Gcd modulo a primary triangular set of dimension zero

Dahan Xavier

Ochanomizu Univeristy, Faculty of General Educational Research
Tokyo, Japan

ISSAC 2017, July 24-28 — Kaiserslautern

Introduction

Two polynomials $a, b \in R[y]$, R commutative ring. Known gcd:

- Unique Factorization Domains: Example: $R = k[x_1, \ldots, x_n]$.
- Over a field $R = K$. Bézout identity: $au + bv = g$ ($\langle g \rangle = \langle a, b \rangle$).

  Example: $R = k[x_1, \ldots, x_n]/\mathfrak{p}$, $\mathfrak{p}$ a maximal ideal

- Direct product of fields (Local-Global principle):
  - Typically: $R = k[x_1, \ldots, x_n]/I$, where $I = \cap_\iota \mathfrak{p}_\iota$: $\mathfrak{p}$ maximal and $\mathfrak{p}_\iota + \mathfrak{p}_{\iota'} = \langle 1 \rangle$ for $\iota \neq \iota'$.
  - Computationally: the heart of some triangular decomposition methods.
  - Realized through the CRT and the so-called "D5 principle".
- Gcd notions over more general rings have been introduced, but with some limitation.

Main Result

Address the case of coefficient rings of type $R := k[x_1, \ldots, x_n]/\mathfrak{q}$,

- where $\mathfrak{q}$ is a primary ideal of radical $\sqrt{\mathfrak{q}} = \mathfrak{p}$ a maximal ideal.
- Any non zero element is either nilpotent or invertible.

Result:

- Observation: a "gcd" depends on the "precision" to which coefficients are taken.
- Introduction of the Gcd chain that encompasses all these gcds with a structural isomorphism that generalizes: $\langle a, b\rangle = \langle g\rangle$.
- Computation: assume that $\mathfrak{q}$ is given by a lex GB in a purely triangular form (triangular set).
- Preliminary algorithm based on a subresultant sequence, but:
  - Still relies on an unproved assumption
  - Some "precision" is lost

Background: triangular decomposition method

Triangular decomposition: Wu-Ritt, Lazard, Kalkbrener, Wang, Moreno-Maza, ...

Implementation: `RegularChains` library of MAPLE.

Background: triangular decomposition method

Triangular decomposition: Wu-Ritt, Lazard, Kalkbrener, Wang, Moreno-Maza, ...

Implementation: `RegularChains` library of MAPLE.

Previous work on Gcd modulo a non-radical triangular set:

- [Moreno-Maza, Rioboo'95] Ask the question of a gcd with possibly nilpotent elements in the coefficients.
- [Li,Moreno-Maza, Pan'09] Study more precise conditions for a gcd to exist

Background: triangular decomposition method

Triangular decomposition: Wu-Ritt, Lazard, Kalkbrener, Wang, Moreno-Maza, ...

Implementation: `RegularChains` library of MAPLE.

Previous work on Gcd modulo a non-radical triangular set:

- [Moreno-Maza, Rioboo'95] Ask the question of a gcd with possibly nilpotent elements in the coefficients.
- [Li,Moreno-Maza, Pan'09] Study more precise conditions for a gcd to exist

Previous work on representing multiplicities with triangular set:

- [Cheng, X.-S. Gao'14] , [B.H Li'03]
- [Marcus, Moreno-Maza, Vrbik'12], [Alvandi, Moreno-Maza, Schost, Vrbik'15]

Motivation for non-radical triangular sets

For solving, computing the radical ideal representation is enough. However:

- The radical of a triangular set may not be triangular: more decomposition work may be required, whereas:

Theorem 1

the primary ideals of a triangular set are triangular

- Triangular sets have the ability to represent non-radical ideal (yet not as completely as a lex GB) . . .
- . . . while some other methods, like RUR cannot represent faithfully a non-radical ideal.

Illustrative example

Basic example: $R = k[x]/\mathfrak{q}$, $\mathfrak{q} = \langle x^3 \rangle$.

$$\begin{aligned} a &= y^4 + (2x^2 + 3x + 1)y^3 + (-x^2 - x - 1)y^2 \\ &+ (13x^2 - 4x - 1)y - 7x^2 - 2x \\ b &= y^3 + (3x^2 + 3x)y^2 + (-3x^2 - 3x - 1)y - 10x^2 - 2x. \end{aligned}$$

What could be a gcd of a and b ?

Illustrative example

Basic example: $R = k[x]/\mathfrak{q}$, $\mathfrak{q} = \langle x^3 \rangle$.

$$\begin{aligned} a &= y^4 + (2x^2 + 3x + 1)y^3 + (-x^2 - x - 1)y^2 \\ &+ (13x^2 - 4x - 1)y - 7x^2 - 2x \\ b &= y^3 + (3x^2 + 3x)y^2 + (-3x^2 - 3x - 1)y - 10x^2 - 2x. \end{aligned}$$

What could be a gcd of a and b ?

- Over R (modulo x^3) the largest degree polynomial that divides both a and b is: $y - 1 - x - 2x^2$

Illustrative example

Basic example: $R = k[x]/\mathfrak{q}$, $\mathfrak{q} = \langle x^3 \rangle$.

$$\begin{aligned} a &= y^4 + (2x^2 + 3x + 1)y^3 + (-x^2 - x - 1)y^2 \\ &+ (13x^2 - 4x - 1)y - 7x^2 - 2x \\ b &= y^3 + (3x^2 + 3x)y^2 + (-3x^2 - 3x - 1)y - 10x^2 - 2x. \end{aligned}$$

What could be a gcd of a and b ?

- Over R (modulo x^3) the largest degree polynomial that divides both a and b is: $y - 1 - x - 2x^2$
- And modulo x^2: that is of intermediate precision, the gcd is of degree 2: $(y + 2x)(y - 1 - x)$.

Illustrative example

Basic example: $R = k[x]/\mathfrak{q}$, $\mathfrak{q} = \langle x^3 \rangle$.

$$\begin{aligned} a &= y^4 + (2x^2 + 3x + 1)y^3 + (-x^2 - x - 1)y^2 \\ &+ (13x^2 - 4x - 1)y - 7x^2 - 2x \\ b &= y^3 + (3x^2 + 3x)y^2 + (-3x^2 - 3x - 1)y - 10x^2 - 2x. \end{aligned}$$

What could be a gcd of a and b ?

- Over R (modulo x^3) the largest degree polynomial that divides both a and b is: $y - 1 - x - 2x^2$
- And modulo x^2: that is of intermediate precision, the gcd is of degree 2: $(y + 2x)(y - 1 - x)$.
- Finally modulo x (less precise coefficients), the gcd is of higher degree: $y(y + 1)(y - 1)$

Illustrative example 2

A primary lexicographic ideal can be seen as a precision ring:

Here $\mathfrak{q} = \langle x^3 \rangle$ is of precision 3.

And the degree of the gcd decreases with precision:
(e.g. $y \mid (y+x)(y+1) \bmod \langle x \rangle$ but $y \nmid (y+x)(y+1) \bmod \langle x^2 \rangle$)

Illustrative example 2

A primary lexicographic ideal can be seen as a precision ring:

Here $\mathfrak{q} = \langle x^3 \rangle$ is of precision 3.

And the degree of the gcd decreases with precision:
(e.g. $y \mid (y+x)(y+1) \bmod \langle x \rangle$ but $y \nmid (y+x)(y+1) \bmod \langle x^2 \rangle$)

Definition 2 (Gcd chain)

In the example: $[(g_1, \langle x \rangle), (g_2, \langle x^2 \rangle), (g_3, \langle x^3 \rangle)]$. It verifies:

- $(R/\langle x \rangle)[y]/\langle a, b \rangle \simeq (R/\langle x \rangle)[y]/\langle g_1 \rangle$

Illustrative example 2

A primary lexicographic ideal can be seen as a precision ring:
Here $\mathfrak{q} = \langle x^3 \rangle$ is of precision 3.

And the degree of the gcd decreases with precision:
(e.g. $y \mid (y+x)(y+1) \bmod \langle x \rangle$ but $y \nmid (y+x)(y+1) \bmod \langle x^2 \rangle$)

Definition 2 (Gcd chain)

In the example: $[(g_1, \langle x \rangle), (g_2, \langle x^2 \rangle), (g_3, \langle x^3 \rangle)]$. It verifies:

- $(R/\langle x \rangle)[y]/\langle a, b \rangle \simeq (R/\langle x \rangle)[y]/\langle g_1 \rangle$
- $(R/\langle x^2 \rangle)[y]/\langle a, b \rangle \simeq (R/\langle x^2 \rangle)[y]/\langle g_2 \rangle \times (R/\langle x \rangle)[y]/\langle g_1/g_2 \rangle$

Illustrative example 2

A primary lexicographic ideal can be seen as a precision ring:
Here $\mathfrak{q} = \langle x^3 \rangle$ is of precision 3.

And the degree of the gcd decreases with precision:
(e.g. $y \mid (y+x)(y+1) \bmod \langle x \rangle$ but $y \nmid (y+x)(y+1) \bmod \langle x^2 \rangle$)

Definition 2 (Gcd chain)

In the example: $[(g_1, \langle x \rangle), (g_2, \langle x^2 \rangle), (g_3, \langle x^3 \rangle)]$. It verifies:

- $(R/\langle x \rangle)[y]/\langle a, b \rangle \simeq (R/\langle x \rangle)[y]/\langle g_1 \rangle$
- $(R/\langle x^2 \rangle)[y]/\langle a, b \rangle \simeq (R/\langle x^2 \rangle)[y]/\langle g_2 \rangle \times (R/\langle x \rangle)[y]/\langle g_1/g_2 \rangle$
- $(R/\langle x^3 \rangle)[y]/\langle a, b \rangle \simeq$
  $(R/\langle x^3 \rangle)[y]/\langle g_3 \rangle \times (R/\langle x^2 \rangle)[y]/\langle g_2/g_3 \rangle \times (R/\langle x \rangle)[y]/\langle g_1/g_2 \rangle$

Illustrative example 2

A primary lexicographic ideal can be seen as a precision ring:
Here $\mathfrak{q} = \langle x^3 \rangle$ is of precision 3.

And the degree of the gcd decreases with precision:
(e.g. $y \mid (y+x)(y+1) \bmod \langle x \rangle$ but $y \nmid (y+x)(y+1) \bmod \langle x^2 \rangle$)

Definition 2 (Gcd chain)

In the example: $[(g_1, \langle x \rangle), (g_2, \langle x^2 \rangle), (g_3, \langle x^3 \rangle)]$. It verifies:

- $(R/\langle x \rangle)[y]/\langle a, b \rangle \simeq (R/\langle x \rangle)[y]/\langle g_1 \rangle$
- $(R/\langle x^2 \rangle)[y]/\langle a, b \rangle \simeq (R/\langle x^2 \rangle)[y]/\langle g_2 \rangle \times (R/\langle x \rangle)[y]/\langle g_1/g_2 \rangle$
- $(R/\langle x^3 \rangle)[y]/\langle a, b \rangle \simeq$
  $(R/\langle x^3 \rangle)[y]/\langle g_3 \rangle \times (R/\langle x^2 \rangle)[y]/\langle g_2/g_3 \rangle \times (R/\langle x \rangle)[y]/\langle g_1/g_2 \rangle$

Actually...

- $(R/\langle x^{10} \rangle)[y]/\langle a, b \rangle \simeq$
  $(R/\langle x^{10} \rangle)[y]/\langle g_3 \rangle \times (R/\langle x^2 \rangle)[y]/\langle g_2/g_3 \rangle \times (R/\langle x \rangle)[y]/\langle g_1/g_2 \rangle$

General case: "Precision ring"

Fact: $\sqrt{\mathfrak{q}} := \mathfrak{p}$ has a triangular lex GB represented by polynomials:

$$(p_1(x_1)\ ,\ p_2(x_1, x_2)\ ,\ \ldots\ ,\ p_n(x_1, \ldots, x_n)),$$

where p_{i+1} is irreducible over the field $k[x_1, \ldots, x_i]/\langle p_1, \ldots, p_i \rangle$.
This encodes a "tower of fields extension".

General case: "Precision ring"

Fact: $\sqrt{\mathfrak{q}} := \mathfrak{p}$ has a triangular lex GB represented by polynomials:

$$(p_1(x_1)\ ,\ p_2(x_1,x_2)\ ,\ \ldots\ ,\ p_n(x_1,\ldots,x_n)),$$

where p_{i+1} is irreducible over the field $k[x_1,\ldots,x_i]/\langle p_1,\ldots,p_i\rangle$.
This encodes a "tower of fields extension".

Proposition 1 (Reformulation of Gianni-Trager-Zaccharias)

Any primary triangular ideal can be written as:

$$\begin{aligned} T_1(x_1) &= p_1^{e_1} \\ T_2(x_1,x_2) &= p_2^{e_2} + \sum_{i_1=1}^{e_1-1}\sum_{i_2=0}^{e_2-1} c[i_1,i_2]p_1^{i_1}p_2^{i_2} \\ &\vdots \\ T_n(x_1,\ldots,x_n) &= p_n^{e_n} + \sum_{i_1=1}^{e_1-1}\cdots\sum_{i_n=0}^{e_n-1} c[i_1,\ldots,i_n]p_1^{i_1}\cdots p_n^{i_n} \end{aligned}$$

$T_\ell \equiv p_\ell^{e_\ell} \bmod p_1,\ldots,p_{\ell-1} \Rightarrow c[0,\ldots,0,i_\ell] = 0$ *for all* i_ℓ.

General case: "Precision ring" 2

Proposition 2 (Reformulation of Gianni-Trager-Zaccharias)

$$\vdots$$

$$T_n(x_1,\ldots,x_n) = p_n^{e_n} + \sum_{i_1=1}^{e_1-1}\cdots\sum_{i_n=0}^{e_n-1} c[i_1,\ldots,i_n]p_1^{i_1}\cdots p_n^{i_n}$$

$$T_\ell \equiv \langle p_\ell^{e_\ell} \bmod p_1,\ldots,p_{\ell-1}\rangle \Rightarrow c[0,\ldots,0,i_\ell] = 0 \text{ for all } i_\ell.$$

Remarks:

- If $p_i = x_i - \alpha_i$ then this is Taylor expansion:
$$c[i_1,\ldots,i_n] = \frac{1}{i_1!i_2!\cdots i_{n-1}!i_n!}\frac{\partial^{i_1+\cdots+i_n}T_n}{\partial x_1^{i_1}\ldots\partial x_n^{i_n}}(\alpha_1,\ldots,\alpha_n)$$

General case: "Precision ring" 2

Proposition 2 (Reformulation of Gianni-Trager-Zaccharias)

$$\vdots$$

$$T_n(x_1,\ldots,x_n) = p_n^{e_n} + \sum_{i_1=1}^{e_1-1}\cdots\sum_{i_n=0}^{e_n-1} c[i_1,\ldots,i_n]p_1^{i_1}\cdots p_n^{i_n}$$

$$T_\ell \equiv \langle p_\ell^{e_\ell} \bmod p_1,\ldots,p_{\ell-1}\rangle \Rightarrow c[0,\ldots,0,i_\ell] = 0 \text{ for all } i_\ell.$$

Remarks:

- If $p_i = x_i - \alpha_i$ then this is Taylor expansion:
$$c[i_1,\ldots,i_n] = \frac{1}{i_1!i_2!\cdots i_{n-1}!i_n!}\frac{\partial^{i_1+\cdots+i_n}T_n}{\partial x_1^{i_1}\ldots\partial x_n^{i_n}}(\alpha_1,\ldots,\alpha_n)$$
- Enhance symbolic thinking: examples with $p_1 = x_1, p_2 = x_2, \ldots, p_n = x_n$ are essentially enough.

General case: "Precision ring" 2

Proposition 2 (Reformulation of Gianni-Trager-Zaccharias)

$$\vdots$$

$$T_n(x_1,\ldots,x_n) = p_n^{e_n} + \sum_{i_1=1}^{e_1-1}\cdots\sum_{i_n=0}^{e_n-1} c[i_1,\ldots,i_n]p_1^{i_1}\cdots p_n^{i_n}$$

$$T_\ell \equiv \langle p_\ell^{e_\ell} \bmod p_1,\ldots,p_{\ell-1}\rangle \Rightarrow c[0,\ldots,0,i_\ell] = 0 \text{ for all } i_\ell.$$

Remarks:

- If $p_i = x_i - \alpha_i$ then this is Taylor expansion:
$$c[i_1,\ldots,i_n] = \frac{1}{i_1!i_2!\cdots i_{n-1}!i_n!}\frac{\partial^{i_1+\cdots+i_n}T_n}{\partial x_1^{i_1}\ldots\partial x_n^{i_n}}(\alpha_1,\ldots,\alpha_n)$$
- Enhance symbolic thinking: examples with $p_1 = x_1, p_2 = x_2, \ldots, p_n = x_n$ are essentially enough.
- Talking about precision makes sense.

General case: "Precision ring" 2

Proposition 2 (Reformulation of Gianni-Trager-Zaccharias)

$$\vdots$$

$$T_n(x_1,\ldots,x_n) = p_n^{e_n} + \sum_{i_1=1}^{e_1-1}\cdots\sum_{i_n=0}^{e_n-1} c[i_1,\ldots,i_n]p_1^{i_1}\cdots p_n^{i_n}$$

$$T_\ell \equiv \langle p_\ell^{e_\ell} \bmod p_1,\ldots,p_{\ell-1}\rangle \Rightarrow c[0,\ldots,0,i_\ell] = 0 \text{ for all } i_\ell.$$

Remarks:

- If $p_i = x_i - \alpha_i$ then this is Taylor expansion:
$$c[i_1,\ldots,i_n] = \frac{1}{i_1!i_2!\cdots i_{n-1}!i_n!}\frac{\partial^{i_1+\cdots+i_n}T_n}{\partial x_1^{i_1}\ldots\partial x_n^{i_n}}(\alpha_1,\ldots,\alpha_n)$$
- Enhance symbolic thinking: examples with $p_1 = x_1, p_2 = x_2, \ldots, p_n = x_n$ are essentially enough.
- Talking about precision makes sense.
disclaimer: This is not exactly the usual sense where it refers to "truncation" (power series, p-adic numbers) by pure powers of uniformizers...

General case: Henselian ring

Since $R = k[x_1, \ldots, x_n]/\mathfrak{q}$ is local of dimension zero, abstract algebra tells that it is Henselian:

Theorem 3

Any factorization into coprimes of a monic polynomial over the field $k[x_1, \ldots, x_n]/\sqrt{\mathfrak{q}}$ lifts into a unique factorization into coprimes over $R = k[x_1, \ldots, x_n]/\mathfrak{q}$.

General case: Henselian ring

Since $R = k[x_1, \ldots, x_n]/\mathfrak{q}$ is local of dimension zero, abstract algebra tells that it is Henselian:

Theorem 3

Any factorization into coprimes of a monic polynomial over the field $k[x_1, \ldots, x_n]/\sqrt{\mathfrak{q}}$ lifts into a unique factorization into coprimes over $R = k[x_1, \ldots, x_n]/\mathfrak{q}$.

- The article contains a short constructive proof which clarifies the link between primary decomposition (unique since in dimension zero).

General case: Henselian ring

Since $R = k[x_1, \ldots, x_n]/\mathfrak{q}$ is local of dimension zero, abstract algebra tells that it is Henselian:

Theorem 3

Any factorization into coprimes of a monic polynomial over the field $k[x_1, \ldots, x_n]/\sqrt{\mathfrak{q}}$ lifts into a unique factorization into coprimes over $R = k[x_1, \ldots, x_n]/\mathfrak{q}$.

- The article contains a short constructive proof which clarifies the link between primary decomposition (unique since in dimension zero).
- this is fundamental to define the new gcd notion called gcd chain. (seems to have been overlooked in previous work)

General case: Henselian ring

Since $R = k[x_1, \ldots, x_n]/\mathfrak{q}$ is local of dimension zero, abstract algebra tells that it is Henselian:

Theorem 3

Any factorization into coprimes of a monic polynomial over the field $k[x_1, \ldots, x_n]/\sqrt{\mathfrak{q}}$ lifts into a unique factorization into coprimes over $R = k[x_1, \ldots, x_n]/\mathfrak{q}$.

- The article contains a short constructive proof which clarifies the link between primary decomposition (unique since in dimension zero).
- this is fundamental to define the new gcd notion called gcd chain. (seems to have been overlooked in previous work)
- Talk of Carlos Sircana "Factorization of polynomials over $\mathbb{Z}/\langle p^\ell \rangle$".
  - Implicitly uses the Henselian property over the local ring $\mathbb{Z}/\langle p^\ell \rangle$.

Framework

According to unique coprime factorization, write:

$$\begin{aligned} a &= a_1 \cdots a_\ell \cdot a_{\ell+1} \cdots a_s \cdot A \\ b &= b_1 \cdots b_\ell \cdot b_{\ell+1} \cdots b_s \cdot B \end{aligned}$$

- $\gcd(A, B) \equiv 1 \bmod \mathfrak{p}$

Framework

According to unique coprime factorization, write:

$$\begin{aligned} a &= a_1 \cdots a_\ell \cdot a_{\ell+1} \cdots a_s \cdot A \\ b &= b_1 \cdots b_\ell \cdot b_{\ell+1} \cdots b_s \cdot B \end{aligned}$$

- $\gcd(A, B) \equiv 1 \bmod \mathfrak{p}$
- for $i \leq \ell$, $\langle a_i, b_i \rangle \equiv \langle a_i \rangle \equiv \langle \rho_i^{\lambda_i} \rangle \bmod \mathfrak{p}$, ρ_i irreducible in $k[x_1, \ldots, x_n]/\mathfrak{p}$.

Framework

According to unique coprime factorization, write:

$$\begin{aligned} a &= a_1 \cdots a_\ell \cdot a_{\ell+1} \cdots a_s \cdot A \\ b &= b_1 \cdots b_\ell \cdot b_{\ell+1} \cdots b_s \cdot B \end{aligned}$$

- $\gcd(A, B) \equiv 1 \bmod \mathfrak{p}$
- for $i \leq \ell$, $\langle a_i, b_i \rangle \equiv \langle a_i \rangle \equiv \langle \rho_i^{\lambda_i} \rangle \bmod \mathfrak{p}$, ρ_i irreducible in $k[x_1, \ldots, x_n]/\mathfrak{p}$.
- for $\ell < i \leq s$, $\langle a_i, b_i \rangle \equiv \langle b_i \rangle \equiv \langle \rho_i^{\nu_i} \rangle \bmod \mathfrak{p}$.

Framework

According to unique coprime factorization, write:

$$\begin{aligned} a &= a_1 \cdots a_\ell \cdot a_{\ell+1} \cdots a_s \cdot A \\ b &= b_1 \cdots b_\ell \cdot b_{\ell+1} \cdots b_s \cdot B \end{aligned}$$

- $\gcd(A, B) \equiv 1 \bmod \mathfrak{p}$
- for $i \leq \ell$, $\langle a_i, b_i \rangle \equiv \langle a_i \rangle \equiv \langle \rho_i^{\lambda_i} \rangle \bmod \mathfrak{p}$, ρ_i irreducible in $k[x_1, \ldots, x_n]/\mathfrak{p}$.
- for $\ell < i \leq s$, $\langle a_i, b_i \rangle \equiv \langle b_i \rangle \equiv \langle \rho_i^{\nu_i} \rangle \bmod \mathfrak{p}$.
- $i \leq \ell$, $b_i \equiv \rho^{\nu_i - \lambda_i} a_i + r_i$, ($r_i$ nilpotent)

Framework

According to unique coprime factorization, write:

$$\begin{aligned} a &= a_1 \cdots a_\ell \cdot a_{\ell+1} \cdots a_s \cdot A \\ b &= b_1 \cdots b_\ell \cdot b_{\ell+1} \cdots b_s \cdot B \end{aligned}$$

- $\gcd(A, B) \equiv 1 \bmod \mathfrak{p}$
- for $i \leq \ell$, $\langle a_i, b_i \rangle \equiv \langle a_i \rangle \equiv \langle \rho_i^{\lambda_i} \rangle \bmod \mathfrak{p}$, ρ_i irreducible in $k[x_1, \ldots, x_n]/\mathfrak{p}$.
- for $\ell < i \leq s$, $\langle a_i, b_i \rangle \equiv \langle b_i \rangle \equiv \langle \rho_i^{\nu_i} \rangle \bmod \mathfrak{p}$.
- $i \leq \ell$, $b_i \equiv \rho^{\nu_i - \lambda_i} a_i + r_i$, $i > \ell$, $a_i \equiv \rho^{\lambda_i - \nu_i} b_i + r_i$ (r_i nilpotent)

Framework

According to unique coprime factorization, write:

$$\begin{aligned} a &= a_1 \cdots a_\ell \cdot a_{\ell+1} \cdots a_s \cdot A \\ b &= b_1 \cdots b_\ell \cdot b_{\ell+1} \cdots b_s \cdot B \end{aligned}$$

- $\gcd(A, B) \equiv 1 \bmod \mathfrak{p}$
- for $i \leq \ell$, $\langle a_i, b_i \rangle \equiv \langle a_i \rangle \equiv \langle \rho_i^{\lambda_i} \rangle \bmod \mathfrak{p}$, ρ_i irreducible in $k[x_1, \ldots, x_n]/\mathfrak{p}$.
- for $\ell < i \leq s$, $\langle a_i, b_i \rangle \equiv \langle b_i \rangle \equiv \langle \rho_i^{\nu_i} \rangle \bmod \mathfrak{p}$.
- $i \leq \ell$, $b_i \equiv \rho^{\nu_i - \lambda_i} a_i + r_i$, $i > \ell$, $a_i \equiv \rho^{\lambda_i - \nu_i} b_i + r_i$ (r_i nilpotent)

$$a = a_1 \cdots a_\ell \cdot \prod_{i=\ell+1}^{s} (\rho_i^{\lambda_i - \nu_i} b_i + r_i) \cdot A$$

$$b = \prod_{i=1}^{\ell} (\rho_i^{\nu_i - \lambda_i} a_i + r_i) \cdot b_{\ell+1} \cdots b_s \cdot B$$

General gcd chain

Any sequence of $\mathfrak{p} = \sqrt{\langle T \rangle}$-primary ideals contained in $\langle T \rangle$:

- $\mathfrak{q} = \langle T \rangle \subset \mathfrak{m}_1 \subsetneq \mathfrak{m}_2 \subsetneq \cdots \subsetneq \mathfrak{m}_{u-1} \subsetneq \mathfrak{m}_u$
  These define "precision" for coefficients of gcds.

General gcd chain

Any sequence of $\mathfrak{p} = \sqrt{\langle T \rangle}$-primary ideals contained in $\langle T \rangle$:

- $\mathfrak{q} = \langle T \rangle \subset \mathfrak{m}_1 \subsetneq \mathfrak{m}_2 \subsetneq \cdots \subsetneq \mathfrak{m}_{u-1} \subsetneq \mathfrak{m}_u$
  These define "precision" for coefficients of gcds.
- at least one r_{ℓ_i} is in $\mathfrak{m}_i$ but not in $\mathfrak{m}_{i-1}$ for
  $\Leftrightarrow \mathfrak{c}(r_{\ell_i}) := \langle \text{coefficients of } r_{\ell_i} \rangle \Rightarrow \mathfrak{c}(r_{\ell_i}) \subset \mathfrak{m}_i,\ \mathfrak{c}(r_{\ell_i}) \subsetneq \mathfrak{m}_{i-1}$

General gcd chain

Any sequence of $\mathfrak{p} = \sqrt{\langle T \rangle}$-primary ideals contained in $\langle T \rangle$:

- $\mathfrak{q} = \langle T \rangle \subset \mathfrak{m}_1 \subsetneq \mathfrak{m}_2 \subsetneq \cdots \subsetneq \mathfrak{m}_{u-1} \subsetneq \mathfrak{m}_u$
  These define "precision" for coefficients of gcds.
- at least one r_{ℓ_i} is in $\mathfrak{m}_i$ but not in $\mathfrak{m}_{i-1}$ for
  $\Leftrightarrow \mathfrak{c}(r_{\ell_i}) := \langle \text{coefficients of } r_{\ell_i} \rangle \Rightarrow \mathfrak{c}(r_{\ell_i}) \subset \mathfrak{m}_i,\ \mathfrak{c}(r_{\ell_i}) \subsetneq \mathfrak{m}_{i-1}$
- Define $G_v \equiv \prod_{i \leq \ell \mid r_i \in \mathfrak{m}_v,\ r_i \notin \mathfrak{m}_{v-1}} a_i \cdot \prod_{i > \ell \mid r_i \in \mathfrak{m}_v,\ r_i \notin \mathfrak{m}_{v-1}} b_i \bmod \mathfrak{m}_v$

General gcd chain

Any sequence of $\mathfrak{p} = \sqrt{\langle T \rangle}$-primary ideals contained in $\langle T \rangle$:

- $\mathfrak{q} = \langle T \rangle \subset \mathfrak{m}_1 \subsetneq \mathfrak{m}_2 \subsetneq \cdots \subsetneq \mathfrak{m}_{u-1} \subsetneq \mathfrak{m}_u$
  These define "precision" for coefficients of gcds.
- at least one r_{ℓ_i} is in $\mathfrak{m}_i$ but not in $\mathfrak{m}_{i-1}$ for
  $\Leftrightarrow \mathfrak{c}(r_{\ell_i}) := \langle \text{coefficients of } r_{\ell_i} \rangle \Rightarrow \mathfrak{c}(r_{\ell_i}) \subset \mathfrak{m}_i,\ \mathfrak{c}(r_{\ell_i}) \subsetneq \mathfrak{m}_{i-1}$
- Define $G_v \equiv \prod_{i \le \ell \mid r_i \in \mathfrak{m}_v,\ r_i \notin \mathfrak{m}_{v-1}} a_i \cdot \prod_{i > \ell \mid r_i \in \mathfrak{m}_v,\ r_i \notin \mathfrak{m}_{v-1}} b_i \bmod \mathfrak{m}_v$
- $[\ (\ \prod_{v=1}^{i}\ G_v\ ,\ \mathfrak{m}_i\ )_{i=1,\ldots,u}\ ]$ is a gcd chain, that is:

General gcd chain

Any sequence of $\mathfrak{p} = \sqrt{\langle T \rangle}$-primary ideals contained in $\langle T \rangle$:

- $\mathfrak{q} = \langle T \rangle \subset \mathfrak{m}_1 \subsetneq \mathfrak{m}_2 \subsetneq \cdots \subsetneq \mathfrak{m}_{u-1} \subsetneq \mathfrak{m}_u$
  These define "precision" for coefficients of gcds.
- at least one r_{ℓ_i} is in $\mathfrak{m}_i$ but not in $\mathfrak{m}_{i-1}$ for
  $\Leftrightarrow \mathfrak{c}(r_{\ell_i}) := \langle \text{coefficients of } r_{\ell_i} \rangle \Rightarrow \mathfrak{c}(r_{\ell_i}) \subset \mathfrak{m}_i,\ \mathfrak{c}(r_{\ell_i}) \subsetneq \mathfrak{m}_{i-1}$
- Define $G_v \equiv \prod_{i \le \ell \mid r_i \in \mathfrak{m}_v,\ r_i \notin \mathfrak{m}_{v-1}} a_i \cdot \prod_{i > \ell \mid r_i \in \mathfrak{m}_v,\ r_i \notin \mathfrak{m}_{v-1}} b_i \bmod \mathfrak{m}_v$
- $[\ (\ \prod_{v=1}^{i}\ G_v\ ,\ \mathfrak{m}_i\ )_{i=1,\ldots,u}\ ]$ is a gcd chain, that is:
  - $(R/\mathfrak{m}_u)[y]/\langle a, b \rangle \simeq (R/\mathfrak{m}_u)[y]/\langle \prod_{i=1}^{u} G_i \rangle$.

General gcd chain

Any sequence of $\mathfrak{p} = \sqrt{\langle T \rangle}$-primary ideals contained in $\langle T \rangle$:

- $\mathfrak{q} = \langle T \rangle \subset \mathfrak{m}_1 \subsetneq \mathfrak{m}_2 \subsetneq \cdots \subsetneq \mathfrak{m}_{u-1} \subsetneq \mathfrak{m}_u$
  These define "precision" for coefficients of gcds.
- at least one r_{ℓ_i} is in $\mathfrak{m}_i$ but not in $\mathfrak{m}_{i-1}$ for
  $\Leftrightarrow \mathfrak{c}(r_{\ell_i}) := \langle \text{coefficients of } r_{\ell_i} \rangle \Rightarrow \mathfrak{c}(r_{\ell_i}) \subset \mathfrak{m}_i,\ \mathfrak{c}(r_{\ell_i}) \subsetneq \mathfrak{m}_{i-1}$
- Define $G_v \equiv \prod_{i \le \ell \mid r_i \in \mathfrak{m}_v,\ r_i \notin \mathfrak{m}_{v-1}} a_i \cdot \prod_{i > \ell \mid r_i \in \mathfrak{m}_v,\ r_i \notin \mathfrak{m}_{v-1}} b_i \bmod \mathfrak{m}_v$
- $[\ (\ \prod_{v=1}^{i} G_v\ ,\ \mathfrak{m}_i\ )_{i=1,\ldots,u}\ ]$ is a gcd chain, that is:
  - $(R/\mathfrak{m}_u)[y]/\langle a, b \rangle \simeq (R/\mathfrak{m}_u)[y]/\langle \prod_{i=1}^{u} G_i \rangle$.
  - $(R/\mathfrak{m}_{u-1})[y]/\langle a, b \rangle \simeq (R/\mathfrak{m}_{u-1})[y]/\langle \prod_{i=1}^{u-1} G_i \rangle \times (R/\mathfrak{m}_u)[y]/\langle G_u \rangle$

General gcd chain

Any sequence of $\mathfrak{p} = \sqrt{\langle T \rangle}$-primary ideals contained in $\langle T \rangle$:

- $\mathfrak{q} = \langle T \rangle \subset \mathfrak{m}_1 \subsetneq \mathfrak{m}_2 \subsetneq \cdots \subsetneq \mathfrak{m}_{u-1} \subsetneq \mathfrak{m}_u$
  These define "precision" for coefficients of gcds.
- at least one r_{ℓ_i} is in $\mathfrak{m}_i$ but not in $\mathfrak{m}_{i-1}$ for
  $\Leftrightarrow \mathfrak{c}(r_{\ell_i}) := \langle \text{coefficients of } r_{\ell_i} \rangle \Rightarrow \mathfrak{c}(r_{\ell_i}) \subset \mathfrak{m}_i,\ \mathfrak{c}(r_{\ell_i}) \subsetneq \mathfrak{m}_{i-1}$
- Define $G_v \equiv \prod_{i \le \ell \mid r_i \in \mathfrak{m}_v,\ r_i \notin \mathfrak{m}_{v-1}} a_i \cdot \prod_{i > \ell \mid r_i \in \mathfrak{m}_v,\ r_i \notin \mathfrak{m}_{v-1}} b_i \bmod \mathfrak{m}_v$
- $[\ (\ \prod_{v=1}^{i} G_v\ ,\ \mathfrak{m}_i\ )_{i=1,\ldots,u}\ ]$ is a gcd chain, that is:
  - $(R/\mathfrak{m}_u)[y]/\langle a, b \rangle \simeq (R/\mathfrak{m}_u)[y]/\langle \prod_{i=1}^{u} G_i \rangle$.
  - $(R/\mathfrak{m}_{u-1})[y]/\langle a, b \rangle \simeq (R/\mathfrak{m}_{u-1})[y]/\langle \prod_{i=1}^{u-1} G_i \rangle \times (R/\mathfrak{m}_u)[y]/\langle G_u \rangle$
  - $\vdots \quad \vdots \quad \vdots$
  - $(R/\mathfrak{m}_1)[y]/\langle a, b \rangle \simeq (R/\mathfrak{m}_1)[y]/\langle G_1 \rangle \times \cdots \times (R/\mathfrak{m}_u)[y]/\langle G_u \rangle$

Computation through a subresultant sequence

Let $[\ (\ \prod_{v=1}^{i}\ G_v\ ,\ \mathfrak{m}_i\ )_{i=1,\ldots,u}\ ]$ be a notation for gcd chain.

Summary of outcomes:

- always possible to compute $(\prod_{v=1}^{u} G_v\ ,\ \mathfrak{m}_u)$.
  largest degree gcd: $(R/\mathfrak{m}_u)[y]/\langle a, b\rangle \simeq (R/\mathfrak{m}_u)[y]/\langle \prod_{v=1}^{u} G_v\rangle$

Computation through a subresultant sequence

Let $[\ (\ \prod_{v=1}^{i}\ G_v\ ,\ \mathfrak{m}_i\ )_{i=1,\ldots,u}\ ]$ be a notation for gcd chain.

Summary of outcomes:

- always possible to compute $(\prod_{v=1}^{u} G_v\ ,\ \mathfrak{m}_u)$.
  largest degree gcd: $(R/\mathfrak{m}_u)[y]/\langle a, b\rangle \simeq (R/\mathfrak{m}_u)[y]/\langle \prod_{v=1}^{u} G_v\rangle$
- more difficult to compute the other blocks
  $(\ \prod_{v=1}^{i}\ G_v\ ,\ \mathfrak{m}_i\ )_{i=1,\ldots,u-1}$
  - attempt with some recursive calls...
  - ...OK in the case $n = 1$ of one variable: $R = k[x_1]$
  - ...some "precision" loss in the process
  - ...general case: still built upon a strong assumption that mimicks the case $n = 1$.

Computation through a subresultant sequence

Let $[\ (\ \prod_{v=1}^{i}\ G_v\ ,\ \mathfrak{m}_i\ )_{i=1,\ldots,u}\ ]$ be a notation for gcd chain.

Summary of outcomes:

- always possible to compute $(\prod_{v=1}^{u} G_v\ ,\ \mathfrak{m}_u)$.
  largest degree gcd: $(R/\mathfrak{m}_u)[y]/\langle a, b\rangle \simeq (R/\mathfrak{m}_u)[y]/\langle \prod_{v=1}^{u} G_v\rangle$
- more difficult to compute the other blocks
  $(\ \prod_{v=1}^{i}\ G_v\ ,\ \mathfrak{m}_i\ )_{i=1,\ldots,u-1}$
  - attempt with some recursive calls...
  - ...OK in the case $n = 1$ of one variable: $R = k[x_1]$
  - ...some "precision" loss in the process
  - ...general case: still built upon a strong assumption that mimicks the case $n = 1$.
- $\rightarrow$ perspective for future work.

Subresultant

Computed over the ring $R/\langle T \rangle$ given in input.

Theorem 4 (Last non-nilpotent subresultant criterion)

Let $\{a, b, S_{d_b-1}(a, b), \ldots\}$ *be the subresultant chain of* a *and* b.

Subresultant

Computed over the ring $R/\langle T \rangle$ given in input.

Theorem 4 (Last non-nilpotent subresultant criterion)

Let $\{a, b, S_{d_b-1}(a,b), \ldots\}$ *be the subresultant chain of* a *and* b. *Assume that* $S_\ell(a,b) \neq 0$, *and* $S_k(a,b) = 0$, *for* $k = \ell - 1, \ldots, 0$.

Subresultant

Computed over the ring $R/\langle T \rangle$ given in input.

Theorem 4 (Last non-nilpotent subresultant criterion)

Let $\{a, b, S_{d_b-1}(a,b), \ldots\}$ be the subresultant chain of a and b. Assume that $S_\ell(a,b) \neq 0$, and $S_k(a,b) = 0$, for $k = \ell - 1, \ldots, 0$. Find from $r = \ell$ to d_b, the last non-nilpotent coefficient $lc(S_t)$ of the subresultant.

Subresultant

Computed over the ring $R/\langle T \rangle$ given in input.

Theorem 4 (Last non-nilpotent subresultant criterion)

Let $\{a, b, S_{d_b-1}(a,b), \ldots\}$ be the subresultant chain of a and b. Assume that $S_\ell(a,b) \neq 0$, and $S_k(a,b) = 0$, for $k = \ell - 1, \ldots, 0$. Find from $r = \ell$ to d_b, the last non-nilpotent coefficient $lc(S_t)$ of the subresultant.
Then $lc(S_t)^{-1} S_t \equiv \prod_{v=1}^{u} G_v \bmod \langle T \cup \{\text{coefficients of } S_{t+1}\}\rangle$.

Subresultant

Computed over the ring $R/\langle T \rangle$ given in input.

Theorem 4 (Last non-nilpotent subresultant criterion)

Let $\{a, b, S_{d_b-1}(a,b), \ldots\}$ be the subresultant chain of a and b. Assume that $S_\ell(a,b) \neq 0$, and $S_k(a,b) = 0$, for $k = \ell - 1, \ldots, 0$. Find from $r = \ell$ to d_b, the last non-nilpotent coefficient $lc(S_t)$ of the subresultant.
Then $lc(S_t)^{-1} S_t \equiv \prod_{v=1}^{u} G_v \bmod \langle T \cup \{\text{coefficients of } S_{t+1}\}\rangle$.
$(\ lc(S_t)^{-1} S_t \ , \ \langle T \cup \{\text{coefficients of } S_{t+1}\}\rangle \ ) \ = \ (\prod_{v=1}^{u} G_v \ , \ \mathfrak{m}_u \ )$.

Subresultant

Computed over the ring $R/\langle T\rangle$ given in input.

Theorem 4 (Last non-nilpotent subresultant criterion)

Let $\{a, b, S_{d_b-1}(a,b), \ldots\}$ be the subresultant chain of a and b. Assume that $S_\ell(a,b) \neq 0$, and $S_k(a,b) = 0$, for $k = \ell - 1, \ldots, 0$. Find from $r = \ell$ to d_b, the last non-nilpotent coefficient $lc(S_t)$ of the subresultant.
Then $lc(S_t)^{-1} S_t \equiv \prod_{v=1}^{u} G_v \bmod \langle T \cup \{\text{coefficients of } S_{t+1}\}\rangle$.
$(\ lc(S_t)^{-1} S_t \ , \ \langle T \cup \{\text{coefficients of } S_{t+1}\}\rangle \ ) \ = \ (\prod_{v=1}^{u} G_v \ , \ \mathfrak{m}_u \ )$.

Need to detect nilpotent mod T: iterative resultant:

Subresultant

Computed over the ring $R/\langle T\rangle$ given in input.

Theorem 4 (Last non-nilpotent subresultant criterion)

Let $\{a, b, S_{d_b-1}(a,b), \ldots\}$ be the subresultant chain of a and b. Assume that $S_\ell(a,b) \neq 0$, and $S_k(a,b) = 0$, for $k = \ell - 1, \ldots, 0$. Find from $r = \ell$ to d_b, the last non-nilpotent coefficient $lc(S_t)$ of the subresultant.
Then $lc(S_t)^{-1} S_t \equiv \prod_{v=1}^{u} G_v \bmod \langle T \cup \{\text{coefficients of } S_{t+1}\}\rangle$.
$(\; lc(S_t)^{-1} S_t \; , \; \langle T \cup \{\text{coefficients of } S_{t+1}\}\rangle \;) \; = \; (\prod_{v=1}^{u} G_v \; , \; \mathfrak{m}_u \;)$.

Need to detect nilpotent mod T: iterative resultant:

f is nilpotent if and only if :
$\mathrm{Res}_{x_1}(\mathrm{Res}_{x_2}(\cdots \mathrm{Res}_{x_{n-1}}(\mathrm{Res}_{x_n}(f, T_n), T_{n-1})\cdots), T_2), T_1) = 0$

Subresultant 2

1. Compute a subresultant sequence $a, b, S_{r_1}, \ldots, S_{r_t}$, $r_i > r_{i+1}$, modulo T, until to get a zero: $S_{r_t} \equiv 0 \bmod \langle T \rangle$.
2. $j = t$
3. While isNil($\mathrm{lc}(S_{r_j})$) do
   1. $j = j - 1$
4. $g_u = \mathrm{Monic}(S_{r_j})$ `// Invert leading Coeff.`
5. $\mathfrak{m}_u := \langle T \rangle + \langle \text{ coeff of } S_{r_{j+1}} \rangle$
7. Return $[(g_u, \mathfrak{m}_u)$]

Subresultant 2

1. Compute a subresultant sequence $a, b, S_{r_1}, \ldots, S_{r_t}$, $r_i > r_{i+1}$, modulo T, until to get a zero: $S_{r_t} \equiv 0 \bmod \langle T \rangle$.
2. $j = t$
3. While isNil($\mathrm{lc}(S_{r_j})$) do
   1. $j = j - 1$
4. $g_u = \mathrm{Monic}(S_{r_j})$ `// Invert leading Coeff.`
5. $\mathfrak{m}_u := \langle T \rangle + \langle \text{ coeff of } S_{r_{j+1}} \rangle$
6. $p_{next} = InvP^{-1}(\frac{S_{r_{j+1}}}{NilP})$ `// Assumption`
7. Return $[(g_u, \mathfrak{m}_u), p_{next}]$

Case of $n = 1$ variable: iteration

$n = 1$: $T = (T_1(x_1)) = (p_1^{e_1})$, where $p_1 \in k[x_1]$ is irreducible.

- After having found $g_u = \tilde{S}_t := \mathrm{lc}(S_t)^{-1} S_t$, p_{next}, and $\mathfrak{m}_u := \langle p_1^{r_1} \rangle$, $1 \leq r_1 < e_1$.

Case of $n = 1$ variable: iteration

$n = 1$: $T = (T_1(x_1)) = (p_1^{e_1})$, where $p_1 \in k[x_1]$ is irreducible.

- After having found $g_u = \tilde{S}_t := \mathrm{lc}(S_t)^{-1} S_t$, p_{next}, and $\mathfrak{m}_u := \langle p_1^{r_1} \rangle$, $1 \leq r_1 < e_1$.
- iterate the same algorithm with:
- Input: $\tilde{S}_t = g_u$, $\mathrm{Monic}(S_{t+1}) = p_{next}$ and $p_1^{r_1}$. instead of a, b and $T = (p_1^{e_1})$.

Case of $n = 1$ variable: iteration

$n = 1$: $T = (T_1(x_1)) = (p_1^{e_1})$, where $p_1 \in k[x_1]$ is irreducible.

- After having found $g_u = \tilde{S}_t := \mathrm{lc}(S_t)^{-1} S_t$, p_{next}, and $\mathfrak{m}_u := \langle p_1^{r_1} \rangle$, $1 \leq r_1 < e_1$.
- iterate the same algorithm with:
- Input: $\tilde{S}_t = g_u$, $\mathrm{Monic}(S_{t+1}) = p_{next}$ and $p_1^{r_1}$. instead of a, b and $T = (p_1^{e_1})$.
  - where $\mathrm{Monic}(A) = InvP(A)^{-1} \frac{A}{NilP(A)}$.
    The "nilpotent part" $NilP(A)$ divides A and we can invert the remaining invertible part $InvP(A)$.

Case of $n = 1$ variable: iteration

$n = 1$: $T = (T_1(x_1)) = (p_1^{e_1})$, where $p_1 \in k[x_1]$ is irreducible.

- After having found $g_u = \tilde{S}_t := \mathrm{lc}(S_t)^{-1} S_t$, p_{next}, and $\mathfrak{m}_u := \langle p_1^{r_1} \rangle$, $1 \leq r_1 < e_1$.
- iterate the same algorithm with:
- Input: $\tilde{S}_t = g_u$, $\mathrm{Monic}(S_{t+1}) = p_{next}$ and $p_1^{r_1}$. instead of a, b and $T = (p_1^{e_1})$.
  - where $\mathrm{Monic}(A) = InvP(A)^{-1} \frac{A}{NilP(A)}$.
    The "nilpotent part" $NilP(A)$ divides A and we can invert the remaining invertible part $InvP(A)$.
- It ouptuts, $g_{u-1} := \prod_{v=1}^{u-1} G_v \bmod p_1^{r_1}$ instead of $\bmod p_1^{e_1}$ (precision loss).

Case of $n = 1$ variable: iteration

$n = 1$: $T = (T_1(x_1)) = (p_1^{e_1})$, where $p_1 \in k[x_1]$ is irreducible.

- After having found $g_u = \tilde{S}_t := \mathrm{lc}(S_t)^{-1} S_t$, p_{next}, and $\mathfrak{m}_u := \langle p_1^{r_1} \rangle$, $1 \leq r_1 < e_1$.
- iterate the same algorithm with:
- Input: $\tilde{S}_t = g_u$, $\mathrm{Monic}(S_{t+1}) = p_{next}$ and $p_1^{r_1}$. instead of a, b and $T = (p_1^{e_1})$.
  - where $\mathrm{Monic}(A) = InvP(A)^{-1} \frac{A}{NilP(A)}$.
    The "nilpotent part" $NilP(A)$ divides A and we can invert the remaining invertible part $InvP(A)$.
- It ouptuts, $g_{u-1} := \prod_{v=1}^{u-1} G_v \bmod p_1^{r_1}$ instead of $\bmod p_1^{e_1}$ (precision loss).

And repeat to find the next block: $g_{u-1} \bmod p_1^{r_2}$, $r_2 < r_1 < e_1$.

Remarks on the general case $n > 1$

For $n > 1$ variables, it is more delicate to iterate the subresultant routine:

- No simple equivalent for switching $p_1^{e_1} \leftrightarrow p_1^{e_1 - r_1}$ in the recursive call.
- No evidence that the nilpotent part of the leading coefficient of S_{t+1} divides the whole S_{t+1}.

Some examples show that it still work though.

Conclusion

Contributions:

- Clarification of the meaning of gcd.
- Preliminaries algorithms based on subresultant
- Well identified problems to consider the case of $n > 1$ variables.

Perspective:

- Remove the restriction of one primary ideal to a general non-radical triangular set.
- conisder "saturated ideals" in positive dimension.
  By putting the free variables as coefficients.

Vielen Dank