Algorithms for Regular Chains of Dimension One

Msc thesis defense

Juan Pablo Gonzalez Trochez

supervised by Marc Moreno Maza

University of Western Ontario

April 20, 2022

jgonza55@uwo.ca

Agenda

Outline

Solving polynomial systems incrementally

- Most algorithms for solving polynomial systems **symbolically** proceed
  - *incrementally*, that is, solving one equation after another, against the solutions of the previously solved equations, or
  - by *projection and lifting*, that is, by successively **eliminating** one variable after another, and then proceeding by **back-substitution** as in linear system solving.
- The algorithm Triangularize of Maple's `RegularChains` library belongs to the category of incremental solving.
- Without entering technical details, we illustrate this algorithm in the following slides.

Incremental solving: a toy example

$$F = \begin{cases} y + w \\ 5w^2 + y \\ xz + z^3 + z \\ x^5 + x^3 + z \end{cases} = 0$$

$$\emptyset \xrightarrow{F[1]} \{y + w\}$$

$$F[2]: \quad \begin{Bmatrix} 5y + 1 \\ 5w - 1 \end{Bmatrix}, \quad \begin{Bmatrix} y \\ w \end{Bmatrix}$$

$$F[3]: \quad \begin{Bmatrix} x + z^2 + 1 \\ 5y + 1 \\ 5w - 1 \end{Bmatrix}, \begin{Bmatrix} 5y + 1 \\ z \\ 5w - 1 \end{Bmatrix}, \begin{Bmatrix} x + z^2 + 1 \\ y \\ w \end{Bmatrix}, \begin{Bmatrix} y \\ z \\ w \end{Bmatrix}$$

$$F[4]: \quad \begin{Bmatrix} x + z^2 + 1 \\ 5y + 1 \\ z^8 + \cdots \\ 5w - 1 \end{Bmatrix}, \begin{Bmatrix} x - z \\ 5y + 1 \\ z^2 + z + 1 \\ 5w - 1 \end{Bmatrix}, \begin{Bmatrix} x \\ 5y + 1 \\ z \\ 5w - 1 \end{Bmatrix}, \begin{Bmatrix} x^2 + 1 \\ 5y + 1 \\ z \\ 5w - 1 \end{Bmatrix}, \begin{Bmatrix} x + z^2 + 1 \\ y \\ z^8 + \cdots \\ w \end{Bmatrix}, \begin{Bmatrix} x - z \\ y \\ z^2 + z + 1 \\ w \end{Bmatrix}, \begin{Bmatrix} x^2 + 1 \\ y \\ z \\ w \end{Bmatrix}, \begin{Bmatrix} x \\ y \\ z \\ w \end{Bmatrix}$$

Incremental solving: a real-life example

```
> R := PolynomialRing([x,y,z,t,u]);F := [2*x + 2*y + 2*z + 2*t + u - 1, 2*x^2 + 2*y^2 + 2*
  z^2 + 2*t^2 + u^2 - u, 2*x*y + 2*y*z + 2*z*t + 2*t*u - t, 2*x*z + 2*y*t + t^2 + 2*z*u -
  z, 2*x*t + 2*z*t + 2*y*u - y];rc := Empty(R); lrc := [rc];
```

$$R := polynomial\_ring$$

$$F := [2\,x+2\,y+2\,z+2\,t+u-1, 2\,t^2+u^2+2\,x^2+2\,y^2+2\,z^2-u, 2\,t\,u+2\,z\,t+2\,x\,y+2\,y\,z-t, t^2+2\,y\,t +2\,z\,u+2\,x\,z-z, 2\,x\,t+2\,z\,t+2\,y\,u-y]$$

$$rc := regular\_chain$$

$$lrc := [rc] \tag{1}$$

```
> R := PolynomialRing([x,y,z,t,u]);F := [2*x + 2*y + 2*z + 2*t + u - 1, 2*x^2 + 2*y^2 + 2*
  z^2 + 2*t^2 + u^2 - u, 2*x*y + 2*y*z + 2*z*t + 2*t*u - t, 2*x*z + 2*y*t + t^2 + 2*z*u -
  z, 2*x*t + 2*z*t + 2*y*u - y];rc := Empty(R); lrc := [rc];
```

$$R := polynomial\_ring$$

$$F := [2\,x + 2\,y + 2\,z + 2\,t + u - 1, 2\,t^2 + u^2 + 2\,x^2 + 2\,y^2 + 2\,z^2 - u, 2\,t\,u + 2\,z\,t + 2\,x\,y + 2\,y\,z - t, t^2 + 2\,y\,t + 2\,z\,u + 2\,x\,z - z, 2\,x\,t + 2\,z\,t + 2\,y\,u - y]$$

$$rc := regular\_chain$$

$$lrc := [rc] \qquad \textbf{(1)}$$

```
> ## solving F[1] against lrc
> a:= time(): lrc := [ seq ( op(Intersect(F[1], ts, R)), ts=lrc ) ]; map(Dimension, lrc, R)
  ; time() - a;
```

$$lrc := [regular\_chain]$$

$$[4]$$

$$0.008 \qquad \textbf{(2)}$$

```
> R := PolynomialRing([x,y,z,t,u]);F := [2*x + 2*y + 2*z + 2*t + u - 1, 2*x^2 + 2*y^2 + 2*
  z^2 + 2*t^2 + u^2 - u, 2*x*y + 2*y*z + 2*z*t + 2*t*u - t, 2*x*z + 2*y*t + t^2 + 2*z*u -
  z, 2*x*t + 2*z*t + 2*y*u - y];rc := Empty(R); lrc := [rc];
> ## solving F[1] against lrc
> a:= time(): lrc := [ seq ( op(Intersect(F[1], ts, R)), ts=lrc ) ]; map(Dimension, lrc, R)
  ; time() - a;
```

$$lrc := [regular\_chain]$$

$$[4]$$

$$0.008 \tag{1}$$

```
> ## solving F[2] against lrc
> a := time() ; lrc := [ seq ( op(Intersect(F[2], ts, R)), ts=lrc ) ]; map(Dimension, lrc,
  R);time() - a;
```

$$a := 0.272$$

$$lrc := [regular\_chain]$$

$$[3]$$

$$0.036 \tag{2}$$

```
> R := PolynomialRing([x,y,z,t,u]);F := [2*x + 2*y + 2*z + 2*t + u - 1, 2*x^2 + 2*y^2 + 2*
  z^2 + 2*t^2 + u^2 - u, 2*x*y + 2*y*z + 2*z*t + 2*t*u - t, 2*x*z + 2*y*t + t^2 + 2*z*u -
  z, 2*x*t + 2*z*t + 2*y*u - y];rc := Empty(R); lrc := [rc];
> ## solving F[1] against lrc
> a:= time(): lrc := [ seq ( op(Intersect(F[1], ts, R)), ts=lrc ) ]; map(Dimension, lrc, R)
  ; time() - a;
> ## solving F[2] against lrc
> a := time() ; lrc := [ seq ( op(Intersect(F[2], ts, R)), ts=lrc ) ]; map(Dimension, lrc,
  R);time() - a;
```

$$a := 0.272$$
$$lrc := [regular\_chain]$$
$$[3]$$
$$0.036 \tag{1}$$

```
> ## solving F[3] against lrc
> a := time(): lrc := [ seq ( op(Intersect(F[3], ts, R)), ts=lrc ) ]; map(Dimension, lrc,
  R);time() - a;
```

$$lrc := [regular\_chain, regular\_chain]$$
$$[2, 1]$$
$$0.043 \tag{2}$$

```
> R := PolynomialRing([x,y,z,t,u]);F := [2*x + 2*y + 2*z + 2*t + u - 1, 2*x^2 + 2*y^2 + 2*
  z^2 + 2*t^2 + u^2 - u, 2*x*y + 2*y*z + 2*z*t + 2*t*u - t, 2*x*z + 2*y*t + t^2 + 2*z*u -
  z, 2*x*t + 2*z*t + 2*y*u - y];rc := Empty(R); lrc := [rc];
> ## solving F[1] against lrc
> a:= time(): lrc := [ seq ( op(Intersect(F[1], ts, R)), ts=lrc ) ]; map(Dimension, lrc, R)
  ; time() - a;
> ## solving F[2] against lrc
> a := time() ; lrc := [ seq ( op(Intersect(F[2], ts, R)), ts=lrc ) ]; map(Dimension, lrc,
  R);time() - a;
> ## solving F[3] against lrc
> a := time(): lrc := [ seq ( op(Intersect(F[3], ts, R)), ts=lrc ) ]; map(Dimension, lrc,
  R);time() - a;
> ## solving F[4] against lrc
> a:= time(): lrc := [ seq ( op(Intersect(F[4], ts, R)), ts=lrc ) ]; map(Dimension, lrc, R)
  ;time() - a;
```

lrc := [*regular_chain*, *regular_chain*, *regular_chain*, *regular_chain*, *regular_chain*, *regular_chain*, *regular_chain*, *regular_chain*, *regular_chain*]

[1, 0, 0, 0, 0, 0, 0, 0, 0]

0.383 **(1)**

```
> ## solving F[1] against lrc
> a:= time(): lrc := [ seq ( op(Intersect(F[1], ts, R)), ts=lrc ) ]; map(Dimension, lrc, R)
  ; time() - a;
> ## solving F[2] against lrc
> a := time() ; lrc := [ seq ( op(Intersect(F[2], ts, R)), ts=lrc ) ]; map(Dimension, lrc,
  R);time() - a;
> ## solving F[3] against lrc
> a := time(): lrc := [ seq ( op(Intersect(F[3], ts, R)), ts=lrc ) ]; map(Dimension, lrc,
  R);time() - a;
> ## solving F[4] against lrc
> a:= time(): lrc := [ seq ( op(Intersect(F[4], ts, R)), ts=lrc ) ]; map(Dimension, lrc, R)
  ;time() - a;
```

$lrc := [regular\_chain, regular\_chain, regular\_chain, regular\_chain, regular\_chain, regular\_chain, regular\_chain, regular\_chain, regular\_chain]$

$$[1, 0, 0, 0, 0, 0, 0, 0, 0]$$

$$0.011 \tag{1}$$

```
> ## solving F[5] against the first regular chain in lrc
> a := time() : Intersect(F[5], lrc[1], R); time() -a ;
```

$$[regular\_chain, regular\_chain]$$

$$2.512 \tag{2}$$

```
> ## solving F[3] against lrc
> a := time(): lrc := [ seq ( op(Intersect(F[3], ts, R)), ts=lrc ) ]; map(Dimension, lrc, R);time() - a;
> ## solving F[4] against lrc
> a:= time(): lrc := [ seq ( op(Intersect(F[4], ts, R)), ts=lrc ) ]; map(Dimension, lrc, R);time() - a;
```

$lrc := [regular\_chain, regular\_chain, regular\_chain, regular\_chain, regular\_chain, regular\_chain, regular\_chain, regular\_chain, regular\_chain]$

$$[1, 0, 0, 0, 0, 0, 0, 0, 0]$$

$$0.011 \quad (1)$$

```
> ## solving F[5] against the first regular chain in lrc
> a := time() : Intersect(F[5], lrc[1], R); time() -a ;
```

$$[regular\_chain, regular\_chain]$$

$$2.512 \quad (2)$$

```
> ## solving F[5] against the other chains in lrc
> a:= time() ; [ seq ( op(Intersect(F[5], ts, R)), ts=lrc[2..-1] )]; time() - a;
```

$$a := 3.493$$

$$[regular\_chain, regular\_chain]$$

$$0.022 \quad (3)$$

A 1-dimensional regular chain T over $\mathbb{K}[x_1 < x_2 < \cdots < x_n]$ looks like

$$T : \begin{cases} t_2(x_1, x_2) &= h_2(x_1)x_2^{d_2} + \cdots \\ t_3(x_1, x_2, x_3) &= h_3(x_1)x_3^{d_3} + \cdots \\ \vdots & \vdots \quad \vdots \\ t_n(x_1, x_2, \ldots, x_n) &= h_n(x_1)x_n^{d_n} + \cdots, \end{cases} \tag{1}$$

- T can be seen as a **parametrization** of a space curve C, namely $C = W(T) := V(T) \setminus V(h)$, where $h := \prod_{i=2}^{n} h_i$
- $\overline{W(T)} \setminus W(T) = \{$limits points of C when x_1 approaches $\zeta \mid \zeta$ a root of $h\}$.
- We can compute these **limit points by factorizing** $t_2, t_3, \ldots, t_n$ over the field $\mathbb{C}((x_1^*))$ of univariate **Puiseux series** in x_1.

Example

Let $T \subseteq \mathbb{K}[x > y > z]$ be a regular chain

$$T := \begin{cases} z\,x - y^2 \\ y^5 - z^4 \end{cases}.$$

In this case: $h = z$ and $\zeta = 0$.
Then, over $\mathbb{C}((x_1^*))$

$$\mathcal{V}(T) = \{(x = z^{3/5}, y = z^{4/5})\}$$

Thus we have:

$$\overline{W(T)} \setminus W(T) = \{(0,0,0)\}.$$

Example

Consider $T \subseteq \mathbb{K}[x > y > z]$:

$$T := \begin{cases} z\,x - y^2 = 0 \\ y^5 - z^2 = 0 \end{cases}.$$

In this case: $h = z$ and $\zeta = 0$.
Then, over $\mathbb{C}((x_1^*))$

$$\mathcal{V}(T) = \{(x = z^{-1/5}, y = z^{2/5})\}$$

Since the Puiseux series $z^{-1/5}$ has a **negative order**, we have:

$$\overline{W(T)} \setminus W(T) = \emptyset.$$

Outline

Outline

Regular chains

Let $\mathbb{K}$ be a perfect field, and $\mathbb{K}[X]$ have ordered vars. $X = X_1 < \cdots < X_n$.

A **triangular set** $T \subset \mathbb{K}[X]$ is a **regular chain** if either T is empty, or T_v^- is a regular chain and h is regular modulo $\mathrm{sat}(T_v^-)$.

$$T = \left\{ \begin{array}{l} T_v = h\, v^d + \mathrm{tail}(T_v) \\ \\ T_v^- = \left\{ \quad \right\} \end{array} \right\}$$

$$T = \left\{ \begin{array}{r} (2y + ba)x - by + a^2 \\ 2y^2 - by - a^2 \\ a + b \end{array} \right\} \subset \mathbb{Q}[b < a < y < x]$$

Saturated ideal of a regular chain:

- $\mathrm{sat}(T) = (\mathrm{sat}(T_v^-) + T_v) : h^\infty$
- $\mathrm{sat}(\emptyset) = \langle 0 \rangle$

Quasi-component of a regular chain:

- $W(T) := V(T) \setminus V(h_T)$, $h_T := \prod_{p \in T} h_p$
- $\overline{W(T)} = V(\mathrm{sat}(T))$

The algorithms Intersect and Triangularize

Intersect

Let $p \in \mathbb{K}[X]$ and let $T \subseteq \mathbb{K}[X]$ be a regular chain. The function call Intersect(p, T) computes regular chains $T_1, \ldots, T_e \subseteq \mathbb{K}[X]$ such that:

$$V(p) \cap W(T) \subseteq W(T_1) \cup \cdots \cup W(T_e) \subseteq V(p) \cap \overline{W(T)}. \tag{2}$$

Triangularize

Given a finite set $F = \{f_0, f_1, f_2, \ldots\} \subseteq \mathbb{K}[X]$, Triangularize$(F)$ compute regular chains $T_1, \ldots, T_e \subseteq \mathbb{K}[X]$ **encoding the solutions** of $V(F)$:

$$V(F) = W(T_1) \cup \cdots \cup W(T_e). \tag{3}$$

This is achieved by successively applying Intersect to $f_0, f_1, f_2, \ldots$ on the previously obtained regular chains.

Outline

Input: $f, t, b \in \mathbb{K}[x > y > z]$ with $\{t, b\}$ regular chain $\mathrm{mvar}(t) = x, \mathrm{mvar}(b) = y$.

Output: Intersect$(f, \{t, b\})$.

Hypothesis:

$$\mathrm{mvar}(f) = x.$$

Input: $f, t, b \in \mathbb{K}[x > y > z]$ with $\{t, b\}$ regular chain $\mathrm{mvar}(t) = x, \mathrm{mvar}(b) = y$.

Output: Intersect$(f, \{t, b\})$.

Hypothesis:

$$\mathrm{mvar}(f) = x.$$

Let $r = \mathrm{res}(t, f, x)$ and ℓ be the subresultants of index 0 and 1 of f and t.

Hypothesis:

$$r \notin \mathbb{K} \text{ and } \mathrm{mvar}(r) = y.$$

Input: $f, t, b \in \mathbb{K}[x > y > z]$ with $\{t, b\}$ regular chain $\mathrm{mvar}(t) = x, \mathrm{mvar}(b) = y$.

Output: Intersect$(f, \{t, b\})$.

Hypothesis:

$$\mathrm{mvar}(f) = x.$$

Let $r = \mathrm{res}(t, f, x)$ and ℓ be the subresultants of index 0 and 1 of f and t.

Hypothesis:

$$r \notin \mathbb{K} \text{ and } \mathrm{mvar}(r) = y.$$

Let $s = \mathrm{res}(r, b, y)$ and g be the subresultants of index 0 and 1 of r and b.

Hypothesis:

$$C := \{s, g, \ell\} \text{ is a regular chain.}$$

Hypothesis:

$$\mathrm{lc}(t, x) \text{ invertible modulo } < s, g > .$$

Input: $f, t, b \in \mathbb{K}[x > y > z]$ with $\{t, b\}$ regular chain $\mathrm{mvar}(t) = x, \mathrm{mvar}(b) = y$.

Let $r = \mathrm{res}(t, f, x)$ and ℓ be the subresultants of index 0 and 1 of f and t.

Let $s = \mathrm{res}(r, b, y)$ and g be the subresultants of index 0 and 1 of r and b.

Output: $\mathrm{Intersect}(f, \{t, b\})$.

Hypothesis:

$$\mathrm{mvar}(f) = x.$$

Hypothesis:

$$r \notin \mathbb{K} \text{ and } \mathrm{mvar}(r) = y.$$

Hypothesis:

$$C := \{s, g, \ell\} \text{ is a regular chain.}$$

Hypothesis:

$$\mathrm{lc}(t, x) \text{ invertible modulo } < s, g > .$$

Theorem:

$$V(f, t, b) = V(s, g, \ell).$$

$R := PolynomialRing([x, y, z])$:

$f := (y + z) * x\verb|^|2 + x + 1;$
$t := z * x\verb|^|2 + y * x + 1;$
$b := (z+1) * y\verb|^|2 + y + 2;$

$$f := (y+z)\,x^2 + x + 1$$
$$t := z\,x^2 + y\,x + 1$$
$$b := (z+1)\,y^2 + y + 2 \tag{1}$$

$src1 := SubresultantChain(f, t, x, R)$:
$l := SubresultantOfIndex(1, src1, R);\ r := SubresultantOfIndex(0, src1, R);$

$$l := x\,y^2 + x\,y\,z - x\,z + y$$
$$r := y^3 + y^2 z - 2\,y\,z + z \tag{2}$$

$src2 := SubresultantChain(r, b, y, R)$:
$g := SubresultantOfIndex(1, src2, R);\ \ s := SubresultantOfIndex(0, src2, R);$

$$g := -2\,y\,z^3 - 5\,y\,z^2 + z^3 - 5\,y\,z - y - z + 2$$
$$s := z^5 + 9\,z^4 + 24\,z^3 + 38\,z^2 + 13\,z + 8 \tag{3}$$

$sol := Chain([s], Empty(R), R) :\ IsRegular(Initial(g, R), sol, R);$

$$true \tag{4}$$

$sol2 := Chain([g], sol, R) : IsRegular(Initial(l, R), sol2, R);$

$$true \tag{5}$$

$IsRegular(Initial(t, R), sol2, R);$

$$true \tag{6}$$

$sol3 := Chain([l], sol2, R) : Display(sol3, R);$

$$\begin{cases} (y^2 + y\,z - z)\,x + y = 0 \\ (-2\,z^3 - 5\,z^2 - 5\,z - 1)\,y + z^3 - z + 2 = 0 \\ z^5 + 9\,z^4 + 24\,z^3 + 38\,z^2 + 13\,z + 8 = 0 \\ y^2 + y\,z - z \neq 0 \\ -2\,z^3 - 5\,z^2 - 5\,z - 1 \neq 0 \end{cases} \tag{7}$$

$dec3 := Triangularize([f, t, b], R) : Display(dec3[1], R);$

$$\begin{cases} (y^2 + y\,z - z)\,x + y = 0 \\ (2\,z^3 + 5\,z^2 + 5\,z + 1)\,y - z^3 + z - 2 = 0 \\ z^5 + 9\,z^4 + 24\,z^3 + 38\,z^2 + 13\,z + 8 = 0 \\ y^2 + y\,z - z \neq 0 \\ 2\,z^3 + 5\,z^2 + 5\,z + 1 \neq 0 \end{cases} \tag{8}$$

Outline

The Modular Method

Key ideas

- Computing the **subresultants** $r = S_0(t, f, x)$, $\ell = S_1(t, f, x)$, $s = S_0(r, b, y)$, $g = S_1(r, b, y)$ by **evaluation and interpolation**.

The Modular Method

Key ideas

- Computing the **subresultants** $r = S_0(t, f, x)$, $\ell = S_1(t, f, x)$, $s = S_0(r, b, y)$, $g = S_1(r, b, y)$ by **evaluation and interpolation**.
- (Probabilistic approach) Use the **Bézout bound** of the (zero-dimensional) variety $V(f, t, b)$ for this evaluation and interpolation process.

The Modular Method

Key ideas

- Computing the **subresultants** $r = S_0(t, f, x)$, $\ell = S_1(t, f, x)$, $s = S_0(r, b, y)$, $g = S_1(r, b, y)$ by **evaluation and interpolation**.
- (Probabilistic approach) Use the **Bézout bound** of the (zero-dimensional) variety $V(f, t, b)$ for this evaluation and interpolation process.
- Verify the **genericity assumptions** as we recover ℓ, s, g from the evaluation and interpolation process, returning an **error** if one of those assumptions is not met.

The implementation

Algorithm 1 IntersectBySpecialization

---

while $i \leq bnd := 2 * BezoutBdn + 1$ **do**
    Select a point v and specialize f, t, b at $z = v$.
    if f, t, b does not specialize well **then**
        Next
    Normalize T to $T_v = \{t_v, b_v\}$.
    Compute $r_v = S_0(t_v, f_v, x)$, $\ell_v = S_1(t_v, f_v, x)$.
    Check assumptions about r.
    Compute $s_v = S_0(r_v, b_v, y)$, $g_v = S_1(r_v, b_v, y)$.
Interpolate s_v, g_v, ℓ_v into s, g, ℓ.
Apply Rational Function Reconstruction to s, g, ℓ.
Replace s, g, ℓ by their numerators.
Compute the squarefree part of s, $\overline{s}$.
Check that $C = \{\overline{s}, g, \ell\}$ is a regular chain and the initial of t.

Outline

A first example

Example

- Prime characteristic 469762049.

A first example

Example

- Prime characteristic 469762049.
- $t = zx^2 + yx + 1$,
- $b = (z+1)y^2 + y + 2$,
- $f = (y+z)x^2 + x + 1$.

A first example

Example

- Prime characteristic 469762049.
- $t = zx^2 + yx + 1$,
- $b = (z+1)y^2 + y + 2$,
- $f = (y+z)x^2 + x + 1$.
- **Intersect time:** 0.010s, **Intersect by Specialization time:** 0.114s

A first example

Example

- Prime characteristic 469762049.
- $t = zx^2 + yx + 1$,
- $b = (z+1)y^2 + y + 2$,
- $f = (y+z)x^2 + x + 1$.
- **Intersect time:** 0.010s, **Intersect by Specialization time:** 0.114s
- $s = z^5 + 9z^4 + 2 * z^3 + 38z^2 + 13z + 8$.

A first example

Example

- Prime characteristic 469762049.
- $t = zx^2 + yx + 1$,
- $b = (z + 1)y^2 + y + 2$,
- $f = (y + z)x^2 + x + 1$.
- **Intersect time:** 0.010s, **Intersect by Specialization time:** 0.114s
- $s = z^5 + 9z^4 + 2 * z^3 + 38z^2 + 13z + 8$.
- $g = z^3 + 469762048z + 2 + (469762047z^3 + 469762044z^2 + 469762044z + 469762048)y$.

A first example

Example

- Prime characteristic 469762049.
- $t = zx^2 + yx + 1$,
- $b = (z+1)y^2 + y + 2$,
- $f = (y+z)x^2 + x + 1$.
- **Intersect time:** 0.010s, **Intersect by Specialization time:** 0.114s
- $s = z^5 + 9z^4 + 2 * z^3 + 38z^2 + 13z + 8$.
- $g = z^3 + 469762048z + 2 + (469762047z^3 + 469762044z^2 + 469762044z + 469762048)y$.
- $\ell = z^3 + 469762048z + 2 + (469762047z^3 + 469762044z^2 + 469762044z + 469762048)y$.

A second example

Example

- Prime characteristic 469762049.

A second example

Example

- Prime characteristic 469762049.
- $t = 4x^9 - 40x^5y^2z + 6x^3y^3z + 27xy^6 + 68xy^3z^2 - 11z^5$,
- $b = -33y^8z + 8y^5z^2 - 69y^4z^2 - 34z^6 - 58y^5 - 53yz^2$,
- $f = -7x^3y^2z^4 - 50y^4z^5 - 70x^3y^5 + 19xy^5 - 5y^3z + 48x$.

A second example

Example

- Prime characteristic 469762049.
- $t = 4x^9 - 40x^5y^2z + 6x^3y^3z + 27xy^6 + 68xy^3z^2 - 11z^5$,
- $b = -33y^8z + 8y^5z^2 - 69y^4z^2 - 34z^6 - 58y^5 - 53yz^2$,
- $f = -7x^3y^2z^4 - 50y^4z^5 - 70x^3y^5 + 19xy^5 - 5y^3z + 48x$.
- **Intersect time:** 298.017s, **Intersect by Specialization time:** 30.187s

A second example

Example

- Prime characteristic 469762049.
- $t = 4x^9 - 40x^5y^2z + 6x^3y^3z + 27xy^6 + 68xy^3z^2 - 11z^5$,
- $b = -33y^8z + 8y^5z^2 - 69y^4z^2 - 34z^6 - 58y^5 - 53yz^2$,
- $f = -7x^3y^2z^4 - 50y^4z^5 - 70x^3y^5 + 19xy^5 - 5y^3z + 48x$.
- **Intersect time:** 298.017s, **Intersect by Specialization time:** 30.187s
- $\deg(s) = 573$, $\deg(g) = 504$, $\deg(\ell) = 64$.

Benchmark

Prime characteristic 469762049.

N	deg(t)	deg(b)	deg(f)	bound B	Num. Iterations	Intersect	Intersect by Specialization	Intersect by Specialization (BPAS)
1	5	4	5	201	201	**0.184s**	1.705s	0.0983s
2	5	4	4	161	161	**0.126s**	0.377s	0.0392s
3	5	4	5	201	201	**0.200s**	0.673s	0.0772s
4	5	4	5	201	201	**0.433s**	1.091s	0.1038s
5	8	8	8	1025	1025	24.687s	**13.763s**	2.6651s
6	8	8	8	1025	1025	43.324s	**18.497s**	4.1805s
7	8	8	8	1025	1025	43.557s	**16.778s**	3.4076s
8	8	8	8	1025	1025	**5.700s**	12.683s	2.4368s

Table: Examples 1

N	deg(t)	deg(b)	deg(f)	bound B	Num. Iterations	Intersect	Intersect by Specialization	Intersect by Specialization (BPAS)
9	8	8	8	1025	1025	**1.696s**	7.075s	0.9383s
10	7	6	7	589	589	13.110s	**11.313s**	1.3616s
11	8	7	8	897	897	17.246s	**16.084s**	2.1516s
12	8	7	8	897	897	20.584s	**17.331s**	2.8275s
13	9	9	9	1459	1459	301.062s	**27.999s**	7.6849s
14	8	8	8	1153	1153	63.850s	**23.085s**	4.6934s
15	8	7	8	897	897	15.580s	**15.870s**	2.2245s
16	8	7	8	897	897	**10.970s**	16.910s	2.3988s
17	8	8	8	1025	1025	24.418s	**12.920s**	2.7127s
18	9	8	9	1153	1153	70.321s	**24.952s**	4.6852s

Table: Examples 2

Outline

Outline

Cones

skip slide

We require additional constrains for the definition of a cone.

Cones

skip slide We require additional constrains for the definition of a cone.

Definition

A set $C \subseteq \mathbb{R}^p$ is a ***cone*** when the following properties hold:

Cones

skip slide We require additional constrains for the definition of a cone.

Definition

A set $C \subseteq \mathbb{R}^p$ is a ***cone*** when the following properties hold:

1. if $\mathbf{v} \in C$ and $c \geq 0$ hold, then we have $c \cdot \mathbf{v} \in C$.

Cones

▸▸ skip slide We require additional constrains for the definition of a cone.

Definition

A set $C \subseteq \mathbb{R}^p$ is a ***cone*** when the following properties hold:

1. if $\mathbf{v} \in C$ and $c \geq 0$ hold, then we have $c \cdot \mathbf{v} \in C$.
2. C is **finitely generated**, i.e., there exist $\mathbf{r}_1, \ldots, \mathbf{r}_m \in \mathbb{R}^p$ such that

$$C = \{z_1\mathbf{r}_1 + \cdots + z_n\mathbf{r}_m \mid z_1, \ldots, z_m \geq 0\}.$$

The set $\mathbf{R} := \{\mathbf{r}_1, \ldots, \mathbf{r}_m\}$ is called a *generating set* of C, and its members are called rays of the cone C.

Cones

skip slide We require additional constrains for the definition of a cone.

Definition

A set $C \subseteq \mathbb{R}^p$ is a ***cone*** when the following properties hold:

1. if $\mathbf{v} \in C$ and $c \geq 0$ hold, then we have $c \cdot \mathbf{v} \in C$.
2. C is **finitely generated**, i.e., there exist $\mathbf{r}_1, \ldots, \mathbf{r}_m \in \mathbb{R}^p$ such that

$$C = \{z_1\mathbf{r}_1 + \cdots + z_n\mathbf{r}_m \mid z_1, \ldots, z_m \geq 0\}.$$

   The set $\mathbf{R} := \{\mathbf{r}_1, \ldots, \mathbf{r}_m\}$ is called a *generating set* of C, and its members are called rays of the cone C.

3. C is **rational**, i.e., C is finitely generated and has a generating set $\{\mathbf{r}_1, \ldots, \mathbf{r}_m\} \subset \mathbb{Z}^p$.

Additive total order

We said that a **total order** $\preceq$ on $\mathbb{Z}^p$ is ***additive*** if for all $\mathbf{i}, \mathbf{j}, \mathbf{k} \in \mathbb{Z}^p$, we have:

$$\mathbf{i} \preceq \mathbf{j} \implies \mathbf{i} + \mathbf{k} \preceq \mathbf{j} + \mathbf{k}.$$

Additive total order

We said that a **total order** $\preceq$ on $\mathbb{Z}^p$ is ***additive*** if for all $\mathbf{i}, \mathbf{j}, \mathbf{k} \in \mathbb{Z}^p$, we have:

$$\mathbf{i} \preceq \mathbf{j} \implies \mathbf{i} + \mathbf{k} \preceq \mathbf{j} + \mathbf{k}.$$

Definition

An additive order $\preceq$ on $\mathbb{Z}^p$ is said to be ***compatible*** *with a cone* $C \subseteq \mathbb{R}^p$ if $\mathbf{0} \preceq \mathbf{k}$ holds, for all $\mathbf{k} \in C \cap \mathbb{Z}^p$.

Additive total order

We said that a **total order** $\preceq$ on $\mathbb{Z}^p$ is ***additive*** if for all $\mathbf{i}, \mathbf{j}, \mathbf{k} \in \mathbb{Z}^p$, we have:

$$\mathbf{i} \preceq \mathbf{j} \implies \mathbf{i} + \mathbf{k} \preceq \mathbf{j} + \mathbf{k}.$$

Definition

An additive order $\preceq$ on $\mathbb{Z}^p$ is said to be ***compatible*** *with a cone* $C \subseteq \mathbb{R}^p$ if $\mathbf{0} \preceq \mathbf{k}$ holds, for all $\mathbf{k} \in C \cap \mathbb{Z}^p$.

Line-free cone

An another property of cones that we use through this document is the following: C is said to be ***line-free*** if for every $\mathbf{v} \in C \setminus \{\mathbf{0}\}$, we have $-\mathbf{v} \notin C$.

Lemma (see [2])

Let $C, D \subseteq \mathbb{R}^p$ be cones and let $\preceq$ be an **additive order** *on $\mathbb{Z}^p$. Let $\{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ be a set of generators of C.*

Lemma (see [2])

*Let $C, D \subseteq \mathbb{R}^p$ be cones and let $\preceq$ be an **additive order** on $\mathbb{Z}^p$. Let $\{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ be a set of generators of C.*

1. *If C is **compatible** with $\preceq$, then C is line-free.*

Lemma (see [2])

*Let $C, D \subseteq \mathbb{R}^p$ be cones and let $\preceq$ be an **additive order** on $\mathbb{Z}^p$. Let $\{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ be a set of generators of C.*

1. *If C is **compatible** with $\preceq$, then C is line-free.*
2. *C is **compatible** with $\preceq$, if and only if $\mathbf{0} \preceq \mathbf{v}_i$ for all i.*

Lemma (see [2])

*Let $C, D \subseteq \mathbb{R}^p$ be cones and let $\preceq$ be an **additive order** on $\mathbb{Z}^p$. Let $\{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ be a set of generators of C.*

1. *If C is **compatible** with $\preceq$, then C is line-free.*
2. *C is **compatible** with $\preceq$, if and only if $\mathbf{0} \preceq \mathbf{v}_i$ for all i.*
3. *If C, D are **compatible** with $\preceq$, then $C + D$ is also compatible with $\preceq$.*

Outline

Notation

Let $\mathbb{K}$ be a field, $\mathbf{x} = x_1, \ldots, x_p$ and $\mathbf{u} = u_1, \ldots, u_m$ be ordered indeterminates with $m \geq p$. We follow the ideas exposed by Monforte and Kauers presented in [2].

Notation

Let $\mathbb{K}$ be a field, $\mathbf{x} = x_1, \ldots, x_p$ and $\mathbf{u} = u_1, \ldots, u_m$ be ordered indeterminates with $m \geq p$. We follow the ideas exposed by Monforte and Kauers presented in [2].

- $\mathbb{K}[[\mathbf{u}]]$: ring of multivariate formal power series.
- $g(\mathbf{u}) \in \mathbb{K}[[\mathbf{u}]]$ means:

$$g(\mathbf{u}) = \sum_{\mathbf{k} \in \mathbb{N}^m} a_{\mathbf{k}} \mathbf{u}^{\mathbf{k}},$$

for some $a_{\mathbf{k}}$ in $\mathbb{K}$, and $\mathbf{u}^{\mathbf{k}}$ is a notation for $u_1^{k_1} \cdots u_m^{k_m}$ where $k_, \ldots, k_m$ are non-negative integers.

Notation

Let $\mathbb{K}$ be a field, $\mathbf{x} = x_1, \ldots, x_p$ and $\mathbf{u} = u_1, \ldots, u_m$ be ordered indeterminates with $m \geq p$. We follow the ideas exposed by Monforte and Kauers presented in [2].

- $\mathbb{K}[[\mathbf{u}]]$: ring of multivariate formal power series.
- $g(\mathbf{u}) \in \mathbb{K}[[\mathbf{u}]]$ means:

$$g(\mathbf{u}) = \sum_{\mathbf{k} \in \mathbb{N}^m} a_{\mathbf{k}} \mathbf{u}^{\mathbf{k}},$$

for some $a_{\mathbf{k}}$ in $\mathbb{K}$, and $\mathbf{u}^{\mathbf{k}}$ is a notation for $u_1^{k_1} \cdots u_m^{k_m}$ where $k_, \ldots, k_m$ are non-negative integers.

- $\mathbb{K}((\mathbf{x}))$: field of multivariate formal Laurent series.
- $f(\mathbf{x}) \in \mathbb{K}((\mathbf{x}))$ means:

$$f(\mathbf{x}) := \sum_{\mathbf{k} \in \mathbb{Z}^p} a_{\mathbf{k}} \mathbf{x}^{\mathbf{k}},$$

where the $a_{\mathbf{k}}$ are elements of $\mathbb{K}$.

- Let $C \subseteq \mathbb{R}^p$ be a line-free cone. Then, we denote by $\mathbb{K}_C[[\mathbf{x}]]$ the set of the Laurent series f over $\mathbb{K}$, with variables $\mathbf{x}$, such that:

$$\mathrm{supp}(f(\mathbf{x})) := \{\mathbf{k} \in \mathbb{Z}^p \mid a_{\mathbf{k}} \neq 0\} \subseteq C.$$

- Let $C \subseteq \mathbb{R}^p$ be a **line-free** cone. Then, we denote by $\mathbb{K}_C[[\mathbf{x}]]$ the set of the Laurent series f over $\mathbb{K}$, with variables $\mathbf{x}$, such that:

$$\mathrm{supp}(f(\mathbf{x})) := \{\mathbf{k} \in \mathbb{Z}^p \mid a_{\mathbf{k}} \neq 0\} \subseteq C.$$

- $\mathbb{K}_C[[\mathbf{x}]]$ together with the natural addition and multiplication is an **integral domain**.

- Let $C \subseteq \mathbb{R}^p$ be a **line-free** cone. Then, we denote by $\mathbb{K}_C[[\mathbf{x}]]$ the set of the Laurent series f over $\mathbb{K}$, with variables $\mathbf{x}$, such that:

$$\operatorname{supp}(f(\mathbf{x})) := \{\mathbf{k} \in \mathbb{Z}^p \mid a_{\mathbf{k}} \neq 0\} \subseteq C.$$

- $\mathbb{K}_C[[\mathbf{x}]]$ together with the natural addition and multiplication is an **integral domain**.
- Let $f(\mathbf{x}) = \sum_{\mathbf{k}} a_{\mathbf{k}} \mathbf{x}^{\mathbf{k}} \in \mathbb{K}_C[[\mathbf{x}]]$. Then, there exists $g(\mathbf{x}) \in \mathbb{K}_C[[\mathbf{x}]]$ with $f(\mathbf{x})g(\mathbf{x}) = 1$, if and only if $a_{\mathbf{0}} \neq 0$.

- Let $C \subseteq \mathbb{R}^p$ be a line-free cone. Then, we denote by $\mathbb{K}_C[[\mathbf{x}]]$ the set of the Laurent series f over $\mathbb{K}$, with variables $\mathbf{x}$, such that:

$$\mathrm{supp}(f(\mathbf{x})) := \{\mathbf{k} \in \mathbb{Z}^p \mid a_{\mathbf{k}} \neq 0\} \subseteq C.$$

- $\mathbb{K}_C[[\mathbf{x}]]$ together with the natural addition and multiplication is an integral domain.
- Let $f(\mathbf{x}) = \sum_{\mathbf{k}} a_{\mathbf{k}} \mathbf{x}^{\mathbf{k}} \in \mathbb{K}_C[[\mathbf{x}]]$. Then, there exists $g(\mathbf{x}) \in \mathbb{K}_C[[\mathbf{x}]]$ with $f(\mathbf{x})g(\mathbf{x}) = 1$, if and only if $a_{\mathbf{0}} \neq 0$.

- Let $\preceq$ be an additive order in $\mathbb{Z}^p$ and let $\mathcal{C}$ be the set of all cones $C \subseteq \mathbb{R}^p$ which are compatible with $\preceq$.

- Let $C \subseteq \mathbb{R}^p$ be a **line-free** cone. Then, we denote by $\mathbb{K}_C[[\mathbf{x}]]$ the set of the Laurent series f over $\mathbb{K}$, with variables $\mathbf{x}$, such that:

$$\mathrm{supp}(f(\mathbf{x})) := \{\mathbf{k} \in \mathbb{Z}^p \mid a_{\mathbf{k}} \neq 0\} \subseteq C.$$

- $\mathbb{K}_C[[\mathbf{x}]]$ together with the natural addition and multiplication is an **integral domain**.
- Let $f(\mathbf{x}) = \sum_{\mathbf{k}} a_{\mathbf{k}} \mathbf{x}^{\mathbf{k}} \in \mathbb{K}_C[[\mathbf{x}]]$. Then, there exists $g(\mathbf{x}) \in \mathbb{K}_C[[\mathbf{x}]]$ with $f(\mathbf{x})g(\mathbf{x}) = 1$, if and only if $a_{\mathbf{0}} \neq 0$.

- Let $\preceq$ be an **additive order** in $\mathbb{Z}^p$ and let $\mathcal{C}$ be the set of all cones $C \subseteq \mathbb{R}^p$ which are **compatible** with $\preceq$.
- Define

$$\mathbb{K}_{\preceq}[[\mathbf{x}]] := \bigcup_{C \in \mathcal{C}} \mathbb{K}_C[[\mathbf{x}]] \quad \text{and} \quad \mathbb{K}_{\preceq}((\mathbf{x})) := \bigcup_{\mathbf{e} \in \mathbb{Z}^p} \mathbf{x}^{\mathbf{e}} \mathbb{K}_{\preceq}[[\mathbf{x}]],$$

- Let $C \subseteq \mathbb{R}^p$ be a **line-free** cone. Then, we denote by $\mathbb{K}_C[[\mathbf{x}]]$ the set of the Laurent series f over $\mathbb{K}$, with variables $\mathbf{x}$, such that:

$$\operatorname{supp}(f(\mathbf{x})) := \{\mathbf{k} \in \mathbb{Z}^p \mid a_{\mathbf{k}} \neq 0\} \subseteq C.$$

- $\mathbb{K}_C[[\mathbf{x}]]$ together with the natural addition and multiplication is an **integral domain**.
- Let $f(\mathbf{x}) = \sum_{\mathbf{k}} a_{\mathbf{k}} \mathbf{x}^{\mathbf{k}} \in \mathbb{K}_C[[\mathbf{x}]]$. Then, there exists $g(\mathbf{x}) \in \mathbb{K}_C[[\mathbf{x}]]$ with $f(\mathbf{x})g(\mathbf{x}) = 1$, if and only if $a_{\mathbf{0}} \neq 0$.

- Let $\preceq$ be an **additive order** in $\mathbb{Z}^p$ and let $\mathcal{C}$ be the set of all cones $C \subseteq \mathbb{R}^p$ which are **compatible** with $\preceq$.
- Define

$$\mathbb{K}_{\preceq}[[\mathbf{x}]] := \bigcup_{C \in \mathcal{C}} \mathbb{K}_C[[\mathbf{x}]] \quad \text{and} \quad \mathbb{K}_{\preceq}((\mathbf{x})) := \bigcup_{\mathbf{e} \in \mathbb{Z}^p} \mathbf{x}^{\mathbf{e}} \mathbb{K}_{\preceq}[[\mathbf{x}]],$$

- $\mathbb{K}_{\preceq}[[\mathbf{x}]]$ is a **ring** and $\mathbb{K}_{\preceq}((\mathbf{x}))$ is a **field**.

Outline

Graded reverse lexicographic order

The ***graded reverse lexicographic order*** or ***grevlex order***

1. Denoted it by $<_{glex}$ (see [4]).
2. The grevlex order compares first the **total degree**;
3. then uses a **reverse lexicographic order** as tie-breaker;

Example

Set $\mathbf{v}_1 = (1, 0, -1)$, $\mathbf{v}_2 = (0, 0, 0)$, $\mathbf{v}_3 = (1, 1, -1)$, and $\mathbf{v}_4 = (2, -1, -1)$. Then,

$$\mathbf{v}_2 <_{glex} \mathbf{v}_1 <_{glex} \mathbf{v}_4 <_{glex} \mathbf{v}_3.$$

The Laurent series object

Proposition

Let $g \in \mathbb{K}[[\boldsymbol{u}]]$ be a power series, $\boldsymbol{e} \in \mathbb{Z}^p$ be a point, and $\boldsymbol{R} := \{\boldsymbol{r}_1, \ldots, \boldsymbol{r}_m\} \subset \mathbb{Z}^p$ be set of ***grevlex non-negative*** *rays. Then,*

$$f = \mathbf{x}^{\boldsymbol{e}} g(\mathbf{x}^{\boldsymbol{r}_1}, \ldots, \mathbf{x}^{\boldsymbol{r}_m}),$$

is a ***Laurent series*** *living in $\mathbf{x}^{\boldsymbol{e}}\mathbb{K}_C[[\mathbf{x}]]$, where C is the cone generated by $\boldsymbol{R}$. We denote: $\mathbf{x}^{\boldsymbol{R}} = \mathbf{x}^{\boldsymbol{r}_1}, \ldots, \mathbf{x}^{\boldsymbol{r}_m}$.*

The Laurent series object

Proposition

*Let $g \in \mathbb{K}[[\boldsymbol{u}]]$ be a power series, $\boldsymbol{e} \in \mathbb{Z}^p$ be a point, and $\boldsymbol{R} := \{\boldsymbol{r}_1, \ldots, \boldsymbol{r}_m\} \subset \mathbb{Z}^p$ be set of **grevlex non-negative** rays. Then,*

$$f = \mathbf{x}^{\boldsymbol{e}} g(\mathbf{x}^{\boldsymbol{r}_1}, \ldots, \mathbf{x}^{\boldsymbol{r}_m}),$$

*is a **Laurent series** living in $\mathbf{x}^{\boldsymbol{e}}\mathbb{K}_C[[\mathbf{x}]]$, where C is the cone generated by $\boldsymbol{R}$. We denote: $\mathbf{x}^{\boldsymbol{R}} = \mathbf{x}^{\boldsymbol{r}_1}, \ldots, \mathbf{x}^{\boldsymbol{r}_m}$.*

- Our implementation encodes multivariate Laurent series obtained by the previous proposition, that is, the parameters $(\mathbf{x}, \mathbf{u}, \mathbf{e}, \mathbf{R}, g)$.

The Laurent series object

Proposition

*Let $g \in \mathbb{K}[[\boldsymbol{u}]]$ be a power series, $\boldsymbol{e} \in \mathbb{Z}^p$ be a point, and $\boldsymbol{R} := \{\boldsymbol{r}_1, \ldots, \boldsymbol{r}_m\} \subset \mathbb{Z}^p$ be set of **grevlex non-negative** rays. Then,*

$$f = \mathbf{x}^{\boldsymbol{e}} g(\mathbf{x}^{\boldsymbol{r}_1}, \ldots, \mathbf{x}^{\boldsymbol{r}_m}),$$

*is a **Laurent series** living in $\mathbf{x}^{\boldsymbol{e}}\mathbb{K}_C[[\mathbf{x}]]$, where C is the cone generated by $\boldsymbol{R}$. We denote: $\mathbf{x}^{\boldsymbol{R}} = \mathbf{x}^{\boldsymbol{r}_1}, \ldots, \mathbf{x}^{\boldsymbol{r}_m}$.*

- Our implementation encodes multivariate Laurent series obtained by the previous proposition, that is, the parameters $(\mathbf{x}, \mathbf{u}, \mathbf{e}, \mathbf{R}, g)$.
- However, we do not know whether every multivariate Laurent series can be implemented in this way.

Example

Consider

$$f := x^{-4}y^{5}\sum_{i=0}^{\infty} x^{2i}y^{-i}.$$

Example

Consider

$$f := x^{-4}y^5 \sum_{i=0}^{\infty} x^{2i}y^{-i}.$$

If we want to encode f as an LSO, we can choose the following parameters:

$$\begin{aligned}
\mathbf{x} &= [x, y], \\
\mathbf{u} &= [u, v], \\
g &= \text{Inverse}(\text{PowerSeries}(1 + uv)), \\
\mathbf{R} &= [[1, 0], [1, -1]], \\
\mathbf{e} &= [x = -4, y = 5].
\end{aligned}$$

Example

Consider

$$f := x^{-4} y^5 \sum_{i=0}^{\infty} x^{2i} y^{-i}.$$

If we want to encode f as an LSO, we can choose the following parameters:

$$\begin{aligned}
\mathbf{x} &= [x, y], \\
\mathbf{u} &= [u, v], \\
g &= \text{Inverse}(\text{PowerSeries}(1 + uv)), \\
\mathbf{R} &= [[1, 0], [1, -1]], \\
\mathbf{e} &= [x = -4, y = 5].
\end{aligned}$$

Notice that $[1, 0] \geq_{glex} [0, 0]$ and $[1, -1] \geq_{glex} [0, 0]$, so the ring $\mathbb{K}_C[[\mathbf{x}]]$ is well defined. Also, the cone C defines a change of variable equal to $u = x$ and $v = xy^{-1}$.

Addition and multiplication

Notation

- Let $C_1, C_2 \subseteq \mathbb{Z}^p$ be cones generated, repsectively, by the sets of **grevlex non-negative** rays, $\mathbf{R}_1 := \{\mathbf{r}'_1, \ldots, \mathbf{r}'_m\} \subset \mathbb{Z}^p$ and $\mathbf{R}_2 := \{\mathbf{r}''_1, \ldots, \mathbf{r}''_m\} \subset \mathbb{Z}^p$, with $m \geq p$.

Addition and multiplication

Notation

- Let $C_1, C_2 \subseteq \mathbb{Z}^p$ be cones generated, repsectively, by the sets of **grevlex non-negative** rays, $\mathbf{R}_1 := \{\mathbf{r}'_1, \ldots, \mathbf{r}'_m\} \subset \mathbb{Z}^p$ and $\mathbf{R}_2 := \{\mathbf{r}''_1, \ldots, \mathbf{r}''_m\} \subset \mathbb{Z}^p$, with $m \geq p$.
- Consider
$$f_1 = \mathbf{x}^{\mathbf{e}_1} g_1(\mathbf{x}^{\mathbf{R}_1}) \text{ and } f_2 = \mathbf{x}^{\mathbf{e}_2} g_2(\mathbf{x}^{\mathbf{R}_2}),$$
with $g_1, g_2 \in \mathbb{K}[[\mathbf{u}]]$ and $\mathbf{e}_1, \mathbf{e}_2 \in \mathbb{Z}^p$.

Addition and multiplication

Notation

- Let $C_1, C_2 \subseteq \mathbb{Z}^p$ be cones generated, repsectively, by the sets of **grevlex non-negative** rays, $\mathbf{R}_1 := \{\mathbf{r}'_1, \ldots, \mathbf{r}'_m\} \subset \mathbb{Z}^p$ and $\mathbf{R}_2 := \{\mathbf{r}''_1, \ldots, \mathbf{r}''_m\} \subset \mathbb{Z}^p$, with $m \geq p$.
- Consider
$$f_1 = \mathbf{x}^{\mathbf{e}_1} g_1(\mathbf{x}^{\mathbf{R}_1}) \text{ and } f_2 = \mathbf{x}^{\mathbf{e}_2} g_2(\mathbf{x}^{\mathbf{R}_2}),$$
with $g_1, g_2 \in \mathbb{K}[[\mathbf{u}]]$ and $\mathbf{e}_1, \mathbf{e}_2 \in \mathbb{Z}^p$.

We have:

$$f_1 f_2 = \mathbf{x}^{\mathbf{e}_1+\mathbf{e}_2} \left(g_1(\mathbf{x}^{\mathbf{R}_1}) g_2(\mathbf{x}^{\mathbf{R}_2}) \right).$$

Addition and multiplication

Notation

- Let $C_1, C_2 \subseteq \mathbb{Z}^p$ be cones generated, repsectively, by the sets of **grevlex non-negative** rays, $\mathbf{R}_1 := \{\mathbf{r}'_1, \ldots, \mathbf{r}'_m\} \subset \mathbb{Z}^p$ and $\mathbf{R}_2 := \{\mathbf{r}''_1, \ldots, \mathbf{r}''_m\} \subset \mathbb{Z}^p$, with $m \geq p$.
- Consider

$$f_1 = \mathbf{x}^{\mathbf{e}_1} g_1(\mathbf{x}^{\mathbf{R}_1}) \text{ and } f_2 = \mathbf{x}^{\mathbf{e}_2} g_2(\mathbf{x}^{\mathbf{R}_2}),$$

with $g_1, g_2 \in \mathbb{K}[[\mathbf{u}]]$ and $\mathbf{e}_1, \mathbf{e}_2 \in \mathbb{Z}^p$.

We have:

$$f_1 f_2 = \mathbf{x}^{\mathbf{e}_1+\mathbf{e}_2} \left(g_1(\mathbf{x}^{\mathbf{R}_1}) g_2(\mathbf{x}^{\mathbf{R}_2}) \right).$$

Assume $\mathbf{e} = \mathbf{e}_1$ is the **grevlex-minimum** between $\mathbf{e}_1$ and $\mathbf{e}_2$. Then,

$$f_1 + f_2 = \mathbf{x}^{\mathbf{e}} \left(g_1(\mathbf{x}^{\mathbf{R}_1}) + \mathbf{x}^{\mathbf{e}_2 - \mathbf{e}} g_2(\mathbf{x}^{\mathbf{R}_2}) \right).$$

Algorithm 2 MakeRaysCompatible

Require: $\mathbf{R}_1$, $\mathbf{R}_2$, $\mathbf{R}_3$ sets of grevlex-non negative rays, a field $\mathbb{K}$, ordered indeterminates $\mathbf{x} := (x_1, \ldots, x_p)$.
Ensure: A set of p rays $\mathbf{R}$ such that $C(\mathbf{R}) \supseteq C(\mathbf{R}_1) \cup C(\mathbf{R}_2) \cup C(\mathbf{R}_3)$.

$W := \mathbf{R}_1 \cup \mathbf{R}_2 \cup \mathbf{R}_3$
for i **from** p **to** 1 **do**
  $S := \{\mathbf{w} \in W \mid \mathbf{w} \cdot \mathbf{1}_i > 0\}$ ▷ We get all the rays in W with positive i-weight.
  if $|S| > 1$ **then** ▷ $|S|$ denotes the number of elements in S.
    $S' := \{\mathbf{s}/(\mathbf{s} \cdot \mathbf{1}_i) \mid \mathbf{s} \in S\}$ ▷ We "normalize" the elements of S
    ▷ to make them comparable.
    $\mathbf{v} := \min_{glex}(S')$ ▷ We get the grevlex smallest element of S'.
    $\mathbf{v}' :=$ LookForGreatestGrevlexLess($\mathbf{v}$) ▷ $\mathbf{v} \in \mathbb{Q}^p$, so we look for $\mathbf{v}' \in \mathbb{Z}^p$
    ▷ such that $\mathbf{v} \geq_{glex} \mathbf{v}'$ and $|\mathbf{v}| = |\mathbf{v}'|$.
  else
    $\mathbf{v}' := S[1]$

  $\mathbf{R}[i] := \mathbf{v}'$ ▷ We save $\mathbf{v}'$.
  for $\mathbf{w} \in W$ **do**
    if $\mathbf{w} \in S$ **then**
      $\mathbf{w} := \mathbf{w} - \frac{\mathbf{w} \cdot \mathbf{1}_i}{\mathbf{R}[i] \cdot \mathbf{1}_i} \cdot \mathbf{R}[i]$ ▷ We subtract a multiple of $\mathbf{R}[i]$
      ▷ to achieve $\mathbf{w} \cdot \mathbf{1}_i = 0$.
return R

Algorithm 3 Multiply

Require: Laurent series $f_1(\mathbf{x}) = \mathbf{x}^{\mathbf{e}_1} g_1(\mathbf{x}^{\mathbf{R}_1}), f_2(\mathbf{x}) = \mathbf{x}^{\mathbf{e}_2} g_2(\mathbf{x}^{\mathbf{R}_2})$. Remember $\mathbf{R}_1 := \{\mathbf{r}'_1, \ldots, \mathbf{r}'_m\} \subset \mathbb{Z}^p$ and $\mathbf{R}_2 := \{\mathbf{r}''_1, \ldots, \mathbf{r}''_m\} \subset \mathbb{Z}^p$.

Ensure: $\mathbf{x}^{\mathbf{e}} g(\mathbf{x}^{\mathbf{R}})$ the product of f_1 and f_2.

$\mathbf{e} := \mathbf{e}_1 + \mathbf{e}_2$ ▷ We get the exponent of $\mathbf{x}^{\mathbf{e}_1}\mathbf{x}^{\mathbf{e}_2}$.

$\mathbf{R} := \text{MakeRaysCompatible}([\mathbf{R}_1, \mathbf{R}_2], \mathbf{x})$ ▷ We get the rays of a cone C such that

▷ $C_1 \cup C_2 \subseteq C$.

$\mathbf{u}' := \mathbf{x}^{\mathbf{R}}$ ▷ We compute the new change of variable.

for i **from** 1 **to** m **do** ▷ We see $g_1(\mathbf{u})$ and $g_2(\mathbf{u})$ as a function of $\mathbf{u}'$:

  Solve$(\mathbf{r}'_i = \overline{\mathbf{R}} \cdot \mathbf{k}_i^T)$ ▷ We compute $\mathbf{k}_i$ such that $\mathbf{r}'_i = \overline{\mathbf{R}} \cdot \mathbf{k}_i^T$.

  Solve$(\mathbf{r}''_i = \overline{\mathbf{R}} \cdot (\mathbf{k}'_i)^T)$ ▷ We compute $\mathbf{k}'_i$ such that $\mathbf{r}''_i = \overline{\mathbf{R}} \cdot (\mathbf{k}'_i)^T$.

$g'_1(\mathbf{u}') := g_1((\mathbf{u}')^{\mathbf{k}_1}, \ldots, (\mathbf{u}')^{\mathbf{k}_m})$ ▷ $g'_1(\mathbf{u}') \in \mathbb{K}[[\mathbf{u}']]$.

$g'_2(\mathbf{u}') := g_2((\mathbf{u}')^{\mathbf{k}'_1}, \ldots, (\mathbf{u}')^{\mathbf{k}'_m})$ ▷ $g'_2(\mathbf{u}') \in \mathbb{K}[[\mathbf{u}']]$.

$g := g'_1 g'_2$ ▷ We multiply Power Series in $\mathbb{K}[[\mathbf{u}']]$.

return $\mathbf{x}, \mathbf{u}', g, \mathbf{R}, \mathbf{e}$

Inversion

Notation

Let $C \subseteq \mathbb{Z}^p$ be a line-free cone described by the set of **grevlex non-negative** rays, $\mathbf{R} := \{\mathbf{r}_1, \ldots, \mathbf{r}_m\} \subset \mathbb{Z}^p$, and let $\mathbf{e} \in \mathbb{Z}^p$ be a point. Now, consider

$$0 \neq f = \mathbf{x}^{\mathbf{e}} g(\mathbf{x}^{\mathbf{R}}) \in \mathbf{x}^{\mathbf{e}} \mathbb{K}_C[[\mathbf{x}]],$$

with $g \in \mathbb{K}[[\mathbf{u}]]$.

Inversion

Notation

Let $C \subseteq \mathbb{Z}^p$ be a line-free cone described by the set of **grevlex non-negative** rays, $\mathbf{R} := \{\mathbf{r}_1, \ldots, \mathbf{r}_m\} \subset \mathbb{Z}^p$, and let $\mathbf{e} \in \mathbb{Z}^p$ be a point. Now, consider

$$0 \neq f = \mathbf{x}^{\mathbf{e}} g(\mathbf{x}^{\mathbf{R}}) \in \mathbf{x}^{\mathbf{e}} \mathbb{K}_C[[\mathbf{x}]],$$

with $g \in \mathbb{K}[[\mathbf{u}]]$.

Lemma

We have

$$\mathrm{supp}(g(\mathbf{x}^{\boldsymbol{R}})) = \{(\boldsymbol{r}_1^T, \ldots, \boldsymbol{r}_m^T) \cdot \boldsymbol{k}^T \mid \boldsymbol{k} \in \mathrm{supp}(g)\} \subseteq \mathbb{Z}^p.$$

Multivariate power series in Maple are created in a **lazy manner** ([1]).This implies the following:

Multivariate power series in Maple are created in a **lazy manner** ([1]).This implies the following:

- In general, we may not easily find the **smallest monomial** of in the support a power series. Consider a power series with all its terms up to degree $10^{10000000}$ equal to **zero**.

Multivariate power series in Maple are created in a **lazy manner** ([1]).This implies the following:

- In general, we may not easily find the **smallest monomial** of in the support a power series. Consider a power series with all its terms up to degree $10^{10000000}$ equal to **zero**.
- Finding the **smallest element** of a power series does not guarantee that we can find the **grevlex-minimum** element of a Laurent series.

Consider a power series $g \in \mathbb{K}[[u, v]]$ with support equal to

$$\{(0,0),(1,1),(1,2),(1,4),(2,2),(2,3),(3,2),(3,3),(3,4),(4,0),(4,1),(4,2),(4,4),(5,2),\ldots\},$$

a random infinite set.

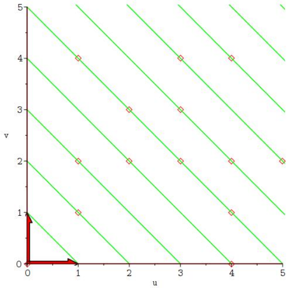

Figure: Support of $g(u, v)$

Then, the support of $g(xy, xy^{-1})$ is going to be equal to

$$\{(0,0),(2,0),(3,-1),(5,-3),(4,0),(5,-1),(5,1),(6,0),(7,-1),(4,4),(5,3),(6,2),(8,0),(7,3),\ldots\}.$$

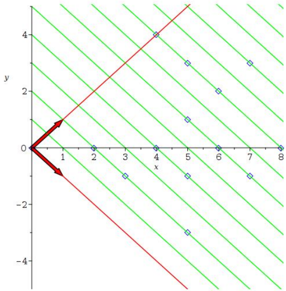

Figure: Support of $g(xy, xy^{-1})$

Proposition

*If $\boldsymbol{R}$ is a set of **grevlex-positive** rays, then*

$$\min \operatorname{supp}(g(\mathbf{x}^{\boldsymbol{R}})) = \min \left\{ \overline{\boldsymbol{R}} \cdot \boldsymbol{k}^{T} \mid \boldsymbol{k} \in \operatorname{supp}(g) \textit{ with } \left| \overline{\boldsymbol{R}} \cdot \boldsymbol{k}^{T} \right| \leq \left| \overline{\boldsymbol{R}} \cdot \overline{\boldsymbol{k}}^{T} \right| \right\},$$

with $\overline{\boldsymbol{k}}$ the smallest element in $\operatorname{supp}(g)$ and $\overline{\boldsymbol{R}} = (\boldsymbol{r}_1^{T}, \ldots, \boldsymbol{r}_m^{T})$.

Proposition

If $\boldsymbol{R}$ is a set of ***grevlex-positive*** *rays, then*

$$\min \operatorname{supp}(g(\mathbf{x}^{\boldsymbol{R}})) = \min \left\{ \overline{\boldsymbol{R}} \cdot \boldsymbol{k}^T \mid \boldsymbol{k} \in \operatorname{supp}(g) \text{ with } \left| \overline{\boldsymbol{R}} \cdot \boldsymbol{k}^T \right| \leq \left| \overline{\boldsymbol{R}} \cdot \overline{\boldsymbol{k}}^T \right| \right\},$$

with $\overline{\boldsymbol{k}}$ the smallest element in $\operatorname{supp}(g)$ and $\overline{\boldsymbol{R}} = (\boldsymbol{r}_1^T, \ldots, \boldsymbol{r}_m^T)$.

To handle our **zero-ray** case, we decided to implement an *internal bound* B. We assume that the minimum element of $\operatorname{supp}(f)$ is:

$$\overline{\mathbf{e}} = \min \left\{ \overline{\mathbf{R}} \cdot \mathbf{k}^T \mid \mathbf{k} \in \operatorname{supp}(g) \text{ with } \left| \overline{\mathbf{R}} \cdot \mathbf{k}^T \right| \leq B \right\}.$$

Proposition

If $\boldsymbol{R}$ *is a set of* ***grevlex-positive*** *rays, then*

$$\min \operatorname{supp}(g(\mathbf{x}^{\boldsymbol{R}})) = \min \left\{ \overline{\boldsymbol{R}} \cdot \boldsymbol{k}^T \mid \boldsymbol{k} \in \operatorname{supp}(g) \text{ with } \left| \overline{\boldsymbol{R}} \cdot \boldsymbol{k}^T \right| \le \left| \overline{\boldsymbol{R}} \cdot \overline{\boldsymbol{k}}^T \right| \right\},$$

with $\overline{\boldsymbol{k}}$ *the smallest element in* $\operatorname{supp}(g)$ *and* $\overline{\boldsymbol{R}} = (\boldsymbol{r}_1^T, \ldots, \boldsymbol{r}_m^T)$.

To handle our **zero-ray** case, we decided to implement an *internal bound* B. We assume that the minimum element of $\operatorname{supp}(f)$ is:

$$\overline{\mathbf{e}} = \min \left\{ \overline{\mathbf{R}} \cdot \mathbf{k}^T \mid \mathbf{k} \in \operatorname{supp}(g) \text{ with } \left| \overline{\mathbf{R}} \cdot \mathbf{k}^T \right| \le B \right\}.$$

Definition

We refer to B (when we have a cone generated by at least a zero-ray) or to the bound $\left| \overline{\mathbf{R}} \cdot \overline{\mathbf{k}}^T \right|$ (as in Proposition 2) as the ***inversion bound*** of our Laurent series f.

Analytic expression

- Power series with a ***defined analytic expression***: a convergent power series with a known sum (that we call analytic expression) stored in the LSO data-structure. Such series are closed under addition, multiplication and inversion.
- Power series with an ***undefined analytic expression*** ([1]): all the other power series.

Analytic expression

- Power series with a ***defined analytic expression***: a convergent power series with a known sum (that we call analytic expression) stored in the LSO data-structure. Such series are closed under addition, multiplication and inversion.
- Power series with an ***undefined analytic expression*** ([1]): all the other power series.

Algorithm 5 Inverse

Require: Laurent series $f(\mathbf{x}) = \mathbf{x}^{\mathbf{e}} g(\mathbf{x}^{\mathbf{R}})$.
Ensure: The inverse f^{-1} of f.
1: **if** AnalyticExpression(f) = **Undefined** or **non-rational then**
2: **return** $\mathbf{x}^{-\mathbf{e}}$InverseOfUndefinedAnalyticExpression($g(\mathbf{x}^{\mathbf{R}})$)
3: **else**
4: $q :=$ AnalyticExpression(f) ▷ The analytic expression of f.
5: **return** $\mathbf{x}^{-\mathbf{e}}$InverseOfAnalyticExpression($q, \mathbf{x}^{\mathbf{R}}$)

Algorithm 6 InverseOfAnalyticExpression

Require: $q(\mathbf{u}) = \frac{q_1(\mathbf{u})}{q_2(\mathbf{u})}$, with $q_1(\mathbf{u}), q_2(\mathbf{u})$ polynomials. $\mathbf{x}^{\mathrm{R}}$ a change of variables with $\mathbf{R} := \{\mathbf{r}_1, \ldots, \mathbf{r}_m\} \subset \mathbb{Z}^p$.

Ensure: $q^{-1}(\mathbf{x}^{\mathrm{R}})$ the inverse of q.

if HasConstantTerm(q_1) **then**
    return $\frac{q_2(\mathrm{x}^{\mathrm{R}})^{-1}}{q_1(\mathrm{x}^{\mathrm{R}})^{-1}}$ ▷ If q_1 has a constant term, then q is invertible.
else
    $\overline{\mathbf{e}} := \min_{glex} \operatorname{supp}(q_1(\mathbf{x}^{\mathrm{R}}))$ ▷ We get the grevlex-smallest element in $\operatorname{supp}(q_1(\mathbf{x}^{\mathrm{R}}))$.
    Solve($\overline{\mathbf{e}} = \overline{\mathbf{R}} \cdot \mathbf{s}^T$) ▷ We compute $\mathbf{s}$ such that $\overline{\mathbf{e}} = \overline{\mathbf{R}} \cdot \mathbf{s}$.
    $q_1''(\mathbf{u}) := \dfrac{q_1(\mathbf{u})}{\mathbf{u}^{\mathbf{s}}}$ ▷ We define a new function. Note q_1'' could not be a power series.
    $\mathbf{R}_1 := \{\mathbf{k} - \overline{\mathbf{e}} | \mathbf{k} \in \operatorname{supp}(q_1(\mathbf{x}^{\mathrm{R}}))\} \cup \{\overline{\mathbf{e}}\}$ ▷ A set of grevlex non-negative terms.
    $\mathbf{R}' :=$ MakeRaysCompatible($\mathbf{R}, \mathbf{R}_1, \mathbb{K}, \mathbf{x}$) ▷ We get the rays for our new cone.
    for i **from** 1 **to** m **do**
        Solve($\mathbf{r}_i = \overline{\mathbf{R}'} \cdot \mathbf{k}_i^T$) ▷ We compute $\mathbf{k}_i$ such that $\mathbf{r}_i' = \overline{\mathbf{R}'} \cdot \mathbf{k}_i^T$.
    $\mathbf{v} := v_1, \ldots, v_p$ ▷ New ordered variables for our power series.
    $q_1'(\mathbf{v}) := q_1''(\mathbf{v}^{\mathbf{k}_1}, \ldots, \mathbf{v}^{\mathbf{k}_m})$ ▷ $q_1'(\mathbf{v}) \in \mathbb{K}[[\mathbf{v}]]$.
    $q_2'(\mathbf{v}) := q_2(\mathbf{v}^{\mathbf{k}_1}, \ldots, \mathbf{v}^{\mathbf{k}_m})$ ▷ $q_2'(\mathbf{v}) \in \mathbb{K}[[\mathbf{v}]]$.
    return $\mathbf{x}^{-\overline{\mathrm{e}}} \frac{(q_2')^{-1}(\mathrm{x}^{\mathrm{R}'})}{(q_1')^{-1}(\mathrm{x}^{\mathrm{R}'})}$

Algorithm 7 InverseOfUndefinedAnalyticExpression

Require: Laurent series $g(\mathbf{x}^{\mathbf{R}})$ with **undefined** or **non-rational** analytic expression and $\mathbf{R} := \{\mathbf{r}_1, \ldots, \mathbf{r}_m\} \subset \mathbb{Z}^p$.

Ensure: The inverse $g^{-1}(\mathbf{x}^{\mathbf{R}})$ of g.

if HasConstantTerm(g) **then**
 return $g^{-1}(\mathbf{x}^{\mathbf{R}})$ ▷ If g has a constant term, then g is invertible as a power series.
else
 $B, \bar{\mathbf{e}} :=$ LookForSmallestTerm($g(\mathbf{x}^{\mathbf{R}})$) ▷ Smallest term in $\operatorname{supp}(g(\mathbf{x}^{\mathbf{R}}))$.
 $S := \{\overline{\mathbf{R}} \cdot \mathbf{k} - \bar{\mathbf{e}} \mid |\overline{\mathbf{R}} \cdot \mathbf{k}| \leq B \text{ and } \mathbf{k} \in \operatorname{supp}(g)\} \cup \{\mathbf{r} - \bar{\mathbf{e}} \mid \mathbf{r} \in \mathbf{R} \text{ and } \mathbf{r} >_{glex} \bar{\mathbf{e}}\}$
 $\mathbf{R}' :=$ MakeRaysCompatible($\mathbf{R}, S, \mathbb{K}, \mathbf{x}$) ▷ We get the rays for our new cone.
 for i **from** 1 **to** m **do**
  Solve($\mathbf{r}_i = \overline{\mathbf{R}'} \cdot \mathbf{k}_i^T$) ▷ We compute $\mathbf{k}_i$ such that $\mathbf{r}'_i = \overline{\mathbf{R}'} \cdot \mathbf{k}_i^T$.
 $\mathbf{v} := v_1, \ldots, v_p$ ▷ New ordered variables for our power series.
 Solve($\bar{\mathbf{e}} = \overline{\mathbf{R}'} \cdot \mathbf{s}^T$) ▷ We compute $\mathbf{s}$ such that $\bar{\mathbf{e}} = \overline{\mathbf{R}'} \cdot \mathbf{s}^T$.
 $g''(\mathbf{u}) := g(\mathbf{u})/\mathbf{u}^{\mathbf{s}}$ ▷ We factor $\mathbf{u}^{\mathbf{s}}$ out from g.
 $g'(\mathbf{v}) := g''(\mathbf{v}^{\mathbf{k}_1}, \ldots, \mathbf{v}^{\mathbf{k}_m})$ ▷ $g'(\mathbf{v}) \in \mathbb{K}[[\mathbf{v}]]$.
 return $\mathbf{x}^{-\bar{\mathbf{e}}}(g')^{-1}(\mathbf{x}^{\mathbf{R}'})$

Outline

```
> with(MultivariatePowerSeries);
[Add, ApproximatelyEqual, ApproximatelyZero, Copy, Degree, Divide, EvaluateAtOrigin, Exponentiate, GeometricSeries,
    GetAnalyticExpression, GetCoefficient, HenselFactorize, HomogeneousPart, Inverse, IsUnit, MainVariable, Multiply, Negate,
    PowerSeries, Precision, SetDefaultDisplayStyle, SetDisplayStyle, Substitute, Subtract, SumOfAllMonomials, TaylorShift,
    Truncate, UnivariatePolynomialOverPowerSeries, UpdatePrecision, Variables, WeierstrassPreparation]
> kernelopts(opaquemodules = false) :
  LaurentSeries := MultivariatePowerSeries:-LaurentSeriesObject :
  kernelopts(opaquemodules = true) :
```

Figure: Laurent series object

```
> X := [x, y] : U := [u, v] :
  g1 := Inverse(PowerSeries(1 + u*v)) :
  e := [x = -5, y = 3] :
  R := [[1, 0], [1, -1]] :
> f1 := LaurentSeries(g1, X, U, R, e);
```

$$f_1 := \left[\text{LaurentSeries of } \frac{y^3}{\left(\frac{x^2}{y}+1\right) x^5} : \frac{y^3}{x^5} - \frac{y^2}{x^3} + \frac{y}{x} - x + \frac{x^3}{y} - \frac{x^5}{y^2} + \frac{x^7}{y^3} - \frac{x^9}{y^4} + \ldots \right]$$

```
> LaurentSeries:-Truncate(f1, 8);
```

$$\frac{y^3 \left(\frac{x^8}{y^4} - \frac{x^6}{y^3} + \frac{x^4}{y^2} - \frac{x^2}{y} + 1 \right)}{x^5}$$

```
> g2 := PowerSeries(1/(1 + u)) :
  mp := [u = x^(-1)*y^2] : e := [x = 3, y = -4] :
> f2 := LaurentSeries(g2, mp, e);
```

$$f_2 := \left[\text{LaurentSeries of } \frac{x^3}{\left(1+\frac{y^2}{x}\right) y^4} : \frac{x^3}{y^4} + \ldots \right]$$

```
> LaurentSeries:-Truncate(f2, 8);
```

$$\frac{x^3 \left(\frac{y^{16}}{x^8} - \frac{y^{14}}{x^7} + \frac{y^{12}}{x^6} - \frac{y^{10}}{x^5} + \frac{y^8}{x^4} - \frac{y^6}{x^3} + \frac{y^4}{x^2} - \frac{y^2}{x} + 1 \right)}{y^4}$$

Figure: Creation Laurent series

> $f := LaurentSeries\text{:-}BinaryMultiply(f_1, f_2);$

$$f := \left[\text{LaurentSeries of } \frac{1}{\left(\frac{x^2}{y}+1\right)\left(1+\frac{y^2}{x}\right)x^2\,y} : \frac{1}{x^2\,y} + \ldots \right]$$

> $LaurentSeries\text{:-}Truncate(f, 8);$

$$\frac{\frac{y^{16}}{x^8} - \frac{y^7}{x^2} + \frac{x^4}{y^2} - \frac{y^{14}}{x^7} + \frac{y^5}{x} + \frac{y^{12}}{x^6} - y^3 - \frac{y^{10}}{x^5} + x\,y + \frac{y^8}{x^4} - \frac{x^2}{y} - \frac{y^6}{x^3} + \frac{y^4}{x^2} - \frac{y^2}{x} + 1}{x^2\,y}$$

Figure: Multiplication of Laurent series

> $f := LaurentSeries\text{:-}BinaryAdd(f_1, f_2);$

$$f := \left[\text{LaurentSeries of } \frac{\left(\frac{1}{\frac{x^2}{y}+1} + \frac{x^8}{\left(1+\frac{y^2}{x}\right)y^7}\right)y^3}{x^5} : \frac{y^3}{x^5} + \ldots \right]$$

> $LaurentSeries\text{:-}Truncate(f, 15);$

$$\frac{y^3\left(-x^3\,y^3 + x^4\,y - \frac{x^5}{y} - \frac{x^7}{y^5} + \frac{x^8}{y^7} + \frac{x^4}{y^2} - \frac{x^2}{y} + 1\right)}{x^5}$$

Figure: Addition of Laurent series

> $f := LaurentSeries\text{:-}Inverse(f_1);$

$$f := \left[\text{LaurentSeries of } \frac{\left(\frac{x^2}{y}+1\right)x^5}{y^3} : \frac{x^5}{y^3} + \ldots\right]$$

> $h := LaurentSeries\text{:-}BinaryMultiply(f_1, f);$

$$h := [\text{LaurentSeries: } 1]$$

> $LaurentSeries\text{:-}Truncate(h, 100);$

$$1$$

Figure: Inverse of a Laurent series

Outline

Concluding remarks: modular intersect

Theoretical aspects

- We have presented a **modular algorithm** for solving a trivariate polynomial system:
$$f = t = b = 0$$
under **genericity assumptions**.
- To be more precise, this is a modular method for the call Intersect$(f, \{t, b\})$.
- A follow-up work will extend this modular method to solve the same problem with an arbitrary number of variables.

Practical aspects

- The preliminary implementation and experimentation in Maple bring **promising results** for this modular method.
- To be more precise, for generic input systems of sufficiently **large** Bézout bound, the modular method outperforms the non-modular implementation of the command Intersect.
- There still **room for improvement**. The BPAS version of our modular intersect can be optimized. We can consider experiments using the **Fast Fourier Transform**, and also we can **parallelize** our modular algorithm.

Concluding remarks: Laurent series

- We have successfully written a **first implementation** a Laurent series object inside Maple.
- We are able to define multivariate Laurent series, multiply them, add them and find their inverse (in most of the cases).
- A next possible direction of research is the implementation of **Puiseux series**. Also, Nowak's construction [3] for the famous **Newton-Puiseux** algorithm.

Outline

Bibliography I

Mohammadali Asadi, Alexander Brandt, Mahsa Kazemi, Marc Moreno Maza, and Erik J. Postma.
Multivariate power series in maple.
In Robert M. Corless, Jürgen Gerhard, and Ilias S. Kotsireas, editors, *Maple in Mathematics Education and Research*, pages 48–66, Cham, 2021. Springer International Publishing.

Ainhoa Aparicio Monforte and Manuel Kauers.
Formal laurent series in several variables.
Expositiones Mathematicae, 31(4):350–367, 2013.

Krzysztof Jan Nowak.
Some elementary proofs of puiseux's theorems.
Univ. Iagel. Acta Math, 38:279–282, 2000.

Bibliography II

Wikipedia contributors.
Monomial order — Wikipedia, the free encyclopedia.
https://en.wikipedia.org/w/index.php?title=Monomial_order&oldid=1004440098, 2021.