Triangular Decompositions of Polynomial Systems: From Theory to Practice

Marc Moreno Maza

Univ. of Western Ontario, Canada

IPM workshop on differential algebra and related topics
21-25 June 2014
Why a tutorial on triangular decompositions?

• The theory is mature:
  - the objects are well understood,
  - the interactions with other theories also,
  - notions and terminologies are unifying.

• The algorithms are evolving very quickly:
  - modular algorithms are available now,
  - complexity estimates also,
  - fast polynomial and matrix arithmetic start to be used.

• The implementation effort is growing
  - triangular decompositions are available in major computer algebra systems,
  - implementation techniques are a priority.
Where are triangular decompositions used?

• Books and Papers, for instance:

  - difference polynomial systems (Gao & Luo, 2004)
  - polynomial systems (Chen & M3, 2011)
  - automatic theorem proving (Wu, 1984), (Chou, 1988)
  - geometric computation (Chen & Wang, 2004)
  - primary decomposition (Shimoyama & Yokoyama, 1994)
  - isolating real roots (Rioboo, 1992), (Aubry, Rouillier & Safey El Din, 2001), (Boulier, Chen, Lemaire & M3, 2009)
  - structured polynomial systems (Boulier, Lemaire & M3, 2001), (Dahan, Jin, M3 & Schost, 2006)
- cryptology (Schost & Gaudry, 2003)

- algebraic geometry (Alvandi, Chen, Marcus, M^3, Schost & Vrbik, 2012-2014)

- real algebraic geometry (Chen, Davenport, M^3, Xia & Xiao, 2010)

- symbolic-numeric computations (M^3, Reid, Scott & Wu, 2005)

- theoretical physics (Foursov & M^3, 2001)

- classification problems in geometry (Kogan & M^3, 2002).

- ...

- Software, for instance:
  
  - Diffalg by Boulier and Hubert in MAPLE
  
  - Dynamic Evaluation by Duval and Gómez Díaz in AXIOM
  
  - RealClosure by Rioboo in AXIOM
  
  - RAG’lib by Safey El Din in MAPLE
- *Epsilon* by Wang in MAPLE
- *Discoverer* by Xia in MAPLE
- for primary decomposition in MAGMA and SINGULAR
- *RegularChains* by Alvandi, Chen, Lemaire, M³ and Xie in MAPLE see also [www.regularchains.org](http://www.regularchains.org)
- *RegularChains* in AXIOM and ALDOR by M³
- *Elimino* parallel implementation by Wu, Liao, Lin, and Wang in C
- *Basic Polynomial Algebra Subprograms* by Chen, Covanov, M³ Xie & Xie in CilkPlus.

- Related concepts
  - resultants
  - Gröbner bases
  - geometric resolutions
  - comprehensive Gröbner bases.
Acknowledgments

• The IPM and Prof. Amir Hashemi

• My former and current PhD students: Parisa Alvandi, Changbo Chen, Xiaohui Chen, Sardar Anisul Haque, Liyun Li, Xin Li, Wei Pan, Paul Vrbik, Ning Xie, Yuzhen Xie.


• My current collaborators on the subject of triangular decompositions:
  - François Boulier & François Lemaire (Univ. Lille 1, France)
  - Xavier Dahan (Kyushu Univ., Japan)
  - James Davenport (Univ. of Bath, UK)
  - Jürgen Gerhard and John May (Maplesoft)
  - Wenyuan Wu (CIGIT, Chinese Academy of Science, China)
  - Bican Xia (Peking Univ., China)
An overview of this tutorial

• **Main objective:** an introduction for non-experts.

• **Prerequisites:** some familiarity with Gröbner bases would be useful, but not necessary.

• **Outline:**

  **Day 1:** the case of polynomial systems with finitely many solutions

  **Day 2:** the general case: triangular sets, characteristic sets, Wu’s method, regular chains, reduction to dimension zero

  **Day 3:** the RegularChains library in MAPLE and an overview of its solvers

  **Day 4:** Applications to real algebraic geometry

  **Day 5:** Applications to the study of dynamical systems
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:

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

9
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 \( \mathcal{P} \).

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

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

\[
\mathbf{V}(\mathcal{P}) = \mathbf{W}(T) \cup \mathbf{W} \left\{ \begin{array}{c}
dx + ey - f \\
hy - i \\
(ie - fh)a + (-ib + ch)d \\
g
\end{array} \right\} \cup \mathbf{W} \left\{ \begin{array}{c}
gx + hy - i \\
(ha - bg)y - ia + cg \\
hd - eg \\
ie - fh
\end{array} \right\}
\]

\[
\cup \mathbf{W} \left\{ \begin{array}{c}
x \\
(hd - eg)y - id + fg \\
fb - ce \\
ie - fh
\end{array} \right\} \cup \mathbf{W} \left\{ \begin{array}{c}
ax + by - c \\
hy - i \\
d \\
g
\end{array} \right\} \cup \ldots
\]

where \( \mathbf{W}(T) \) denotes the generic zeros of \( T \). We have : \( \mathbf{W}(T) \subseteq \mathbf{V}(T) \). 10
Structured examples: implicitization, ranking conversions

• For $R = x > y > z > s > t$ and $\overline{R} = t > s > z > y > x$ we have:

$$\text{convert}\left(\begin{cases} x - t^3 \\ y - s^2 - 1 \\ z - s t \end{cases}, R, \overline{R}\right) = \begin{cases} s t - z \\ (x y + x)s - z^3 \\ z^6 - x^2 y^3 - 3x^2 y^2 - 3x^2 y - x^2 \end{cases}$$

• For $R = \cdots > v_{xx} > v_{xy} > \cdots > u_{xy} > u_{yy} > v_x > v_y > u_x > u_y > v > u$ and $\overline{R} = \cdots u_x > u_y > u > \cdots > v_{xx} > v_{xy} > v_{yy} > v_x > v_y > v$ we have:

$$\text{convert}\left(\begin{cases} v_{xx} - u_x \\ 4u v_y - (u_x u_y + u_x u_y u) \\ u_x^2 - 4u \\ u_y^2 - 2u \end{cases}, R, \overline{R}\right) = \begin{cases} u - u_{yy}^2 \\ v_{xx} - 2v_{yy} \\ v_y v_{xy} - v_{yy}^3 + v_{yy} \\ v_{yy}^4 - 2v_{yy}^2 - 2v_y^2 + 1 \end{cases}$$
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

\[
\begin{align*}
  f_1 &= y^2 + (2z^2 - 1)y - 2z^2 + z + z^4 \\
  f_2 &= y^2 + z - y - z^2
\end{align*}
\]

• 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:

\[
\begin{array}{c|c}
  f_1 & f_2 \\
  f_3 & 1
\end{array}
\]

\( f_3 = 2z^2y - z^2 + 2z^2 - z \).
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 $z^3 + z^2 - 3z = 1$.

  • **Case $z = 0$.** Then $f_3 = 0$ and $f_2 = y^2 - y$ is the GCD.

  • **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

\[
\begin{array}{c|cc}
  & f_2 & \tilde{f}_3 \\
  \hline
  0 & y - (1/2)z^2 - (1/2) \\
\end{array}
\]

• Finally $\gcd(f_1, f_2, \mathbb{L}[y]) = \begin{cases} 
y^2 - y & \text{if } z = 0 \\
2y + z^2 - 1 & \text{if } z^3 + z^2 - 3z = -1
\end{cases}$
How those triangular sets look like? (I)

• Let us consider again the system

\[
\begin{align*}
    y^2 + (-1 + 2z^2)y - 2z^2 + z + z^4 &= 0 \\
    y^2 + z - y - z^2 &= 0
\end{align*}
\]

• Let \( \alpha_1 \) and \( \alpha_2 \) 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?

\[
\begin{align*}
\begin{cases}
z = 0 \\
y = 1 \\
x = 0
\end{cases} & \cup \\
\begin{cases}
z = 0 \\
y = 0 \\
x = 1
\end{cases} & \cup \\
\begin{cases}
z = 1 \\
y = 0 \\
x = 0
\end{cases} & \cup \\
\begin{cases}
z^2 + 2z - 1 = 0 \\
y = z \\
x = z
\end{cases}
\end{align*}
\]

\[
\begin{align*}
\downarrow \quad \text{CRT} \quad \downarrow
\end{align*}
\]

\[
\begin{align*}
\begin{cases}
z = 0 \\
y^2 - y = 0 \\
x + y = 1
\end{cases} & \cup \\
\begin{cases}
z = 1 \\
y = 0 \\
x = 0
\end{cases} & \cup \\
\begin{cases}
z^2 + 2z - 1 = 0 \\
y = z \\
x = z
\end{cases}
\end{align*}
\]

\[
\begin{align*}
\downarrow \quad \text{CRT} \quad \downarrow
\end{align*}
\]

\[
\begin{align*}
\begin{cases}
z = 0 \\
y^2 - y = 0 \\
x + y = 1
\end{cases} & \cup \\
\begin{cases}
z^3 + z^2 - 3z = -1 \\
2y + z^2 = 1 \\
2x + z^2 = 1
\end{cases}
\end{align*}
\]
From a lexicographical Gröbner basis to a triangular
decomposition (I)

• Let us consider again (last time) the polynomials
\[
\begin{align*}
  f_1 &= y^2 + (2z^2 - 1)y - 2z^2 + z + z^4 \\
  f_2 &= y^2 + z - y - z^2
\end{align*}
\]

• 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:
\[
\begin{align*}
  g_1 &= z^6 - 4z^4 + 4z^3 - z^2 \\
  g_2 &= 2z^2 y + z^4 - z^2 \\
  g_3 &= y^2 - y - z^2 + z
\end{align*}
\]

• We initialize \(T := \{g_1\}\). We would add \(g_2\) into \(T\) provided that \(\text{lcm}(g_2, y)\) is a
  unit.
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.

- **Case $z^2 = 0$**. In this case $g_2$ vanishes and $g_3 = y^2 - y + z$, leading to $T^1 := \{z^2, y^2 - y + z\}$

- **Case $z^4 - 4z^2 + 4z - 1$**. In this case $\text{lc}(g_2, y)$ 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

\[
\begin{array}{c|c}
\text{g3} & \tilde{g}_2 \\
0 & y - (1/2)z^2 - (1/2) \\
\end{array}
\]

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 $\pi_i^j$ 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 $\pi_i^j$ from $V_i$ to $V_j$.

**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 \( i = 1 \cdots n \)

\[ T_i = x_i^{d_i} + a_{d_i-1} x_i^{d_i-1} + \cdots + a_1 x_i + a_0 \]

with

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

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 \( \mathbb{A}^n(\overline{\mathbb{K}}) \). 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

\[
\pi^j_i : V_j \twoheadrightarrow V_i \quad (x_1, \ldots, x_j) \rightarrow (x_1, \ldots, x_i)
\]

where \( V_i = \pi^n_i(V) \) and \( V_j = \pi^n_j(V) \).

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

\[
|\pi^{-1}_i(M)| = d_{i+1} \cdots d_j.
\]
Equiprojectable varieties

**Definition.** Let $i$ and $j$ be integers such that $1 \leq i < j \leq n$ 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 $(\pi^j_i)^{-1}(V_i)$ 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) $\implies$ (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. ⊲
The interpolation formulas: sketch (I)

• Let $V \subset A^n(\overline{K})$ be (finite and) equiprojectable. Let $K$ be a field, with $K \subseteq K \subseteq \overline{K}$ such that every point of $V$ has its coordinates in $K$.

• 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 $K$) 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

$$V_{\alpha}^1 = \{ \beta = (\beta_1, \ldots, \beta_\ell, \beta_{\ell+1}) \in V_{\ell+1} \mid \beta_1 \neq \alpha_1 \}$$

$$V_{\alpha}^2 = \{ \beta = (\alpha_1, \beta_2, \ldots, \beta_\ell, \beta_{\ell+1}) \in V_{\ell+1} \mid \beta_2 \neq \alpha_2 \}$$

$$\cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots$$

$$V_{\alpha}^\ell = \{ \beta = (\alpha_1, \ldots, \alpha_\ell-1, \beta_\ell, \beta_{\ell+1}) \in V_{\ell+1} \mid \beta_\ell \neq \alpha_\ell \}$$

$$V_{\alpha}^{\ell+1} = \{ \beta = (\alpha_1, \ldots, \alpha_\ell, \beta_{\ell+1}) \in V_{\ell+1} \}$$

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 $T_{\alpha,\ell+1} = T_i(\alpha_1, \ldots, \alpha_\ell, x_{\ell+1}) \in K[x_{\ell+1}]$. 

24
We consider also the projections

\[ v_1^\alpha = \pi_1^{\ell+1}(V_1^\alpha) = \{(\beta_1) \in V_1 \mid \beta_1 \neq \alpha_1\} \]

\[ v_2^\alpha = \pi_2^{\ell+1}(V_2^\alpha) = \{(\alpha_1, \beta_2) \in V_2 \mid \beta_2 \neq \alpha_2\} \]

\[ \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \]

\[ v_\ell^\alpha = \pi_\ell^{\ell+1}(V_\ell^\alpha) = \{(\alpha_1, \ldots, \alpha_{\ell-1}, \beta_\ell) \in V_\ell \mid \beta_\ell \neq \alpha_\ell\} \]

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

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

Then, we have:

\[ T_{\alpha,\ell+1} = \prod_{\beta \in V_\alpha^{\ell+1}} (x_{\ell+1} - \beta_{\ell+1}) \]

\[ T_{\ell+1} = \sum_{\alpha \in V_\ell} \frac{E_\alpha T_{\alpha,\ell+1}}{E_\alpha(\alpha)} \]

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

$$f = x^p - t = x^p - \alpha^p = (x - \alpha)^p \quad (1)$$

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

27
Polynomial GCDs over DPF, quasi-inverses (I)

**Definition.** (M³ & 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 \( ((g_i, \mathbb{L}_i), 1 \leq i \leq s) \) 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 \( \mathbb{L} \)
- \( g_i \in \mathbb{L}_i \), for all \( 1 \leq i \leq s \),
- 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 \( 1 \leq i \leq s \).

**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 $V \subset A^n(\overline{K})$ be finite. Consider the projection $\pi : V \hookrightarrow \overline{K}^{n-1}$ 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 $V(F) \subset A^n(\overline{K})$ be finite with $F \subset K[x_1, \ldots, x_n]$. There exist Lazard triangular sets $T^1, \ldots, T^s \subset K[x_1, \ldots, x_n]$ such that

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

They form a **triangular decomposition** of $V(F)$.
Equiprojectable variety definition (1/3)
Equiprojectable variety definition (2/3)
Equiprojectable variety definition (3/3)
Equiprojectable decomposition definition (1/3)
Equiprojectable decomposition definition (2/3)
Equiprojectable decomposition definition (3/3)
From triangular to equiprojectable decomposition

**Notation.** Let \( V(F) \subset A^n(\overline{K}) \) be finite with \( F \subset K[x_1, \ldots, x_n] \). Let \( \Delta \) be a triangular decomposition of \( V(F) \).

**Proposition.** We compute from \( \Delta \) another triangular decomposition \( \{T^1, \ldots, T^d\} \) of \( V \) such that \( V(T^1), \ldots, V(T^d) \) is the equiprojectable decomposition of \( V \).

**Proof.** We proceed into two steps:

- **split:** reducing what we call critical pairs by means of GCD computations modulo Lazard triangular sets,

- **merge:** reducing what we call solvable pairs by means of CRT computations modulo Lazard triangular sets.

**Remark.** Among all possible triangular decompositions of \( V(F) \), the equiprojectable decomposition is a canonical choice: it depends only on the variable order and \( V(F) \).
Example: *split + merge* modulo 7

\[
\begin{align*}
\text{C} & \quad C_2 = y^2 + 6yx^2 + 2y + x, & \quad D & \quad D_2 = y + 6 \\
& \quad C_1 = x^3 + 6x^2 + 5x + 2, & \quad & \quad D_1 = x + 6
\end{align*}
\]
**Example: split+merge modulo 7**

\[
\begin{array}{c|c|c}
C & C_2 = y^2 + 6yx^2 + 2y + x, & D_2 = y + 6 \\
   & C_1 = x^3 + 6x^2 + 5x + 2 & D_1 = x + 6 \\
\end{array}
\]

\[
\downarrow \text{Split } C : \text{GCD} \downarrow
\]

\[
\begin{array}{c|c|c}
E & C_2' = y^2 + x, & D_2 = y + 6 \\
   & C_1' = x^2 + 5 & D_1 = x + 6 \\
\end{array}
\]

\[
F | C_2'' = y^2 + y + 1, \quad C_1'' = x + 6 \\
\]

\[
D | D_2 = y + 6, \quad D_1 = x + 6
\]

![Diagram](image-url)
### Example: split+merge modulo 7

<table>
<thead>
<tr>
<th></th>
<th>( C )</th>
<th>( D )</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>( C_2 = y^2 + 6yx^2 + 2y + x ), ( C_1 = x^3 + 6x^2 + 5x + 2 )</td>
<td>( D_2 = y + 6 ), ( D_1 = x + 6 )</td>
</tr>
</tbody>
</table>

\[ \downarrow \text{Split } C : \text{GCD} \ \downarrow \]

<table>
<thead>
<tr>
<th></th>
<th>( E )</th>
<th>( F )</th>
<th>( D )</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>( C_2' = y^2 + x )</td>
<td>( C_2'' = y^2 + y + 1 )</td>
<td>( D_2 = y + 6 )</td>
</tr>
<tr>
<td></td>
<td>( C_1' = x^2 + 5 )</td>
<td>( C_1'' = x + 6 )</td>
<td>( D_1 = x + 6 )</td>
</tr>
</tbody>
</table>

\[ \downarrow \text{Merge } F \text{ and } D : \text{CRT} \ \downarrow \]

<table>
<thead>
<tr>
<th></th>
<th>( E )</th>
<th>( G )</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>( C_2' = y^2 + x )</td>
<td>( G_2 = y^3 + 6 )</td>
</tr>
<tr>
<td></td>
<td>( C_1' = x^2 + 5 )</td>
<td>( G_1 = x + 6 )</td>
</tr>
</tbody>
</table>

\[ \text{Diagram: Split } C \rightarrow \text{Split } C' \rightarrow \text{Merge } F \text{ and } D \rightarrow \text{Merge } C' \]
Specialization properties: sketch

Oversimplified case: Assume all points $V(F)$ are in $\mathbb{Q}^n$. Let $p \in \mathbb{Z}$ prime. if
1. $p$ divides no denominator of the coordinates; (V mod $p$ is well defined)
2. the cardinality of none of the projections of $V$ decreases mod $p$;
then the equiprojectable decomposition specializes mod $p$. Below, is a bad case.

General case: Under similar assumptions, every coordinate of every point of $V$ lies in a direct sum $\mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p$ where $\mathbb{Z}_p$ is the ring of $p$-adic integers.

THEOREM. (Dahan, M$^3$, Schost, Wu & Xie, 2005) Let $h$ the maximum length of a coefficient in $F$, and $d$ the maximum degree in $F$. There exists $A \in \mathbb{N}$ s. t.:
(1) $h(A) \leq 2n^2 d^{2n+1}(3h + 7 \log(n + 1) + 5n \log d + 10)$.
(1) If $p \not| A$, then the equiprojectable decomposition specializes well mod $p$. 
A probabilistic algorithm

Random choice of two primes: \( p_1 \) and \( p_2 \)

Triangular decomposition mod \( p_1 \)

Equiprojectable decomposition mod \( p_1 \)

Hensel lifting
Triangular sets \( \mod p_1^2 \), \( p_1^4 \), \( p_1^8 \), . . .

Rational reconstruction

FAILS

Triangular sets over \( \mathbb{Q} \) (good ones?)

SUCCEEDS

Triangular decomposition mod \( p_2 \)

Equiprojectable decomposition mod \( p_2 \)

Not lifted enough?

\begin{align*}
\text{NO} \quad \text{?} \quad \text{?} \quad \text{?} \quad \text{?} \\
\text{YES} \quad \text{Is each triangular set in green equals to one of the red ones?}
\end{align*}

Algorithm succeeds

Reduction modulo \( p_2 \)

\begin{align*}
\text{SUCCEEDS} \quad \text{\begin{align*}
\text{SUCCEEDS} \quad \text{\begin{align*}
\text{SUCCEEDS} \quad \text{\begin{align*}
\text{SUCCEEDS}
\end{align*}}
\end{align*}}
\end{align*}}
\end{align*}
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 $\text{lc}(T_i, x_i) = 1$, for all $1 \leq i \leq n$,
- 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. $h_i := \text{lc}(C_i, x_i)$ 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 $T_1 = \text{lc}(C_1)^{-1} C_1$ 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

\[
D_\ell = \prod_{1 \leq i \leq \ell - 1} \frac{\partial T_i}{\partial x_i} \mod \langle T_1, \ldots, T_{\ell - 1} \rangle
\]

\[
N_\ell = D_\ell T_\ell \mod \langle T_1, \ldots, T_{\ell - 1} \rangle
\]

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 \( V(T) \) if \( K = \mathbb{Q} \), that is the minimum size of a data set encoding \( V(T) \),
- the degree of \( V(T^\downarrow) \) if \( K \) 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

\[
\begin{align*}
11474127946569256007468619671388225994546322534047768700511994762261926900489014476185343948464697342622310665345135093195323564185839650189693651393545601231022260010343965391013603161618331054181976135382209910495948519012063920629615932045724589651442741444943587304777556223820376199033996054351301919398450811043401539767435245829758618270875989463831973885970439654459159240773157947028995544307815442694326841805687077911765761917873238393662798997120827671296735352087075871215616119541262433845931685369080754130154719452119621523713394865899778769339534459634212652321688102858941028295140149607477959605181480664573334972485639134741063277706156095111089627563494088702934461198572429832808992812870412765974147039531182770901475269211462030823759341810040325817543392095814567632394138225663551675769080400536438309191296130950729973668595636802112563524969324865875138127923901717040324245316310945016304034566836868396416454909450908686183665824904206376739708532798694710183488870918177495466758475933774815682380070072559306520563109135581811542014656070637988617107330377650533573060376765291256264154608045527569292338754337973797843824713701855230758768236174292732015095209063005663023451206412469538581957864228527528797540201566899450200204776059460451559860111513017617067305346652396615265985718824532042488802422296773818429373789169917697659429318767468848486488142387103357657535971492012495647461071880315070337681297841719718775576117319500000077875129232958889104193239787108649287987286424755607482454864690786827841184696976286133386057538173722098997859322480
\]
• 5737063973284628003734098356941129977273162670238843502559973811130963450244507283092671974233
  17126050058202862102854051702189834445407041921409912212858453794696093319533564185839650189693
  699349416725564387706041955516121939729771831066168137301361047433161675729521509773976564819862
  469803305737200436962857230940384594351690145609608094579328266981168648539093657866617523596721
  3624577949998087226523064237197118238681455387434685379217170814307753153223785029557758914206492
  182558840983141129257028601685384373297644771129092120128266359787322504095639220690574114647888
  151384178466066258299897889869742667512277813383969304602672093549761989645144274
  44394335873903477558622382037619903399605543513019193984508110344015397674352445829758618270875
  239889463831973885970439654459159240773157947028995584430781544269432684180568707791767576191787
  273833966279899712882771296735352080757871215616119541262423348593168536908075413015471945211962
  152371339486589977786393534459634212652323168810285894102895140146907477956051840866457334972
  485639134741063277706156095111089627563494088702934461198572429832808992812870412765974147039531
  1827709014752692114620308283759341810040325817543392095814567632394138225663533167569680400536438
  309191296130957029973668595368021125635249669324865875138127923901717040322453163109041630403456
  6838688396641645449094509086868136658249042063767397085327989647101834888709181774954667584758393
  7481568238007075259306520563109135581811542014656070637888617107330377650533573063765291526264
  1546080455275692923217437018552037863236174292780519209063056630234512064
  12469538581957864228527528797540201566899450200477065094640515598601115130175167063705343665239
  661526598571882453202424888024222967381848293737891699176976594293187676488484684814238710335767
  107682408338385308982455918634325305664726893856491630963372387378085153378287004125
  23978710864928798728642475560748245864690786827841184696976286133386057573817722098997859322480
• 3125z^{20} - 9375z^{16} - 40000000000z^{15} - 2015999988750z^{12} - 156000000000z^{11} + 192000000000000z^{10} - 12165125356800000000z^{8} - 652800000000z^{6} - 40960000000000000z^{5} - 169869086392334783997975^{4} - 14155767152640302400000000z^{3} - 589823873280000000000z^{2} - 12288000000000000z - 6195303619231982878732441600243

• Applying the transformation of Dahan and Schost leads to 1787 characters.

• (20z^{19} + (-48z^{15}) + (-192000000z^{14}) + (-38707199784/5)z^{11}) + (-549120000z^{10}) + 61440000000000z^{9} + (-778568022835200432/25)z^{7}) + (-33030148999680000z^{6}) + (-1253376000000000z^{5}) + (-655360000000000000000z^{4}) + (-2717905382277335654399676/125)z^{3}) + (-1358953646653469030400z^{2}) + (-3774872788992000000000z) - 393216000000000000
\[
3200000z^{15} + 161280000z^{12} + 124800000z^{11} + (-30720000000000z^{10}) + 1946419628544000z^{8} + 235929617856000z^{7} + 104448000000000z^{6} + 9830400000000000z^{5} + 407685987827227827200z^{4} + 33973848244224192000z^{3} + 141557739724800000000z^{2} + 294912000000000000000z + 198249699507965678059615328
\]

- \((20z^{19} + (-48z^{15}) + (-192000000z^{14}) + (-38707199784/5)z^{11}) + (-549120000z^{10}) + 61440000000000z^{9} + (-778568022835200432/25)z^{7}) + (-33030148996800000z^{6}) + (-125337600000000000z^{5}) + (-655360000000000000000z^{4}) + (-271790538227735654399676/125)z^{3}) + (-13589536466534690304000z^{2}) + (-377487278899200000000z) - 393216000000000000000000z) + (-12z^{16}) + (-9676799856/5)z^{12}) + (-1996800000z^{11}) + (-194642219980800648/25)z^{9}) + (-141557781713920000z^{7}) + (-835584000000000000z^{6}) + (-679471833416273049598704/125)z^{4}) + (-9059676821914761216000z^{3}) + (-566230715596800000000000z^{2}) + (-1572864000000000000000z) + (-2038432221757477324800972/625)

- \(z^{20} + (-3z^{16}) + (-128000000z^{15}) + (-3225599982/5)z^{12}) + (-499200000z^{11}) + 614400000000000z^{10} + (-973210028544000054/25)z^{8}) + (-4718592714240000z^{7}) + (-20889600000000000z^{6}) + (-131072000000000000000z^{5}) + (-6794763455833913599919/125)z^{4}) + (-452984548844896768000z^{3}) + (-188743639449600000000000z^{2}) + (-393216000000000000000z) + (-6195303619231982878732441600243/3125)

- One can do better! Here’s the regular chain produced by the Triangularize algorithm of the RegularChains library, counting 963 characters.

- \(20x - 1y + z\)

- \((4375z^{12} + 52800011625z^{8} + 320000000000z^{7} + 110591902080000295z^{4} + 614399808000000000z^{3} + 1280000000000000z^{2} + 1875z^{13} - 9600010125z^{9} + 2000000000000z^{8} - 73727147520045z^{5} + 30720024000000000z^{4} + 128000000000000000000z^{3} - 22118403456000135z + 2359296368640014400000000

- \(3125z^{20} - 9375z^{16} - 400000000000z^{15} - 201599998750z^{12} - 1560000000000z^{11} + 192000000000000000z^{10} - 1216512535680006750z^{8} - 14745602232000000000z^{7} - 65280000000000000000z^{6} - 409600000000000000000z^{5} - 169869086393347839997975z^{4} - 141557671526403024000000000z^{3} - 589823873280000000000000z^{2} - 122880000000000000000000z - 6195303619231982878732441600243\)
Gröbner bases (I)

**Notation.** Fix \( \leq \) a term order on \( M = \{ x_1^{i_1} \ldots x_n^{i_n} \mid i_j \geq 0 \} \), i.e., a total order on \( M \) satisfying \( 1 \leq u \) and \( u \leq v \) \( \Rightarrow uw \leq vw \) for all \( u, v, w \in M \).

For \( f \in \mathbb{K}[x_1, \ldots, x_n] \), \( f \neq 0 \), the **leading (\textit{= greatest}) monomial** w.r.t. \( \leq \) in \( f \) is denoted \( \text{lm}\ f \) and its coefficient in \( f \) is the **leading coefficient** of \( f \), denoted \( \text{lc}\ f \).

For \( F \subset \mathbb{K}[X] \setminus \{0\} \), we write \( \text{lm}\ F = \{ \text{lm}\ f \mid f \in F \} \).

**Definition.** \( f \in \mathbb{K}[X] \) is **reduced** w.r.t. \( g \in \mathbb{K}[X] \), \( g \neq 0 \) if \( \text{lm}\ g \) does not divide any monomial in \( f \).

**Notation.** If \( f \) is not reduced w.r.t. one of the polynomials \( b_1, \ldots, b_k \in \mathbb{K}[X] \), then the operation \( \text{Reduce}(f, \{b_1, \ldots, b_k\}) \)

(1) computes polynomials \( r, q_1, \ldots, q_k \in \mathbb{K}[X] \) such that
\[
 f = q_1 b_1 + \cdots + q_k b_k + r
\]
holds and \( r \) is reduced w.r.t. all \( b_1, \ldots, b_k \in \mathbb{K}[X] \),

(2) if \( r \) is not zero, then replaces \( r \) by \( r/(\text{lc}\ f) \),

(3) and returns \( r \).
Gröbner bases (II)

**Notation.** For $A, B$ finite subsets of $\mathbb{K}[X] \setminus \{0\}$ the collection of the $\text{Reduce}(a, B)$, for $a \in A$, is denoted by $\text{Reduce}(A, B)$.

**Definition.** A subset $B \subset \mathbb{K}[X] \setminus \{0\}$ is **auto-reduced** if for all $b \in B$ the polynomial $b$ is reduced w.r.t. $B \setminus \{b\}$ and $\text{lcb} = 1$.

**Proposition.** *(Dickson’s Lemma)* Every auto-reduced set is finite.

**Definition.** For $A, B \subseteq F$ auto-reduced sets, we write $A \leq B$ whenever
\[
[\text{lm}B \subseteq \text{lm}A] \text{ or } [\min(\text{lm}A \setminus \text{lm}B) < \min(\text{lm}B \setminus \text{lm}A)].
\]

**Definition.** For an ideal $\mathcal{I} \subset \mathbb{K}[x_1, \ldots, x_n]$, a minimal auto-reduced subset $B \subset I$ is called a **reduced Gröbner basis** of $\mathcal{I}$.

**Proposition.** Every ideal $\mathcal{I} \subset \mathbb{K}[x_1, \ldots, x_n]$ admits a reduced Gröbner basis; moreover an auto-reduced subset $B \subset \mathcal{I}$ is a reduced Gröbner basis of $\mathcal{I}$ iff we have for all $f \in \mathbb{K}[x_1, \ldots, x_n]$\[
f \in \mathcal{I} \iff \text{Reduce}(f, B) = 0.
\]
Buchberger’s Algorithm for computing Gröbner bases

**Input:** $F \subset \mathbb{K}[X]$ and a term order $\leq$.

**Output:** $G$ a reduced Gröbner basis w.r.t. $\leq$ of the ideal $\langle F \rangle$ generated by $F$.

repeat

(S) $B := \text{MinimalAutoreducedSubset}(F, \leq)$

(R) $A := S\_\text{Polynomials}(B) \cup F$;

$R := \text{Reduce}(A, B, \leq)$

(U) $R := R \setminus \{0\}; F := F \cup R$

until $R = \emptyset$

return $B$

**Notation.** For $f, g \in \mathbb{K}[X]\{0\}$, let $L = \text{lcm}(\text{lm} f, \text{lm} g)$; then

$$S(f, g) := \frac{L}{\text{lm}_\leq f} f - \frac{L}{\text{lm}_\leq g} g$$

and $S\_\text{Polynomials}(F)$ returns the $S(f, g)$ for all pairs $\{f, g\} \subseteq F$. 
A recursive vision of polynomials

**Definition.** Let \( f, g \in \mathbb{K}[X] \) with \( g \not\in \mathbb{K} \).

- \( \text{mvar}(g) \): the greatest variable in \( g \) is the **leader** or **main variable** of \( g \),
- \( \text{init}(g) \): the leading coefficient of \( g \) w.r.t. \( \text{mvar}(g) \) is the **initial** of \( g \),
- \( \text{mdeg}(g) \): the degree of \( g \) w.r.t. \( \text{mvar}(g) \),
- \( \text{rank}(g) = v^d \) where \( v = \text{mvar}(g) \) and \( d = \text{mdeg}(g) \),
- \( \text{pdivide}(f, g) = (q, r) \) with \( q, r \in \mathbb{K}[X] \), \( \deg(r, v_g) < d_g \) and \( h_g^e f = q g + r \) where \( h_g = \text{init}(g) \), \( e = \max(\deg(f, v) - d_g + 1, 0) \), \( v_g = \text{mvar}(g) \) and \( d_g = \text{mdeg}(g) \),
- \( \text{prem}(f, g) = r \) if \( \text{pdivide}(f, g) = (q, r) \). \( f \in \mathbb{K}[X] \) is said **(pseudo-)reduced** w.r.t. \( g \in \mathbb{K}[X] \not\in \mathbb{K} \) if \( \deg(f, \text{mvar}(g)) < \text{mdeg}(g) \).

**Example.**

Assume \( n \geq 3 \). If \( p = x_1 x_3^2 - 2x_2 x_3 + 1 \), then we have \( \text{mvar}(p) = x_3 \), \( \text{mdeg}(p) = 2 \), \( \text{init}(p) = x_1 \) and \( \text{rank}(p) = x_3^2 \).
Triangular sets and auto-reduced sets

**Definition.** A finite subset $B \subset \mathbb{K}[X] \setminus \mathbb{K}$ is

- a **triangular set** if for all $f, g \in B$ we have $f \neq g \Rightarrow \text{mvar}(f) \neq \text{mvar}(g)$,

- **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 $B = \emptyset$ we write $\text{prem}(f, B) = f$. Otherwise let $b \in B$ with largest main variable; we write $\text{prem}(f, B) = \text{prem}(\text{prem}(f, b), B \setminus \{b\})$. For $A \subset \mathbb{K}[X]$ write $\text{prem}(A, B) = \{\text{prem}(a, B) \mid a \in A\}$.

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

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

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

53
The saturated ideal of a triangular set (I)

**Definition.** Let $T \subset \mathbb{K}[X]$ be a triangular set. The set
\[
\text{Sat}(T) = \{ f \in \mathbb{K}[X] \mid (\exists e \in \mathbb{N}) \ h_T^e \ f \in \langle T \rangle \}
\]
is the **saturated ideal** of $T$. (Clearly Sat$(T)$ is an ideal.)

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

\[
\text{prem}(f, T) = 0 \Rightarrow f \in \text{Sat}(T).
\]

**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:

\[
\text{prem}(p, T) = \text{prem}(q, T) = 0.
\]

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

54
The saturated ideal of a triangular set (II)

- 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:
  - $\text{Sat}(T) = \langle F \rangle$.
  - $\text{Sat}(T)$ is an ideal strictly larger than $\langle T \rangle$.
  - In fact $\langle T \rangle \subset \text{Sat}(T) \cap \langle g, h, i \rangle$,
  - and none of Sat$(T)$ or $\langle g, h, i \rangle$ contains the other.
Relations between Gröbner bases and regular chains

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

\[ \mathcal{V}(\mathcal{P}) = \mathcal{W}(T) \cup \mathcal{W} \]

\[ \cup \mathcal{W} \]

\[ \cup \mathcal{W} \]

Lex base (P):

\[ \begin{cases} 
  xa + yb - c \\
  yae - ydb - af + dc \\
  ae\textbf{i} - ahf - dbi + dhc + gb\textbf{f} - gec 
\end{cases} \]

\[ \begin{cases} 
  xd + ye - f \\
  yah - ygb - ai + gc \\
  ydh - yge - di + gf 
\end{cases} \]

- For more details see (Aubry, Lazard & M3, 1997).
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

\[ W(T) = V(T) \setminus V\{h_T\} \]

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 $\text{Sat}(T) = \langle x_2 \rangle$.

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

\[ \overline{W(T)} = V(\text{Sat}(T)). \]

**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 $W(T) = \emptyset = V(T)$. 

57
Characteristic sets (I)

**Notation.** If \( f, g \not\in \mathbb{K} \), we write \( \text{rank}(f) < \text{rank}(g) \) if \( \text{mvar}(f) < \text{mvar}(g) \) or, \( \text{mvar}(f) = \text{mvar}(g) \) and \( \text{mdeg}(f) < \text{mdeg}(g) \). For \( F \subset \mathbb{K}[X] \setminus \mathbb{K} \), we write \[ \text{rank}(F) = \{ \text{rank}(f) \mid f \in F \} \].

**Definition.** For auto-reduced sets, we write \( A \leq B \) whenever

\[ [\text{rank}(B) \subseteq \text{rank}(A)] \text{ or } [\min(\text{rank}(A) \setminus \text{rank}(B)) < \min(\text{rank}(B) \setminus \text{rank}(A))] \].

**Definition.** For an ideal \( \mathcal{I} \subset \mathbb{K}[X] \), a minimal auto-pseudo-reduced subset \( B \subset I \) is called a **Ritt (or Kolchin) characteristic set** of \( \mathcal{I} \).

**Proposition.** Every ideal \( \mathcal{I} \subset \mathbb{K}[X] \) admits a **Ritt characteristic set**; an auto-reduced \( B \subset \mathcal{I} \) is a Ritt characteristic set of \( \mathcal{I} \) iff \( \text{prem}(f, B) = 0 \) for all \( f \in \mathcal{I} \).
Characteristic sets (II)

**Definition.** For a set $F \subset \mathbb{K}[X]$, an auto-pseudo-reduced subset $B \subseteq F$ such that $\text{prem}(F, B) \subset \mathbb{K}$ is called a **Wu characteristic set** of $F$.

**Proposition.** If $B \subseteq F$ is a **Wu characteristic set** of $F \subset \mathbb{K}[X]$, then

- If $\text{prem}(F, B)$ contains a non-zero constant then $V(F) = \emptyset$,
- If $\text{prem}(F, B) = \{0\}$ then

$$V(F) = W(B) \cup \bigcup_{b \in B} V(F \cup \{\text{init}(b)\}).$$

**Proof.** Indeed, $\text{prem}(f, B) = 0$ implies that there exists a product $h$ of the initials of $B$ such that $hf \in \langle B \rangle$. Hence $W(B) \subseteq V(F)$. Thus any $\zeta \in V(F)$ either belongs to $W(B)$ or cancels one of the initials of $B$. ⊳

**Theorem.** (Wu, 1987) For any $F \subset \mathbb{K}[X]$, one can compute finitely many triangular sets $T^1, \ldots, T^s$ such that

$$V(F) = W(T^1) \cup \cdots \cup W(T^s).$$
Wu’s Method

Input: \( F \subset \mathbb{K}[X] \) and a variable ordering \( \leq \).

Output: \( C \) a Wu characteristic set of \( F \).

\[
\text{repeat} \\
\text{(S)} \quad B := \text{MinimalAutoreducedSubset}(F, \leq) \\
\text{(R)} \quad A := F \setminus B; \\
\quad R := \text{prem}(A, B) \\
\text{(U)} \quad R := R \setminus \{0\}; F := F \cup R \\
\text{until } R = \emptyset \\
\text{return } B
\]

• Repeated calls to this procedure computes a decomposition of \( V(F) \).

• Cannot detect whether a quasi-component is empty.

\( \Rightarrow \) This leads to the theory of regular chains. (Kalkbrener, 1991) and (Yang & Zhang, 1991).
**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 $p \not\in \mathcal{P}$, 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 $i = 2 \cdot \cdots \cdot s$ 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 $\text{Sat}(T)$ is a proper ideal of $\mathbb{K}[X]$ and, thus, $W(T) \neq \emptyset$. 
Reduction to dimension zero (I)

**Theorem.** (Chou & Gao, 1991), (Kalkbrener, 1991), (Aubry, 1999), (Boulier, Lemaire & M$^3$, 2006) Let $T = \{T_{d+1}, \ldots, T_n\}$ be a triangular set. Assume that \( \text{mvar}(T_i) = x_i \) for all \( d + 1 \leq i \leq n \) and assume \( \text{Sat}(T) \) is a proper ideal of \( \mathbb{K}[X] \). Then, every prime ideal \( \mathcal{P} \) associated with \( \text{Sat}(T) \) 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
\[
\mathbb{K}[x_1, \ldots, x_d] \setminus \{0\}; \text{ in other words, we map our polynomials from } \mathbb{K}[x_1, \ldots, x_n]\]
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 \( \text{Sat}(T) \). Then, the following conditions are equivalent:

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

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

62
Reduction to dimension zero (II)

**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 $\text{Sat}(T_0)$ radical.)

**Notation.** Let $T$ be 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 $\text{Sat}(T)$, then $Z(p, T)$ is either empty or it is contained in a variety of dimension strictly less than the dimension of $\overline{W(T)}$. 
Regular chains and characteristic sets

**Theorem.** (Aubry, Lazard & \(M^3\), 1997) Let \(C \subset \mathbb{K}[X]\) be an auto-(pseudo-)reduced set. Then, we have

\[
\text{Sat}(C) = \{ p \mid \text{prem}(p, C) = 0 \}
\]

\(\Uparrow\)

\(C\) regular chain

\(\Uparrow\)

\(C\) characteristic set of \(\text{Sat}(C)\)
Incremental triangular decompositions: a geometrical approach

\[
\begin{align*}
&\begin{cases}
x^2 + y + z = 1
\end{cases} \\
&\begin{cases}
x^2 + y + z = 1 \\
x + y^2 + z = 1
\end{cases} \\
&\begin{cases}
x^2 + y + z = 1 \\
x + y^2 + z = 1 \\
x + y + z^2 = 1
\end{cases}
\end{align*}
\]
\[
\begin{align*}
\begin{cases}
  x^2 + y + z &= 1 \\
y^4 + (2z - 2)y^2 + y - z + z^2 &= 0
\end{cases}
\end{align*}
\begin{align*}
\begin{cases}
  x + y^2 + z &= 1 \\
y^2 - y &= z = 0
\end{cases}
\end{align*}
\begin{align*}
\begin{cases}
  x + y &= 1 \\
2x + z^2 &= 2y + z^2 = 1 \\
2x + z^2 &= 2y + z^2 = 1 \\
z^3 + z^2 - 3z &= -1
\end{cases}
\end{align*}
\]
Incremental Solving

Let $F \subset \mathbb{K}[x_1, \ldots, x_n]$, $f \in \mathbb{K}[x_1, \ldots, x_n]$, $T, T^m \ldots, T^e \subset \mathbb{K}[x_1, \ldots, x_n]$ reg. chains. Assume we have solved $F$ as $V(F) = W(T^i) \cup \cdots \cup W(T^e)$.

Assume that we have an operation 
$$(f, T) \mapsto \text{Intersect}(f, T) = (C_1, \ldots, C_d)$$ such that 
$$V(f) \cap W(T) \subseteq \cup_i W(C_i) \subseteq V(f) \cap \overline{W(T)}.$$ 

Then solving $F \cup f$ reduces to $\text{Intersect}(f, T^i)$ for all $i$.

$\implies$ the core routine operates on well behaved objects.

$\implies$ the decomposition can be reduced to regular GCD computation, allowing modular methods and fast arithmetic.
Incremental Solving

- Let $F \subset \mathbb{K}[x_1, \ldots, x_n]$, $f \in \mathbb{K}[x_1, \ldots, x_n]$, $T, T^m \ldots, T^e \subset \mathbb{K}[x_1, \ldots, x_n]$ reg. chains. Assume we have solved $F$ as $V(F) = W(T^i) \cup \cdots \cup W(T^e)$.

- Assume that we have an operation

  $$(f, T) \mapsto \text{Intersect}(f, T) = (C_1, \ldots, C_d)$$

  such that

  $$V(f) \cap W(T) \subseteq \bigcup_i W(C_i) \subseteq V(f) \cap \overline{W(T)}.$$ 

  Then solving $F \cup f$ reduces to Intersect($f, T^i$) for all $i$.

  $\implies$ the core routine operates on well behaved objects.

  $\implies$ the decomposition can be reduced to regular GCD computation, allowing modular methods and fast arithmetic.

**Remark.** (D. Lazard 91) proposes the principle. (M^3 . 00) gives a complete incremental algorithm which, in addition, generates components by decreasing order of dimension.
The notion of a Regular GCD

• Let \( P, Q, G \in \mathbb{K}[x_1 < \cdots < x_n][y] \) and \( T \subset \mathbb{K}[x_1 < \cdots < x_n] \) reg. chain. \( G \) is a *regular GCD* of \( P, Q \) modulo \( \text{sat}(T) \) if
  
  (i) \( \text{lc}(G, y) \) is a regular modulo \( \text{sat}(T) \),
  
  (ii) \( G \in \langle P, Q \rangle \) modulo \( \text{sat}(T) \),
  
  (iii) \( \deg_y(G) > 0 \Rightarrow \text{prem}_y(P, G), \text{prem}_y(Q, G) \in \text{sat}(T) \).

• If both \( T \cup P \) and \( T \cup Q \) are regular chains and if \( G \) is a GCD of \( P, Q \) modulo \( \text{sat}(T) \) with \( \deg_y(G) > 0 \) then we have

\[
W(T \cup P) \cap V(Q) \subseteq W(T \cup G) \cup \\
W(T \cup P) \cap V(Q, h_G) \subseteq \sqrt{\text{sat}(T \cup P)} \cap V(Q).
\]

One can compute \( T^1, \ldots, T^e \) and \( G_1, \ldots, G_e \) such that \( G_i \) is a reg. GCD of \( P, Q \) mod \( \text{sat}(T_i) \) and \( \sqrt{\text{sat}(T)} = \bigcap_{i=0}^{e} \sqrt{\text{sat}(T_i)} \).
Regularity test

- **Regularity test** is a fundamental operation:

  \[ \text{Regularize}(p, \mathcal{I}) \mapsto (\mathcal{I}_1, \ldots, \mathcal{I}_e) \]

  such that:

  \[ \sqrt{\mathcal{I}} = \bigcap_{i=0}^{e} \sqrt{\mathcal{I}_i} \text{ and } p \in \mathcal{I}_i \text{ or } p \text{ regular modulo } \mathcal{I}_i \]

- Regularity test reduces to regular GCD computation.
Related work

• This notion of a regular GCD was proposed in (M^3 2000)

• In previous work (Kalkbrener 1993) and (Rioboo & M^3 1995), other regular GCDs modulo regular chains were introduced, but with limitations.

• In other work (Wang 2000), (Yang etc. 1995) and (Jean Della Dora, Claire Dicrescenzo, Dominique Duval 85), related techniques are used to construct triangular decompositions.

• Regular GCDs modulo regular chains generalize GCDs over towers of field extensions for which specialized algorithms are available, (van Hoeij and Monagan 2002 & 2004).

• Asymptotically fast algorithms (when sat(T) is zero-dimensional and radical) appear in (Xavier Dahan, M^3, Éric Schost, Yuzhen Xie, 2006) and (Xin Li, M^3, Wei Pan, 2009).