Zero Decomposition for Theorem Proving in Geometry

Dongming Wang
LIFIA–IMAG, 46, avenue Félix Viallet, 38031 Grenoble Cedex, France

(Extended Abstract)

Let $\boldsymbol{K}$ be a field of characteristic 0 and $\tilde{\boldsymbol{K}}$ an algebraic closure of $\boldsymbol{K}$. By a *polynomial* we mean one in $\boldsymbol{K}[x_1,\ldots,x_n]$, the ring of polynomials in the variables $x_1,\ldots,x_n$ (abbreviated sometimes to x) with coefficients in $\boldsymbol{K}$. A polynomial system is a pair $[\mathbb{P},\mathbb{Q}]$ of finite sets of polynomials in $\boldsymbol{K}[x]$, with which the zero set

$$\mathrm{Zero}(\mathbb{P}/\mathbb{Q}) = \{x \in \tilde{\boldsymbol{K}}^n \mid P(x)=0, Q(x)\neq 0,\ \forall P\in\mathbb{P}, Q\in\mathbb{Q}\}$$

is of concern.

For any non-constant polynomial P, $\mathrm{lv}(P)$ denotes the variable x_p which has biggest index p and effectively appears in P. The leading coefficient of P with respect to (wrt) $\mathrm{lv}(P)$ is called the *initial* of P and denoted by $\mathrm{ini}(P)$. An ordered set of non-constant polynomials

$$\mathbb{T} = [T_1, T_2, \ldots, T_r]$$

is called a *triangular set* if

$$\mathrm{lv}(T_1) \prec \mathrm{lv}(T_2) \prec \cdots \prec \mathrm{lv}(T_r).$$

A triangular set $\mathbb{T}$ is called a (non-contradictory) *ascending set* if in $\mathrm{lv}(T_i)$ the degree of T_j is less than the degree of T_i for each pair $j > i$. For any two polynomials P and Q, denote by $\mathrm{prem}(Q,P)$ the *pseudo-remainder* of Q wrt P in $\mathrm{lv}(P)$. Let $\mathbb{T}$ be a triangular set as above and $\mathbb{Q}$ any polynomial set. We write $\mathrm{prem}(Q,\mathbb{T})$ for $\mathrm{prem}(\cdots\mathrm{prem}(Q,T_r),\ldots,T_1)$ and $\mathrm{prem}(\mathbb{Q},\mathbb{T})$ for $\{\mathrm{prem}(Q,\mathbb{T}) \mid Q\in\mathbb{Q}\}$.

Given any polynomial system $[\mathbb{P},\mathbb{Q}]$, by using Ritt-Wu's decomposition algorithm [2, 6, 10, 11] one can compute a finite sequence of ascending sets $\mathbb{C}_1,\ldots,\mathbb{C}_e$ such that

$$\mathrm{Zero}(\mathbb{P}/\mathbb{Q}) = \bigcup_{i=1}^{e} \mathrm{Zero}(\mathbb{C}_i/\mathbb{I}_i\cup\mathbb{Q}_i), \tag{1}$$

where $\mathbb{I}_i = \{\mathrm{ini}(C) \mid C\in\mathbb{C}_i\}$, $\mathbb{Q}_i = \mathrm{prem}(\mathbb{Q},\mathbb{C}_i)$ and $0\notin\mathbb{Q}_i$ for each i. We assume $e=0$ if $\mathrm{Zero}(\mathbb{P}/\mathbb{Q})=\emptyset$ is detected.

A polynomial system $[\mathbb{T},\mathbb{U}]$ is called a *triangular system* if $\mathbb{T}$ is a triangular set such that $\mathrm{ini}(T)$ does not vanish on $\mathrm{Zero}(\mathbb{T}/\mathbb{U})$ for all $T\in\mathbb{T}$.

A triangular system $[\mathbb{T},\mathbb{U}]$ is said to be *fine* if $0\notin\mathrm{prem}(\mathbb{U},\mathbb{T})$.

In [7], the author proposed a decomposition algorithm which computes, for any polynomial system $[\mathbb{P}, \mathbb{Q}]$, a sequence of fine triangular systems $[\mathbb{T}_1, \mathbb{U}_1], \ldots, [\mathbb{T}_e, \mathbb{U}_e]$ such that

$$\mathrm{Zero}(\mathbb{P}/\mathbb{Q}) = \bigcup_{i=1}^{e} \mathrm{Zero}(\mathbb{T}_i/\mathbb{U}_i). \tag{2}$$

This algorithm employs a top-down elimination with splitting. Its key step is to produce a triangular system $[\mathbb{T}, \mathbb{U}]$ from an arbitrary polynomial system $[\mathbb{P}, \mathbb{Q}]$ by successively eliminating the variables using pseudo-division for the polynomials in $\mathbb{P}$ and meanwhile reducing the polynomials in $\mathbb{Q}$. During the computation of $[\mathbb{T}, \mathbb{U}]$, other polynomial systems are generated (by replacing the dividing polynomial with its initial and reductum whenever pseudo-division is performed), and to each of them the same procedure is applied recursively.

As another algorithm, we propose using subresultant polynomial remainder sequences (SPRS, cf. [1, 3]). For any given polynomial system $[\mathbb{P}, \mathbb{Q}]$, we perform an elimination top-down from x_n to x_1 with two kinds of splitting. For each x_k, a single polynomial P with $\mathrm{lv}(P) = x_k$ is produced by means of forming SPRS iteratively; this polynomial is then used to pseudo-divide the polynomials in $\mathbb{Q}$. One kind of splitting is performed according as the initials of the considered polynomials vanish or not (as in the algorithm mentioned in the preceding paragraph), and the other is performed for variable elimination according to the following fact:

Let $P_1, P_2, \ldots, P_s$ be an SPRS of P_1 and P_2 wrt x_k and let I_i be the leading coefficient of P_i wrt x_k for each i. Then $P_1 = 0, P_2 = 0$ and $I_1 I_2 \neq 0$ if and only if $P_i = 0, I_{i+1} = 0, \ldots, I_s = 0$ and $I_1 I_2 I_i \neq 0$ for some $2 \leq i \leq s$ (see [1, 3, 8]).

In each case of splitting, one produced system is taken to update the current system $[\mathbb{P}, \mathbb{Q}]$ and the others are collected and to be treated similarly.

In this way, we can compute a zero decomposition of the same form (2) with the formation of SPRS as basic operation.

By renaming the variables, a triangular set can be written in the form

$$\mathbb{T} = [T_1(u, y_1), T_2(u, y_1, y_2), \ldots, T_r(u, y_1, y_2, \ldots, y_r)], \tag{3}$$

where u stands for $u_1, \ldots, u_d$ and $d + r = n$. A fine triangular set $\mathbb{T}$ as above is said to be *irreducible* if $T_i(u, \eta_1, \ldots, \eta_{i-1}, y_i)$ considered as a polynomial in y_i is irreducible over the extension field $\boldsymbol{K}(u, \eta_1, \ldots, \eta_{i-1})$ obtained from $\boldsymbol{K}$ by successively adjoining the transcendental elements u and the algebraic elements $\eta_1, \ldots, \eta_{i-1}$ with $T_1, \ldots, T_{i-1}$ as minimal polynomials for $i = 1, \ldots, r$.

If $\mathbb{T}$ is reducible, then there exists a minimal k such that T_k can be factorized into irreducible factors $G_1, \ldots, G_t$ over $\boldsymbol{K}(u, \eta_1, \ldots, \eta_{k-1})$. Here the irreducibility and the polynomials $G_1, \ldots, G_t$ can be exactly determined with polynomial operations (cf. [11]).

Making use of algebraic factorization, one can further decompose each reducible $\mathbb{T}_i$ into triangular sets, and finally into irreducible ones. Therefore, one can compute the zero decomposition (2) with each $\mathbb{T}_i$ irreducible.

A triangular set $\mathbb{T}$ of the form (3) is said to be *regular* if $\mathrm{ini}(T_i)(u, \eta_1, \ldots, \eta_{i-1}) \neq 0$ for every zero $(\eta_1, \ldots, \eta_{i-1})$ of $T_1, \ldots, T_{i-1}$ in any extension field of $\boldsymbol{K}(u)$, $i = 1, \ldots, r$.

By computing *conditional* greatest common divisors (GCD), we can decompose any triangular set into regular ones. Therefore, the zero decomposition (2) can also be computed with each $\mathbb{T}_i$ regular.

A fine triangular system $[\mathbb{T}, \mathbb{U}]$ is called a *simple system* if $\mathbb{T} \cup \mathbb{U}$ can be reordered as a triangular set, and for every $P \in \mathbb{T} \cup \mathbb{U}$ with $\mathrm{lv}(P) = x_p$, $P(\bar{x}_1, \ldots, \bar{x}_{p-1}, x_p)$ is squarefree wrt x_p for any $(\bar{x}_1, \ldots, \bar{x}_{p-1}) \in \mathrm{Zero}(\mathbb{T} \cap \boldsymbol{K}[x_1, \ldots, x_{p-1}]/\mathbb{U} \cap \boldsymbol{K}[x_1, \ldots, x_{p-1}])$ and P is primitive wrt x_p.

As described in [8], by forming SPRS we can decompose any given polynomial system into simple systems. It follows that (2) can be computed with each $[\mathbb{T}_i, \mathbb{U}_i]$ a simple system as well. Note that in theory decomposing polynomial systems into regular triangular systems or simple systems does not require algebraic polynomial factorization.

To prove geometric theorems which may be formulated algebraically in the form

$$(\forall x_1 \cdots \forall x_n)\,[H_1 = 0 \wedge \cdots \wedge H_h = 0 \wedge D_1 \neq 0 \wedge \cdots \wedge D_d \neq 0 \Longrightarrow C = 0] \qquad (4)$$

with $H_i, D_j, C \in \boldsymbol{K}[x]$, one can devise several algorithms on the basis of the decomposition algorithms explained before.

Following Wu's method, we first compute a zero decomposition of the form (1) or (2) with $\mathbb{P} = \{H_1, \ldots, H_h\}$ and $\mathbb{Q} = \{D_1, \ldots, D_d\}$, and then determine whether C vanishes on $\mathrm{Zero}(\mathbb{T}_i/\mathbb{U}_i)$ for each i. The latter can be done straightforwardly by using pseudo-division:

1. if $\mathrm{prem}(C, \mathbb{T}_i) = 0$, then C vanishes on $\mathrm{Zero}(\mathbb{T}_i/\mathbb{U}_i)$;

2. if C vanishes on $\mathrm{Zero}(\mathbb{T}_i/\mathbb{U}_i)$ and $\mathbb{T}_i$ is irreducible or $[\mathbb{T}_i, \mathbb{U}_i]$ is a simple system, then $\mathrm{prem}(C, \mathbb{T}_i) = 0$.

In particular, we advocate using irreducible zero decomposition; based on this, a prover has been implemented which can decide whether the algebraic form (4) of a geometric theorem is true universally or only for some part of the hypothesis configuration defined by $\mathrm{Zero}(\mathbb{P}/\mathbb{Q})$. Determining the latter is of interest not only for ruling out the degenerate cases in which the theorem may be meaningless or false, but also for dealing with such theorems which involve reducibility or whose precise algebraic formulation involves inequalities.

Decomposing polynomial systems into simple systems provides a method for deciding whether a geometric theorem is universally true. However, computing simple systems using the algorithm presented in [8] may be expensive. Now we adopt an alternative approach: first computing triangular systems using the most efficient algorithm on hand and then computing simple systems from the triangular systems. We also determine for which components a geometric theorem is true by computing regular triangular systems and simple systems, making use of the devices suggested in [4, 12].

Experiments have been made for the various decomposition algorithms with a number of selected examples and in comparison for theorem proving in elementary geometry. These examples include the Steiner Theorem, Steiner-Lehmus Theorem, Morley Theorem and Thébault-Taylor Theorem in which the reducibility problem may occur. Some of our algorithms perform very well. Ritt-Wu's and one of our decomposition algorithms can be extended to the differential case. Several theorems from differential geometry have also been proved by using our implementation of the algorithms.

Zero decomposition for geometry theorem proving was investigated previously in [2, 5] using Ritt-Wu's algorithm, in [4, 12] by means of computing regular triangular sets, resultants and GCD over extension fields, and in [9] using elimination procedures based on the concept of triangular systems. The present work is a continuation of our approach with new developments on algorithms for computing regular triangular sets, simple systems and the mixing of different decomposition techniques.

References

[1] Brown, W. S. The subresultant p.r.s. algorithm. *ACM Trans. Math. Softw.* **4** (1978), 237–249.

[2] Chou, S. C. and Gao, X. S. Ritt-Wu's decomposition algorithm and geometry theorem proving. In: *Proc. CADE-10, Lecture Notes in Comput. Sci.* **449** (1990), pp. 207–220.

[3] Collins, G. E. Subresultants and reduced polynomial remainder sequences. *J. ACM* **14** (1967), 128–142.

[4] Kalkbrener, M. A generalized Euclidean algorithm for geometry theorem proving. *Ann. Math. Artif. Intell.* **13** (1995), 73–96.

[5] Ko, H. P. Geometry theorem proving by decomposition of quasi-algebraic sets: An application of the Ritt-Wu principle. *Artificial Intelligence* **37** (1988), 95–122.

[6] Ritt, J. F. *Differential Algebra*. New York: Amer. Math. Soc. (1950).

[7] Wang, D. M. An elimination method for polynomial systems. *J. Symbolic Computation* **16** (1993), 83–114.

[8] Wang, D. M. Decomposing polynomial systems into simple systems. Preprint, LIFIA–Institut IMAG (1994).

[9] Wang, D. M. Elimination procedures for mechanical theorem proving in geometry. *Ann. Math. Artif. Intell.* **13** (1995), 1–24.

[10] Wu, W.-T. Basic principles of mechanical theorem proving in elementary geometries. *J. Sys. Sci. & Math. Scis.* **4** (1984), 207–235; *J. Automated Reasoning* **2**, 221–252 (1986).

[11] Wu, W.-T. *Mechanical Theorem Proving in Geometries: Basic Principles* (translated from the Chinese by X. Jin and D. Wang). Wien-New York: Springer-Verlag (1994).

[12] Yang, L., Zhang, J. Z. and Hou, X. R. An efficient decomposition algorithm for geometry theorem proving without factorization. *MM Research Preprints* **9** (1993), 115–131.