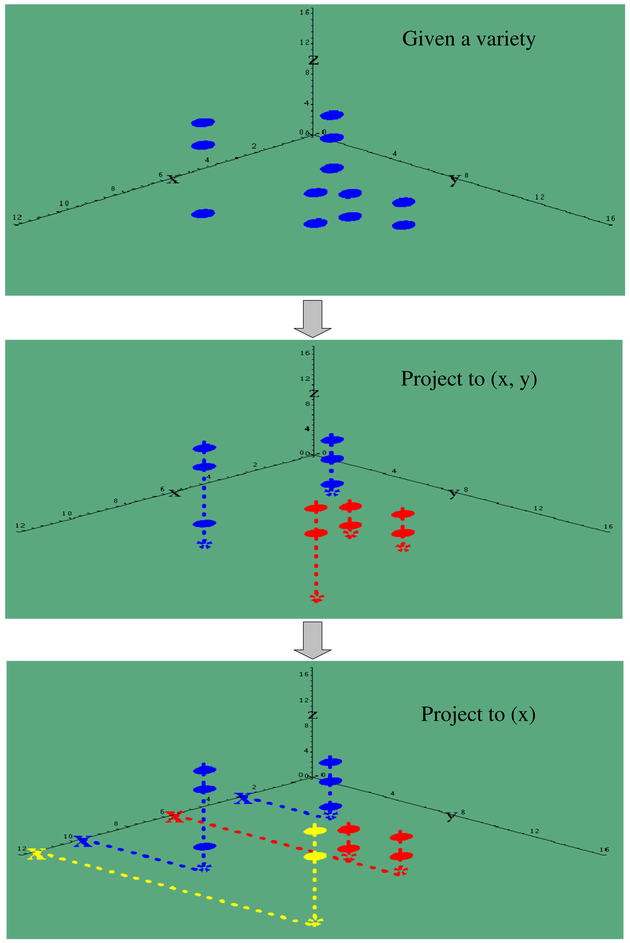
Equiprojectable Decomposition of Zero-dimensional Varieties

X. Dahan, M. Moreno Maza, É. Schost, W. Wu & Y. Xie

LIX, École polytechnique, 91128 Palaiseau, France.
ORCCA, University of Western Ontario, London, Canada.

July, 2005

1. Equiprojectable decomposition of a variety



2. The split-and-merge algorithm

Let's illustrate it with an example.

- Consider the zero-dimensional variety defined over $\mathbb{Q}$ by
  $\{326x - 10y^6 + 51y^5 + 17y^4 + 306y^2 + 102y + 34,\ y^7 + 6y^4 + 2y^3 + 12\}$.
  The unique decomposition for $x < y$ is A and B (the equiprojectable decomposition). Modulo $p = 7$, the zeros can be described by C and D. The triangular sets C and D are not the modular images of A and B.

$$A \left| \begin{array}{l} y^3+6 \\ x-1 \end{array} \right. , \quad B \left| \begin{array}{l} y^2+x \\ x^2+2 \end{array} \right. \quad \| \quad C \left| \begin{array}{l} y^2+6yx^2+2y+x \\ x^3+6x^2+5x+2 \end{array} \right. , \quad D \left| \begin{array}{l} y+6 \\ x+6 \end{array} \right.$$

- We compute from C and D the equiprojectable decomposition by the split-and-merge modulo 7:

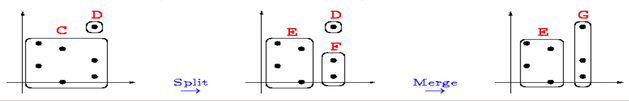
$$C \left| \begin{array}{l} C_2 = y^2+6yx^2+2y+x \\ C_1 = x^3+6x^2+5x+2 \end{array} \right. , \quad D \left| \begin{array}{l} D_2 = y+6 \\ D_1 = x+6 \end{array} \right.$$

↓ Split C by GCD ↓

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

↓ Merge F and D by CRT ↓

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



Framework: Polynomial system solving

- This research aims at developing fast algorithms and modular methods to solve systems of polynomials by way of *triangular decomposition*.
- Why triangular decomposition?
  - Classical algorithms for Gröbner bases do not make use of geometrical information; this makes a sharp modular method hard to design.
  - Primitive element representation lacks of canonicity.
- Among all possible triangular decompositions, the irreducible decomposition is canonical but does not have good specialization properties.
- We introduce a *canonical* triangular decomposition adapted to *sharp modular computations*:

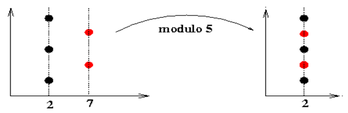
  The equiprojectable decomposition

Outline

1. Let V be a zero-dimensional variety defined over $\mathbb{Q}$. The equiprojectable decomposition of V is based on a combinatorial process which splits V according to cardinalities of projection fibers.
2. From any triangular decomposition of V, we show how to compute the equiprojectable decomposition of V by the *split-and-merge* algorithm.
3. We show that the equiprojectable decomposition of V has good specialization properties modulo a prime number p.
4. Using Hensel lifting techniques, we deduce a modular algorithm for computing the equiprojectable decomposition of V.
5. We implement this modular algorithm on top of the *RegularChains* library in Maple, and test it with challenging well-known benchmark problems.

3. Specialization properties

- **Simplified case.** First assume that all points of V are in $\mathbb{Q}^n$.
  Theorem 1. *If:*
  (1) p divides no denominator of the coordinates;
  (2) the cardinality of none of the projections of V decreases mod p;
  then the equiprojectable decomposition specializes mod p.

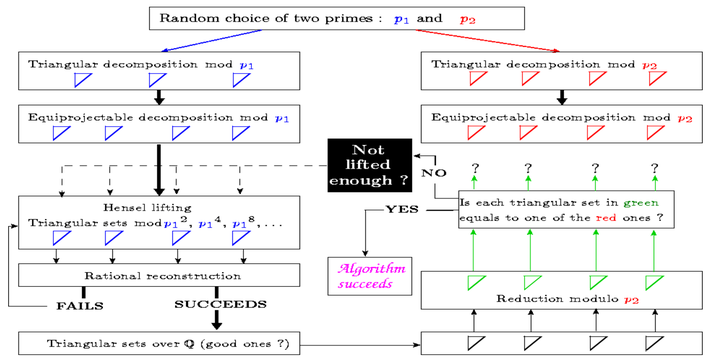


Note: on this figure assumption (2) does not hold.

- **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. This implies that $V \mod p$ is well defined.
- **Estimates for prime of good reduction:**
  Let F be a polynomial system with $V = V(F)$. Let h be the maximum number of digits among all coefficients of F, and let d be the maximum total degree among all monomials of F.
  Theorem 2. *There exists $A \in \mathbb{N} - \{0\}$ such that:*
  (1) $\text{height}(A) \leq 2n^2 d^{2n+1}(3h + 7\log(n+1) + 5n\log d + 10)$.
  (2) If p is a prime which does not divide A, then the equiprojectable decomposition specializes well mod p.

4. A modular algorithm for triangular decomposition

- **Choice of primes:**
  For a *deterministic* algorithm the prime p of reduction must be larger than A. However, A is often *too large* for an efficient modular method. So, we present a *probabilistic* algorithm involving smaller primes:
  - the probability of success is explicitly quantified and can be made arbitrarily close to 1,
  - the choice of $p \simeq \log A$ leads to more than 99% of success.
- **The modular algorithm:**
  INPUT: V zero-dimensional, smooth and given by $F \subseteq \mathbb{Q}[x_1, \ldots, x_n]$ with $n = \#F$.
  OUTPUT: The equiprojectable decomposition of V (with a quantified probability).



5. Implementation and experimentation

Table 1: Features of the polynomial systems and prime numbers for the modular algorithm

Sys	Name	n	d	h	p_1
1	fabfaux	3	3	13	121458749
2	geneig	6	3	2	303179363351
3	eco6	6	3	0	509110405373
4	Weispfenning-94	3	5	0	3441898787
5	Issac97	4	2	2	49956859
6	dessin-2	10	2	7	2011551274283
7	eco7	7	3	0	543376732989
8	Reimer-4	4	5	1	180771302617
9	Methan61	10	2	16	3557395585699
10	Uteshev-Bikker	4	3	3	2197378999

Table 2: Experimental results from Maple

Sys	△ mod (sec)	Triangularize (sec)	gsolve (sec)	△ Mod (MB)	Triangularize (MB)	gsolve (MB)
1	27	512	1041	9	275	34
2	18	2.5	-	5	4	fail
3	50	5	9	6	5	5
4	100	3000	4950	12	250	66
5	161	-	1050	20	fail	31
6	524	-	-	14	fail	error
7	3795	1593	-	18	18	fail
8	5575	-	-	38	fail	fail
9	6184	∞	-	12	-	fail
10	8726	-	-	64	fail	fail

△ mod: our modular algorithm for triangular decomposition.
Triangularize: non-modular algorithm for triangular decomposition.
gsolve: decomposition via Gröbner bases.

Conclusions

- We have introduced a way of encoding the solution set of a polynomial system, the **Equiprojectable Decomposition**, which has good computational properties.
- Using Hensel lifting techniques we designed an efficient modular algorithm for solving polynomial systems of dimension zero.
- Our experimentation shows the capacity of this approach to solve problems out of the scope of other comparable solvers.
- Work is in progress on the complexity analysis of *split-and-merge*: see the poster *On the complexity of the D5 principle*.
- We aim at extending this work to variable specialization
  - to speed up modular triangular decompositions,
  - to treat systems of positive dimension.
- An optimized implementation for our algorithm is in progress.