_{j-1}, x_{j+1}, \ldots, x_n][z]$;
- $\alpha_{ij}, \beta_{ij} \in \mathbb{Z}$.

Example

Consider

$$((x_1 - 2x_2)x_3 + x_4)((4x_1 - 8x_2 - 6x_3 + 5x_4)^2 + 1)(2x_1 - 4x_2 - 3x_3)$$

Example

Consider

$$\underbrace{((x_1 - 2x_2)x_3 + x_4)((4x_1 - 8x_2 - 6x_3 + 5x_4)^2 + 1)(2x_1 - 4x_2 - 3x_3)}_{p}$$

Example

Consider

$$\underbrace{((x_1 - 2x_2)x_3 + x_4)((4x_1 - 8x_2 - 6x_3 + 5x_4)^2 + 1)(2x_1 - 4x_2 - 3x_3)}_{p}$$

- $p \in \mathbb{Z}[x_3, x_4][x_1, x_2]$

$$((x_1 - 2x_2)x_3 + x_4)((4x_1 - 8x_2 - 6x_3 + 5x_4)^2 + 1)(2x_1 - 4x_2 - 3x_3)$$

Example

Consider

$$\underbrace{((x_1 - 2x_2)x_3 + x_4)((4x_1 - 8x_2 - 6x_3 + 5x_4)^2 + 1)(2x_1 - 4x_2 - 3x_3)}_{p}$$

- $p \in \mathbb{Z}[x_3, x_4][x_1, x_2]$

$$(\boxed{(x_1 - 2x_2)}x_3 + x_4)((\boxed{4x_1 - 8x_2} - 6x_3 + 5x_4)^2 + 1)(\boxed{2x_1 - 4x_2} - 3x_3)$$

Example

Consider

$$\underbrace{((x_1 - 2x_2)x_3 + x_4)((4x_1 - 8x_2 - 6x_3 + 5x_4)^2 + 1)(2x_1 - 4x_2 - 3x_3)}_{p}$$

- $p = P(-x_1 + 2x_2)$ with

$$P(z) = (-zx_3 + x_4)((-4z - 6x_3 + 5x_4)^2 + 1)(-2z - 3x_3)$$

Example

Consider

$$\underbrace{((x_1 - 2x_2)x_3 + x_4)((4x_1 - 8x_2 - 6x_3 + 5x_4)^2 + 1)(2x_1 - 4x_2 - 3x_3)}_{p}$$

- $p = P(-x_1 + 2x_2)$ with

  $$P(z) = (-zx_3 + x_4)((-4z - 6x_3 + 5x_4)^2 + 1)(-2z - 3x_3)$$

- $P(z) \in \mathbb{Z}[x_4][z, x_3]$

  $$(-zx_3 + x_4)((-4z - 6x_3 + 5x_4)^2 + 1)(-2z - 3x_3)$$

Example

Consider

$$\underbrace{((x_1-2x_2)x_3+x_4)((4x_1-8x_2-6x_3+5x_4)^2+1)(2x_1-4x_2-3x_3)}_{p}$$

- $p = P(-x_1+2x_2)$ with

$$P(z) = (-zx_3+x_4)((-4z-6x_3+5x_4)^2+1)(-2z-3x_3)$$

- $P(z) \in \mathbb{Z}[x_4][z, x_3]$

$$(\boxed{-zx_3}+x_4)((\boxed{-4z-6x_3}+5x_4)^2+1)(\boxed{-2z-3x_3})$$

Example

Consider

$$\underbrace{((x_1 - 2x_2)x_3 + x_4)((4x_1 - 8x_2 - 6x_3 + 5x_4)^2 + 1)(2x_1 - 4x_2 - 3x_3)}_{p}$$

- $p = P(-x_1 + 2x_2)$ with

$$P(z) = (-zx_3 + x_4)((-4z - 6x_3 + 5x_4)^2 + 1)(-2z - 3x_3)$$

- $P(z) = P_0'(z, x_3) \cdot P_1'(2z + 3x_3)$ with

$$P_0'(z, x_3) = -zx_3 + x_4 \quad \text{and} \quad P_1'(z) = ((-2z + 5x_4)^2 + 1)(-z)$$

Example

Consider

$$\underbrace{((x_1 - 2x_2)x_3 + x_4)((4x_1 - 8x_2 - 6x_3 + 5x_4)^2 + 1)(2x_1 - 4x_2 - 3x_3)}_{p}$$

- $p = P(-x_1 + 2x_2)$ with

  $$P(z) = (-zx_3 + x_4)((-4z - 6x_3 + 5x_4)^2 + 1)(-2z - 3x_3)$$

- $P(z) = P_0'(z, x_3) \cdot P_1'(2z + 3x_3)$ with

  $$P_0'(z, x_3) = -zx_3 + x_4 \quad \text{and} \quad P_1'(z) = ((-2z + 5x_4)^2 + 1)(-z)$$

Example

Consider

$$\underbrace{((x_1 - 2x_2)x_3 + x_4)((4x_1 - 8x_2 - 6x_3 + 5x_4)^2 + 1)(2x_1 - 4x_2 - 3x_3)}_{p}$$

- $p = P(-x_1 + 2x_2)$ with

  $$P(z) = (-zx_3 + x_4)((-4z - 6x_3 + 5x_4)^2 + 1)(-2z - 3x_3)$$

- $p = P_0 \cdot P_1'(-2x_1 + 4x_2 + 3x_3)$ with

  $$P_0 = (x_1 - 2x_2)x_3 + x_4 \quad \text{and} \quad P_1'(z) = ((-2z + 5x_4)^2 + 1)(-z)$$

Example

Consider

$$\underbrace{((x_1-2x_2)x_3+x_4)((4x_1-8x_2-6x_3+5x_4)^2+1)(2x_1-4x_2-3x_3)}_{p}$$

- $p = P(-x_1+2x_2)$ with

  $$P(z) = (-zx_3+x_4)((-4z-6x_3+5x_4)^2+1)(-2z-3x_3)$$

- $p = P_0 \cdot P_1'(-2x_1+4x_2+3x_3)$ with

  $$P_0 = (x_1-2x_2)x_3+x_4 \quad \text{and} \quad P_1'(z) = ((-2z+5x_4)^2+1)(-z)$$

- $P_1'(z) \in \mathbb{Z}[z, x_4]$

  $$((-2z+5x_4)^2+1)(-z)$$

Example

Consider

$$\underbrace{((x_1 - 2x_2)x_3 + x_4)((4x_1 - 8x_2 - 6x_3 + 5x_4)^2 + 1)(2x_1 - 4x_2 - 3x_3)}_{p}$$

- $p = P(-x_1 + 2x_2)$ with
$$P(z) = (-zx_3 + x_4)((-4z - 6x_3 + 5x_4)^2 + 1)(-2z - 3x_3)$$
- $p = P_0 \cdot P_1'(-2x_1 + 4x_2 + 3x_3)$ with
$$P_0 = (x_1 - 2x_2)x_3 + x_4 \quad \text{and} \quad P_1'(z) = ((-2z + 5x_4)^2 + 1)(-z)$$
- $P_1'(z) \in \mathbb{Z}[z, x_4]$
$$(\boxed{-2z + 5x_4})^2 + 1)\boxed{-z})$$

Example

Consider

$$\underbrace{((x_1 - 2x_2)x_3 + x_4)((4x_1 - 8x_2 - 6x_3 + 5x_4)^2 + 1)(2x_1 - 4x_2 - 3x_3)}_{p}$$

- $p = P(-x_1 + 2x_2)$ with

  $$P(z) = (-zx_3 + x_4)((-4z - 6x_3 + 5x_4)^2 + 1)(-2z - 3x_3)$$

- $p = P_0 \cdot P_1'(-2x_1 + 4x_2 + 3x_3)$ with

  $$P_0 = (x_1 - 2x_2)x_3 + x_4 \quad \text{and} \quad P_1'(z) = ((-2z + 5x_4)^2 + 1)(-z)$$

- $P_1'(z) = P_1(-2z + 5x_4) \cdot P_2(z)$ with

  $$P_1(z) = z^2 + 1 \quad \text{and} \quad P_2(z) = -z$$

Example

Consider

$$\underbrace{((x_1 - 2x_2)x_3 + x_4)((4x_1 - 8x_2 - 6x_3 + 5x_4)^2 + 1)(2x_1 - 4x_2 - 3x_3)}_{p}$$

- $p = P(-x_1 + 2x_2)$ with

$$P(z) = (-zx_3 + x_4)((-4z - 6x_3 + 5x_4)^2 + 1)(-2z - 3x_3)$$

- $p = P_0 \cdot P_1'(\boxed{-2x_1 + 4x_2 + 3x_3})$ with

$$P_0 = (x_1 - 2x_2)x_3 + x_4 \quad \text{and} \quad P_1'(z) = ((-2z + 5x_4)^2 + 1)(-z)$$

- $P_1'(z) = P_1(-2z + 5x_4) \cdot P_2(z)$ with

$$P_1(z) = z^2 + 1 \quad \text{and} \quad P_2(z) = -z$$

Example

Consider

$$\underbrace{((x_1-2x_2)x_3+x_4)((4x_1-8x_2-6x_3+5x_4)^2+1)(2x_1-4x_2-3x_3)}_{p}$$

- $p = P(-x_1+2x_2)$ with

  $$P(z) = (-zx_3+x_4)((-4z-6x_3+5x_4)^2+1)(-2z-3x_3)$$

- $p = P_0 \cdot P_1'(-2x_1+4x_2+3x_3)$ with

  $$P_0 = (x_1-2x_2)x_3+x_4 \quad \text{and} \quad P_1'(z) = ((-2z+5x_4)^2+1)(-z)$$

- $p = P_0 \cdot P_1(4x_1-8x_2-6x_3+5x_4) \cdot P_2(-2x_1+4x_2+3x_3)$ with

  $$P_0 = (x_1-2x_2)x_3+x_4, \quad P_1(z) = z^2+1 \quad \text{and} \quad P_2(z) = -z$$

Example

Consider

$$\underbrace{((x_1 - 2x_2)x_3 + x_4)((4x_1 - 8x_2 - 6x_3 + 5x_4)^2 + 1)(2x_1 - 4x_2 - 3x_3)}_{p}$$

- $p = P(-x_1 + 2x_2)$ with

$$P(z) = (-zx_3 + x_4)((-4z - 6x_3 + 5x_4)^2 + 1)(-2z - 3x_3)$$

- $p = P_0 \cdot P_1'(-2x_1 + 4x_2 + 3x_3)$ with

$$P_0 = (x_1 - 2x_2)x_3 + x_4 \quad \text{and} \quad P_1'(z) = ((-2z + 5x_4)^2 + 1)(-z)$$

- $\boxed{p = P_0 \cdot P_1(4x_1 - 8x_2 - 6x_3 + 5x_4) \cdot P_2(-2x_1 + 4x_2 + 3x_3)}$ with

$$P_0 = (x_1 - 2x_2)x_3 + x_4, \quad P_1(z) = z^2 + 1 \quad \text{and} \quad P_2(z) = -z$$

Algorithm MultivariateILD

Input. $p \in R[x_1, \ldots, x_n]$ and R admits effective rational root finding.

Output. The integer-linear decomposition of p.

```
If $p \in R$, return $p$; else $c = \mathrm{cont}_{x_1,\ldots,x_n}(p)$ and $p = p/c$.
If $n = 1$, return. If $n = 2$, call **BivariateILD** on $p$ and return.
Call algorithm recursively on $\mathrm{cont}_{x_1,x_2}(p)$ and update $P_i, p$.
If $p = 1$, return $cP_0 \prod_{i=1}^{m} P_i(\lambda_{i1}x_1 + \cdots + \lambda_{in}x_n)$.
Set $\Lambda_1 = \{((1), p(x_0, x_2, \ldots, x_n))\}$ with $x_0$ an indeterminate.
For $k = 1, \ldots, n-1$ and $((\mu_1, \ldots, \mu_k), h(x_0, x_{k+1}, \ldots, x_n)) \in \Lambda_k$,
    call **BivariateILD** with input $h(x_0, x_{k+1})$ and update $P_0, \Lambda_{k+1}$.
For $((\mu_1, \ldots, \mu_n), h(x_0)) \in \Lambda_n$, update $P_m(\lambda_{m1}x_1 + \cdots + \lambda_{mn}x_n)$.
return $cP_0 \prod_{i=1}^{m} P_i(\lambda_{i1}x_1 + \cdots + \lambda_{in}x_n)$.
```

Complexity over $\mathbb{Z}$

Let $p \in \mathbb{Z}[x_1, \ldots, x_n]$. Then the algorithm **MultivariateILD** takes

$$\left(n + \log \|p\|_\infty + \deg_{x_1,\ldots,x_n}(p)\right)^{O(1)}$$

word operations.

Timings (in seconds)

Test suite: $p = P_0(x_1, \ldots, x_n) \prod_{i=1}^{m} P_i(\lambda_{i1} x_1 + \cdots + \lambda_{in} x_n)$

- $P_i(z) = f_{i1}(z) f_{i2}(z) f_{i3}(z)$, $n, m \in \mathbb{N}$,
- $\deg_{x_1,\ldots,x_n}(P_0) = d_0$ and $\deg_z(f_{ij}) = j \cdot d$.

(n, m, d_0, d)	AL	LZ	MILD
(2, 2, 5, 10)	2.25	3.39	0.77
(2, 2, 5, 15)	9.72	13.80	2.82
(2, 2, 5, 20)	44.20	35.80	6.68
(2, 3, 10, 10)	10.80	13.40	3.14
(2, 3, 20, 10)	17.10	16.00	3.80
(2, 3, 30, 10)	19.40	18.00	5.32
(2, 2, 20, 15)	15.20	16.00	3.34
(2, 3, 20, 15)	129.00	62.00	14.80
(2, 4, 20, 15)	801.00	181.00	47.40
(3, 2, 5, 5)	6.71	10.80	2.52
(4, 2, 5, 5)	710.00	657.00	440.00

Timings (in seconds)

Test suite: $p = P_0(x_1, \ldots, x_n) \prod_{i=1}^{m} P_i(\lambda_{i1} x_1 + \cdots + \lambda_{in} x_n)$

- $P_i(z) = f_{i1}(z) f_{i2}(z) f_{i3}(z)$, $n, m \in \mathbb{N}$,
- $\deg_{x_1,\ldots,x_n}(P_0) = d_0$ and $\deg_z(f_{ij}) = j \cdot d$.

(n, m, d_0, d)	AL	LZ	MILD
(2, 2, 5, 10)	2.25	3.39	0.77
(2, 2, 5, 15)	9.72	13.80	2.82
(2, 2, 5, 20)	44.20	35.80	6.68
(2, 3, 10, 10)	10.80	13.40	3.14
(2, 3, 20, 10)	17.10	16.00	3.80
(2, 3, 30, 10)	19.40	18.00	5.32
(2, 2, 20, 15)	15.20	16.00	3.34
(2, 3, 20, 15)	129.00	62.00	14.80
(2, 4, 20, 15)	801.00	181.00	47.40
(3, 2, 5, 5)	6.71	10.80	2.52
(4, 2, 5, 5)	710.00	657.00	440.00

Summary

Results.

- An efficient algorithm for bivariate integer-linear decomposition
- Generalized to handle general multivariate polynomials as well

Future work.

- q-Integer-linear decomposition for multivariate polynomials