Equiprojectable decomposition of zero-dimensional varieties

X. Dahan⋆, M. Moreno Maza†, É. Schost⋆, W. Wu†, Y. Xie†
⋆: STIX, École polytechnique, 91128 Palaiseau, France.
†: ORCCA, University of Western Ontario, London, Ontario, Canada.
{dahan,schost}@stix.polytechnique.fr
{moreno,wwu25,yxie}@orcca.on.ca

Abstract

We discuss triangular representations of zero-dimensional varieties. We define a notion of equiprojectable decompositions and show its applications for modular computations with triangular sets.

Equiprojectable varieties. We study the representation of zero-dimensional varieties by means of *triangular sets*. Following [4], if k is a field, a triangular set in $k[x_1, \ldots, x_n]$ is a sequence of n polynomials $T_1(x_1), \ldots, T_n(x_1, \ldots, x_n)$ forming a lexicographic reduced Gröbner basis with $x_1 < \cdots < x_n$.
Suppose that k is perfect. A zero-dimensional variety $V \subset \overline{k}^n$ is *equiprojectable* [2] or *characterizable* [3] if its defining ideal is generated by a triangular set. Geometrically, this means that for $i = 1, \ldots, n$, all fibers of the projection $V \subset \overline{k}^n \to \overline{k}^i$ on the space of the first i coordinates have the same cardinality.

Equiprojectable decomposition. If V is not equiprojectable, it can be described, possibly in several ways, as the disjoint union of the zeros of several triangular sets. However, the only *a priori* canonical choice for such a representation corresponds to the irreducible decomposition of V, but it is ill-suited to the applications we have in mind (modular methods, see below). As an alternative, we propose a definition of an *equiprojectable decomposition* of a zero-dimensional variety, into a disjoint union of equiprojectable ones, based on the following combinatorial considerations.
We first look at the projection $\pi : V \subset \overline{k}^n \to \overline{k}^{n-1}$, which forgets the last coordinate. To a point x in V, we associate $N(x) = \#\pi^{-1}(\pi(x))$, that is, the number of points lying in the same π-fiber as x. Then, we split V into the disjoint union $V_1 \cup \cdots \cup V_d$, where for all $i = 1, \ldots, d$, V_i equals $N^{-1}(i)$, that is, the set of points $x \in V$ which have $N(x) = i$. This splitting process is applied recursively to all varieties $V_1, \ldots, V_d$, taking into account the fibers of the successive projections $\overline{k}^n \to \overline{k}^i$, for $i = n-1, \ldots, 1$. In the end, we obtain

a family of pairwise disjoint, equiprojectable varieties, whose reunion equals V; they form the *equiprojectable decomposition* of V.

Algorithms. We propose two algorithms for the computation of this decomposition, starting from different input. Both algorithms have a complexity which is polynomial in the degree of V; more precise estimates can be given in terms of the cost of univariate polynomial multiplication. The first algorithm takes as input a primitive element description of V. It first computes the decomposition of V into $V_1, \ldots, V_d$ as mentioned above, using the square-free factorization of a suitable characteristic polynomial. By an inductive process, it computes the equiprojectable decomposition of each V_i, which is enough to conclude.
The second algorithm takes as input an arbitrary triangular decomposition of the variety V. This algorithm proceeds in two phases, first splitting "critical pairs" of triangular sets, and then merging "solvable pairs", using GCD and CRT computations. In order to sketch this algorithm more precisely, we consider $\{S_1(x_1), \ldots, S_n(x_1, \ldots, x_n)\}$ a second triangular set different from $\{T_1(x_1), \ldots, T_n(x_1, \ldots, x_n)\}$. We define the *level* of the pair $\{S, T\}$ as the smallest variable x_i such that $\{T_1, \ldots, T_i\}$ and $\{S_1, \ldots, S_i\}$ do not generate the same ideal. Let x_i be the level of $\{S, T\}$ and let $\mathcal{I}$ be the ideal generated by $\{T_1, \ldots, T_{i-1}\}$. The pair $\{S, T\}$ is *critical* if the polynomials T_i and S_i are not relatively prime modulo $\mathcal{I}$. The pair is *solvable* if the polynomials T_i and S_i are relatively prime modulo $\mathcal{I}$ and if for $j = i+1, \ldots, n$ the polynomials T_j amd S_j have the same degree w.r.t. x_j.
From the input triangular decomposition, we compute another triangular decomposition of V which has no critical pairs. This process can be achieved by computations of polynomial GCD modulo triangular sets. From there, we obtain a last triangular decomposition of V which has no critical pairs and no solvable pairs. We realize this second phase as follows: CRT computations are employed in order to replace every solvable pair by a single triangular set; processing the solvable pairs by decreasing order of level leads to the equiprojectable decomposition of V.

Application: modular methods. Modular methods are a promising tool for computing triangular sets. Among their fields of applications, we find the resolution of zero-dimensional systems over $\mathbb{Q}$, by specialization modulo a prime p and Hensel lifting, and the description of the generic solutions of systems of positive dimension. Such techniques have already been used for polynomial system solving, see references in [1, 5]. More precisely, an algorithm working in the triangular representation is described in [7]. However, it does not entirely solve the problem, since it is limited to equiprojectable varieties.
To make the difficulties of the non-equiprojectable case explicit, consider for instance the variety V defined over $\mathbb{Q}$ by the polynomials

$$326x - 10y^6 + 51y^5 + 17y^4 + 306y^2 + 102y + 34, \quad y^7 + 6y^4 + 2y^3 + 12.$$

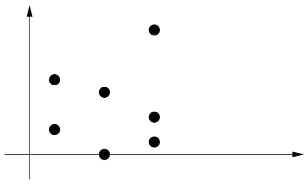
For the order $x < y$, the only possible description of V by triangular sets is

$$\mathfrak{T}_1 : \left| \begin{array}{l} y^3 + 6 \\ x - 1 \end{array} \right. \qquad \mathfrak{T}_2 : \left| \begin{array}{l} y^2 + x \\ x^2 + 2 \end{array} \right.$$

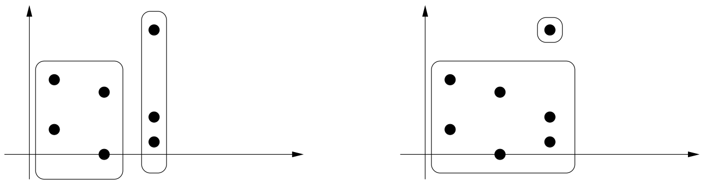
However, taken modulo 7, the zeros of the above system can be described by:

$$\mathfrak{t}_1 : \left| \begin{array}{l} y^2 + 6yx^2 + 2y + x \\ x^3 + 6x^2 + 5x + 2 \end{array} \right. \qquad \mathfrak{t}_2 : \left| \begin{array}{l} y + 6 \\ x - 1 \end{array} \right. ,$$

which are not the reduction of $\mathfrak{T}_1$ and $\mathfrak{T}_2$ modulo 7, and thus cannot be lifted over $\mathbb{Q}$. An algorithm using Hensel lifting should then be able to discard $\mathfrak{t}_1$ and $\mathfrak{t}_2$ as non-suitable, and replace them by a better choice.
We propose such an algorithm, based on the notion of equiprojectable decomposition. On the example, both V and its reduction modulo 7 can be represented as follows (forgetting about the actual coordinates of the solutions):



That is, the projection on the x-axis has cardinality 3; two fibers have cardinality 2, and the last one has cardinality 3. Representing V by $\mathfrak{T}_1$ and $\mathfrak{T}_2$ amounts to grouping its points as on the leftmost picture (this is its equiprojectable decomposition), whereas $\mathfrak{t}_1$ and $\mathfrak{t}_2$ correspond to the rightmost one:



Hence, $\mathfrak{t}_1$ and $\mathfrak{t}_2$ do *not* define the equiprojectable decomposition of the modular solutions, and this explains why they cannot be lifted over $\mathbb{Q}$. Thus, our algorithm first computes the equiprojectable components of the modular solution, and then applies a Hensel lifting operator to all of them.
To establish the soundness of this strategy, we prove that equiprojectable decompositions have good specialization properties: if $F_1, \ldots, F_n$ have degree at most d and integer coefficients of height at most h, success is guaranteed if p does not divide a non-zero integer of height $n^{O(1)} h d^{O(n)}$ (our estimates are explicit). We deduce sharp bit-complexity estimates for the computation of the simple roots of the system $F_1, \ldots, F_n$ by means of triangular sets; the algorithm is probabilistic, and we have explicit estimates on the error probability.
We have realized a preliminary implementation with the TRIADE library developed in MAPLE by F. Lemaire (Université de Lille, France) and based on the algorithms of [6]. Our theoretical results are comforted by these experiments.

References

[1] E. A. Arnold. Modular algorithms for computing Gröbner bases. *J. Symb. Comp.*, 35(4):403–419, 2003.

[2] P. Aubry and A. Valibouze. Using Galois ideals for computing relative resolvents. *J. Symb. Comp.*, 30(6):635–651, 2000.

[3] É. Hubert. Notes on triangular sets and triangulation-decomposition algorithms. In *Lecture Notes in Comput. Sci.*, volume 2630. Springer, 2003.

[4] D. Lazard. Solving zero-dimensional algebraic systems. *J. Symb. Comp.*, 13:117–133, 1992.

[5] G. Lecerf. Quadratic Newton iteration for systems with multiplicity. *Found. Comput. Math.*, 2(3):247–293, 2002.

[6] M. Moreno Maza. On triangular decompositions of algebraic varieties. 2000. MEGA-2000 Conference, Bath, England.

[7] É. Schost. Complexity results for triangular sets. *J. Symb. Comp.*, 36(3-4):555–594, 2003.