Triangular Decompositions of Polynomial Systems: From Theory to Practice

Marc Moreno Maza

Univ. of Western Ontario, Canada

ISSAC tutorial, 9 July 2006

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:
  - differential algebra **(Ritt, 1932), (Kolchin, 1973), (Boulier, Lazard, Ollivier & Petitot, 1995), (Kondratieva, Levin, Mikhalev & Pankratiev, 1999) (Hubert, 2003) (Sit, 2002) (Golubisky, 2004) (Ovchinnikov, 2004)**
  - difference polynomial systems **(Gao & Luo, 2004)**
  - polynomial systems **(Wang, 2001)**
  - 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)**
  - structured polynomial systems **(Boulier, Lemaire & $\mathbf{M^3}$, 2001), (Dahan, Jin, $\mathbf{M^3}$ & Schost, 2006)**
  - cryptology (**Schost & Gaudry, 2003**)

- 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 Lemaire, M^3 and Xie in MAPLE

- triangular decompositions in AXIOM and ALDOR by M^3
- *Elimino* parallel implementation by Wu, Liao, Lin, and Wang in C
- *ParallelTriade* by M^3 and Xie in ALDOR.

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

Acknowledgments

- The ISSAC Tutorial Chair, Stephen M. Watt, and ISSAC organizers.
- My PhD students: Yuzhen Xie and Xin Li.
- My colleagues at UWO: Robert M. Corless, David J. Jeffrey, Gregory J. Reid, Éric Schost and Stephen M. Watt.
- My current collaborators on the subject of *triangular decompositions*:
  - François Boulier & François Lemaire (Univ. Lille 1, France)
  - Xavier Dahan and Éric Schost (École Polytechnique, France)
  - Jurgen Gerhard and Michael Cherkassoff (Maplesoft)
  - Oleg Golubitsky (Queen's Univ., Canada)
  - Marina V. Kondratieva (Moscow State Univ., Russia)
  - Alexey Ovchinnikov (North Carolina State Univ., USA)

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:**
  - an informal introduction of the key ideas
  - the case of polynomial systems with finitely many solutions: Lazard triangular sets
  - the general case: triangular sets, characteristic sets, Wu's method
  - regular chains, reduction to dimension zero
  - the Triade algorithm, its parallel implementation
  - implementation issues
  - the `RegularChains` library in MAPLE.

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:

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

Another one is:

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

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 $\mathcal{P}$.

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

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

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

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

Structured examples: implicitization, ranking conversions

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

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

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

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

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

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

- 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: $\begin{array}{c|c} f_1 & f_2 \\ \hline f_3 & 1 \end{array}$ 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 $i(z) = -(3/2)z^2 - 2z + 4$.

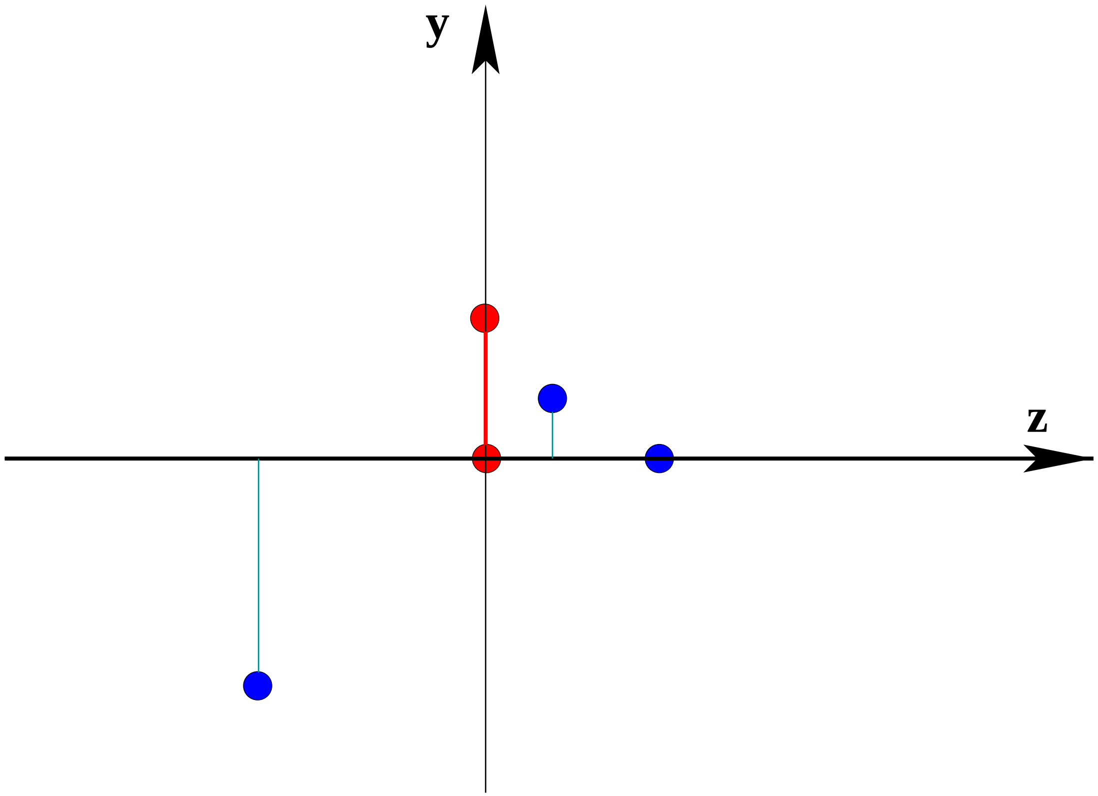
• Thus, the polynomial $\tilde{f_3} = i(z) f_3 = y + (1/2)z^2 - (1/2)$ is monic. So, we can compute
$$\begin{array}{c|c} f_2 & \tilde{f_3} \\ \hline 0 & y - (1/2)z^2 - (1/2) \end{array}.$$

• 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 $\left\{ \begin{array}{r} y^2 + (-1 + 2z^2)y - 2z^2 + z + z^4 = 0 \\ y^2 + z - y - z^2 = 0 \end{array} \right.$

• 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?

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

$$\downarrow \ \text{CRT} \ \downarrow$$

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

$$\downarrow \ \text{CRT} \ \downarrow$$

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

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:

$$\begin{cases} g_1 = z^6 - 4z^4 + 4z^3 - z^2 \\ g_2 = 2z^2 y + z^4 - z^2 \\ g_3 = y^2 - y - z^2 + z \end{cases}$$

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

We will denote by $\overline{\mathbb{K}}$ an **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_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 $i = 1 \cdots n$

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

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

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

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 $1 \leq i < j \leq n$ 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 $(\pi_i^j)^{-1}(V_i)$ 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 $\triangleright$ 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. $\triangleleft$

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

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

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:

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

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

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 $\triangleright$ 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.* $\triangleleft$

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 $\mathbb{F} = Z/pZ(t)$, 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

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

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^3 & 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 $V \subset A^n(\overline{\mathbb{K}})$ 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 $C_1, \ldots, C_d$.

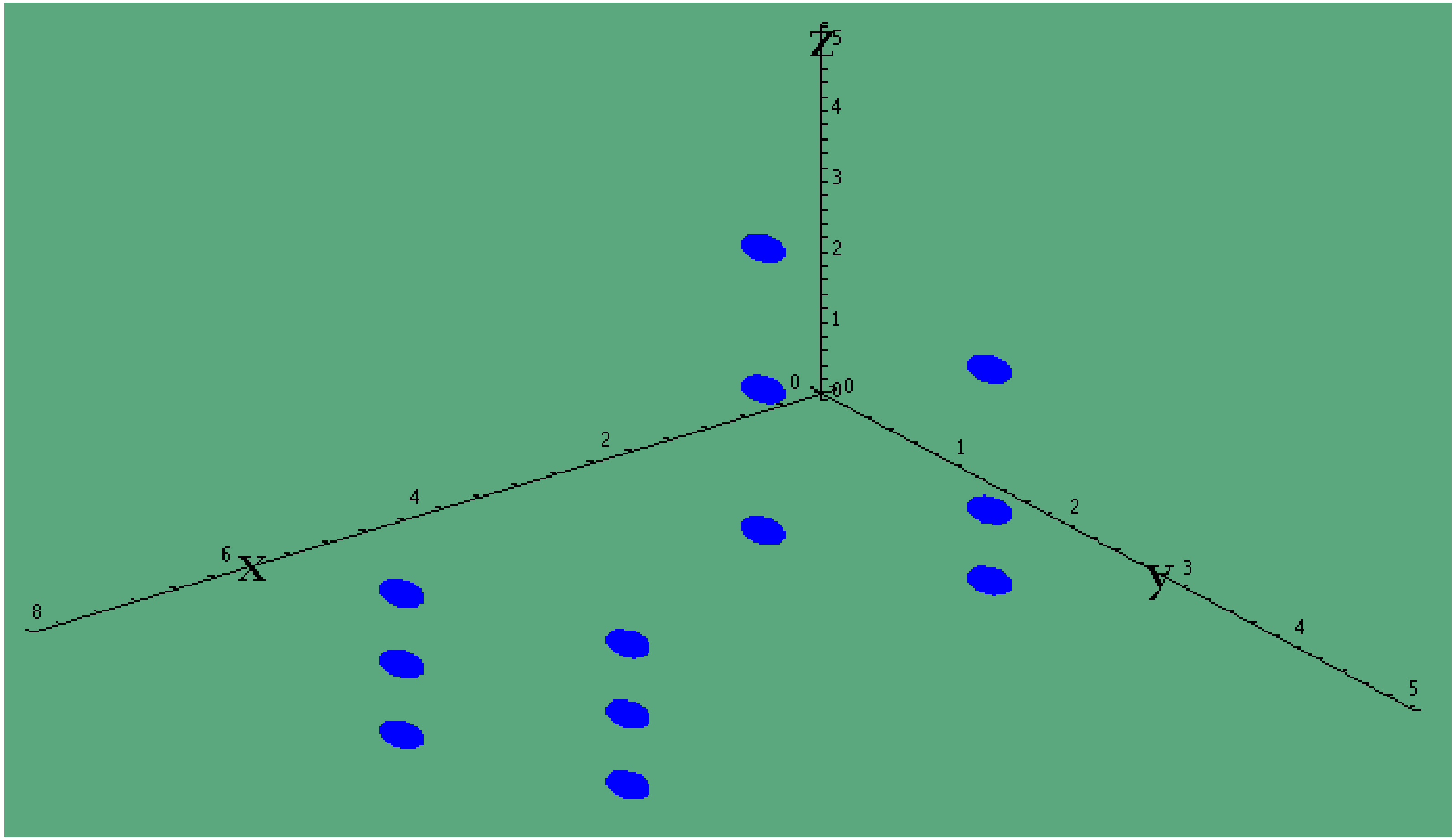
In the end, we obtain a family of pairwise disjoint, equiprojectable varieties, whose reunion equals V. This is the **equiprojectable decomposition** of V.

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

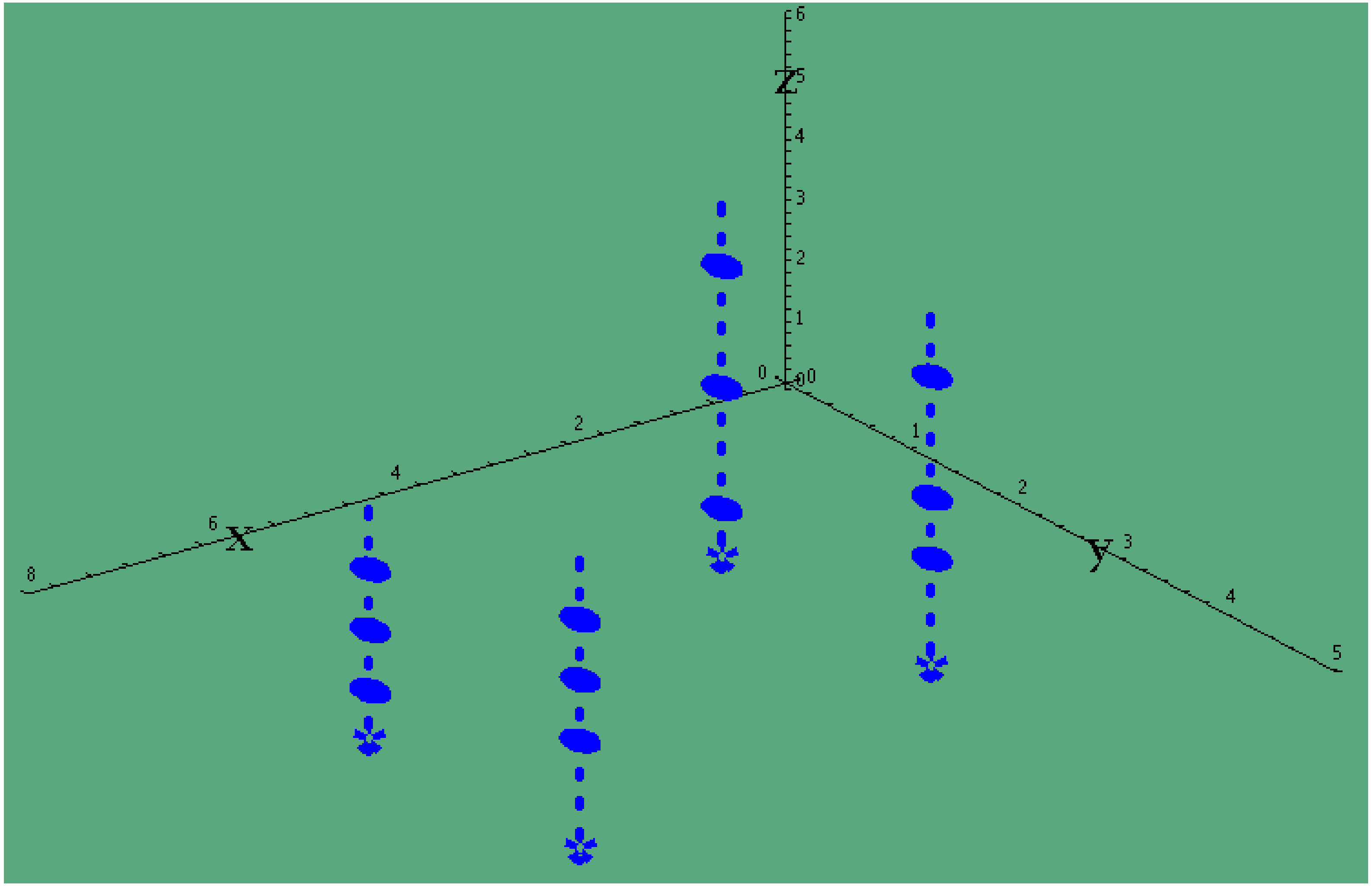
$$V(F) = V(T^1) \cup \cdots \cup V(T^s) \text{ and } i \neq j \Rightarrow V(T^i) \cap V(T^j) = \varnothing.$$

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

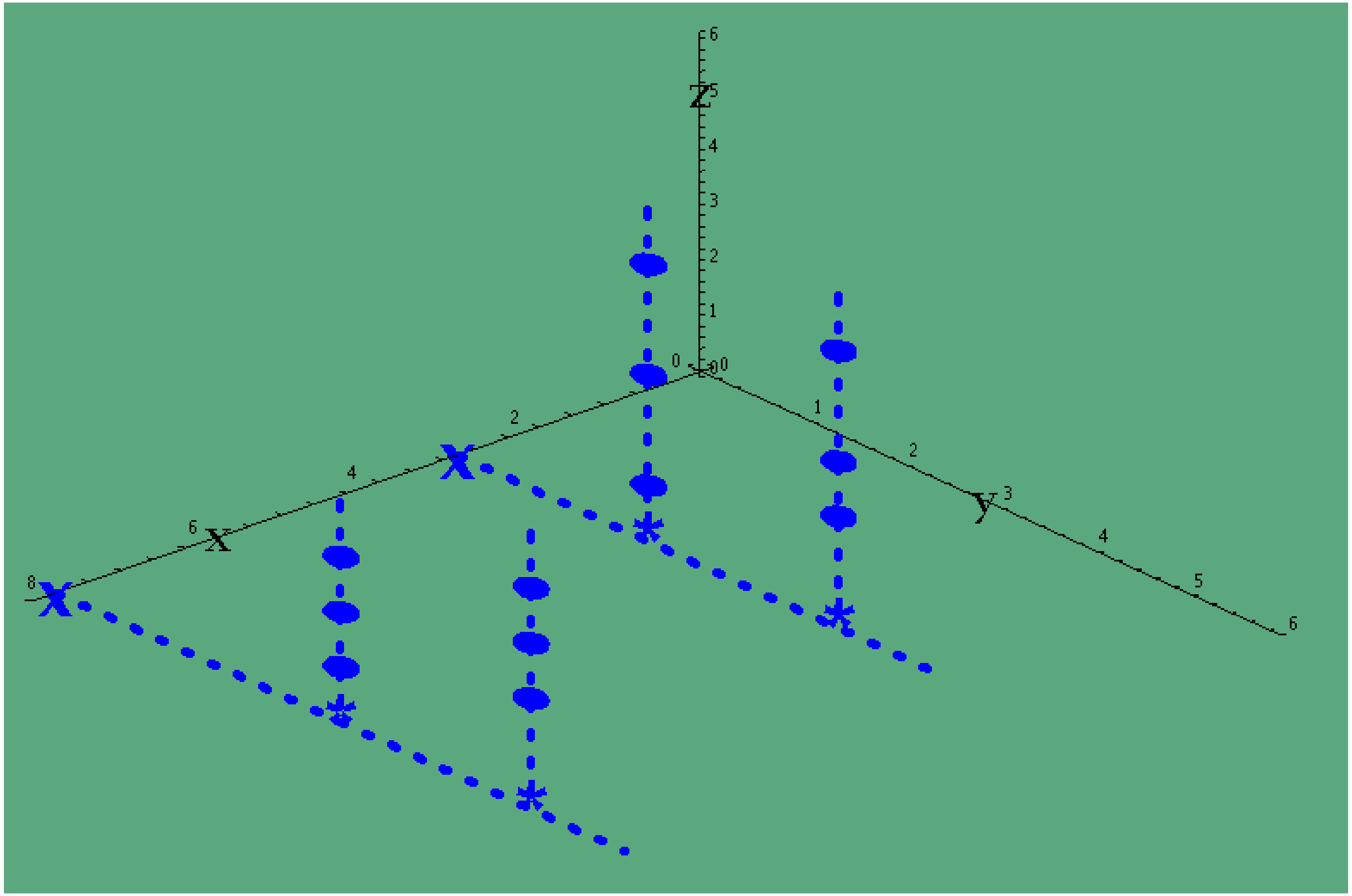
Equiprojectable variety definition (1/3)



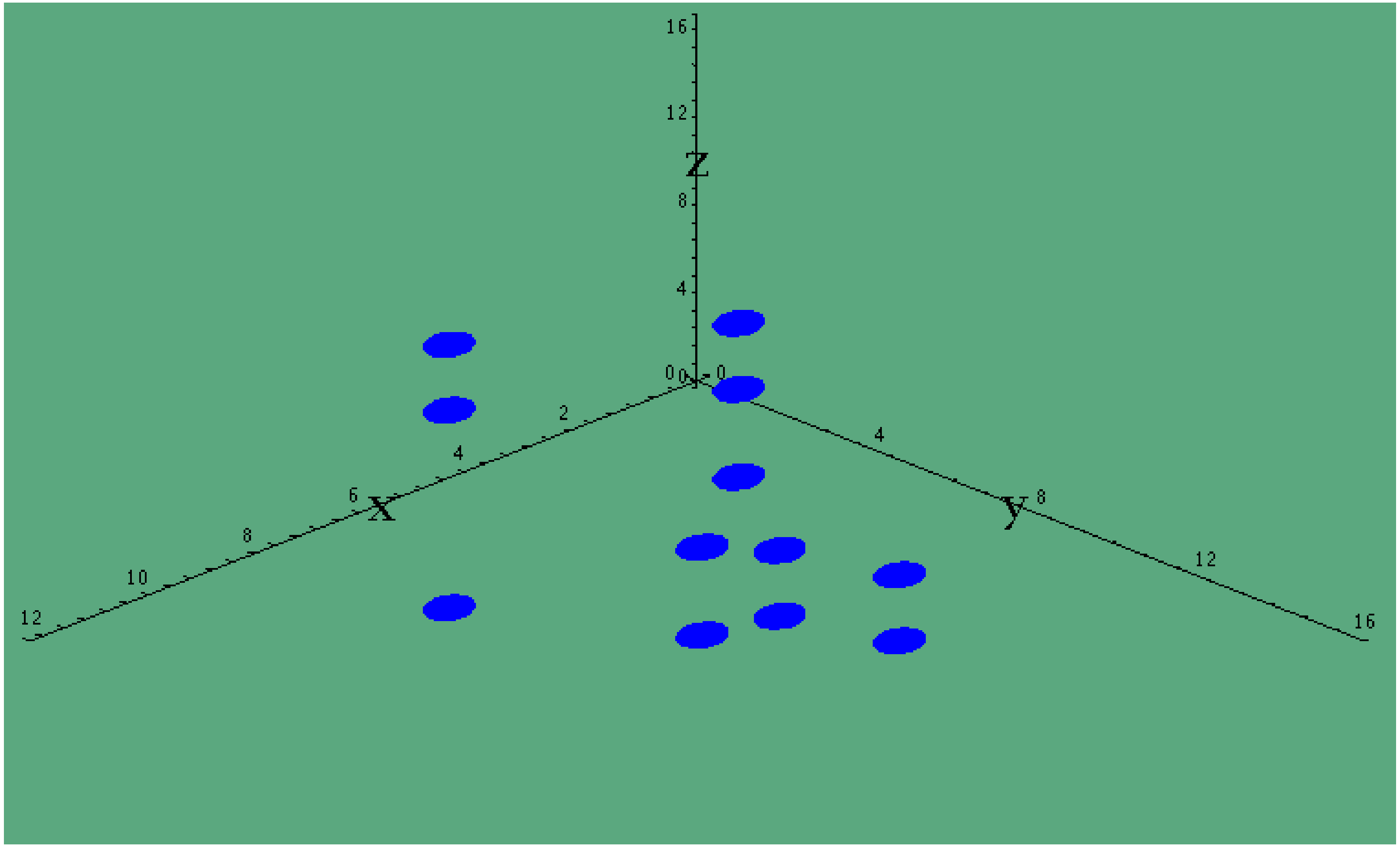
Equiprojectable variety definition (2/3)



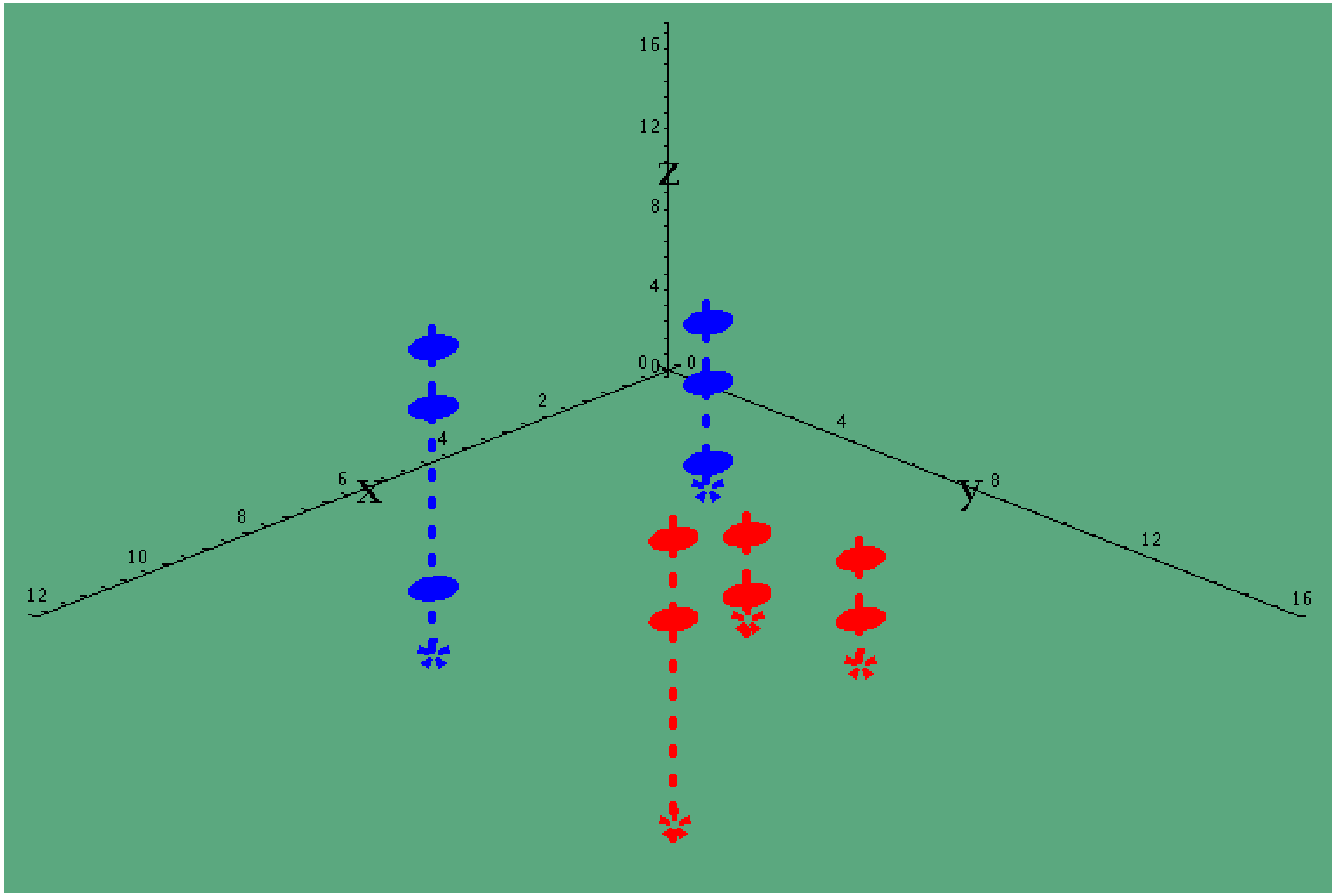
Equiprojectable variety definition (3/3)



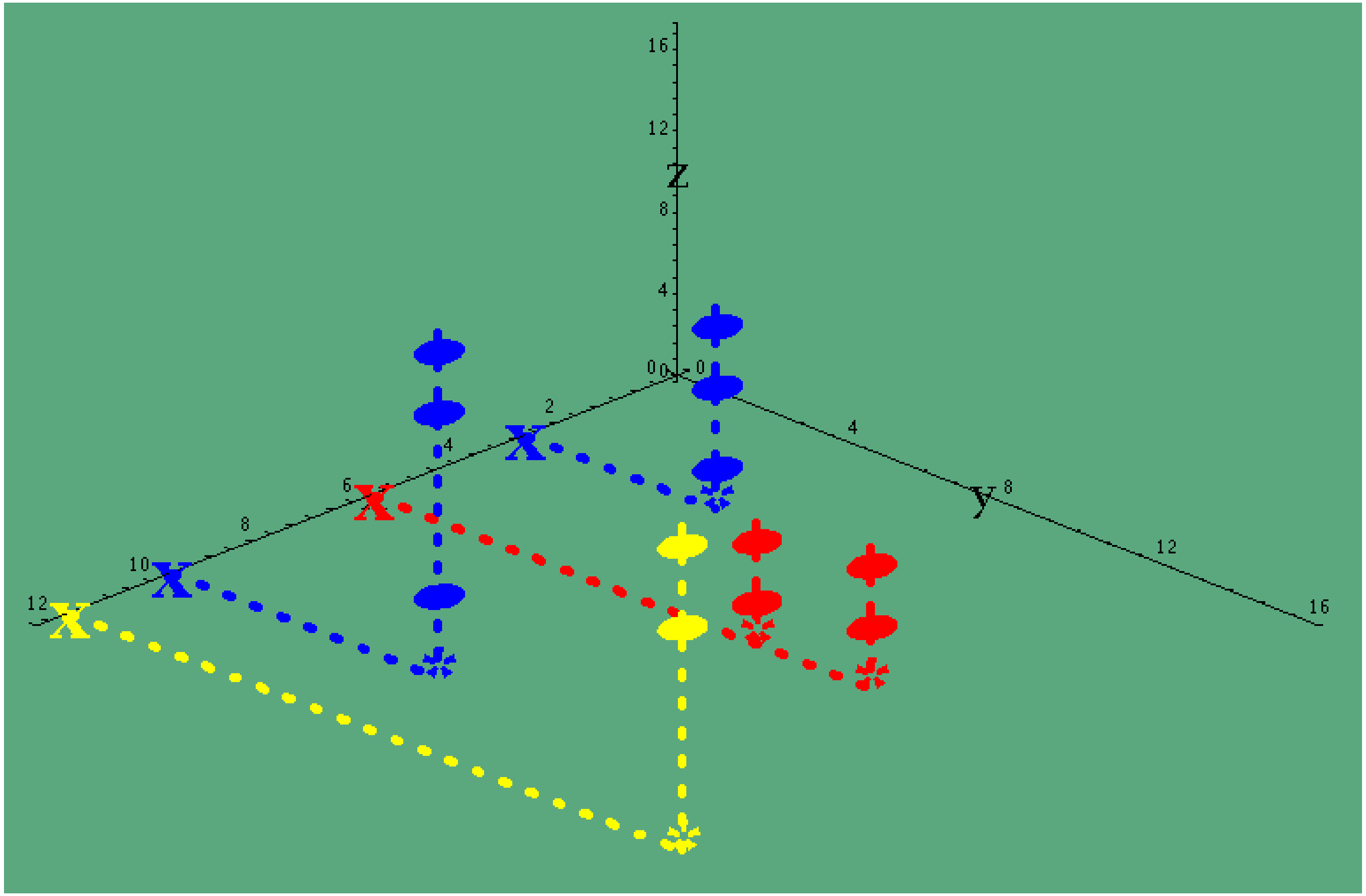
Equiprojectable decomposition definition (1/3)



Equiprojectable decomposition definition (2/3)



Equiprojectable decomposition definition (3/3)



From triangular to equiprojectable decomposition

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

PROPOSITION. We compute from Δ 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 $\triangleright$ We proceed into two steps:

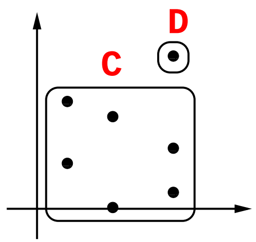
- split: reducing what we call **critical pairs** by means of **GCD** computations modulo Lazard triangular sets,
- merge: reducing what we call **solvable pairs** by means of **CRT** computations modulo Lazard triangular sets.

$\triangleleft$

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

$$C \left| \begin{array}{l} C_2 = y^2 + 6yx^2 + 2y + x \\ C_1 = x^3 + 6x^2 + 5x + 2 \end{array} \right. , \quad D \left| \begin{array}{l} D_2 = y + 6 \\ D_1 = x + 6 \end{array} \right.$$

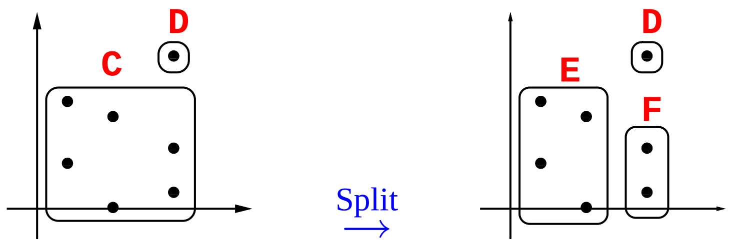


Example: *split+merge* modulo 7

$$C \left| \begin{array}{l} C_2 = y^2 + 6yx^2 + 2y + x \\ C_1 = x^3 + 6x^2 + 5x + 2 \end{array} \right. , \quad D \left| \begin{array}{l} D_2 = y + 6 \\ D_1 = x + 6 \end{array} \right.$$

$\downarrow$ Split C : GCD $\downarrow$

$$E \left| \begin{array}{l} {C_2}' = y^2 + x \\ {C_1}' = x^2 + 5 \end{array} \right. , \quad F \left| \begin{array}{l} C_2'' = y^2 + y + 1 \\ C_1'' = x + 6 \end{array} \right. , \quad D \left| \begin{array}{l} D_2 = y + 6 \\ D_1 = x + 6 \end{array} \right.$$



Example: *split+merge* modulo 7

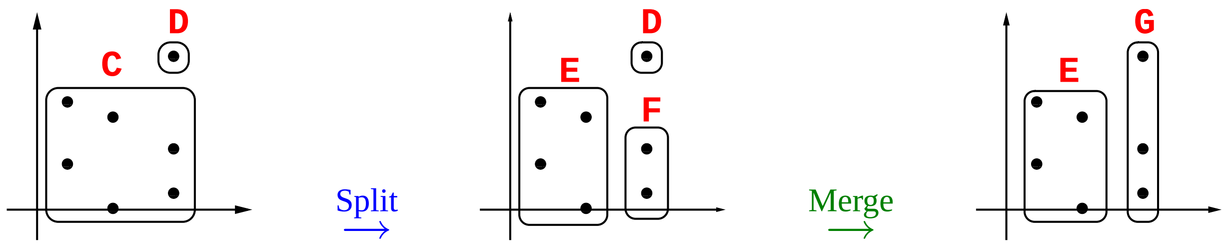
$$C \left| \begin{array}{l} C_2 = y^2 + 6yx^2 + 2y + x \\ C_1 = x^3 + 6x^2 + 5x + 2 \end{array} \right. , \quad D \left| \begin{array}{l} D_2 = y + 6 \\ D_1 = x + 6 \end{array} \right.$$

$\downarrow$ Split C : GCD $\downarrow$

$$E \left| \begin{array}{l} {C_2}' = y^2 + x \\ {C_1}' = x^2 + 5 \end{array} \right. , \quad F \left| \begin{array}{l} C_2'' = y^2 + y + 1 \\ C_1'' = x + 6 \end{array} \right. , \quad D \left| \begin{array}{l} D_2 = y + 6 \\ D_1 = x + 6 \end{array} \right.$$

$\downarrow$ Merge F and D : CRT $\downarrow$

$$E \left| \begin{array}{l} C_2' = y^2 + x \\ C_1' = x^2 + 5 \end{array} \right. , \quad G \left| \begin{array}{l} G_2 = y^3 + 6 \\ G_1 = x + 6 \end{array} \right.$$

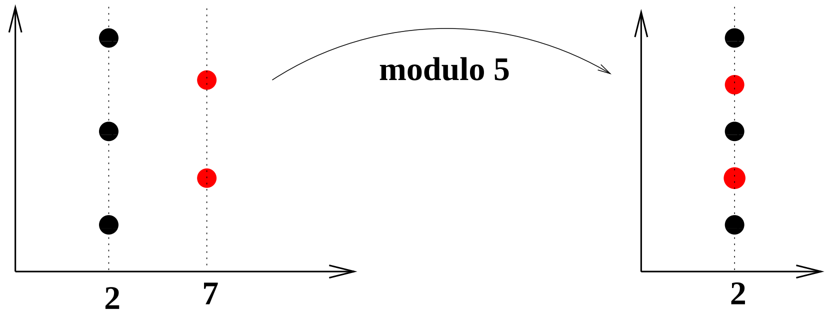


Specialization properties: sketch

Oversimplified case: Assume all points $V(F)$ are in $\mathbb{Q}^n$. Let $p \in Z$ 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.



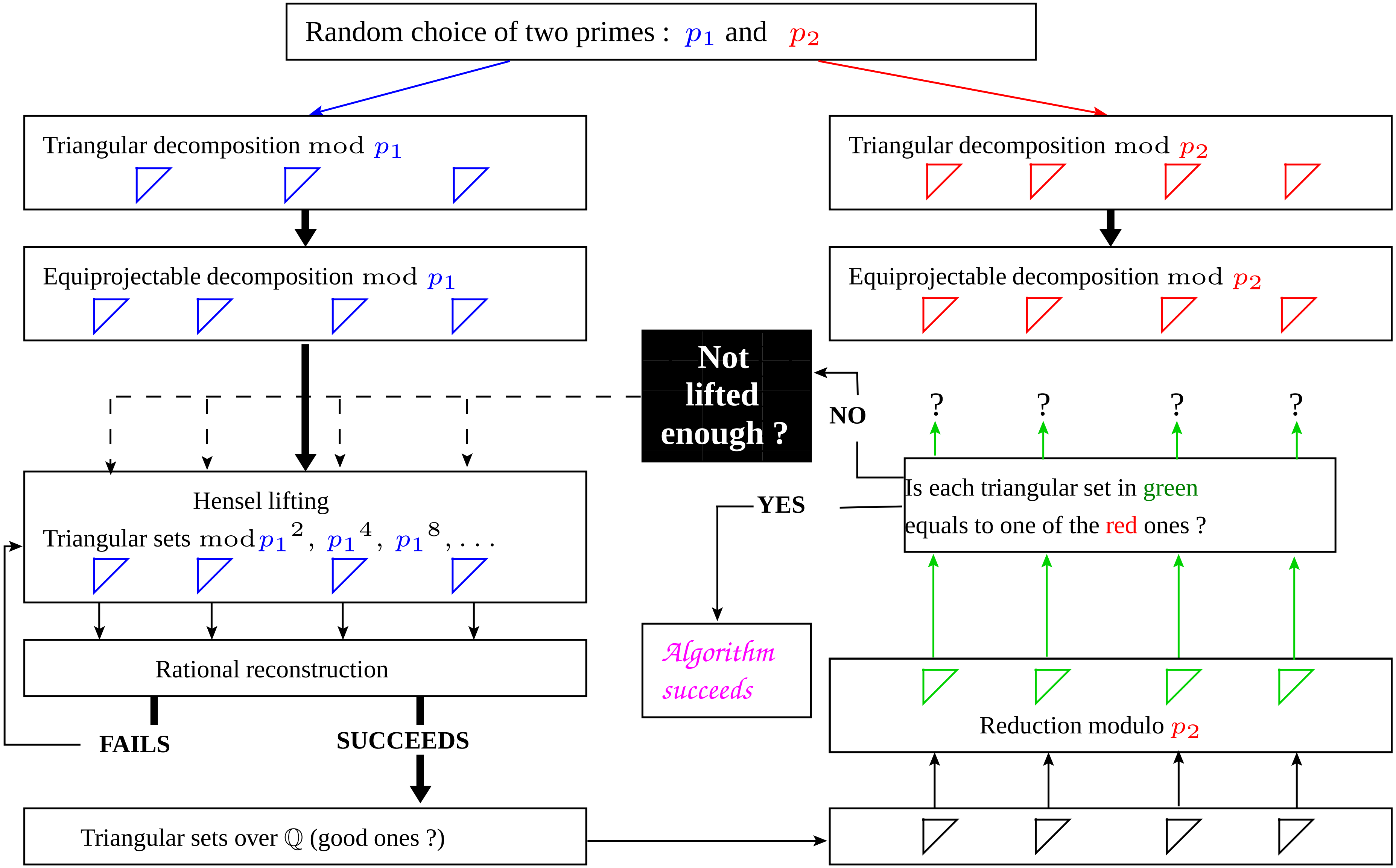
General case: Under *similar* assumptions, every coordinate of every point of V lies in a direct sum $Z_p \oplus \cdots \oplus Z_p$ where Z_p is the ring of p-adic integers.

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 $p \nmid A$, then the equiprojectable decomposition specializes well mod p.

A probabilistic algorithm



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 Gr. basis of $\mathcal{I}$ w.r.t. $x_1, \ldots, x_n$.
- 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 $1 \leq i \leq n$,
- 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) $h_i := \mathrm{lc}(C_i, x_i)$ 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 $\triangleright$ 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

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

$\triangleleft$

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
  - 1147412794656925600746886196713882259945463225340477687005119947622261926900489014476185343948467105712
    1771260505008202862102854051702189834144507041921400912212854357946960933195335641858396501896935850288
    6993494167255643877060419555161219397297718310661681373013610473433161675295215097739765468198629739368
    4698033057372004369628572309403845943516901456096080945793282669881686485390936578666175235967213427460
    3624577949980872265230642371971182386814553874346853792171708143077531532237850295577589142064921396560
    1825588409831441292570286016853843732976447711290921201282663597873225040956392206905741146687704996955
    1513841784606672511835822265889987889624672252665122778133883969304602062740935497619894651442745458136
    4439433587390347755862238203761990339960554351301919398485081103440153976743524458297586182708756446851
    2398894638319738859704396544591592407731579470289955844307815442694326841805687077917675761917871130339
    2738339662798997128827712967353520807578712156161195412624338459316853569080754130154719452119622862823
    1523713394865899777869339534459634212652323168810285894102829514014960747795605184806645733349720228435
    4856391347410632777061560951110896275634940887029344611985724298328089928128704127659741470395314284711
    1827709014752692114620308283759341810040325817543392095814567632394138225663551675690804005364380128824
    3091912961309507299736685953680211256352496932486587513812792390171704032245316310904516304034569023010
    6838688396641645490945090868618366582490420637673970853279869471018348887091817749546675847593376908651
    7481568238007075259306520563109135581811542014656070637988617107330377650533573060376552912562646797163
    1546080455275692923387543379737978438247137018552307587682361742927801505920906300566302345120640667639
    1246953858195786422852752879754020156689945022004770650946405155986011151301751670637053436652391932136
    6615265985718824532042488802422296773818429373789169917697659429318767468848486488142387103357676506542
    5735987149201249564746107188031507033768129784171791787755761173195000000778571292329588891041934271149
    2397871086492879872864247556074824548646907868278411846969762861333860575738177220989978593224804467512

- 5737063973284628003734430983569411299727316126702388435025599738111309634502445072380926719742335528561
1771260505008202862102854051702189834144507041921400912212854357946960933195335641858396501896935850288
6993494167255643877060419555161219397297718310661681373013610473433161675295215097739765468198629739368
4698033057372004369628572309403845943516901456096080945793282669881686485390936578666175235967213427460
3624577949980872265230642371971182386814553874346853792171708143077531532237850295577589142064921396560
1825588409831441292570286016853843732976447711290921201282663597873225040956392206905741146687704996955
1513841784606672511835822265889987889624672252665122778133883969304602062740935497619894651442745458136
4439433587390347755862238203761990339960554351301919398485081103440153976743524458297586182708756446851
2398894638319738859704396544591592407731579470289955844307815442694326841805687077917675761917871130339
2738339662798997128827712967353520807578712156161195412624338459316853569080754130154719452119622862823
1523713394865899777869339534459634212652323168810285894102829514014960747795605184806645733349720228435
4856391347410632777061560951110896275634940887029344611985724298328089928128704127659741470395314284711
1827709014752692114620308283759341810040325817543392095814567632394138225663551675690804005364380128824
3091912961309507299736685953680211256352496932486587513812792390171704032245316310904516304034569023010
6838688396641645490945090868618366582490420637673970853279869471018348887091817749546675847593376908651
7481568238007075259306520563109135581811542014656070637988617107330377650533573060376552912562646797163
1546080455275692923387543379737978438247137018552307587682361742927801505920906300566302345120640667639
1246953858195786422852752879754020156689945022004770650946405155986011151301751670637053436652391932136
6615265985718824532042488802422296773818429373789169917697659429318767468848486488142387103357676506542
1076824083378438988323795537904265959186342530596647269838564916309633723873780051337828700401257411673
2397871086492879872864247556074824548646907868278411846969762861333860575738177220989978593224804467512
- $3125z^{20} - 9375z^{16} - 40000000000z^{15} - 2015999988750z^{12} - 1560000000000z^{11} + 1920000000000000000z^{10} - 1216512535680000 6750z^{8} - 1474560223200000000z^{7} - 6528000000000000000z^{6} - 409600000000000000000000z^{5} - 1698690863923334783999 7975z^{4} - 14155767152640302400000000z^{3} - 589823873280000000000000z^{2} - 122880000000000000000000z - 619530361923198287873244 1600243$

- Applying the transformation of Dahan and Schost leads to 1787 characters.
  - $(20z^{19} + (-48z^{15}) + (-192000000z^{14}) + (-(38707199784/5)z^{11}) + (-5491200000z^{10}) + 614400000000000z^{9} + (-(778568022835200432/25)z^{7}) + (-3303014899968 0000z^{6}) + (-125337600000000000z^{5}) + (-655360000000000000000z^{4}) + (-(27179053822773356543996 76/125)z^{3}) + (-1358953646653469030 4000z^{2}) + (-3774872788992000000000z) - 393216000000000000000)x +$

$3200000z^{15} + 161280000z^{12} + 124800000z^{11} + (-30720000000000z^{10}) + 1946419628544000z^{8} + 2359296178560000z^{7} + 1044480000000000z^{6} + 98304000000000000000z^{5} + 40768598782772278272 00z^{4} + 33973848244224241920 00z^{3} + 14155773972480000000 0z^{2} + 29491200000000000000 0z + 19824969950796567805 96195328$

- $(20z^{19} + (-48z^{15}) + (-192000000z^{14}) + (-(38707199784/5)z^{11}) + (-5491200000z^{10}) + 614400000000000z^{9} + (-(778568022835200432/25)z^{7}) + (-3303014899968 0000z^{6}) + (-12533760000000000z^{5}) + (-65536000000000000000 0z^{4}) + (-(27179053822773356543 99676/125)z^{3}) + (-13589536466534690304 000z^{2}) + (-37748727889920000000 0z) - 39321600000000000000 00)y + (-12z^{1}6) + (-(9676799856/5)z^{12}) + (-1996800000z^{11}) + (-(194642219980800648/25)z^{8}) + (-14155781713920000z^{7}) + (-8355840000000000z^{6}) + (-(67947183341627304959 8704/125)z^{4}) + (-90596768219147612160 00z^{3}) + (-56623071559680000000 00z^{2}) + (-15728640000000000000 00z) + (-20384322217574773248 00972/625)$

- $z^{2}0 + (-3z^{1}6) + (-12800000z^{15}) + (-(3225599982/5)z^{12}) + (-499200000z^{11}) + 61440000000000z^{10} + (-(97321002854400054/25)z^{8}) + (-4718592714240000z^{7}) + (-2088960000000000z^{6}) + (-13107200000000000000 0z^{5}) + (-(67947634556933391359 9919/125)z^{4}) + (-45298454888448967680 00z^{3}) + (-18874363944960000000 00z^{2}) + (-39321600000000000000 0z) + (-61953036192319828787 32441600243/3125)$

• There is even hope to do better! Here's the regular chain produced by the Triade algorithm, counting 963 characters.

- $20x - 1y + z$

- $\Big((4375z^{12} + 52800011625z^{8} + 32000000000z^{7} + 110591902080002925z^{4} + 61439980800000000z^{3} + 1280000000000000$ $1875z^{13} - 9600010125z^{9} + 2000000000z^{8} - 7372714752004545z^{5} + 30720002400000000z^{4} + 12800000000000000z^{3} - 22118403456000135z + 2359296368640014400 0000$

- $3125z^{20} - 9375z^{16} - 40000000000z^{15} - 2015999988750z^{12} - 1560000000000z^{11} + 19200000000000000z^{10} - 1216512535680000675 0z^{8} - 14745602232000000000 z^{7} - 65280000000000000000 z^{6} - 40960000000000000000 00000z^{5} - 16986908639233347839 997975z^{4} - 14155767152640302400 000000z^{3} - 58982387328000000000 0000z^{2} - 12288000000000000000 00000z - 61953036192319828787 32441600243$

Gröbner bases (I)

NOTATION. Fix $\leq$ a term order on $M = \{x_1^{i_1} \dots x_n^{i_n} \mid i_j \geq 0\}$, 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 $f \in \mathbb{K}[x_1, \dots, x_n]$, $f \neq 0$, the **leading (= greatest) monomial** w.r.t. $\leq$ in f is denoted $\boxed{\operatorname{lm} f}$ and its coefficient in f is the **leading coefficient** of f, denoted $\operatorname{lc} f$.

For $F \subset \mathbb{K}[X] \setminus \{0\}$, we write $\boxed{\operatorname{lm} F = \{\operatorname{lm} f \mid f \in F\}.}$

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

NOTATION. If f is not reduced w.r.t. one of the polynomials $b_1, \dots, b_k \in \mathbb{K}[X]$, then the operation $\operatorname{Reduce}(f, \{b_1, \dots, b_k\})$

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

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

(3) and returns r.

Gröbner bases (II)

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

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 $\mathrm{lc} b = 1$.

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

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

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 $f \in \mathbb{K}[x_1, \ldots, x_n]$

$$f \in \mathcal{I} \iff \mathrm{Reduce}(f, B) = 0.$$

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

(R) $A := \mathrm{S\_Polynomials}(B) \cup F$;

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

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

until $R = \emptyset$

return B

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

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

and $\mathrm{S\_Polynomials}(F)$ 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 $g \notin \mathbb{K}$.

mvar(g)**:** the greatest variable in g is the **leader** or **main variable** of g,

init(g)**:** the leading coefficient of g w.r.t. mvar(g) is the **initial** of g,

mdeg(g)**:** the degree of g w.r.t. mvar(g),

rank(g) $= v^d$ where $v = \mathrm{mvar}(g)$ and $d = \mathrm{mdeg}(g)$,

pdivide(f, g) $= (q, r)$ with $q, r \in \mathbb{K}[X]$, $\deg(r, v_g) < d_g$ and $h_g^e f = qg + r$ where $h_g = \mathrm{init}(g)$, $e = \max(\deg(f, v) - d_g + 1, 0)$, $v_g = \mathrm{mvar}(g)$ and $d_g = \mathrm{mdeg}(g)$,

prem(f, g) $= r$ if pdivide$(f, g) = (q, r)$. $f \in \mathbb{K}[X]$ is said **(pseudo-)reduced** w.r.t. $g \in \mathbb{K}[X] \notin \mathbb{K}$ if $\deg(f, \mathrm{mvar}(g)) < \mathrm{mdeg}(g)$.

EXAMPLE.

Assume $n \geq 3$. If $p = x_1 x_3^2 - 2x_2 x_3 + 1$, then we have mvar$(p) = x_3$, mdeg$(p) = 2$, init$(p) = x_1$ and 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 $f \neq g \;\Rightarrow\; \mathrm{mvar}(f) \neq \mathrm{mvar}(g)$,

- **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 (I)

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 (II)

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

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

• 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.

Relations between Gröbner bases and regular chains

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

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

$$\cup \mathbf{W} \begin{cases} x \\ (hd - eg)\, y - id + fg \\ fb - ce \\ ie - fh \end{cases} \cup \mathbf{W} \begin{cases} ax + by - c \\ hy - i \\ d \\ g \\ ie - fh \end{cases} \cup \cdots$$

Lex base (P):

$$\begin{cases} xa + yb - c & xd + ye - f & \boxed{xg + yh - i} \\ yae - ydb - af + dc & yah - ygb - ai + gc & \boxed{ydh - yge - di + gf} \\ \boxed{aei - ahf - dbi + dhc + gbf - gec} & & \end{cases}$$

- For more details see **(Aubry, Lazard & M^3, 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 $\boxed{W(T) = V(T) \setminus V(\{h_T\})}$ 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 $W(T) = \varnothing = V(T)$.

Characteristic sets (I)

NOTATION. If $f, g \notin \mathbb{K}$, we write $\operatorname{rank}(f) < \operatorname{rank}(g)$ if $\operatorname{mvar}(f) < \operatorname{mvar}(g)$ or, $\operatorname{mvar}(f) = \operatorname{mvar}(g)$ and $\operatorname{mdeg}(f) < \operatorname{mdeg}(g)$. For $F \subset \mathbb{K}[X] \setminus \mathbb{K}$, we write $\boxed{\operatorname{rank}(F) = \{\operatorname{rank}(f) \mid f \in F\}.}$

DEFINITION. For A, B auto-reduced sets, we write $A \leq B$ whenever

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

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 $\operatorname{prem}(f, B) = 0$ 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 $V(F) = \varnothing$,
- If $\text{prem}(F, B) = \{0\}$ then

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

PROOF $\triangleright$ 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. $\triangleleft$

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.

repeat

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

(R) $A := F \setminus B$;

$R := \mathrm{prem}(A, B)$

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

until $R = \emptyset$

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 $p \notin \mathcal{P}$, 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, $W(T) \neq \varnothing$.

Reduction to dimension zero (I)

THEOREM. **(Chou & Gao, 1991), (Kalkbrener, 1991), (Aubry, 1999), (Boulier, Lemaire & $\mathbf{M}^3$, 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 (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 $\mathrm{Sat}(T_0)$ 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 $\overline{W(T)}$.

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

$$\mathrm{Sat}(C) = \{p \mid \mathrm{prem}(p, C) = 0\}$$

$$\Updownarrow$$

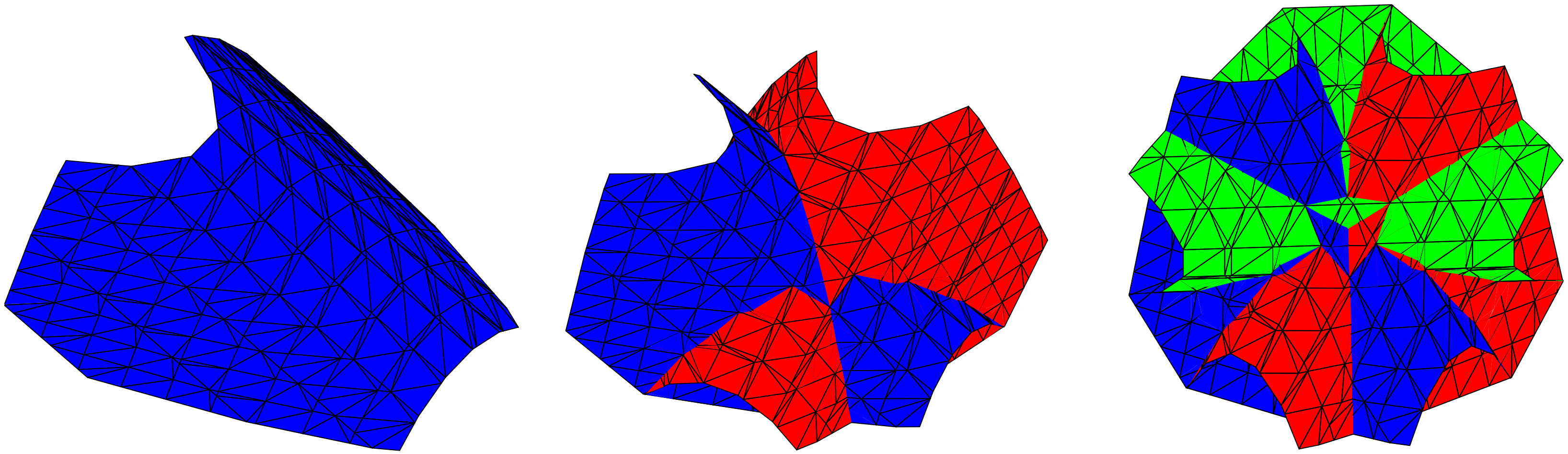
$$C \text{ regular chain}$$

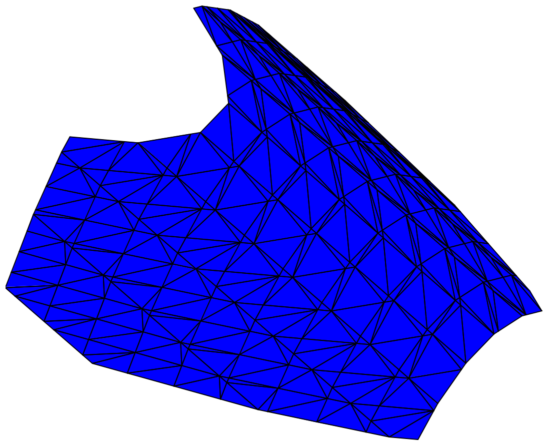
$$\Updownarrow$$

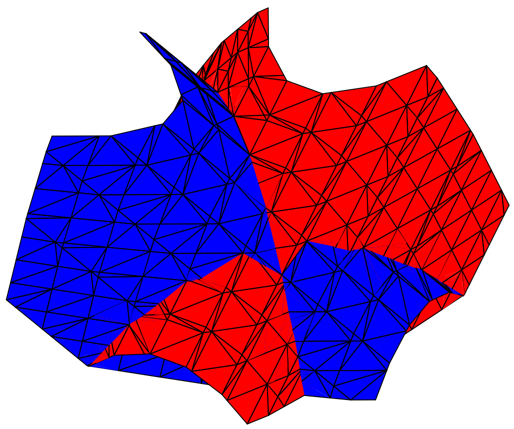
$$C \text{ characteristic set of } \mathrm{Sat}(C)$$

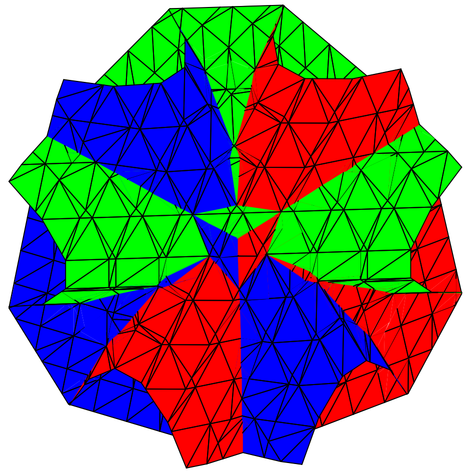
Incremental triangular decompositions: a geometrical approach

$$\left\{ x^2 + y + z = 1 \right. \quad \left\{ \begin{array}{l} x^2 + y + z = 1 \\ x + y^2 + z = 1 \end{array} \right. \quad \left\{ \begin{array}{l} x^2 + y + z = 1 \\ x + y^2 + z = 1 \\ x + y + z^2 = 1 \end{array} \right.$$









$$\left\{ x^2 + y + z = 1 \right.$$

$$\begin{cases} x + y^2 + z = 1 \\ y^4 + (2z-2)y^2 + y - z + z^2 = 0 \end{cases}$$

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

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

Triade: a task manager algorithm (I)

DEFINITION. A **task** is any $[F, T]$ where $F, T \subset \mathbb{K}[X]$ with T regular chain. It is **solved** iff $F = \emptyset$ and **unsolved**, otherwise.

By *solving* a task, we mean computing regular chains $T_1, \ldots, T_\ell$ such that:

$$V(F) \cap W(T) \subseteq \cup_{i=1}^{\ell} W(T_i) \subseteq V(F) \cap \overline{W(T)}.$$

DEFINITION. The tasks $[F_1, T_1], \ldots, [F_d, T_d]$ form a **delayed split** of the task $[F, T]$ and we write $[F, T] \longmapsto_D [F_1, T_1], \ldots, [F_d, T_d]$ if we have:

(D_1) $Z(F_i, T_i) \prec Z(F, T)$,

(D_2) $Z(F, T) \subseteq Z(F_1, T_1) \cup \cdots \cup Z(F_d, T_d)$,

(D_3) $\mathrm{Sat}(T) \subseteq \mathrm{Sat}(T_i)$,

(D_4) $F_i \neq \emptyset \implies F \subseteq F_i$,

(D_5) $F_i = \emptyset \implies W(T_i) \subseteq V(F)$.

Triade: a task manager algorithm (II)

<u>REMARK.</u> Property (D_1) means that each "output" task $[F_i, T_i]$ is *more solved* than the "input" one $[F, T]$. Properties (D_2) to (D_5) imply:

$$V(F) \cap W(T) \subseteq \cup_{i=1}^{d} Z(F_i, T_i) \subseteq V(F) \cap \overline{W(T)}.$$

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

Output: $\mathcal{T}$ a triangular decomposition of $V(F)$ by means of regular chains.

$ToDo := [[F, \emptyset]; \mathcal{T} := [\,]$
repeat
  if $ToDo = \emptyset$ **then break**
(S) $Tasks := \mathrm{Select}(ToDo)$
(R) $Results := \mathrm{LazySolve}(Tasks)$
(U) $(ToDo, \mathcal{T}) := \mathrm{Update}(Results, ToDo, \mathcal{T})$
return $\mathcal{T}$

Polynomial GCDs modulo regular chains

DEFINITION. Let $1 \leq k < n$. Let $T \subset \mathbb{K}[x_1, \ldots, x_k]$ be a regular chain. Let $p, t \in \mathbb{K}[x_1, \ldots, x_n]$ non-constant, with $v := \mathrm{mvar}(p) = \mathrm{mvar}(t) > x_k$. Assume that $T \cup \{p\}$ and $T \cup \{t\}$ are regular chains.

A polynomial $g \in \mathbb{K}[x_1, \ldots, x_n]$ is a **GCD** of p and t w.r.t. T if the following properties hold:

(G_1) g belongs to the ideal generated by p, t and $\mathrm{Sat}(T)$,

(G_2) the leading coefficient h_g of g w.r.t. v is regular w.r.t. $\mathrm{Sat}(T)$,

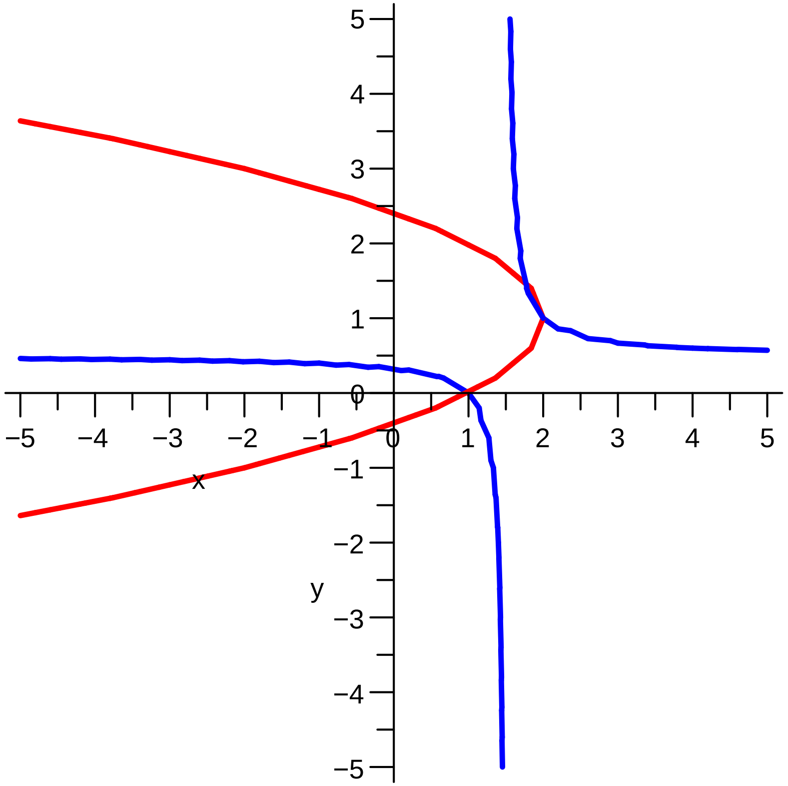
(G_3) if $\mathrm{mvar}(g) = v$ then p and t belong to $\mathrm{Sat}(T \cup \{g\})$.

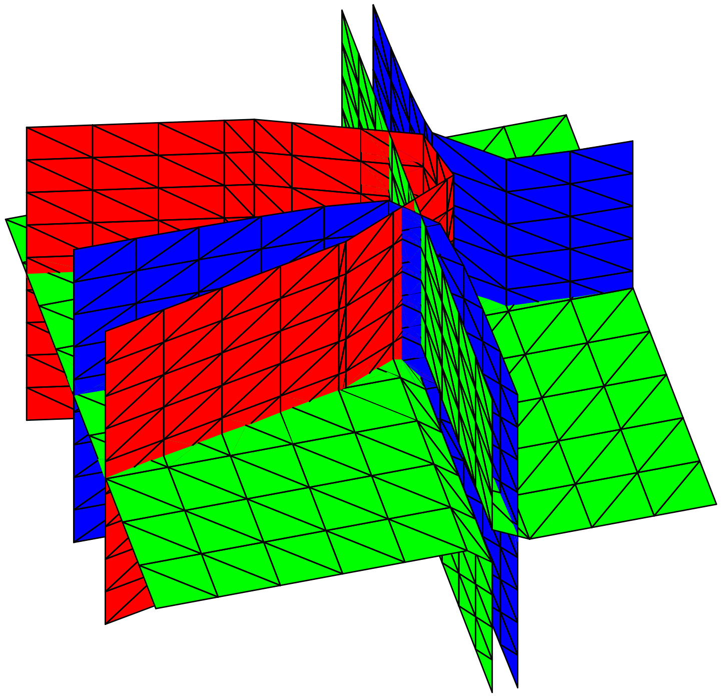
THEOREM.**(M^3 , 2000)** If g is a GCD of p and t w.r.t. T and $\mathrm{mvar}(g) = v$, then

$$[[\{p\}, T \cup \{t\}] \longmapsto_D [\emptyset, T \cup \{g\}], \; [\{h_g, p\}, T \cup \{t\}].$$

COROLLARY. Given $F \subset \mathbb{K}[X]$ and a regular chain $T \subset \mathbb{K}[X]$, one can compute a delayed split $[F_1, T_1], \ldots, [F_d, T_d]$ of $[F, T]$ such that, for all $1 \leq i \leq d$ we have $F_i = \varnothing$ iff $|T_i|$ is minimum (among $|T_1|, \ldots, |T_d|$)

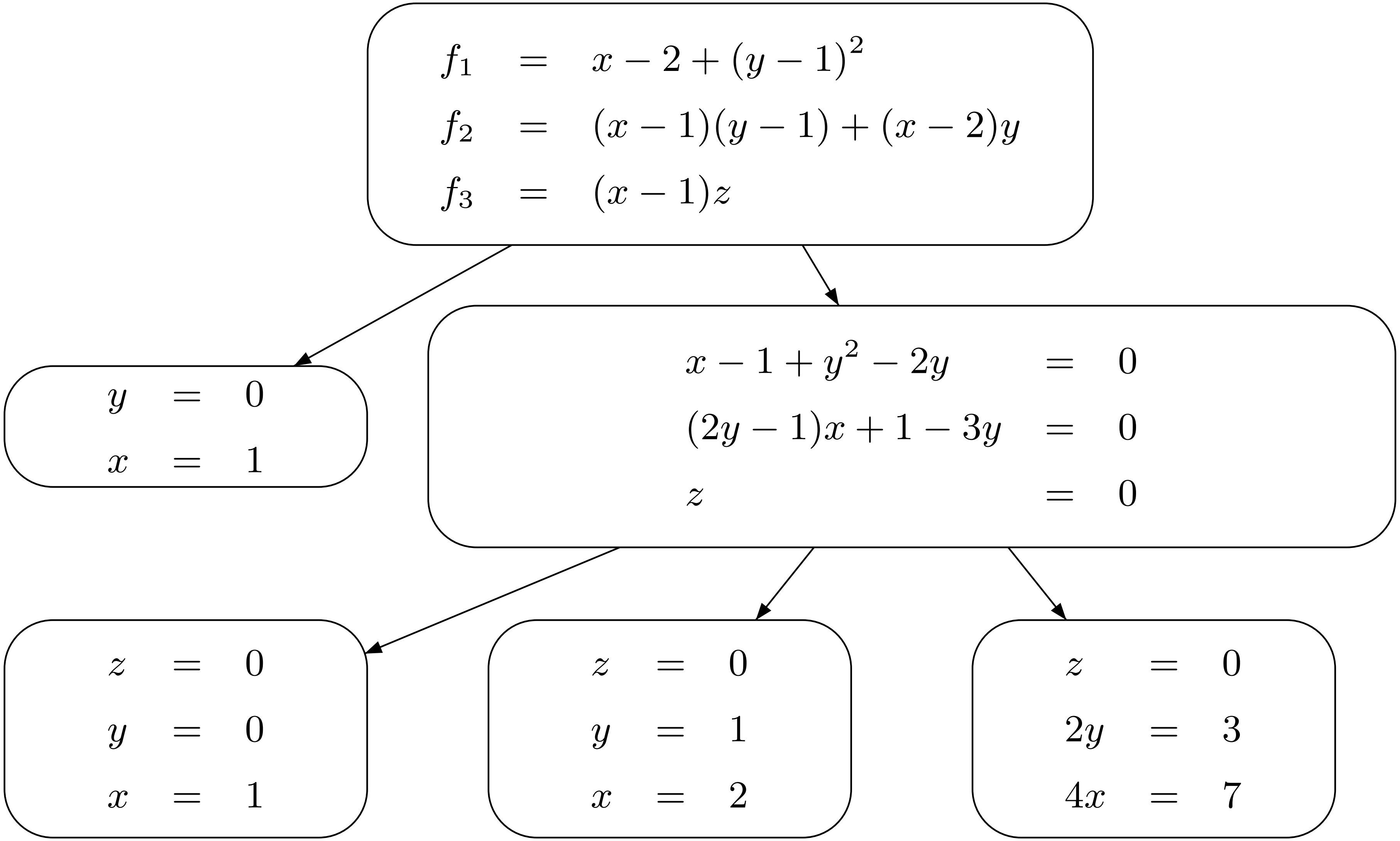
Difficulty 1: redundant and irregular tasks





The red and blue surfaces intersect on the line $x - 1 = y = 0$ contained in the green plane $x = 1$. With the other green plane $z = 0$, they intersect at $(2, 1, 0)$, $(\frac{7}{4}, \frac{3}{2}, 0)$ but also at $x - 1 = y = z = 0$, which is redundant.

Initial task $[\{f_1, f_2, f_3\}, \emptyset]$



Difficulty 2: load balancing

• How do splits occur during decompositions? Gien a polynomial ideal $\mathcal{I}$ and polynomials p, a, b, there are two rules:

- $\mathcal{I} \longmapsto (\mathcal{I} + p, \mathcal{I} : p^{\infty})$.
- $\mathcal{I} + \langle a\, b \rangle \longmapsto (\mathcal{I} + \langle a \rangle, \mathcal{I} + \langle b \rangle)$.

• The second one is more likely to **split computations evenly**. But geometrically, it means that a component is **reducible**.

• Unfortunately, most polynomial systems $F \subseteq \mathbb{Q}[X]$ (both in theory and practice) are **equiprojectable**, that is they can be represented by a single regular chain.

• However, for $F \subseteq Z/pZ[X]$ where p prime, the second rule is more likely to be used.

Key solutions

• We solve completely only in the cases where dimension does not drop and solve lazily the other cases.

$\Rightarrow$ **Computations in lower dimension are delayed toward the end** of the solving process.

• For solving $F \subseteq \mathbb{Q}[X]$ we use modular methods (Dahan, M^3, Schost, Wu, Xie, 2005)

- For p big enough, a triangular decomposition of $V(F)$ can be **reconstructed (= merged + lifted)** from one of $V(F \mod p)$.
- The reconstruction is cheap (comparing to the decomposition phasis).
- This modular approach consumes less resources than the direct one.

A parallel scheme

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

Output: $\mathcal{T}$ a triangular decomposition of $V(F)$ by means of regular chains.

$ToDo$:= $[[F, \emptyset]$; $\mathcal{T}$:= [ ]; d := n;

repeat

if $ToDo = \emptyset$ **then break**

(1) **let** V be all tasks which can produce solved tasks of diemnsion d

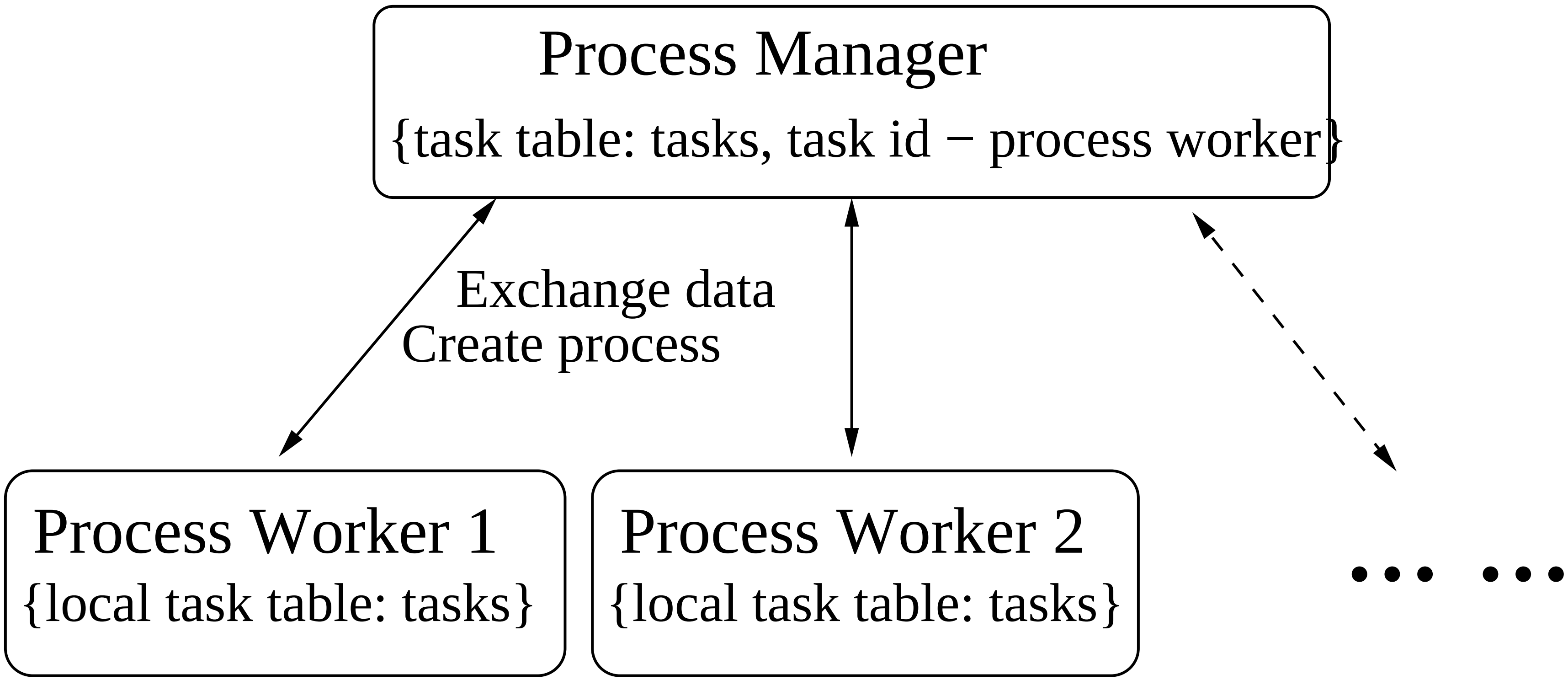
(2) **if** $V \neq \emptyset$ **then**

- lazy-solve these tasks in parallel
- update $ToDo$ and $\mathcal{T}$
- go to (1)

(3) **if** $V = \emptyset$ **then** $d := d - 1$ **and** go to (1)

return $\mathcal{T}$

Target implementation



Current implementation

• In ALDOR on a 4-processor machine using shared memory for data-communication.

• Only the output components are generated by decreasing order of dimension. (This does not hold yet for the intermediate components)

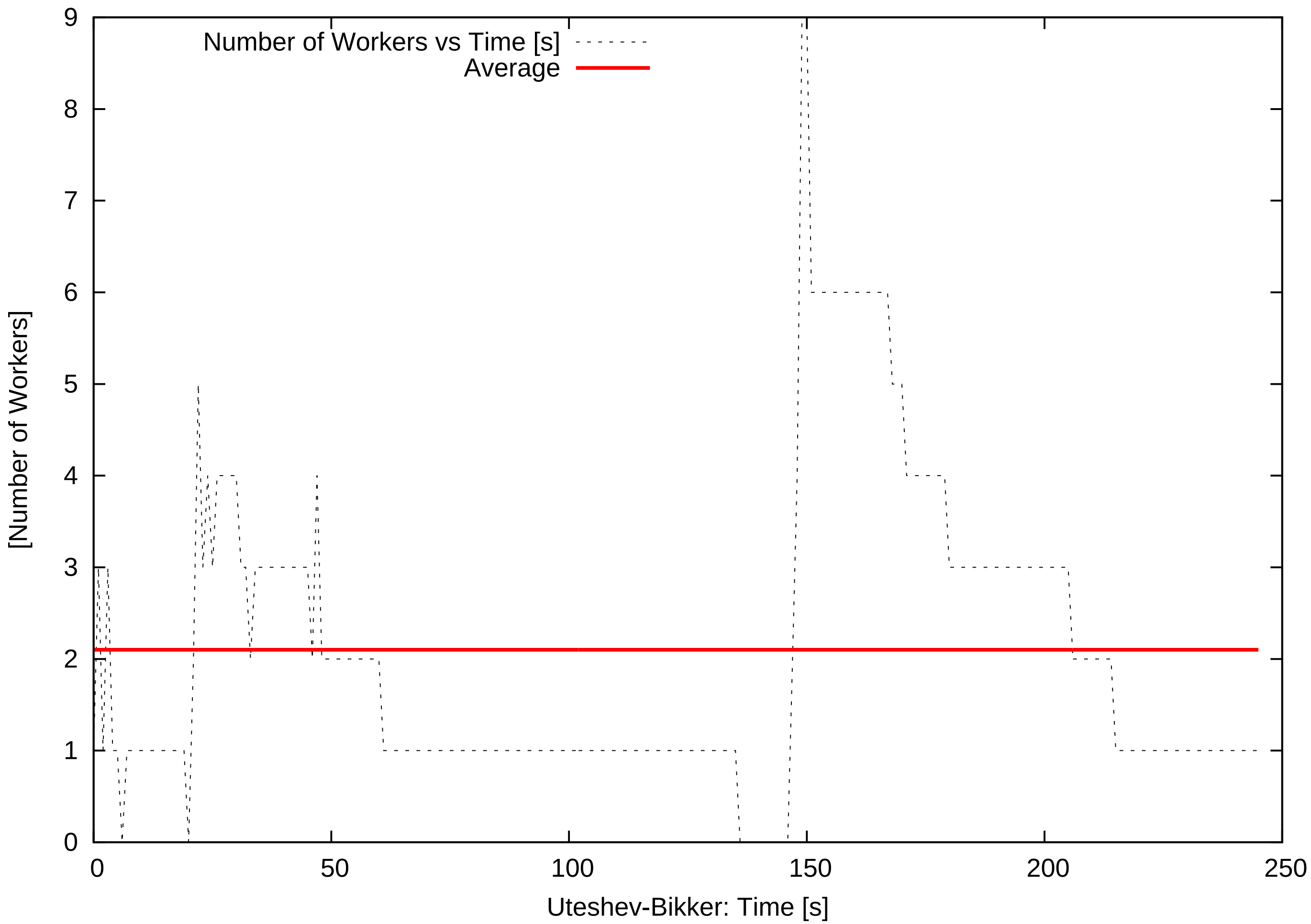
$\Rightarrow$ Hence, we do not implement yet the above parallel scheme, but only an approximation of it.

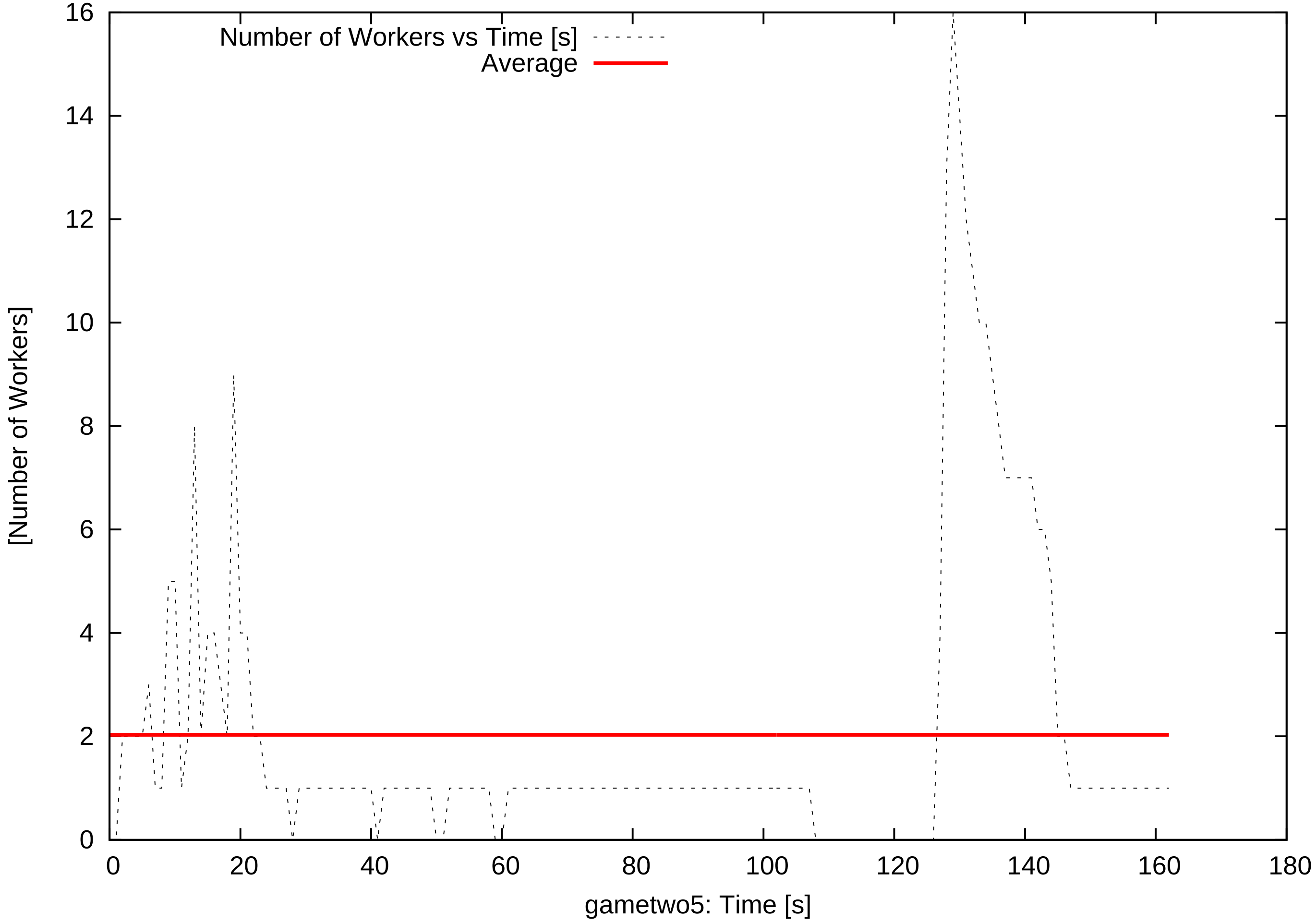
• Splitting (of the 2nd kind) relies only on the *D5 Principle* and univariate polynomial factorization.

• Each *LazySolve* requires to activate a process worker, which terminates after completing this computation.

$\Rightarrow$ Hence, we pay a severe penalty in data-communication and O/S calls w.r.t. our target implementation (work in progress).

Preliminay results




Number of Workers vs Time [s]
Average
[Number of Workers]
gametwo5: Time [s]
0
2
4
6
8
10
12
14
16
0
20
40
60
80
100
120
140
160
180

Work in progress and observations

- Combining the Triade algorithm and modular techniques, we have achieved successful **coarse-grain parallelization** of triangular decompositions **based on geometrical information** detected during the solving process.
- Future work:
  - Increasing the average number of working processors (by making use of multivariate factorization)
  - Reducing data-communicatio (with our target implementation scheme).
  - Making use of medium-grain parallelization (by parallelizing our GCDs/resultants).
- **Parallelizing helps removing arbitrary choices.**
- **Modular methods increase opportunities for parallelism.**

Implementation issues

• Fast algorithms for low-level subroutines

THEOREM. **(Dahan, M^3, Schost & Xie, 2005)** Let $T \subset \mathbb{K}[X]$ be a Lazard triangular set, with $\langle T \rangle$ radical and $\#|V(T)| = \delta$. Define $\mathbb{L} = \mathbb{K}[X]/\langle T \rangle$ There exists $G > 0$, and for any $\varepsilon > 0$, there exists $A_\varepsilon > 0$, such that one can compute a gcd of polynomials in $\mathbb{L}[y]$, with degree at most d, using $G\, A_\varepsilon^n\, d^{1+\varepsilon}\, \delta^{1+\varepsilon}$ operations in $\mathbb{K}$.

See also **(Pascal & Schost, 2006)**.

• Implementation techniques for fast polynomial arithmetic algorithms in high-level programming languages **(Filatei, Li, M^3, Schost, 2006)**.

Topics I did not have time to discuss

- Solving in the senses of Kalkbrener and Lazard.
- Complexity issues. **(Á. Szántó, 1997)**.
- Symbolic-numeric computations **(M^3 , Reid, Scott & Wu, 2005)**.
- and many other things.