Triangular Decompositions of Polynomial Systems: From Theory to Practice

Marc Moreno Maza
ORCCA, University of Western Ontario (UWO)
London, Ontario, Canada
moreno@orcca.on.ca

Triangular decompositions are one of the major tools for solving polynomial systems. For systems of algebraic equations, they provide a convenient way to describe complex solutions and a step toward isolation of real roots or decomposition into irreducible components. Combined with other techniques, they are used for these purposes by several computer algebra systems. For systems of partial differential equations, they provide the main practicable way for determining a symbolic description of the solution set. Moreover, thanks to Rosenfeld's Lemma, techniques from the algebraic case apply to the differential one [3].

Research in this area is following the natural cycle: *theory, algorithms, implementation*, which will be the main theme of this tutorial. We shall also concentrate on the algebraic case and mention the differential one among the applications.

Theory. The concept of a *characteristic set*, introduced by Ritt [14], is the cornerstone of the theory. He described an algorithm for solving polynomial systems by factoring in field extensions and computing characteristic sets of prime ideals. Wu [16] obtained a *factor-free* adaptation of Ritt's algorithm. Several authors continued and improved Wu's approach: among them Chou, Gao [4], Gallo, Mishra [10] Wang [15]. Considering characteristic sets of non-prime ideals leads to difficulties that were overcome by Kalkbrener [11] and, Yang and Zhang [17] who defined particular characteristic sets, called *regular chains*. See also the work of Lazard and his students [1]. The first part of this tutorial will be an introduction to this notion for a general audience.

Algorithms. Regular chains, combined with the D5 Principle [8] and a notion of polynomial GCD [13], have also contributed to improve the efficiency of algorithms for computing triangular decompositions, as reported in [2]. To go further, complexity estimates of the output regular chains were needed. Such results were provided by Dahan and Schost [7]. Together with the notion of *equiprojectable decomposition*, they have brought the first modular algorithm for computing triangular decompositions [5]. The second part of this tutorial will focus on polynomial GCDs modulo regular chains. Using the `RegularChains` library [12] in MAPLE, we show how they are used for producing equiprojectable decompositions.

Implementation. This is certainly the *hot topic* today. Obtaining fast algorithms for the low-level routines used in triangular decompositions [6] and developing implementation techniques for them [9] are the priorities that we shall discuss in the last part of this tutorial.

1. REFERENCES

[1] P. Aubry, D. Lazard, and M. Moreno Maza. On the theories of triangular sets. *J. Symb. Comp.*, 28(1-2):105–124, 1999.

[2] P. Aubry and M. Moreno Maza. Triangular sets for solving polynomial systems: A comparative implementation of four methods. *J. Symb. Comp.*, 28(1-2):125–154, 1999.

[3] F. Boulier, D. Lazard, F. Ollivier, and M. Petitot. Representation for the radical of a finitely generated differential ideal. In *proceedings of ISSAC'95*, pages 158–166, 1995.

[4] S.C. Chou and X.S. Gao. Solving parametric algebraic systems. In *Proc. ISSAC'92*, pages 335–341, Berkeley, California, 1992.

[5] X. Dahan, M. Moreno Maza, É. Schost, W. Wu, and Y. Xie. Lifting techniques for triangular decompositions. In *ISSAC'05*, pages 108–115. ACM Press, 2005.

[6] X. Dahan, M. Moreno Maza, É. Schost, and Y. Xie. On the complexity of the D5 principle. In *Proc. of* Transgressive Computing 2006, Granada, Spain, 2006.

[7] X. Dahan and É. Schost. Sharp estimates for triangular sets. In *ISSAC 04*, pages 103–110. ACM, 2004.

[8] J. Della Dora, C. Dicrescenzo, and D. Duval. About a new method for computing in algebraic number fields. In *Proc. EUROCAL 85 Vol. 2*, volume 204 of *Lect. Notes in Comp. Sci.*, pages 289–290. Springer-Verlag, 1985.

[9] A. Filatei, X. Li, M. Moreno Maza, and É Schost. Implementation techniques for fast polynomial arithmetic in a high-level programming environment. In *Proc. ISSAC'06*. ACM Press, 2006.

[10] G. Gallo and B. Mishra. Efficient algorithms and bounds for Wu-Ritt characteristic sets. In *Proc. MEGA'90*, pages 119–142, 1990.

[11] M. Kalkbrener. *Three contributions to elimination theory*. PhD thesis, Johannes Kepler University, Linz, 1991.

[12] F. Lemaire, M. Moreno Maza, and Y. Xie. The `RegularChains` library. In Ilias S. Kotsireas, editor, Maple Conference 2005, pages 355–368, 2005.

[13] M. Moreno Maza. On triangular decompositions of algebraic varieties. Technical Report TR 4/99, NAG Ltd, Oxford, UK, 1999. http://www.csd.uwo.ca/∼moreno.

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

[15] D. M. Wang. An elimination method for polynomial systems. *J. Symb. Comp.*, 16:83–114, 1993.

[16] W. T. Wu. A zero structure theorem for polynomial equations solving. *MM Research Preprints*, 1:2–12, 1987.

[17] L. Yang and J. Zhang. Searching dependency between algebraic equations: an algorithm applied to automated reasoning. In J. Johnson, S. McKee, and A. Vella, editors, *Artificial intelligence in mathematics*. Oxford University Press, 1994.