Recent advances in triangular decompositions

Marc Moreno Maza

(*Uniersity of Western Ontario*)

ACA 2003
July 29

Dr Modular or How I learned to stop worrying and love symbolics

Marc Moreno Maza

(*Uniersity of Western Ontario*)

ACA 2003

July 29

Joint work with François Boulier and François Lemaire
(University of Lille 1)

- Modular methods for solving polynomial systems.
  - Univariate GCDs
  - Gröbner Bases.
- A first step toward modular methods for triangular decompositions.
  - Triangular decompositions, regular chains, characteristic sets.
  - Modular computation of Wu characteristic sets: the principle, improvements and experiments.
  - Modular computation of Ritt characteristic sets of prime ideals.

- Solving (linear or non-linear) systems in $\mathbb{Z}[x_1, \ldots, x_n]$ or $\mathbb{Q}[x_1, \ldots, x_n]$ lead to expression swell.
- Some techniques like the algorithm of *Bareiss* and the *sub-resultant* help reduce the problem.
- Modular techniques provide efficient solutions once the following sub-problems are solved:
  - How to choose the primes p such that

$$\overline{true - result}^{p} = modular - result?$$

  - How to recover the *true-result* from the *modular-result*?
- Moreover, modular techniques offer also advantages like machine arithmetic, fast arithmetic in $k[x]$, FFT-based techniques.

- Let A be a matrix of order n over $\mathbb{Z}$ with determinant $\det_{\mathbb{Z}}(A)$.
- Let B be a bound for the absolute value of $\det_{\mathbb{Z}}(A)$.
- For a prime $p \in \mathbb{Z}$ consider the symmetric reduction

$$\Phi_p : \begin{array}{ccc} \mathbb{Z} & \longmapsto & \mathbb{Z}/p\mathbb{Z} = [-\frac{p-1}{2}, \frac{p-1}{2}] \\ n & \to & n \text{ rem } p \end{array}$$

- Let $\Phi_p(A)$ be the image of A and $\det_p(\Phi_p(A))$ its determinant.

$$\Phi_p(\det_{\mathbb{Z}}(A)) \;=\; \det_p(\Phi_p(A)). \tag{1}$$

If $p > 2B$ then we have $\Phi_p(\det_{\mathbb{Z}}(A)) \;=\; \det_{\mathbb{Z}}(A)$. Hence for $p > 2B$ we obtain

$$\det_p(\Phi_p(A)) \;=\; \det_{\mathbb{Z}}(A). \tag{2}$$

$\boxed{\textbf{N.B. } \text{Every } \det_p(\Phi_p(A)) \text{ is the image of } \det_{\mathbb{Z}}(A)}$.

- The *modular* system may have more solutions than the *true* system.

$$\begin{cases} f_1 & = & (x+1)(x+p) \\ f_2 & = & (x+1)(x+2p) \end{cases}$$

$$\begin{cases} f_1 & = & x+y \\ f_2 & = & (p+1)x+y \end{cases}$$

- The *modular* system may have *less* solutions than the *true* one.

$$\begin{cases} f_1 & = & (px+1)(x+1) \\ f_2 & = & y+x \end{cases}$$

Input: E, Euclidean domain and $f, g \in E[x]$ primitive.

output: $\gcd(f, g)$.

$b := \gcd(\mathrm{lc}(f), \mathrm{lc}(g))$; $d := \min(\deg(f), \deg(g))$; $(m, g_m) := (1, 0)$
repeat
  choose a prime p not dividing $m\,b$
  $g_p := b\,\mathsf{monicGcd}(f \mod p, g \mod p)$ in $E/\langle p\rangle[x]$
  $\deg(g_p) = 0 \Rightarrow$ **return** 1
  $\deg(g_p) < d \Rightarrow (m, g_m, d) := (p, g_p, \deg(g_p))$ { previous unlucky }
  $\deg(g_p) > d \Rightarrow$ **iterate** { unlucky reduction }
  $w := \mathsf{combine}(p, m)(g_p, g_m)$; $w := \mathsf{symmetricMod}(w, m\,p)$
  if $w = g_m$ **then**
    $h := \mathrm{pp}(w)$
    if $h \mid f$ **and** $h \mid g$ **then return** h
  $(m, g_m) := (m\,p, w)$

Input: $\langle F \rangle \subset \mathbb{Q}[\mathbf{X}]$ homog. ideal and $<$ graded monom. order.

output: G the reduced Gröbner basis of $\langle F \rangle$ w.r.t. $<$.

$m := 1$
repeat
  choose a prime p not dividing m
  $G_p := \mathsf{reducedGB}(F \mod p)$
  $h_p := \mathsf{HilbertFunction}(G_p)$
  $m = 1$ **or** $h_p(d_0) < h_m(d_0)$ => $(m, G_m, h_m) := (p, G_p, h_p)$ { m unlucky }
  $h_p(d_0) > h_m(d_0)$ => **iterate** { p unlucky }
  $W := \mathsf{combine}(p, m)(G_p, G_m)$
  if $W = G_m$ **then**
    $G := \mathsf{rat\_reconstr}(mp, W)$
    $\mathsf{GröbnerBasis?}(G)$ **and** $F \subseteq \langle G \rangle$ => **return** G
  $(m, G_m) := (mp, W)$

Arnold, E.A., 2003. Modular algorithms for computing Gröbner bases. JSC 35 (2003) 403 419.

Davenport, J.H., **Siret**, Y., **Tournier**, E., 1988. Computer Algebra: Systems and algorithms for algebraic computation, AP.

Kaltofen, E., **Monagan**, M., 1999. On the Genericity of the Modular Polynomial GCD Algorithm. Proc. ISSAC 1999.

Gräbe, H., 1994. On lucky primes. JSC 15, 199 209.

von zur Gathen, J., **Gerhard**, J., 1999. Modern Computer Algebra. CUP.

Pauer, F., 1992. On lucky ideals for Gröbner basis computations. JSC 14, 471 - 482.

Traverso, C., 1997. Hilbert functions and the Buchberger's algorithm. JSC 22, 355 - 376.

Winkler, F., 1987. A p-adic approach to the computation of Gröbner bases. JSC 6, 287 - 304.

P. **Aubry**, D. **Lazard**, and M. **Moreno Maza**. On the theories of triangular sets. JSC. 28(1-2):105124, 1999.

F. **Boulier** and F. **Lemaire**. Computing canonical representatives of regular differential ideals. In proc. ISSAC 2000.

M. **Kalkbrener**. A generalized euclidean algorithm for computing triangular representations of algebraic varieties. JSC, 15, 1993.

D. **Lazard**. A new method for solving algebraic systems DAM, 1991.

M. **Moreno Maza**. On triangular decompositions of algebraic varieties. TR 4/99, NAG, 1999. Presented at MEGA-2000.

J. F. **Ritt**. Differential Equations from an Algebraic Standpoint, volume 14. American Mathematical Society, New York, 1932.

É. **Schost**. Degree bounds and lifting techniques for triangular sets. In proc. ISSAC 2002.

Wu. A zero structure theorem for polynomial equations solving. MM Research Preprints, 1:212, 1987.

- Triangular decompositions provide equidimensional decomposition of ideals (algebraic or differential) or affine varieties.
- They proceed in different ways
  - generating one component after another (Wu, 1987)
  - elimination per variable (Kalkbrener, 1993)
  - elimination per equation (Lazard, 1991)
  - elimination per dimension (MMM, 2000)

$\Longrightarrow$ Wu's method is the simplest one and there will be no *searching phase*.

$\triangle$ However we do not know a function like the *degree* or the *Hilbert function* to discard unlucky reductions.

- Let $f, g \in R[x_1 \ldots, x_n]$ with $x_1 < \cdots < x_n$ and $g \notin R$.
- $\mathsf{mvar}(g)$ is the *greatest* variable of g.
- $\mathsf{init}(g)$ and $\mathsf{mdeg}(g)$ are the leading coefficient and the degree of g w.r.t. $\mathsf{mvar}(g)$.
- $\mathsf{rank}(g) = \mathsf{mvar}(g)^{\mathsf{mdeg}(g)}$ is the *rank* of g.
- Let $h = \mathsf{init}(g)$, $v = \mathsf{mvar}(g)$ and $\delta = \deg(f, v) - \mathsf{mdeg}(g) + 1$. $\mathsf{prem}(f, g)$ and $\mathsf{pquo}(f, g)$ are the **unique** polynomials q and r such that

$$h^\delta f = qg + r \quad \text{and} \quad \deg(r, v) < \mathsf{mdeg}(g).$$

- For $p \in R$ prime **not** dividing h we have $\boxed{\mathsf{prem}(\overline{f}^p, \overline{g}^p) = \overline{r}^p}$

$T \subseteq R[x_1, \ldots, x_n]$ is a *triangular set* iff

(i) $T \cap R = \emptyset$,

(ii) $(\forall g_1, g_2 \in T)\ g_1 \neq g_2 \implies \mathsf{mvar}(g_1) \neq \mathsf{mvar}(g_2)$.

- h_T the product of the $\mathsf{init}(g)$ for $g \in T$.
- $\mathsf{red}_{\mapsto 0}(T) = \{f \in R[x_1, \ldots, x_n] \mid \mathsf{prem}(f, T) = 0\}$
- T is *auto-reduced* if $\mathsf{prem}(g, T \setminus \{g\}) = g$ for every $g \in T$.
- $\mathbf{W}(T) = \mathbf{V}(T) \setminus \mathbf{V}(h(T))$ the *Regular Zero Set* of T.
- $\overline{\mathbf{W}(T)} = \mathbf{V}(\mathbf{Sat}(T))$ where $\mathbf{Sat}(T) = \langle T \rangle : h_T^{\infty}$
- There is a noetherian ordering $<_{\mathrm{Ritt}}$ on the auto-reduced triangular sets contained in a given set (every descending chain is ultimately constant).

- Let $F \subset R[x_1, \ldots, x_n]$, $\mathcal{I} = \langle F \rangle$ with $R \cap \mathcal{I} = \{0\}$.
- Let $C \subset \mathcal{I}$ triangular, auto-reduced.
- **Ritt, 1932**: the following conditions are equivalent
  - C is a *basic set* of $\mathcal{I}$ (that is C is $<_{\mathrm{Ritt}}$-minimal among all auto-reduced triangular sets contained in C)
  - $\mathcal{I} \subseteq \mathsf{red}_{\mapsto 0}(C)$.

  If this holds then C is called a *Ritt characteristic set* of $\mathcal{I}$.
- **Wu, 1987**: if C is such that $F \subseteq \mathsf{red}_{\mapsto 0}(C)$ and R is a field, then we have

$$\mathbf{W}(C) \ \subseteq \ \mathbf{V}(F) \ \subseteq \ \mathbf{V}(C) \tag{3}$$

  - If this holds then C is called a *Wu characteristic set* of $\mathcal{I}$ and C can be computed as follows ...
  - if $\mathcal{I}$ is a *prime* ideal then $\mathbf{V}(F) = \overline{\mathbf{W}(C)}$.

$\mathsf{characteristicSet}(F) ==$

$i := 0$

$F_i := F$

repeat

$i := i + 1$

let B_i be a basic set of F_{i-1}

R_i the set of the $\mathsf{prem}(f, g)$ for $f \in F_{i-1} \setminus B_i$ and $g \in B_i$

$R_i = \{0\}$ => **return** B_i

$F_i = B_i \ \cup \ (F_{i-1} \setminus B_i) \ \cup \ R_i$

- $\langle F_0 \rangle = \langle F_1 \rangle = \langle F_2 \rangle = \ldots = \mathcal{I}$.
- For every $i \geq 1$ we have $B_i \subseteq \mathcal{I}$.
- If $R_i \neq \emptyset$ and $i \geq 2$ then $B_i <_{\mathrm{Ritt}} B_{i-1}$.
- Since Ritt ordering is noetherian, the algorithm terminates.

- Computations can be summarized as follows.

$$F_0 \left[\begin{array}{l} x^2 + 5\,x - 1 \\ -y^2 + (-4\,x - 1)\,y - 24\,x + 5 \\ -5\,y^2 + (4\,x - 1)\,y - 4\,x + 1 \end{array}\right.$$

$$F_1 \left[\begin{array}{ll} B_1 & \left[\begin{array}{l} x^2 + 5\,x - 1 \\ -y^2 + (-4\,x - 1)\,y - 24\,x + 5 \end{array}\right. \\ R_1 & \left[\; (-24\,x - 4)\,y - 116\,x + 24 \right. \\ F_0 \setminus B_1 & \left[\; -5\,y^2 + (4\,x - 1)\,y - 4\,x + 1 \right. \end{array}\right.$$

$$B_2 \left[\begin{array}{l} x^2 + 5\,x - 1 \\ (-24\,x - 4)\,y - 116\,x + 24 \end{array}\right.$$

$$R_2 \left[\begin{array}{l} 0 \\ 0 \end{array}\right.$$

- In a more synthetic way

$$
\begin{array}{ll}
F_0 & \left[\begin{array}{l} f_1 \\ f_2 \\ f_3 \end{array}\right. \\
F_1 & \left[\begin{array}{ll} B_1 & \left[\begin{array}{l} f_1 \\ f_2 \end{array}\right. \\ R_1 & \left[\begin{array}{l} f_4 \end{array}\right. \\ F_0 \setminus B_1 & \left[\begin{array}{l} f_3 \end{array}\right. \end{array}\right. \\
\quad B_2 & \left[\begin{array}{l} f_1 \\ f_2 \end{array}\right. \\
\quad R_2 & \emptyset
\end{array}
$$

- Computations modulo 7 can be summarized as follows.

$$F_0 \left[\begin{array}{l} x^2 + 5x + 6 \\ 6y^2 + (3x+6)y + 4x + 5 \\ 2y^2 + (4x+6)y + 3x + 1 \end{array} \right.$$

$$F_1 \left[\begin{array}{ll} B_1 & \left[\begin{array}{l} x^2 + 5x + 6 \\ 6y^2 + (3x+6)y + 4x + 5 \end{array} \right. \\ R_1 & \left[\; (4x+3)y + 3x + 3 \right. \\ F_0 \setminus B_1 & \left[\; 2y^2 + (4x+6)y + 3x + 1 \right. \end{array} \right.$$

$$\begin{array}{ll} B_2 & \left[\begin{array}{l} x^2 + 5x + 6 \\ (4x+3)y + 3x + 3 \end{array} \right. \\ R_2 & \left[\begin{array}{l} 0 \\ 0 \end{array} \right. \end{array}$$

- In a more synthetic way

$$1$$

$$2$$

$$x^2$$

$$y^2$$

$$1$$

$$4$$

$$x^2$$

$$y$$

- The same *history* can be made for the *generic computation*
- $p = 7$ is of good reduction since the *modular-result* is the modular image of the *true-result*.

- Computations modulo 5 can be summarized as follows.

$$
F_0 \left[\begin{array}{l} x^2 + 4 \\ 4y^2 + (x+4)y + x \\ (4x+4)y + x + 1 \end{array}\right.
$$

$$
F_1 \left[\begin{array}{ll} B_1 & \left[\begin{array}{l} x^2 + 4 \\ (4x+4)y + x + 1 \end{array}\right. \\ R_1 & \left[\ 0\right. \end{array}\right.
$$

- Leading to the history $\{1, 2, x^2, y\}$.
- Here the *modular-result* is propositional to the modular image of the *true-result*.

- Computations modulo 2 can be summarized as follows.

$$
F_0 \left[\begin{array}{l} x^2 + x + 1 \\ y^2 + y + 1 \\ y^2 + y + 1 \end{array} \right.
$$

$$
F_1 \left[\begin{array}{ll} B_1 & \left[\begin{array}{l} x^2 + x + 1 \\ y^2 + y + 1 \end{array} \right. \\ R_1 & \left[\; 0 \right. \end{array} \right.
$$

- Leading to the history $\{1, 2, x^2, y^2\}$.

- Here the *modular-result* is **not** propositional to the modular image of the *true-result*.

- For a prime p we perform $\mathsf{characteristicSet}(F \mod p)$. It is legitimate to set $\mathsf{characteristicSet}(F \mod 0) = \mathsf{characteristicSet}(F)$, that is the *non-modular* computation or the computation over R.
- The m input polynomials from F are *numbered* $1, \ldots, m$.
- During the algorithm each new polynomial in a *remainder-set* R_i receives a new number $m+1, m+2, \ldots$.
- We create a file $\mathsf{history}(F, p)$ called the *history* of $\mathsf{characteristicSet}(F \mod p)$ in which we write data during the computations.
- At each step i we write into $\mathsf{history}(F, p)$
  - the number of each polynomial in B_i
  - the rank of each polynomial in B_i

Definition 1 *A prime $p \in R$ is of* good reduction *if* $\mathsf{history}(F, p) = \mathsf{history}(F, 0)$.

Proposition 1 *If the prime $p \in R$ is of good reduction then* $\mathsf{characteristicSet}(F \mod p)$ *is proportional to* $\overline{\mathsf{characteristicSet}(F)}$.

Proposition 2 *There is only a finite number of primes which are* **not** *of good reduction.*

Definition 2 *Two primes $p, p' \in R$* have the same history *if* $\mathsf{history}(F, p) = \mathsf{history}(F, p')$.

- This relation among primes of R defines an equivalence relation.
- There is only a finite number of residue classes for this relation.
- The set of the primes of good reduction is one of this class. Moreover this is the only class which is not finite.
- Now, we *guess* how to compute $\mathsf{characteristicSet}(F)$ modularly ...

$\mathsf{modularCharacteristicSet}(F) ==$

  $tab := \mathsf{table}()$ # a table for the class of primes

  repeat

    choose a new prime p

    $C_p := \mathsf{characteristicSet}(F \mod p)$

    $h_p := \mathsf{history}(F, p)$

    $R_p := \mathsf{searchClass}(tab, h_p)$

    if $R_p = \emptyset$ { new histoty! } **then**

      $R_p := [[p, C_p]]$ { stored in tab }

    else { assume $R_p = [[m, C_m], [p_1, C_{p_1}], \ldots, [p_s, C_{p_s}]]$ }

      $W := \mathsf{combine}(p.m)(C_p, C_m)$

      if $W = C_m$ **then**

        $F \subseteq \mathsf{red}_{\mapsto 0}(C_m)$ **and** $C_m \subseteq \langle F \rangle$ => **return** C_m

      $R_p := [[m\,p, W], [p, C_p], [p_1, C_{p_1}], \ldots, [p_s, C_{p_s}]]$

- Force every C_p to satisfy the following: every polynomial has leading coeff. in $\mathbb{Q}$ (the initial of the initial of $\ldots$) is 1.

$\Longrightarrow$ This limits the coefficient size in the computed C

$\Longrightarrow$ This requires rational reconstruction.

- The test $C_m \subseteq \langle F \rangle$ can be improved in many occasions
  - By default, we use the histories!
  - If F generates a prime ideal $\mathcal{I}$ of dimension d and C has $n - d$ elements then $\mathbf{Sat}(C) = \mathcal{I}$. Moreover, if C is a *regular chain*, then C is a Ritt characteristic set.

- Comparing histories can discard a prime p before concluding the computation $\mathsf{characteristicSet}(F \mod p)$.

Example	Alonso-Li	Trager	Rose	E.Arnold-1
charSet $\mathbb{Z}$	400	RAM overflow	RAM overflow	RAM overflow
mod. charSet	200	1300	6 min.	1 hour
triade	70	20	520	940

- The same code (Aldor) was running Wu's method over $\mathbb{Z}$ and $\mathbb{Z}/p\mathbb{Z}$ without any optimization (fast algorithms over $\mathbb{Z}/p\mathbb{Z}, \ldots$)
- The goal was **not** to improve Wu's method but to show the applicability of these techniques.
- These ideas could apply for *evaluation/interpolation* modular techniques.
- The *searching phase problem* in (MMM, 2000) could be less difficult to deal with since computations move only in a unique dimension.