Regular chain theory

Marc Moreno Maza

CS 9652, March 30, 2020

Plan

Zero-dimensional regular chains

Pseudo-division, subresultants and division-free Euclidean algorithms

Division-free Euclidean algorithms

Computing regular GCDs

Regular chains in arbitrary dimension

Incremental solving

Plan

How triangular decompositions look like?

For the following input polynomial system:

$$F : \begin{cases} x^2 + y + z = 1 \\ x + y^2 + z = 1 \\ x + y + z^2 = 1 \end{cases}$$

One possible triangular decompositions of the solution set of F is:

$$\begin{cases} z = 0 \\ y = 1 \\ x = 0 \end{cases} \cup \begin{cases} z = 0 \\ y = 0 \\ x = 1 \end{cases} \cup \begin{cases} z = 1 \\ y = 0 \\ x = 0 \end{cases} \cup \begin{cases} z^2 + 2z - 1 = 0 \\ y = z \\ x = z \end{cases}$$

Another one is:

$$\begin{cases} z = 0 \\ y^2 - y = 0 \\ x + y = 1 \end{cases} \cup \begin{cases} z^3 + z^2 - 3z = -1 \\ 2y + z^2 = 1 \\ 2x + z^2 = 1 \end{cases}$$

An example in positive dimension

- Every prime ideal $\mathcal{P} = \langle F \rangle$ in a polynomial ring $\mathbb{K}[x_1, \ldots, x_n]$ may be **represented** by a **triangular set** T encoding the **generic zeros** of $\mathcal{P}$.

$$F = \left\{ \begin{array}{l} ax + by - c \\ dx + ey - f \\ gx + hy - i \end{array} \right. \simeq T = \left\{ \begin{array}{l} gx + hy - i \\ (hd - eg)\, y - id + fg \\ (ie - fh)\, a + (ch - ib)\, d + (fb - ce)\, g \end{array} \right.$$

- **All the common zeros** of every polynomial system can be decomposed into **finitely many** triangular sets.

$$\begin{array}{rcl} \mathbf{V}(\mathcal{P}) & = & \mathbf{W}(T) \cup \mathbf{W} \left\{ \begin{array}{l} dx + ey - f \\ hy - i \\ (ie - fh)\, a + (-ib + ch)\, d \\ g \end{array} \right. \cup \mathbf{W} \left\{ \begin{array}{l} gx + hy - i \\ (ha - bg)\, y - ia + cg \\ hd - eg \\ ie - fh \end{array} \right. \\ & & \cup \mathbf{W} \left\{ \begin{array}{l} x \\ (hd - eg)\, y - id + fg \\ fb - ce \\ ie - fh \end{array} \right. \cup \mathbf{W} \left\{ \begin{array}{l} ax + by - c \\ hy - i \\ d \\ g \\ ie - fh \end{array} \right. \cup \cdots \end{array}$$

where $\mathbf{W}(T)$ denotes the generic zeros of T. We have : $\mathbf{W}(T) \subseteq \mathbf{V}(T)$.

How to compute triangular decompositions?

- Consider again solving the system F for $x > y > z$:

$$F : \begin{cases} x^2 + y + z = 1 \\ x + y^2 + z = 1 \\ x + y + z^2 = 1 \end{cases}$$

- Eliminating x leads to $\begin{cases} y^2 + (-1 + 2z^2)y - 2z^2 + z + z^4 = 0 \\ y^2 + z - y - z^2 = 0 \end{cases}$
- Eliminating y^2 and then y we can arrive to $r(z) = 0$ with $r(z) = z^8 - 4z^6 + 4z^5 - z^4$.
- Factorizing $r(z)$ leads to $z^4(z^2 + 2z - 1)(z - 1)^2 = 0$ and thus to $z = 0$, $z = 1$ or $z^2 + 2z = 1$. In each case, it is easy to conclude either by substitution, or by GCD computation in $(\mathbb{Q}[z]/\langle z^2 + 2z - 1\rangle)[y]$.
- Alternatively, one can directly perform GCD computation in $(\mathbb{Q}[z]/\langle r(z)\rangle)[y]$. But this is unusual since $\mathbb{Q}[z]/\langle r(z)\rangle$ is not a field! Let us see this now.

Computing a polynomial GCD over a ring with zero-divisors (I)

- Let us consider again the polynomials

$$\left\{\begin{array}{l} f_1 = y^2 + (2z^2 - 1)y - 2z^2 + z + z^4 \\ f_2 = y^2 + z - y - z^2 \end{array}\right.$$

- Let us compute their GCD in $\mathbb{L}[y]$ with $\mathbb{L} = \mathbb{Q}[z]/\langle s(z)\rangle$ where $s(z) = z(z^2 + 2z - 1)(z - 1)$ is the squarefree part of $r(z)$. (Replacing $r(z)$ with $s(z)$ makes the story simpler.)
- We proceed **as if $\mathbb{L}$ were a field** and run the **Euclidean Algorithm in $\mathbb{L}[y]$**. Of course, before dividing by an element of $\mathbb{L}$ we check whether it is a zero-divisor. We pretend we are not aware of the factorization of $s(z)$.
- Dividing f_1 by f_2 is no problem since f_2 is monic. We obtain: $\begin{array}{l|l} f_1 & f_2 \\ \hline f_3 & 1 \end{array}$

with $f_3 = 2z^2y - z^2 + 2z^2 - z$.

Computing a polynomial GCD over a ring with zero-divisors (II)

• In order to divide f_2 by f_3, we need to check whether $2z^2$ divides zero in $\mathbb{L}$. This is done by computing $\gcd(s(z), 2z^2)$ in $\mathbb{Q}[z]$, which is z.

• Hence $s(z)$ writes $z(z^3 + z^2 - 3z + 1)$ and we split the computations into two cases: $z = 0$ and $z^3 + z^2 - 3z = 1$.

• $\boxed{\text{Case } z = 0.}$ Then $f_3 = 0$ and $f_2 = y^2 - y$ is the GCD.

• $\boxed{\text{Case } z^3 + z^2 - 3z = -1.}$ Since $S(z)$ is square-free, $2z^2$ has an inverse in this case, namely $i(z) = -(3/2)z^2 - 2z + 4$.

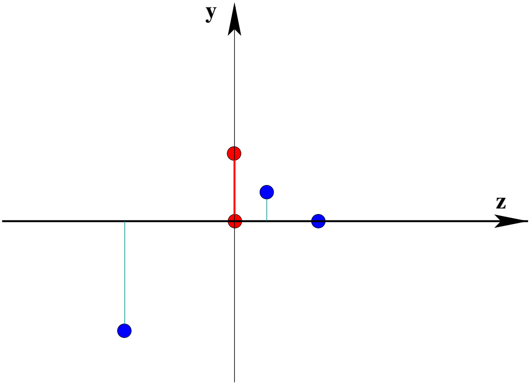
• Thus, the polynomial $\tilde{f_3} = i(z)f_3 = y + (1/2)z^2 - (1/2)$ is monic. So, we can compute $\begin{array}{c|c} f_2 & \tilde{f_3} \\ \hline 0 & y - (1/2)z^2 - (1/2) \end{array}$.

• Finally $\gcd(f_1, f_2, \mathbb{L}[y]) = \begin{cases} y^2 - y & \text{if} \quad z = 0 \\ 2y + z^2 - 1 & \text{if} \quad z^3 + z^2 - 3z = -1 \end{cases}$

How those triangular sets look like? (I)

• Let us consider again the system $\begin{cases} y^2 + (-1 + 2z^2)y - 2z^2 + z + z^4 = 0 \\ y^2 + z - y - z^2 = 0 \end{cases}$

• Let α_1 and α_2 be the roots of $z^2 + 2z - 1 = 0$. After dropping multiplicities, we obtain $(z, y) \in \{(0,0), (0,1), (\alpha_1, \alpha_1), (\alpha_2, \alpha_2), (1,0)\}$.



How to pass from one triangular decomposition to another?

$$\left\{\begin{array}{l} z=0 \\ y=1 \\ x=0 \end{array}\right. \cup \left\{\begin{array}{l} z=0 \\ y=0 \\ x=1 \end{array}\right. \cup \left\{\begin{array}{l} z=1 \\ y=0 \\ x=0 \end{array}\right. \cup \left\{\begin{array}{r} z^2+2z-1=0 \\ y=z \\ x=z \end{array}\right.$$

$$\downarrow \quad \mathrm{CRT} \quad \downarrow$$

$$\left\{\begin{array}{r} z=0 \\ y^2-y=0 \\ x+y=1 \end{array}\right. \cup \left\{\begin{array}{l} z=1 \\ y=0 \\ x=0 \end{array}\right. \cup \left\{\begin{array}{r} z^2+2z-1=0 \\ y=z \\ x=z \end{array}\right.$$

$$\downarrow \quad \mathrm{CRT} \quad \downarrow$$

$$\left\{\begin{array}{r} z=0 \\ y^2-y=0 \\ x+y=1 \end{array}\right. \cup \left\{\begin{array}{r} z^3+z^2-3z=-1 \\ 2y+z^2=1 \\ 2x+z^2=1 \end{array}\right.$$

From a lexicographical Gröbner basis to a triangular decomposition (I)

- Let us consider again (last time) the polynomials

$$\begin{cases} f_1 = y^2 + (2z^2 - 1)y - 2z^2 + z + z^4 \\ f_2 = y^2 + z - y - z^2 \end{cases}$$

- It is natural to ask how we could obtain a triangular decomposition from the reduced lexicographical Gröbner basis of $\{f_1, f_2\}$ for $y > z$. This basis is: $\begin{cases} g_1 = z^6 - 4z^4 + 4z^3 - z^2 \\ g_2 = 2z^2y + z^4 - z^2 \\ g_3 = y^2 - y - z^2 + z \end{cases}$

- We initialize $T := \{g_1\}$. We would **add** g_2 into T provided that $\mathrm{lc}(g_2, y)$ is a **unit**.

From a lexicographical Gröbner basis to a triangular decomposition (II)

- So, we compute $\gcd(2z^2, g_1, \mathbb{Q}[z]) = z^2$. This shows $g_1 = z^2(z^4 - 4z^2 + 4z - 1)$ and splits the computations into two cases.
- $\boxed{\text{Case } z^2 = 0.}$ In this case g_2 **vanishes** and $g_3 = y^2 - y + z$, leading to $T^1 := \{z^2, y^2 - y + z\}$
- $\boxed{\text{Case } z^4 - 4z^2 + 4z - 1.}$ In this case $\mathrm{lc}(g_2, y)$ has $2z^3 + (1/2)z^2 - 8z + 6$ for **inverse**. Multiplying g_2 by this inverse leads to $\tilde{g}_2 = y + (1/2)z^2 - (1/2)$. Then, we observe that $\begin{array}{c|c} g_3 & \tilde{g}_2 \\ \hline 0 & y - (1/2)z^2 - (1/2) \end{array}$ leading to a second component $T^2 := \{z^4 - 4z^2 + 4z - 1, 2y + 1z^2 - 1\}$.
- For more details: **(Gianni, 1987), (Kalkbrener, 1987), (Lazard, 1992)**.

Some notations before we start the theory (I)

Notation

Throughout the talk, we consider a field $\mathbb{K}$ and an ordered set $X = x_1 < \cdots < x_n$ of n variables. Typically $\mathbb{K}$ will be

- *a* **finite field**, *such as $\mathbb{Z}/p\mathbb{Z}$ for a prime p, or*
- *the field $\mathbb{Q}$ of* **rational numbers**, *or*
- *a field of* **rational functions** *over $\mathbb{Z}/p\mathbb{Z}$ or $\mathbb{Q}$.*

We will denote by $\overline{\mathbb{K}}$ the **algebraic closure** *of $\mathbb{K}$.*

Notation

We denote by $\mathbb{K}[x_1, \ldots, x_n]$ the ring of the polynomials with coefficients in $\mathbb{K}$ and variables in X. For $F \subset \mathbb{K}[x_1, \ldots, x_n]$, we write $\langle F \rangle$ and $\sqrt{\langle F \rangle}$ for the ideal generated by F in $\mathbb{K}[x_1, \ldots, x_n]$ and its radical, respectively.

Notation

For $F \subset \mathbb{K}[x_1, \ldots, x_n]$, we are interested in

$$V(F) = \{\zeta \in \overline{\mathbb{K}}^n \mid (\forall f \in F)\ f(\zeta) = 0\},$$

the **zero-set** *of F or* **algebraic variety** *of F in $\overline{\mathbb{K}}^n$.*

Remark

In some circumstances $\overline{\mathbb{K}}^n$ will be denoted $A^n(\overline{\mathbb{K}})$, especially when we consider several n at the same time.

Some notations before we start the theory (II)

Notation

Let i and j be integers such that $1 \leq i \leq j \leq n$ and let $V \subseteq A^n(\overline{\mathbb{K}})$ be a variety over $\mathbb{K}$. We denote by π_i^j the natural projection map from $A^j(\overline{\mathbb{K}})$ to $A^i(\overline{\mathbb{K}})$, which sends $(x_1, \ldots, x_j)$ to $(x_1, \ldots, x_i)$. Moreover, we define $V_i = \pi_i^n(V)$. Often, we will restrict π_i^j from V_j to V_i.

Notation

The algebraic varieties in $\overline{\mathbb{K}}^n$ defined by polynomial sets of $\mathbb{K}[x_1, \ldots, x_n]$ form the **closed sets** *of a topology, called* **Zariski Topology**. *For a subset $W \subset \overline{\mathbb{K}}^n$, we denote by $\overline{W}$ the closure of W for this topology, that is, the intersection of the $V(F)$ containing W, for all $F \subset \mathbb{K}[x_1, \ldots, x_n]$.*

Notation

For $W \subset \overline{\mathbb{K}}^n$, we denote by $I(W)$ the ideal of $\mathbb{K}[x_1, \ldots, x_n]$ generated by the polynomials vanishing at every point of W.

Remark

When $\mathbb{K} = \overline{\mathbb{K}}$ and $W = V(F)$, for some $F \subset \mathbb{K}[x_1, \ldots, x_n]$, recall the Hilbert Theorem of Zeros:

$$\sqrt{\langle F \rangle} = I(V(F)).$$

Lazard triangular sets

Definition

(Lazard, 1992) A subset

$$T \; = \; \{T_1, \ldots T_n\} \; \subset \; \mathbb{K}[x_1 < \cdots < x_n]$$

is a Lazard triangular set if for $i = 1 \cdots n$

$$T_i \; = \; 1\,\mathbf{x_i^{d_i}} + a_{d_i-1}\,\mathbf{x_i^{d_i-1}} + \cdots + a_1\,\mathbf{x_i} + a_0$$

with

$$a_{d_i-1}, \ldots, a_1, a_0 \in \mathbf{k}[x_1, \ldots, x_{i-1}].$$

reduced w.r.t $\langle T_1, \ldots, T_{i-1} \rangle$ in the sense of Gröbner bases.

Theorem

A family T of n polynomials in $\mathbb{K}[x_1 < \cdots < x_n]$ is a **Lazard triangular set** *if and only it is the* **reduced lexicographical Gröbner basis** *of a* **zero-dimensional** *ideal.*

How those triangular sets look like? (II)

Notation

Let $T = \{T_1, \ldots T_n\} \subset \mathbb{K}[x_1, \ldots, x_n]$ *be a Lazard triangular set. Let* V *be its variety in* $A^n(\overline{\mathbb{K}})$. *Let* $d_1 = \deg(T_1, x_1), \ldots, d_n = \deg(T_n, x_n)$.

Notation

For $1 \leq i < j \leq n$*, recall that*

$$\pi_i^j : \begin{array}{ccc} V_j & \longmapsto & V_i \\ (x_1, \ldots, x_j) & \to & (x_1, \ldots, x_i) \end{array}$$

where $V_i = \pi_i^n(V)$ *and* $V_j = \pi_j^n(V)$.

Proposition

For a point $M \in V_i$ *the* fiber *(i.e. the pre-image)* $(\pi_i^j)^{-1}(M)$ *has cardinality* $d_{i+1} \cdots d_j$*, that is*

$$|(\pi_i^j)^{-1}(M)| = d_{i+1} \cdots d_j.$$

Equiprojectable varieties

Definition

Let i and j be integers such that $1 \le i < j \le n$ and let $V \subseteq A^j(\overline{\mathbb{K}})$ be a variety over $\mathbb{K}$. The set V is said

(1) **equiprojectable on** V_i, its projection on $A^i(\overline{\mathbb{K}})$, if there exists an integer c such that for every $M \in V_i$ the cardinality of $(\pi_i^j)^{-1}(V_i)$ is c.

(2) **equiprojectable** if V is equiprojectable on $V_1, \ldots, V_{j-1}$.

Theorem

(Aubry & Valibouze, 2000) *Assume $\mathbb{K}$ is* **perfect** *and let $V \subset A^n(\overline{\mathbb{K}})$ be finite. Assume that there exists $F \subset \mathbb{K}[x_1, \ldots, x_n]$ such that $V = V(F)$. Then, the following conditions are equivalent:*

(1) *V is equiprojectable,*

(2) *There exists a Lazard Triangular set $T \subset \mathbb{K}[x_1, \ldots, x_n\}$ whose zero-set in $A^n(\overline{\mathbb{K}})$ is exactly V.*

Proof.

For proving (1) $\Rightarrow$ (2) one can use the **interpolation formulas** of **(Dahan & Schost, 2004)** to construct a Lazard triangular set in $\overline{\mathbb{K}}[x_1, \ldots, x_n]$. To conclude, one uses the hypothesis $\mathbb{K}$ perfect, $V = V(F)$ together with the Hilbert Theorem of Zeros. $\square$

The interpolation formulas: sketch (I)

- Let $V \subset A^n(\overline{\mathbb{K}})$ be (finite and) equiprojectable. Let $\mathbf{K}$ be a field, with $\mathbb{K} \subseteq \mathbf{K} \subseteq \overline{\mathbb{K}}$ such that every point of V has its coordinates in $\mathbf{K}$.
- We have $T_1 = \prod_{\alpha \in V_1}(x_1 - \alpha)$. Let $1 \leq \ell < n$. We give interpolation formulas for $T_{\ell+1}$ from the coordinates (in $\mathbf{K}$) of the points of $V_{\ell+1}$, for $1 \leq \ell < n$.
- Let $\alpha = (\alpha_1, \ldots, \alpha_\ell) \in V_\ell$. We define the varieties

$$\begin{array}{llclcr}
V_\alpha^1 & = \{ & \beta = (\beta_1, \ldots, \beta_\ell, \beta_{\ell+1}) \in V_{\ell+1} & \mid & \beta_1 \neq \alpha_1 \} \\
V_\alpha^2 & = \{ & \beta = (\alpha_1, \beta_2, \ldots, \beta_\ell, \beta_{\ell+1}) \in V_{\ell+1} & \mid & \beta_2 \neq \alpha_2 \} \\
\cdots & \cdots & \cdots & \cdots & \cdots \\
V_\alpha^\ell & = \{ & \beta = (\alpha_1, \ldots, \alpha_{\ell-1}, \beta_\ell, \beta_{\ell+1}) \in V_{\ell+1} & \mid & \beta_\ell \neq \alpha_\ell \} \\
V_\alpha^{\ell+1} & = \{ & \beta = (\alpha_1, \ldots, \alpha_\ell, \beta_{\ell+1}) \in V_{\ell+1} & & \}
\end{array}$$

The sets $V_\alpha^1, V_\alpha^2, V_\alpha^3, \ldots, V_\alpha^\ell, V_\alpha^{\ell+1}$ form a partition of $V_{\ell+1}$.

- The intermediate goal is to build $T_{\alpha,\ell+1} = T_i(\alpha_1, \ldots, \alpha_\ell, x_{\ell+1}) \in \mathbf{K}[x_{\ell+1}]$.

The interpolation formulas: sketch (II)

- We consider also the projections

$$\begin{array}{ccccccc} v_\alpha^1 & = & \pi_1^{\ell+1}(V_\alpha^1) & = & \{(\beta_1) \in V_1 & \mid & \beta_1 \neq \alpha_1\} \\ v_\alpha^2 & = & \pi_2^{\ell+1}(V_\alpha^2) & = & \{(\alpha_1, \beta_2) \in V_2 & \mid & \beta_2 \neq \alpha_2\} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ v_\alpha^\ell & = & \pi_\ell^{\ell+1}(V_\alpha^\ell) & = & \{(\alpha_1, \ldots, \alpha_{\ell-1}, \beta_\ell) \in V_\ell & \mid & \beta_\ell \neq \alpha_\ell\} \end{array}$$

- For $1 \leq i \leq \ell$, define $e_{\alpha,i} := \prod_{\beta \in v_\alpha^i} (x_i - \beta_i) \in \mathbf{K}[x_i]$ and

$\boxed{E_\alpha := \prod_{1 \leq i \leq \ell} e_{\alpha,i} \in \mathbf{K}[x_1, \ldots, x_\ell].}$

- Then, we have:

$$\begin{array}{ccl} T_{\alpha,\ell+1} & = & \prod_{\beta \in V_\alpha^{\ell+1}} (x_{\ell+1} - \beta_{\ell+1}) \\ T_{\ell+1} & = & \sum_{\alpha \in V_\ell} \frac{E_\alpha \, T_{\alpha,\ell+1}}{E_\alpha(\alpha)} \end{array}$$

- Related work: **(Abbot, Bigatti, Kreuzer & Robbiano, 1999)**, ...

Direct product of fields, the D5 Principle (I)

Proposition

Let $f \in \mathbb{K}[x]$ be a non-constant and **square-free** *univariate polynomial. Then $\mathbb{L} = \mathbb{K}[x]/\langle f \rangle$ is a direct product of fields (DPF).*

Proof.

The factors of f are **pairwise coprime**. Then, apply the **Chinese Remaindering Theorem**. (If $f = f_1 f_2$ then $\mathbb{L} \simeq \mathbb{K}[x]/\langle f_1 \rangle \times \mathbb{K}[x]/\langle f_2 \rangle$. □

PRINCIPLE. **(Della Dora, Dicrescenzo & Duval, 1985)** If $\mathbb{L}$ is a DPF, then one can compute with $\mathbb{L}$ as **if it were a field**: it suffices to **split** the computations into cases whenever a **zero-divisor** is met.

Proposition

Let $\mathbb{L}$ be a DPF and $f \in \mathbb{L}[x]$ be a non-constant monic polynomial such that f and its derivative generate $\mathbb{L}[x]$, that is, $\langle f, f' \rangle = \mathbb{L}[x]$. Then $\mathbb{L}[x]/\langle f \rangle$ is another DPF.

Proof.

It is convenient to establish the following more general theorem: *A Noetherian ring is isomorphic with a direct product of fields if and only if every non-zero element is either a unit or a non-nilpotent zero-divisor.* □

Direct product of fields, the D5 Principle (II)

Proposition

Let $T \subset \mathbb{K}[x_1, \ldots, x_n]$ be a Lazard triangular set such that $\langle T \rangle$ is **radical**. *Then, we have*

- $\mathbb{K}[x_1, \ldots, x_n]/\langle T \rangle$ *is a DPF,*
- *if $\mathbb{K}$ is* **perfect** *then $\overline{\mathbb{K}}[x_1, \ldots, x_n]/\langle T \rangle$ is a DPF.*

Remark

Recall the trap! *Consider $\mathbb{F} = \mathbb{Z}/p\mathbb{Z}(t)$, for a prime p. Consider the polynomial $f = x^p - t \in \mathbb{F}[x]$ and $\overline{\mathbb{F}}$ an algebraic closure of $\mathbb{F}$.*
Since f is not constant, it has a root $\alpha \in \overline{\mathbb{F}}$ and we have

$$f = x^p - t = x^p - \alpha^p = (x - \alpha)^p \tag{1}$$

in $\overline{\mathbb{F}}[x]$, which is clearly not square-free. However f is irreducible, and thus squarefree, in $\mathbb{F}[x]$.

Polynomial GCDs over DPF, quasi-inverses (I)

Definition

(M. & Rioboo, 1995) Let $\mathbb{L}$ be a DPF. The polynomial $h \in \mathbb{L}[y]$ is a **GCD** of the polynomials $f, g \in \mathbb{L}[y]$ if the ideals $\langle f, g \rangle$ and $\langle h \rangle$ are equal.

Remark

Another trap! *Even if f, g are both* **monic**, *there* **may not exist a monic** *polynomial h in $\mathbb{L}[y]$ such that $\langle f, g \rangle = \langle h \rangle$ holds. Consider for instance $f = y + \frac{a+1}{2}$ (assuming that 2 is invertible in $\mathbb{L}$) and $g = y + 1$ where $a \in \mathbb{L}$ satisfies $a^2 = a$, $a \neq 0$ and $a \neq 1$.*

Remark

In practice, polynomial GCDs over DPF are computed via the D5 Principle. Moreover, only monic GCDs are useful. So, we generalize:

Definition

Let $\mathbb{L}$ be a DPF and $f, g \in \mathbb{L}[y]$. A **GCD** of f, g in $\mathbb{L}[y]$ is a sequence of pairs $((h_i, \mathbb{L}_i), 1 \leq i \leq s)$ such that

- $\mathbb{L}_i$ is a DPF, for all $1 \leq i \leq s$ and the direct product of $\mathbb{L}_1, \ldots, \mathbb{L}_s$ is isomorphic to $\mathbb{L}$,
- h_i is a null or monic polynomial in $\mathbb{L}_i[y]$, for all $1 \leq i \leq s$,
- h_i is a GCD (in the above sense) of the projections of f, g to $\mathbb{L}_i[y]$, for all $1 \leq i \leq s$.

Polynomial GCDs over DPF, quasi-inverses (II)

Definition

Let $\mathbb{L}$ be a DPF and let $f \in \mathbb{L}$. A **quasi-inverse** of f is a sequence of pairs $((g_i, \mathbb{L}_i), 1 \le i \le s)$ such that

- $\mathbb{L}_i$ is a DPF, for all $1 \le i \le s$ and the direct product of $\mathbb{L}_1, \ldots, \mathbb{L}_s$ is isomorphic to $\mathbb{L}$
- $g_i \in \mathbb{L}_i$, for all $1 \le i \le s$,
- let f_i be the projection of f to $\mathbb{L}_i$; either $f_i = g_i = 0$ or $f_i g_i = 1$ hold, for all $1 \le i \le s$.

Proposition

Let $T \subset \mathbb{K}[x_1, \ldots, x_n]$ be a Lazard triangular set such that $\langle T \rangle$ is **radical**. *We define $\mathbb{L} = \mathbb{K}[x_1, \ldots, x_n]/\langle T \rangle$.*

(1) *For all $f \in \mathbb{K}[x_1, \ldots, x_n]$ (reduced w.r.t. T) one can compute a* **quasi-inverse** *in $\mathbb{L}$ of f (regarded as an element of $\mathbb{L}$).*

(1) *For all $f, g \in \mathbb{L}[y]$ one can compute a* **GCD** *of f and g in $\mathbb{L}[y]$.*

Equiprojectable decomposition

Remark

Not every variety is equiprojectable, for instance $V = \{(0,1),(0,0),(1,0)\}$.

Definition

Let $V \subset A^n(\overline{\mathbb{K}})$ be finite. Consider the projection $\pi : V \longmapsto \overline{\mathbb{K}}^{n-1}$ which forgets x_n. To every $x \in V$ we associate

$$N(x) = \#\pi^{-1}(\pi(x)).$$

We write $V = C_1 \cup \cdots \cup C_d$ where $C_i = \{x \in V \mid N(x) = i\}$. This splitting process is applied recursively to all varieties $C_1, \ldots, C_d$.
In the end, we obtain a family of pairwise disjoint, equiprojectable varieties, whose reunion equals V. This is the **equiprojectable decomposition** of V.

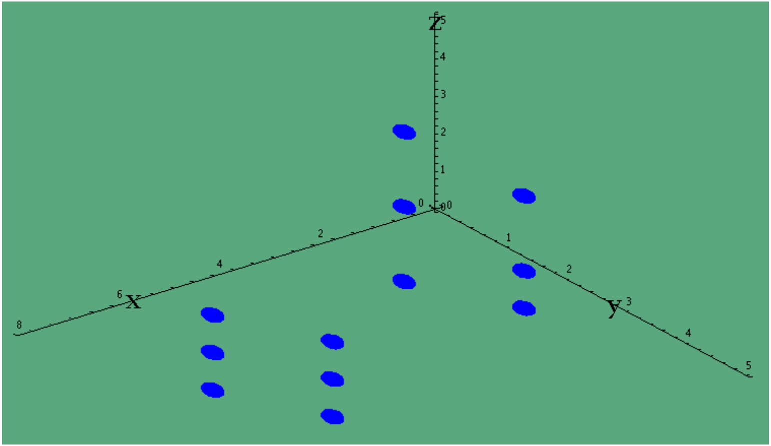
Proposition

Let $V(F) \subset A^n(\overline{\mathbb{K}})$ *be finite with* $F \subset \mathbb{K}[x_1, \ldots, x_n]$. *There exist Lazard triangular sets* $T^1, \ldots, T^s \subset \mathbb{K}[x_1, \ldots, x_n]$ *such that*

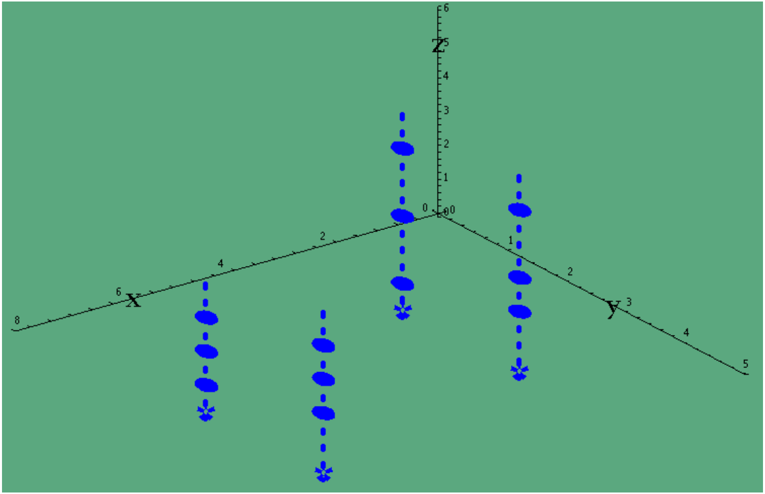
$$V(F) = V(T^1) \cup \cdots \cup V(T^s) \;\; \text{and} \;\; i \neq j \;\Rightarrow\; V(T^i) \cap V(T^j) = \varnothing.$$

They form a **triangular decomposition** of $V(F)$.

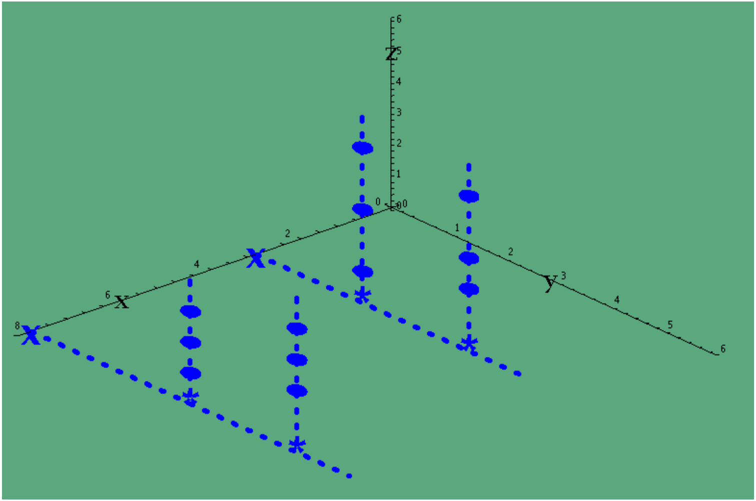
Equiprojectable variety definition (1/3)

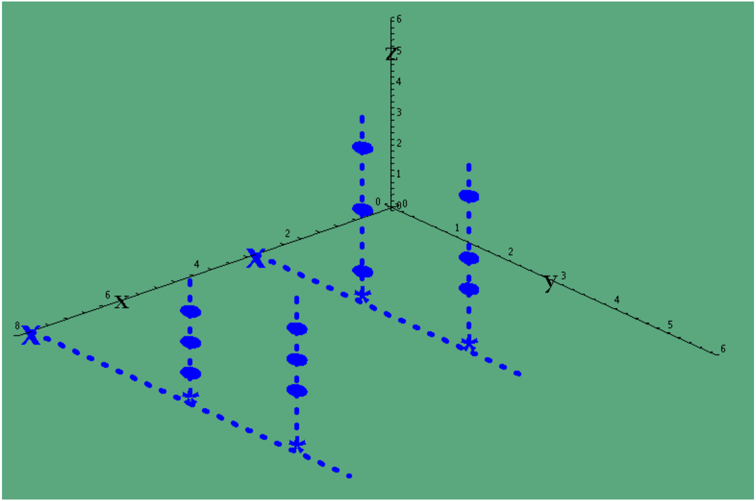


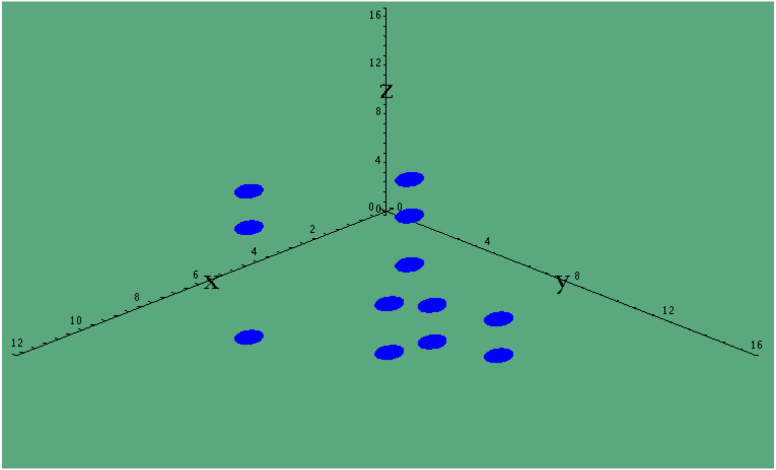
Equiprojectable variety definition (2/3)



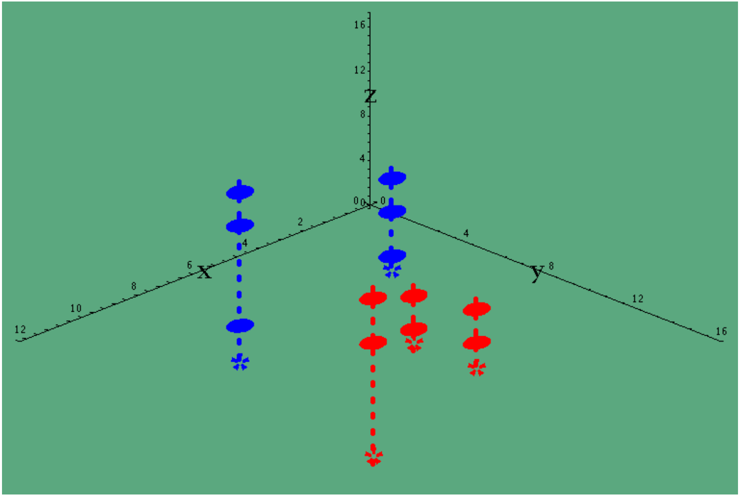
Equiprojectable variety definition (3/3)



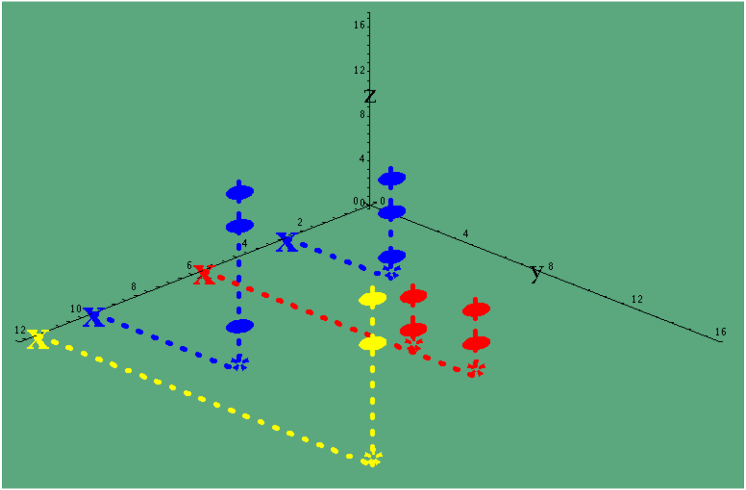

Z
X
Y
6
5
4
3
2
1
0
0
0
2
4
6
8
1
2
3
4
5
6



16
12
z
8
4
0
0
0
2
4
6
x
8
10
12
4
y
8
12
16



z
x
y
16
12
8
4
0
2
4
6
8
10
12
4
8
12
16



16
12
z
8
4
0
0
0
2
4
6
8
10
12
x
x
x
x
y
4
8
12
16

Generalizing Lazard triangular sets

Remark

Let $T = \{T_1, \ldots, T_n\} \subset \mathbb{K}[x_1, \ldots, x_n]$ *be a Lazard triangular set. Let* $\mathcal{I} := \langle T \rangle$. *We have shown that given* $p \in \mathbb{K}[x_1, \ldots, x_n]$,

- *one can decide whether* $p \in \mathcal{I}$. *Indeed* T *is a Gröbner basis of* $\mathcal{I}$.
- *assuming* $\mathcal{I}$ *radical, one can decide whether* $p^{-1} \mod \mathcal{I}$ *exists. Indeed* $\mathbb{K}[x_1, \ldots, x_n]/\mathcal{I}$ *is a DPF.*

We aim at:

- *first, relaxing the hypothesis* $\mathrm{lc}(T_i, x_i) = 1$, *for all* $1 \le i \le n$,
- *second, relaxing the* **as many polynomials as variables** *constraint.*

while preserving a **triangular shape** *together with the above* **algorithmic properties**.

Zero-dimensional regular chains

Definition

A subset $C = \{C_1, \ldots, C_n\} \subset \mathbb{K}[x_1 < \cdots < x_n]$ is a **zero-dimensional regular chain** if for all $i = 1 \cdots n$ we have

(1) $C_i \in \mathbb{K}[x_1, \ldots, x_i]$,
(2) $\deg(C_i, x_i) > 0$,
(3) $h_i := \mathrm{lc}(C_i, x_i)$ is **invertible** modulo the ideal $\langle C_1, \ldots, C_{i-1} \rangle$.

Proposition

Let $C \subset \mathbb{K}[x_1, \ldots, x_i]$ be a **zero-dimensional regular chain**. *There exists a Lazard triangular set $T \subset \mathbb{K}[x_1, \ldots, x_i]$ such that $\langle C \rangle = \langle T \rangle$.*

Proof.

By induction on n.

- For $n = 1$ we have $T_1 = \mathrm{lc}(C_1)^{-1} C_1$ and the claim follows clearly.
- For $n > 1$ we compute $\tilde{h}_n$ the inverse of h_n modulo $\langle T_1, \ldots, T_{n-1} \rangle$ and observe

$$\langle T_1, \ldots, T_{n-1}, \tilde{h}_n C_n \rangle = \langle T_1, \ldots, T_{n-1}, C_n \rangle.$$

□

The Dahan-Schost Transform (I)

Proposition

Consider $T = \{T_1, \ldots, T_n\}$ a Lazard triangular set. Assume T generates a radical ideal. Let $D_1 = 1$ and $N_1 = T_1$. For $2 \leq \ell \leq n$, define

$$\begin{array}{rcl} D_\ell & = & \prod_{1 \leq i \leq \ell-1} \frac{\partial T_i}{\partial x_i} \mod \langle T_1, \ldots, T_{\ell-1} \rangle \\ N_\ell & = & D_\ell T_\ell \mod \langle T_1, \ldots, T_{\ell-1} \rangle \end{array}$$

Then $N = \{N_1, \ldots, N_n\}$ is a zero-dimensional regular chain with $\langle T \rangle = \langle N \rangle$.

Remark

The results of **(Dahan & Schost, 2004)** *"essentially" show that the height (or "size") of each coefficient in N is upper bounded by*

- *the height of $\mathbf{V}(T)$ if $\mathbb{K} = \mathbb{Q}$, that is the minimum size of a data set encoding $\mathbf{V}(T)$,*
- *the degree of $\mathbf{V}(T^{\downarrow})$ if $\mathbb{K}$ is a field $k(t_1, \ldots, t_m)$ of rational functions and $T^{\downarrow}$ is T regarded in $k[t_1, \ldots, t_m, x_1, \ldots, x_n]$.*

See the authors' article for precise statements.

The Dahan-Schost Transform (II)

- Consider the system F (Barry Trager).

$$-x^5 + y^5 - 3y - 1 = 5y^4 - 3 = -20x + y - z = 0$$

We solve it for $z < y < x$.

- $V(F)$ is equiprojectable and its Lazard triangular set is
  - [illegible]
  - [illegible]
  - $3125z^{20} - 9375z^{16} - 40000000000z^{15} - 2015999988750z^{12} - 1560000000000z^{11} + 1920000000000000000z^{10} - 12165125356800006750z^8 - 14745602232000000000z^7 - 6528000000000000000z^6 - 4096000000000000000000z^5 - 16986908639233347839997975z^4 - 14155767152640302400000000z^3 - 5898238732800000000000000z^2 - 12288000000000000000000000z - 6195303619231982878732441600243$
- Applying the transformation of Dahan and Schost leads to 1787 characters.
  - $(20z^{19} + (-48z^{15}) + (-192000000z^{14}) + (-(38707199784/5)z^{11}) + (-5491200000z^{10}) + 614400000000000z^9 + (-(778568022835200432/25)z^7) + (-330301489996800000z^6) + (-12533760000000000z^5) + (-6553600000000000000000z^4) + (-(2717905382277335654399676/125)z^3) + (-13589536466534690304000z^2) + (-377487278899200000000z) - 39321600000000000000)x + 3200000z^{15} + 161280000z^{12} + 124800000z^{11} + (-30720000000000z^{10}) + 1946419628544000z^8 + 2359296178560000z^7 + 1044480000000000z^6 + 98304000000000000000z^5 + 4076859878277227827200z^4 + 3397384824422424192000z^3 + 1415577397248000000000z^2 + 294912000000000000000z + 1982496995079656780596195328$
  - $(20z^{19} + (-48z^{15}) + (-192000000z^{14}) + (-(38707199784/5)z^{11}) + (-5491200000z^{10}) + 614400000000000z^9 + (-(778568022835200432/25)z^7) + (-330301489996800000z^6) + (-12533760000000000z^5) + (-6553600000000000000000z^4) + (-(2717905382277335654399676/125)z^3) + (-13589536466534690304000z^2) + (-377487278899200000000z) - 39321600000000000000)y + (-12z^16) + (-(9676799856/5)z^{12}) + (-1996800000z^{11}) + (-(194642219980800648/25)z^8) + (-14155781713920000z^7) + (-8355840000000000z^6) + (-(679471833416273049598704/125)z^4) + (-9059676821914761216000z^3) + (-566230715596800000000z^2) + (-157286400000000000000z) + (-2038432221757477324800972/625)$
  - $z^20 + (-3z^16) + (-12800000z^{15}) + (-(3225599982/5)z^{12}) + (-499200000z^{11}) + 614400000000000z^{10} + (-(97321002854400054/25)z^8) + (-4718592714240000z^7) + (-2088960000000000z^6) + (-1310720000000000000000z^5) + (-(679476345569333913599919/125)z^4) + (-4529845488844896768000z^3) + (-188743639449600000000z^2) + (-39321600000000000000z) + (-6195303619231982878732441600243/3125)$
- One can do better! Here's the regular chain produced by the `Triangularize` algorithm of the `RegularChains` library, counting 963 characters.
  - $20x - 1y + z$
  - $\left((4375z^{12} + 52800011625z^8 + 32000000000z^7 + 110591902080002925z^4 + 61439980800000000z^3 + 12800000000000000z^2 + 56623117271041036800027\right)y - 1875z^{13} - 9600010125z^9 + 2000000000z^8 - 7372714752004545z^5 + 30720002400000000z^4 + 12800000000000000z^3 - 22118403456000135z + 23592963686400144000000$
  - $3125z^{20} - 9375z^{16} - 40000000000z^{15} - 2015999988750z^{12} - 1560000000000z^{11} + 1920000000000000000z^{10} - 12165125356800006750z^8 - 14745602232000000000z^7 - 6528000000000000000z^6 - 4096000000000000000000z^5 - 16986908639233347839997975z^4 - 14155767152640302400000000z^3 - 5898238732800000000000000z^2 - 12288000000000000000000000z - 6195303619231982878732441600243$

Plan

- Throughout this section, we consider a commutative ring $\mathbb{A}$ with identity element, a symbol x and the ring $\mathbb{A}[x]$ of the univariate polynomials in x with coefficients in $\mathbb{A}$.
- Let $a, b \in A[x]$ be univariate polynomials such that b has a positive degree w.r.t. x.

Definition

We say that a polynomial $q \in \mathbb{A}[x]$ (resp. $r \in \mathbb{A}[x]$) is a *pseudo-quotient* (resp. *pseudo-remainder*) of a by b if there exists a non-negative integer e and a polynomial $r \in \mathbb{A}[x]$ (resp. $q \in \mathbb{A}[x]$) such that we have

$$\mathrm{lc}(b)^e a = qb + r \quad \text{and} \quad (r = 0 \quad \text{or} \quad \deg(r) < \deg(b)). \tag{2}$$

Proposition

Assuume that the leading coefficient of is regular. We define $e = \min(0, \deg(a) - \deg(b) + 1)$. *Then there exists a unique couple* (q, r) *of polynomials in* $\mathbb{A}[x]$ *such that* q *and* r *are a pseudo-quotient and a pseudo-remainder of* a *by* b. *The polynomial* q *(resp.* r*) is called the* the pseudo-quotient (the pseudo-remainder) *of* a *by* b *and denoted by* $\mathrm{prem}(a, b)$ $(\mathrm{pquo}(a, b))$. *The map* $(a, b) \longmapsto (q, r)$ *is called the* pseudo-division *of* a *by* b. *In addition, the following algorithm computes this couple.*

Input: $a, b \in \mathbb{A}[x]$ with $b \notin \mathbb{A}$.

Output: $q, r \in \mathbb{A}[x]$ satisfying Relation (2) with
$e = \min(0, \deg(a) - \deg(b) + 1)$.

$r := a$
$q := 0$
$e := \max(0, \deg(a) - \deg(b) + 1)$
while $r \neq 0$ **or** $\deg(r) \geq \deg(b)$ **repeat**
  $d := \deg(r) - \deg(b)$
  $t := \mathrm{lc}(r) y^d$
  $q := \mathrm{lc}(b) q + t$
  $r := \mathrm{lc}(b) r - tb$
  $e := e - 1$
$r := \mathrm{lc}(b)^e r$
$q := \mathrm{lc}(b)^e q$
return (q, r)

Proposition

Let $\mathcal{I}$ be an ideal of $\mathbb{A}$ and $d \in \mathbb{A}$ a regular element. Let $a, b, q, r \in \mathbb{A}[x]$ be univariate polynomials such that the following properties are satisfied:

(*i*) *b has a positive degree w.r.t. y and $\mathrm{lc}(b)$ is not a zero-divisor in $\mathbb{A}$,*

(*ii*) *q and r are the pseudo-quotient and pseudo-remainder of a w.r.t. b in $\mathbb{A}[x]$,*

(*iii*) *$a \in \mathcal{I}[x]$ holds,*

Them we have:

$$q \in \mathcal{I}[x] \quad \text{and} \quad r \in \mathcal{I}[x].$$

Resultant (recall 1/2)

Let $P, Q \in \mathbb{A}[x]$ be two non-zero polynomials of respective degrees m and n such that $n, m > 0$. Suppose that

$$P = a_m x^m + \cdots + a_1 x + a_0 \quad \text{and} \quad Q = b_n x^n + \cdots + b_1 x + b_0.$$

The Sylvester matrix of P and Q is the square matrix of order $n+m$ with coefficients in R, denoted by $\mathrm{sylv}(P,Q,x)$ and defined by

$$\mathrm{sylv}(P,Q,x) = \begin{bmatrix} a_m & & & & b_n & & & & \\ a_{m-1} & a_m & & & b_{n-1} & b_n & & & \\ \vdots & \vdots & \ddots & & \vdots & \vdots & \ddots & & \\ \vdots & \vdots & & a_m & b_1 & \vdots & & \ddots & \\ \vdots & \vdots & & a_{m-1} & b_0 & \vdots & & & \ddots \\ \vdots & \vdots & & \vdots & & b_0 & & & b_n \\ a_0 & \vdots & & \vdots & & & \ddots & & b_{n-1} \\ & a_0 & & \vdots & & & & \ddots & \vdots \\ & & \ddots & \vdots & & & & \ddots & \vdots \\ & & & a_0 & & & & & b_0 \end{bmatrix}$$

whose determinant, denoted by $\mathrm{res}(P,Q,x)$, is the resultant of P and Q.

Resultant (recall 2/2)

Proposition

If $\mathbb{A}$ *is a unique factorization domain (UFD), then* $\gcd(P, Q)$ *is nonconstant in* $\mathbb{A}[x]$ *if and only if* $\mathrm{res}(P, Q, x) = 0$ *in* $\mathbb{A}$*.*

Example

Let $P = ax^2 + bx + c$ and let $Q = 2ax + b$ be the derivative of P w.r.t x. Then the Sylvester matrix of P and Q w.r.t x is

$$S = \begin{bmatrix} a & 2a & 0 \\ b & b & 2a \\ c & 0 & b \end{bmatrix}$$

whose determinant is $\det(S) = a(4ac - b^2)$. Whenever $a \neq 0$, P and Q have a common solution (or equivalently, $P = 0$ has a solution of multiplicity 2) if and only if the resultant $\mathrm{res}(P, Q, x)$ is zero.

Definition (Determinantal polynomial)

Let $m \leq n$ be positive integers. Let M be a $m \times n$ matrix with coefficients in $\mathbb{A}$. Let M_i be the square submatrix of M consisting of the first $m-1$ columns of M and the i-th column of M, for $i = m \cdots n$; let $\det M_i$ be the determinant of M_i. The *determinantal polynomial* of M, denote by $\mathrm{dpol}(M)$, is a polynomial in $\mathbb{A}[x]$, given by

$$\mathrm{dpol}(M) = \det M_m x^{n-m} + \det M_{m+1} x^{n-m-1} + \cdots + \det M_n.$$

If $\mathrm{dpol}(M)$ is not zero then its degree is at most $n-m$.

Notation

Let $P_1, \ldots, P_m$ be polynomials of $\mathbb{A}[x]$ of degree less than n. We denote by $\mathrm{mat}(P_1, \ldots, P_m)$ the $m \times n$ matrix whose i-th row contains the coefficients of P_i, sorting in order of decreasing degree, and such that P_i is treated as a polynomial of degree $n-1$. We denote by $\mathrm{dpol}(P_1, \ldots, P_m)$ the determinantal polynomial of $\mathrm{mat}(P_1, \ldots, P_m)$.

Example

Let $n = 4$, $m = 2$, $P_1 = a_3x^3 + a_2x^2 + a_1x + a_0$ and $P_2 = b_2x^2 + b_1x + b_0$. Then

$$\mathrm{mat}(P_1, P_2) = \begin{bmatrix} a_3 & a_2 & a_1 & a_0 \\ 0 & b_2 & b_1 & b_0 \end{bmatrix},$$

with

$$M_2 = \begin{bmatrix} a_3 & a_2 \\ 0 & b_2 \end{bmatrix}, M_3 = \begin{bmatrix} a_3 & a_1 \\ 0 & b_1 \end{bmatrix}, \text{ and } M_4 = \begin{bmatrix} a_3 & a_0 \\ 0 & b_0 \end{bmatrix}.$$

Consequently, we have $\mathrm{dpol}(P_1, P_2) = a_3b_2x^2 + a_3b_1x + a_3b_0$.

The notion of *subresultants* is a refinement of that of resultant. To define subresultants of two polynomials we need the following definition.

Definition

Let $P, Q \in \mathbb{A}[x]$ be non-constant polynomials of respective degrees m, n with $m \leq n$. Let k be an integer with $0 \leq k < m$. Then the k-th *subresultant* of P and Q, denoted by $S_k(P, Q)$, is

$$S_k(P, Q) = \mathrm{dpol}(x^{n-k-1}P, x^{n-k-2}P, \ldots, P, x^{m-k-1}Q, \ldots, Q).$$

- Observe that if $S_k(P, Q)$ is not zero then its degree is at most k. Indeed the underlying matrix has $m + n - 2k$ rows and $m + n - k$ columns. Nence $S_k(P, Q)$ has $(m + n - k) - (m + n - 2k) + 1 = k + 1$ terms.
- When $S_k(P, Q)$ has degree k, then it is said *regular*; when $S_k(P, Q) \neq 0$ and $\deg(S_k(P, Q)) < d$, $S_k(P, Q)$ is said *defective*.

It is easy to show that $S_0(P, Q)$ is $\mathrm{res}(\mathrm{P, Q, x})$, the resultant of P and Q.

Example

Let $P = b_2x^2 + b_1x + b_0$ and $Q = a_3x^3 + a_2x^2 + a_1x + a_0$. Then

$$S_0(P,Q) = \mathrm{dpol}(x^2P, xP, P, xQ, Q) = \mathrm{dpol}(\begin{bmatrix} b_2 & b_1 & b_0 & & \\ & b_2 & b_1 & b_0 & \\ & & b_2 & b_1 & b_0 \\ a_3 & a_2 & a_1 & a_0 & \\ & a_3 & a_2 & a_1 & a_0 \end{bmatrix})$$

$$= b_2a_2^2b_0^2 - 2b_2^2a_2b_0a_0 - a_2b_0^2a_3b_1 + b_2^3a_0^2 + 3b_2a_0a_3b_1b_0 - b_1b_2a_1a_2b_0 - b_1b_2^2a_1a_0 + b_1^2a_1a_3b_0 + b_2a_2b_1^2a_0 - a_3b_1^3a_0 + b_0b_2^2a_1^2 - 2b_2a_1a_3b_0^2 + a_3^2b_0^3$$

and

$$S_1(P,Q) = \mathrm{dpol}(xP, P, Q) = \mathrm{dpol}(\begin{bmatrix} b_2 & b_1 & b_0 & \\ & b_2 & b_1 & b_0 \\ a_3 & a_2 & a_1 & a_0 \end{bmatrix})$$

$$= (b_2^2a_1 - b_2a_3b_0 - b_2a_2b_1 + a_3b_1^2)\,x - b_2a_2b_0 + b_2^2a_0 + a_3b_1b_0.$$

In particular, when $P = x(x-3) = x^2 - 3x$ and $Q = x(x-1)(x+1) = x^3 - x^2$, we have $S_0(P,Q) = 0$ and $S_1(P,Q) = 6x$, which in fact reflects $\gcd(P,Q) = x$.

Proposition

Assume $\mathbb{A}$ *is a UFD and let* P, Q *be polynomials in* $\mathbb{A}[x]$ *with degrees* m *and* n. *If for some* $0 < k < \min(m, n)$, *we have* $S_k(P, Q) \neq 0$ *and* $S_i(P, Q) = 0$ *for all* $i < k$, *then* $\deg(\gcd(P, Q)) = k$ *holds.*
In fact, $S_k(P, Q)$ *is similar to* $\gcd(P, Q)$ *in the sense that there exist nonzero constants* α *and* β *in* $\mathbb{A}$ *such that* $\alpha \gcd(P, Q) = \beta\, S_k(P, Q)$ *holds.*

According to the above proposition, S_k is a regular subresultant, and we usually call it the *last nonzero subresultant* of P, Q.

Plan

Zero-dimensional regular chains

Pseudo-division, subresultants and division-free Euclidean algorithms

Division-free Euclidean algorithms

Computing regular GCDs

Regular chains in arbitrary dimension

Incremental solving

Notations

We review the previous notions with a couple variable renaming.

- Let $\mathbb{B}$ be another commutative ring with identity and let $m \leq n$ be positive integers.
- Let $P, Q \in \mathbb{B}[y]$ be non-constant polynomials of respective degrees p, q with $q \leq p$. Let d be an integer with $0 \leq d < q$.
- Then the d-th *subresultant* of P and Q, denoted by $S_d(P, Q)$, is

$$S_d(P, Q) = \mathrm{dpol}(y^{q-d-1}P, y^{q-d-2}P, \ldots, P, y^{p-d-1}Q, \ldots, Q).$$

- For convenience, we extend the definition to the q-th subresultant as follows:

$$S_q(P, Q) = \begin{cases} \gamma(Q)Q, & \text{if } p \geq q \text{ and } \mathrm{lc}(Q) \in \mathbb{B} \text{ is regular} \\ \text{undefined}, & \textit{otherwise} \end{cases}$$

  where $\gamma(Q) = \mathrm{lc}(Q)^{p-q-1}$. Note that when p equals q, then $S_q(P, Q) = \mathrm{lc}(Q)^{-1}Q$ is in fact a polynomial over the total fraction ring of $\mathbb{B}$.

We call *specialization property of subresultants* the following statement.

Proposition

Let $\mathbb{A}$ be another commutative ring with identity and Ψ a ring homomorphism from $\mathbb{B}$ to $\mathbb{A}$ such that $\Psi(\mathrm{lc}(P)) \neq 0$ and $\Psi(\mathrm{lc}(Q)) \neq 0$. Then

$$S_d(\Psi(P), \Psi(Q)) = \Psi(S_d(P, Q)).$$

This property will play a central role later.

Divisibility relations of subresultants: integral domain case

Subresultants $S_{q-1}(P,Q)$, $S_{q-2}(P,Q)$, ..., $S_0(P,Q)$ satisfy relations which induce an Euclidean-like algorithm for computing them.

Following (Ducos, 1998) we first assume that $\mathbb{B}$ is an integral domain. For convenience, we simply write S_d instead of $S_d(P,Q)$ for each d. We write $A \sim B$ for $A, B \in \mathbb{B}[y]$ whenever they are associates over $\mathrm{Fr}(\mathbb{B})$ (the field of fractions of $\mathbb{B}$) that is, equal up to a non-zero element of $\mathrm{Fr}(\mathbb{B})$. Then for $d = q-1, \dots, 1$, we have:

(r_{q-1}) $S_{q-1} = \mathrm{prem}(P, -Q)$, the pseudo-remainder of P by $-Q$,

$(r_{<q-1})$ if $S_{q-1} \neq 0$, with $e = \deg(S_{q-1})$, then the following holds:

$$\mathrm{prem}(Q, -S_{q-1}) = \mathrm{lc}(Q)^{(p-q)(q-e)+1} S_{e-1},$$

(r_e) if $S_{d-1} \neq 0$, with $e = \deg(S_{d-1}) < d-1$, thus S_{d-1} is defective, then we have

(1) $\deg(S_d) = d$, thus S_d is non-defective,

(2) $S_{d-1} \sim S_e$ and $\mathrm{lc}(S_{d-1})^{d-e-1} S_{d-1} = {s_d}^{d-e-1} S_e$, thus S_e is non-defective,

(3) $S_{d-2} = S_{d-3} = \cdots = S_{e+1} = 0$,

(r_{e-1}) if both S_d and S_{d-1} are nonzero, with respective degrees d and e then we have $\mathrm{prem}(S_d, -S_{d-1}) = \mathrm{lc}(S_d)^{d-e+1} S_{e-1}$.

Convention. If $p = \deg(P) \geq \deg(Q) = q$, then $S_q = \mathrm{lc}(Q)^{p-q-1} Q$ where lc is the leading coefficient. Of course, if $p = q$, the coefficients of S_q belong to $\mathrm{Frac}(R)$, but the leading coefficient $s_q = \mathrm{lc}(Q)^{p-q}$ always belongs to R.

Subresultant algorithm. (see [2, 3, 8] or [12])
Inputs: $P, Q \in R[X]$ $\quad \deg(P) \geq \deg(Q) \geq 1$
Output: List of non-zero subresultants of P and Q

$S \leftarrow$ empty list
$s \leftarrow \mathrm{lc}(Q)^{\deg(P)-\deg(Q)}$
$A \leftarrow Q; B \leftarrow \mathrm{prem}(P, -Q)$
loop
    $d \leftarrow \deg(A); e \leftarrow \deg(B)$
    — here, $A \sim S_d$ if $d = \deg(Q)$ —
    — here, $A = S_d$ if $d < \deg(Q)$ —
    — here, $B = S_{d-1}, s = \mathrm{lc}(S_d)$ for $d \leq \deg(Q)$ —
    if $B = 0$ then return S
    $S \leftarrow [B] \cup S$
    — here, $S = [S_{d-1}, S_d, \ldots]$ —
    $\delta \leftarrow d - e$
    if $\delta > 1$ then $C \leftarrow \dfrac{\mathrm{lc}(B)^{\delta-1} B}{s^{\delta-1}}; S \leftarrow [C] \cup S$
    else $C \leftarrow B$
    — here, $C = S_e, S = [S_e, \ldots]$ —
    if $e = 0$ then return S
    $B \leftarrow \dfrac{\mathrm{prem}(A, -B)}{s^{\delta} \mathrm{lc}(A)}$
    — here, $B = S_{e-1}$ —
    $A \leftarrow C$
    $s \leftarrow \mathrm{lc}(A)$
end loop

Divisibility relations of subresultants: non-integral domain case

We consider now the case where $\mathbb{B}$ is an arbitrary commutative ring, following Theorem 4.3 in (El Kahoui, 2003). If S_d, S_{d-1} are nonzero, with respective degrees d and e and if s_d is regular in $\mathbb{B}$ then we have

$$\mathrm{lc}(S_{d-1})^{d-e-1} S_{d-1} = s_d{}^{d-e-1} S_e.$$

Moreover, there exists $C_d \in \mathbb{B}[y]$ such that

$$(-1)^{d-1}\,\mathrm{lc}(S_{d-1}) s_e S_d + C_d S_{d-1} = \mathrm{lc}(S_d)^2 S_{e-1}.$$

In addition $S_{d-2} = S_{d-3} = \cdots = S_{e+1} = 0$ also holds.
From these formula we derive the following observation to which we will refer as the *block structure of subresultants*.

Proposition

Let S_i, S_j, S_k be three non-zero subresultants with indices $q \geq i > j > k \geq 0$. Assume that for all $\ell = i-1, \ldots, j+1, j-1, \ldots, k+1$ we have $S_\ell = 0$. Assume that S_j is defective. Then S_i is non-defective and we have $j = i-1$. Moreover S_k is non-defective and we have $S_j \sim S_k$. Observe also that the non-zero subresultant S_d of smallest index d, sometimes called the last subresultant *of P and Q and denoted by* $\mathrm{lsr}(P,Q)$, *is a non-defective subresultant.*

Plan

Regular GCD (recall)

- Let $\mathbb{B}$ again be a commutative ring with units. Let $P, Q \in \mathbb{B}[y]$ be non-constant with regular leading coefficients.
- We say that $G \in \mathbb{B}[y]$ is a *r egular GCD* of P, Q if we have:
  - (i) $\mathrm{lc}(G, y)$ is a regular element of $\mathbb{B}$,
  - (ii) $G \in \langle P, Q \rangle$ in $\mathbb{B}[y]$,
  - (iii) $\deg(G, y) > 0 \;\Rightarrow\; \mathrm{prem}(P, G, y) = \mathrm{prem}(Q, G, y) = 0$.
- In practice $\mathbb{B} = \mathbb{K}[x_1, \ldots, x_n]/\mathrm{Sat}(T)$, with T being a regular chain.
- Such a regular GCD may not exist. However, we shall see that one can compute $\mathcal{I}_i = \mathrm{Sat}(T_i)$ and non-zero polynomials G_i such that

$$\sqrt{\mathcal{I}} = \cap_{i=0}^{e} \sqrt{\mathcal{I}_i} \quad \text{and} \quad G_i \quad \text{regular GCD of} \quad P, Q \bmod \mathcal{I}_i$$

Regularity test

- R egularity test is a fundamental operation:

$$\text{Regularize}(p, \mathcal{I}) \quad \longmapsto \quad (\mathcal{I}_1, \ldots, \mathcal{I}_e)$$

  such that:

$$\sqrt{\mathcal{I}} = \cap_{i=0}^{e} \sqrt{\mathcal{I}_i} \quad \text{and} \quad p \in \mathcal{I}_i \text{ or } p \text{ regular modulo } \mathcal{I}_i$$

- Regularity test reduces to r egular GCD computation.

Regular GCDs (1/6)

- Let $P, Q \in \mathbb{K}[\mathbf{x}][\mathbf{y}]$ with $\mathrm{mvar}(P) = \mathrm{mvar}(Q) = y$.
- Define $R = \mathrm{res}(P, Q, y)$.
- Let $T \subset \mathbb{K}[x_1, \ldots, x_n]$ be a regular chain such that
  - $R \in \mathrm{Sat}(T)$,
  - $\mathrm{init}(P)$ and $\mathrm{init}(Q)$ are regular modulo $\mathrm{Sat}(T)$.
- $\mathbb{A} = \mathbb{K}[x_1, \ldots, x_n]$ and $\mathbb{B} = \mathbb{K}[x_1, \ldots, x_n]/\mathrm{Sat}(T)$.
- For $0 \le j \le \mathrm{mdeg}(Q)$, we write S_j for the j-th subresultant of P, Q in $\mathbb{A}[y]$.

Regular GCDs (2/6)

- Let $1 \leq d \leq q$ such that $S_j \in \mathrm{Sat}(T)$ for all $0 \leq j < d$.

Proposition

If $\mathrm{lc}\, S_d, y$ *is regular modulo* $\mathrm{Sat}(T)$, *then* S_d *is non-defective over* $\mathbb{K}[\mathbf{x}]$.

- Consequently, S_d is the last nonzero subresultant over $\mathbb{B}$, and it is also non-defective over $\mathbb{B}$.
- If $\mathrm{lc}(S_d, x_n)$ is not regular modulo $\mathrm{Sat}(T)$ then S_d may be defective over $\mathbb{B}$.

Regular GCDs (3/6)

- Let $1 \le d \le q$ such that $S_j \in \mathrm{Sat}(T)$ for all $0 \le j < d$.

Proposition

If $\mathrm{lc}\, S_d, y$ *is in* $\mathrm{Sat}(T)$*, then* S_d *is nilpotent modulo* $\mathrm{Sat}(T)$*.*

- Up to sufficient splitting of $\mathrm{Sat}(T)$, S_d will vanish on all the components of $\mathrm{Sat}(T)$.
- The above two lemmas completely characterize the last non-zero subresultant of P and Q over $\mathbb{B}$.

Regular GCDs (4/6)

Example

- Consider P and Q in $\mathbb{Q}[x_1, x_2][y]$:

$$P = x_2^2 y^2 - x_1^4 \quad \text{and} \quad Q = x_1^2 y^2 - x_2^4.$$

- We have:

$$S_1 = x_1^6 - x_2^6 \quad \text{and} \quad R = (x_1^6 - x_2^6)^2.$$

- Let $T = \{R\}$. Then we observe:
  - The last subresultant of P, Q modulo $\mathrm{Sat}(T)$ is S_1, which is a defective one.
  - S_1 is nilpotent modulo $\mathrm{Sat}(T)$.
- P and Q do not admit a regular GCD over $\mathbb{Q}[x_1, x_2]/\mathrm{Sat}(T)$.

Regular GCDs (5/6)

- Let $1 \leq d \leq q$ such that $S_j \in \mathrm{Sat}(T)$ for all $0 \leq j < d$.

Proposition

Assume

- $\mathrm{lc} S_d, y$ *is regular modulo* $\mathrm{Sat}(T)$*,*
- $\mathrm{Sat}(T)$ *is radical.*

Then, S_d *is a regular GCD of* P, Q *modulo* $\mathrm{Sat}(T)$*.*

Regular GCDs (5/6)

- Let $1 \leq d \leq q$ such that $S_j \in \mathrm{Sat}(T)$ for all $0 \leq j < d$.

Proposition

Assume

- $\mathrm{lc} S_d, y$ *is regular modulo* $\mathrm{Sat}(T)$*,*
- $\mathrm{Sat}(T)$ *is radical.*

Then, S_d *is a regular GCD of* P, Q *modulo* $\mathrm{Sat}(T)$*.*

Recall that S_d regular GCD of P, Q modulo $\mathrm{Sat}(T)$ means

(*i*) $\mathrm{lc}(S_d, y)$ is a regular element of $\mathbb{B}$,

(*ii*) $S_d \in \langle P, Q \rangle$ in $\mathbb{B}[y]$,

(*iii*) $\deg(S_d, y) > 0 \quad \Rightarrow \quad \mathrm{prem}(P, S_d, y) = \mathrm{prem}(Q, S_d, y) = 0$.

Regular GCDs (5/6)

- Let $1 \leq d \leq q$ such that $S_j \in \mathrm{Sat}(T)$ for all $0 \leq j < d$.

Proposition

Assume

- $\mathrm{lc}S_d, y$ *is regular modulo* $\mathrm{Sat}(T)$,
- $\mathrm{Sat}(T)$ *is radical.*

Then, S_d *is a regular GCD of* P, Q *modulo* $\mathrm{Sat}(T)$.

Proposition

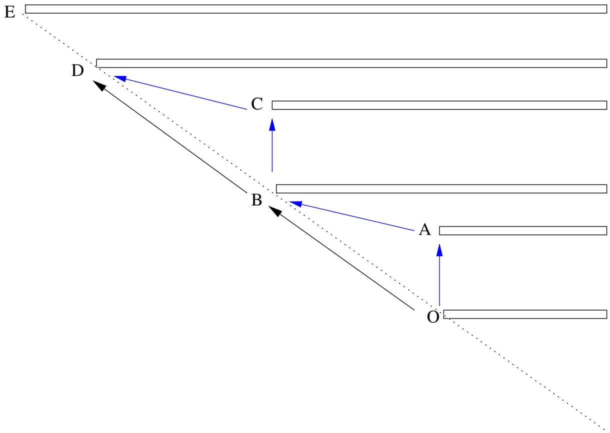
Assume

- $\mathrm{lc}S_d, y$ *is regular modulo* $\mathrm{Sat}(T)$,
- *for all* $d < k \leq q$, $\mathrm{coeff}(S_k, y^k)$ *is either* 0 *or regular modulo* $\mathrm{Sat}(T)$.

Then, S_d *is a regular GCD of* P, Q *modulo* $\mathrm{Sat}(T)$.

Regular GCDs (6/6)

- Assume that the subresultants S_j for $1 \leq j < q$ are computed.
- Then one can compute a regular GCD of P, Q modulo $\mathrm{Sat}(T)$ by performing a bottom-up search.



Plan

Triangular sets and auto-reduced sets

Definition

A subset $B \subset \mathbb{K}[X] \setminus \mathbb{K}$ is

- a **triangular set** if for all $f, g \in B$ we have $f \neq g \;\Rightarrow\; \mathrm{mvar}(f) \neq \mathrm{mvar}(g)$,
- **auto-(pseudo-)reduced** if all $b \in B$ is pseudo-reduced w.r.t. $B \setminus \{b\}$.

Proposition

Every auto-reduced set is finite and is a triangular set.

Notation

Let $f \in \mathbb{K}[X]$ and $B \subset \mathbb{K}[X] \setminus \mathbb{K}$ an auto-reduced set. If $B = \varnothing$ we write $\mathrm{prem}(f, B) = f$. Otherwise let $b \in B$ with largest main variable; we write $\mathrm{prem}(f, B) = \mathrm{prem}(\mathrm{prem}(f, b), B \setminus \{b\})$. For $A \subset \mathbb{K}[X]$ write $\mathrm{prem}(A, B) = \{\mathrm{prem}(a, B) \mid a \in A\}$.

Example

For instance, with $T_4 = \{x_1(x_1 - 1), x_1x_2 - 1\}$ and $p = x_2^2 + x_1x_2 + x_1^2$, we have

$$\mathrm{prem}(p, T) = \mathrm{prem}(\mathrm{prem}(p,\; T_{x_2}),\; T_{x_1}) = \mathrm{prem}(x_1^4 + x_1^2 + 1,\; T_{x_1}) = 2\; x_1 + 1.$$

where $T_{x_1} = x_1(x_1 - 1)$ and $T_{x_2} = x_1x_2 - 1$.

The saturated ideal of a triangular set (1/3)

Definition

Let $T \subset \mathbb{K}[X]$ be a triangular set. The set

$$\mathrm{Sat}(T) = \{f \in \mathbb{K}[X] \mid (\exists e \in \mathbb{N})\ h_T^e f \in \langle T \rangle\}$$

is the **saturated ideal** of T. (**Clearly** $\mathrm{Sat}(T)$ **is an ideal.**)

Proposition

Let $T \subset \mathbb{K}[X]$ be a triangular set and $f \in \mathbb{K}[X]$. We have

$$\mathrm{prem}(f, T) = 0 \ \Rightarrow\ f \in \mathrm{Sat}(T).$$

Remark

The **converse is false.** *Consider $n \geq 2$ and*

$$T = \{x_1(x_1 - 1), x_1 x_2 - 1\}.$$

Consider $p = (x_1 - 1)(x_1 x_2 - 1)$ and $q = -(x_1 - 1)x_1 x_2$. We have:

$$\mathrm{prem}(p, T) = \mathrm{prem}(q, T) = 0.$$

However, we have $p + q = 1 - x_1$, $\mathrm{prem}(p + q, T) \neq 0$ but $p + q \in \mathrm{Sat}(T)$, since $\mathrm{Sat}(T)$ is an ideal. Note that $\mathrm{Sat}(T) = \langle x_1 - 1, x_2 - 1 \rangle$.

The saturated ideal of a triangular set (2/3)

- Consider again for $x > y > a > b > c > d > e > f > g > h > i$

$$F = \begin{cases} ax + by - c \\ dx + ey - f \\ gx + hy - i \end{cases} \quad \text{and} \quad T = \begin{cases} gx + hy - i \\ (hd - eg)\, y - id + fg \\ (ie - fh)\, a + (ch - ib)\, d + (fb - ce)\, g \end{cases}$$

- Using Gröbner basis computations, one can check the following assertions for this example:
  - $\mathrm{Sat}(T) = \langle F \rangle$.
  - $\mathrm{Sat}(T)$ is an ideal stricly larger than $\langle T \rangle$.
  - In fact $\langle T \rangle \ \subset \ \mathrm{Sat}(T) \cap \langle g, h, i \rangle$,
  - and none of $\mathrm{Sat}(T)$ or $\langle g, h, i \rangle$ contains the other.

The quasi-component of a triangular set

Definition

Let $T \subset \mathbb{K}[X]$ be a **triangular set**. Let h_T be the product of the initials of T. The set $\boxed{W(T) = V(T) \setminus V(\{h_T\})}$ is the **quasi-component** of T.

Remark

Clearly $W(T)$ may not be variety. Consider $n = 2$ and $T = \{x_1 x_2\}$. We have $h_T = x_1$ and $W(T)$ is the line $x_2 = 0$ minus the point $(0,0)$.
Observe that $\mathrm{Sat}(T) = \langle x_2 \rangle$.

Proposition

For any **triangular set** $T \subset \mathbb{K}[X]$ *we have*

$$\overline{W(T)} = V(\mathrm{Sat}(T)).$$

Remark

Consider

$$T = \{x_2^2 - x_1, x_1 x_3^2 - 2x_2 x_3 + 1, (x_2 x_3 - 1)x_4 + x_2^2\}.$$

We have $W(T) = \varnothing = V(T)$.

Regular chains

Definition

Let $\mathcal{I}$ be a proper ideal of $\mathbb{K}[X]$. We say that a polynomial $p \in \mathbb{K}[X]$ is **regular** modulo $\mathcal{I}$ if for every prime ideal $\mathcal{P}$ associated with $\mathcal{I}$ we have $p \notin \mathcal{P}$, equivalently, this means that p is neither null modulo $\mathcal{I}$, nor a zero-divisor modulo $\mathcal{I}$.

Definition

Let $T = \{T_1, \ldots, T_s\}$ be a triangular set where polynomials are
sorted by increasing main variables.
The triangular set T is a **regular chain** if for all $i = 2 \cdots s$ the initial of T_i is **regular modulo the saturated ideal** of $T_1, \ldots T_{i-1}$.

Proposition

If T is a regular chain then $\mathrm{Sat}(T)$ is a proper ideal of $\mathbb{K}[X]$ and, thus, $W(T) \neq \varnothing$.

The saturated ideal of a triangular set (3/3)

Theorem

(Aubry, Lazard & M., 1997) *Let $C \subset \mathbb{K}[X]$ be an auto-(pseudo-)reduced set. Then, we have*

$$\begin{array}{c} \mathrm{Sat}(C) = \{p \mid \mathrm{prem}(p, C) = 0\} \\ \Updownarrow \\ C \ \ \text{regular chain} \end{array}$$

Reduction to dimension zero (1/2)

Theorem

(Chou & Gao, 1991), (Kalkbrener, 1991), (Aubry, 1999), (Boulier, Lemaire & M., 2006) *Let $T = \{T_{d+1}, \ldots, T_n\}$ be a triangular set. Assume that $\mathrm{mvar}(T_i) = x_i$ for all $d+1 \leq i \leq n$ and assume $\mathrm{Sat}(T)$ is a proper ideal of $\mathbb{K}[X]$. Then, every prime ideal $\mathcal{P}$ associated with $\mathrm{Sat}(T)$ has dimension d and satisfies*

$$\mathcal{P} \cap \mathbb{K}[x_1, \ldots, x_d] = \langle 0 \rangle.$$

Corollary

With T as above. Consider the localization by $\mathbb{K}[x_1, \ldots, x_d] \setminus \{0\}$; in other words, we map our polynomials from $\mathbb{K}[x_1, \ldots, x_n]$ to $\mathbb{K}(x_1, \ldots, x_d)[x_{d+1}, \ldots, x_n]$.
Let T_0 be the image of T. Let $p \in \mathbb{K}[x_1, \ldots, x_n]$ and p_0 its image in $\mathbb{K}(x_1, \ldots, x_d)[x_{d+1}, \ldots, x_n]$. Assume p non-zero modulo $\mathrm{Sat}(T)$. Then, the following conditions are equivalent:

(1) *p is regular w.r.t. $\mathrm{Sat}(T)$,*
(2) *p_0 is invertible w.r.t. $\mathrm{Sat}(T_0)$.*

In particular T is a regular chain iff T_0 is a (zero-dimensional) regular chain.

Reduction to dimension zero (2/2)

Remark

Consequently, we can generalize to positive dimension our computations of **polynomial GCDs** *defined previously over zero-dimensional regular chains. (Indeed, It is also possible to relax the condition* $\mathrm{Sat}(T_0)$ *radical.)*

Notation

Let T *is a regular chain and* $F \subset \mathbb{K}[X]$ *be a polynomial set. We denote by* $Z(F,T)$ *the intersection* $V(F) \cap W(T)$*, that is the set of the zeros of* F *that are contained in the quasi-component* $W(T)$*. If* $F = \{p\}$*, we write* $Z(p,T)$ *for* $Z(F,T)$*.*

Proposition

Let T *be a regular chain. If* p *is regular modulo* $\mathrm{Sat}(T)$*, then* $Z(p,T)$ *is either empty or it is contained in a variety of dimension strictly less than the dimension of* $\overline{W(T)}$*.*

Plan

Notations

- polynomial ring $R = \mathbb{K}[x_1 < \cdots < x_n]$
- polynomial $p \in R$
- $\mathrm{mvar}(p)$: largest variable appearing in p
- $\mathrm{init}(p)$: leading coefficient of p w.r.t. $\mathrm{mvar}(p)$

- a polynomial set $T \subset R \smallsetminus \mathbb{K}$
- T is a triangular set if $\mathrm{mvar}(p) \neq \mathrm{mvar}(q)$ for all $p \neq q \in T$
- $\mathrm{init}(T)$: the product of the initials of polynomials in T
- $\mathrm{Sat}(T) := \langle T \rangle : \mathrm{init}(T)^{\infty}$

- an element $p \neq 0$ of a ring $\mathbb{A}$ is regular if p is not a zerodivisor in $\mathbb{A}$
- a triangular set $T = \{t_1, \ldots, t_s\}$ is a regular chain if $\{t_1, \ldots, t_{s-1}\}$ is a regular chain and $\mathrm{init}(t_s)$ is regular in $R/\mathrm{Sat}(t_1, \ldots, t_{s-1})$

Example

$$T := \begin{cases} t_2 = (x_1 + x_2){x_3}^2 + x_3 + 1 \\ t_1 = {x_1}^2 - 2. \end{cases}$$

Under the order $x_3 > x_2 > x_1$,

- $\mathrm{mvar}(t_2) = x_3$ and $\mathrm{init}(t_2) = x_1 + x_2$
- $\mathrm{init}(t_2)$ is regular(neither zero or zerodivisor) modulo $\langle t_1 \rangle : 1^\infty = \langle t_1 \rangle$
- T is a regular chain
- $\mathrm{init}(T) := \mathrm{init}(t_2)\mathrm{init}(t_1)$
- $\mathrm{Sat}(T) := \langle T \rangle : \mathrm{init}(T)^\infty$
- quasi-component of T: $W(T) = V(T) \setminus V(\mathrm{init}(T))$.

Triangular decomposition of an algebraic variety

Kalkbrener triangular decomposition

Let $F \subset \mathbb{K}[\mathbf{x}]$. A family of regular chains $T_1, \ldots, T_e$ of $\mathbb{K}[\mathbf{x}]$ is called a Kalkbrener triangular decomposition of $V(F)$ if

$$V(F) = \cup_{i=1}^{e} \overline{W(T_i)}.$$

Lazard-Wu triangular decomposition

Let $F \subset \mathbb{K}[\mathbf{x}]$. A family of regular chains $T_1, \ldots, T_e$ of $\mathbb{K}[\mathbf{x}]$ is called a Lazard-Wu triangular decomposition of $V(F)$ if

$$V(F) = \cup_{i=1}^{e} W(T_i).$$

Incremental algorithm and intersect operation

Intersect operation

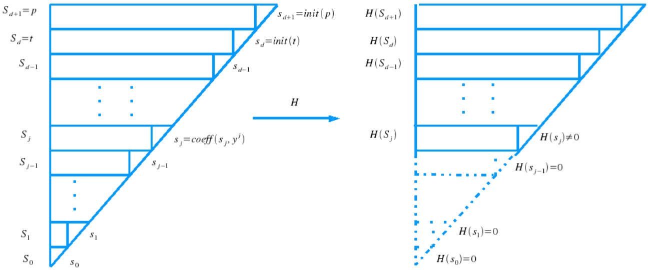
- Let $R = \mathbb{K}[x_1 < \cdots < x_n]$.
- Let $p \in R$ and T be a regular chain of R.
- Intersect(p, T, R) returns regular chains $T_1, \ldots, T_e \subset R$ such that

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

Triangularize(F, R)

- **if** $F = \{\ \}$ **then** return $\{\varnothing\}$
- Choose a polynomial $p \in F$ with maximal rank
- **for** $T \in$ Triangularize$(F \setminus \{p\}, R)$ **do**
  output Intersect(p, T, R)
  end

Specialization properties of subresultants



Theorem

Let H be a homomorphism from a ring R to a field $\mathbb{L}$. Let $p, t \in R[y]$. Let j be the smallest integer s.t. $H(s_j) \neq 0$. Then $H(S_j) = \gcd(H(p), H(t))$.

Properties of Regular GCD (I)

- Let $R := \mathbb{K}[x_1, \ldots, x_{k-1}]$, where $1 \leq k \leq n$.
- Let $T \subset \mathbb{K}[x_1, \ldots, x_{k-1}]$ be a regular chain.
- Let $p, t, g \in R[x_k]$ be polynomials with main variable x_k.

Proposition

Assume $T \cup \{t\}$ is a regular chain and g is a regular GCD of p and t in $R[x_k]/\sqrt{\mathrm{Sat}(T)}$. We have:

$$\begin{array}{rcl} V(p) \cap W(T \cup t) & \subseteq & W(T \cup g) \cup V(\{p, h_g\}) \cap W(T \cup t) \\ & \subseteq & V(p) \cap \overline{W(T \cup t)}. \end{array}$$

Properties of Regular GCD (II)

- Let $R := \mathbb{K}[x_1, \ldots, x_{k-1}]$, where $1 \leq k \leq n$.
- Let $T \subset \mathbb{K}[x_1, \ldots, x_{k-1}]$ be a regular chain.
- Let $p, t, g \in R[x_k]$ be polynomials with main variable x_k.

Theorem

There exists finitely many regular chains $T_1 \cup g_1, \ldots, T_e \cup g_e$ such that

$$V(p) \cap W(T \cup t) \subseteq \cup_{i=1}^{e} W(T_i \cup g_i) \subseteq V(p) \cap \overline{W(T \cup t)},$$

where g_i is a regular GCD of p and t in $R[x_k]/\sqrt{\mathrm{Sat}(T_i)}$.

Remark

Note that for all T_i, the regular GCD of p and t in $R[x_k]/\sqrt{\mathrm{Sat}(T_i)}$ can be computed by t he same subresultant chain of p and t.