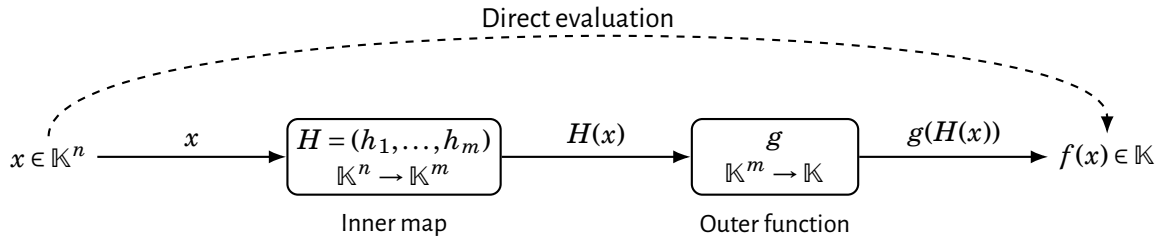


Exploiting Decomposable Structures in Multivariate Polynomial Systems: Algorithms and Applications

Thi Xuan Vu

CFHP, CRISTAL, Université de Lille, France

thi-xuan.vu@univ-lille.fr



Symbolic computation, also known as computer algebra, is the art of manipulating and computing exactly with mathematical objects. It enables the expression and exact solution of mathematical problems using variables, formulas, and symbols (e.g., π , $+\infty$, and $T^2 - 2$ to represent $\sqrt{2}$), as well as mathematical functions. Symbolic computation provides infinite precision, avoiding catastrophic cancellations that can lead to inaccuracies in finite precision. As a result, highly accurate results are obtained. When mathematical objects possess some algebraic structures, symbolic computation becomes a preferred methodology, allowing for the exploitation of algebraic patterns and properties. Hence, symbolic computation is a key technology for solving many difficult mathematical problems, among which polynomial systems appear frequently.

I. Context and Objectives of the Thesis

Decomposable polynomials, that is, polynomials that can be expressed as a composition of lower-degree polynomials, constitute a fundamental topic in computational algebra with several important applications. These include cryptography (see, e.g., [27, 16, 15, 12]), control theory and system identification [14], computer aided geometry [9], signal processing [33], as well as the analysis and reduction of differential equations (cf. [26] and references therein).

Precisely, a polynomial $f \in \mathbb{K}[x_1, \dots, x_n]$ is called *decomposable* if there exist polynomial $g \in \mathbb{K}[y_1, \dots, y_m]$, where $(y_1, \dots, y_m)$ is a set of new variables, and polynomials $H = (h_1, \dots, h_m) \in \mathbb{K}[x_1, \dots, x_n]$ such that

$$f(x_1, \dots, x_n) = g(h_1(x_1, \dots, x_n), \dots, h_m(x_1, \dots, x_n)). \quad (1)$$

A sequence of polynomials $F = (f_1, \dots, f_s)$ is called decomposable if each of polynomial f_i is decomposable. In this case, we write $F = G(H) = G \circ H$.

The aim of this PhD is to investigate several fundamental problems related to decomposable polynomials, including their detection, the computation of explicit decompositions, and the solution of decomposable polynomial systems over a given field, together with applications in areas such as real algebraic geometry and optimization

The *Polynomial Decomposition Problem (PDP)*, known to be NP-hard [11, 35], asks: given a polynomial f , do there exist polynomials $h_1, \dots, h_m$ and a polynomial g such that $g \neq f$, $\deg(g) \leq \deg(f)$, and (1) holds, and if so, how can such a decomposition be computed? Despite its importance, the PDP remains poorly understood in the multivariate setting, and efficient algorithms are known only in restricted cases. In contrast, the univariate functional decomposition problem is well understood; polynomial-time algorithms based on factorization in composition algebras are known [21, 1] and are implemented in major computer algebra systems (for e.g., the `compoly` function in MAPLE). In the multivariate case, however, algorithms are currently known only for homogeneous polynomials of the same degree [16], leaving the general PDP open.

Another fundamental problem in computational algebraic geometry and computer algebra is *polynomial system solving* (PSS). Polynomial systems arise in a wide range of symbolic and scientific applications, including robotics, geometric modeling, signal processing, cryptology, and structural molecular biology. In general, PSS is computationally difficult and is known to be NP-hard [17]. The difficulty frequently encountered in the exact manipulation of mathematical objects is the overhead coming from huge algebraic data, with considerable effort being devoted to finding efficient algorithms. One promising strategy to mitigate this effect is to exploit hidden algebraic structures in the system, such as *decomposability*, in order to reduce complexity and accelerate computations. However, relatively little work has been devoted to systematically exploiting decomposability to obtain faster algorithms.

II. Work Plan

The PhD project will span 36 months, structured as the following.

a. Theoretical Foundations & Decomposition Algorithms

Develop rigorous theoretical and algorithmic foundations for detecting, computing, and exploiting decompositions of multivariate polynomial maps through exact and hybrid symbolic-numeric approaches.

Detecting Decomposability. Investigate decomposability certificates by studying matrix factorizations of the Jacobian $J_F(a) = P(a) \cdot Q(a)$ for points $a \in \overline{\mathbb{K}}^n$ using hybrid symbolic-numeric techniques. In parallel, analyze the imprimitivities of monodromy groups of branched covers to characterize underlying compositional structures. Recently, in [13], the authors used monodromy to recover symmetries of polynomial systems, which can be viewed as a particular case of decomposable structures.

Computing Explicit Decompositions. A standard and robust strategy to compute a decomposition $G \circ H$, when it exists, is to first determine H and then recover G . The recent work of T. X. Vu [36] provides a solution for a particular case of the second step. Specifically, when $H = (h_1, \dots, h_n)$ consists of n algebraically independent polynomials, recovering the outer map G is fully solved. The general case, however, for arbitrary inner polynomials $H = (h_1, \dots, h_m)$, remains open. In this thesis, we will develop a differential approach to functional decomposition based on derivative modules $\mathcal{D}_F = \text{span}\{\frac{\partial F}{\partial x_1}, \dots, \frac{\partial F}{\partial x_n}\}$. Identify integrable generators satisfying $\frac{\partial w_i}{\partial x_j} = \frac{\partial w_j}{\partial x_i}$ to reconstruct the hidden inner map H , extending existing techniques to general multivariate maps.

Solving Decomposable Systems (DPSS). Design symbolic and numerical continuation frameworks to solve $F(x) = (G \circ H)(x) = 0$. Two approaches will be considered in this project: either solving in two steps (outer solving step for G , and lifting step for H), or solving $F = 0$ in a single step, but exploiting the knowledge of the decomposition $F = G \circ H$. To investigate these approaches, we propose to use *homotopy continuation methods*.

- *Symbolic Homotopy:* We will exploit the decomposable structure $F = G \circ H$ to design symbolic homotopy algorithms for computing parametrizations of the solution set, with both arithmetic and bit-complexity

analyses. We will investigate two complementary approaches. First, we solve the outer system $G(y) = 0$ and then lift its solutions through $H(x) = y$ using Newton–Hensel lifting [18, 36, 37]. Second, we solve F directly while exploiting its compositional structure, studying the geometry of the supports and the resulting mixed volumes to obtain sharp solution bounds and suitable starting systems.

- *Numerical Homotopy*: For a decomposable system $F = G \circ H$, the Jacobian factorizes as

$$J_F(a) = J_G(H(a)), J_H(a),$$

which can be exploited to design more efficient predictor-corrector methods. We will adapt existing numerical approaches [6, 7, 3, 23], investigating Newton corrections based on either the full Jacobian or its two factors. We will also develop appropriate condition numbers and complexity bounds for these methods.

- *Validated Symbolic-Numeric Homotopy*: Validated numerics [25, 34, 32, 4] combines the efficiency of floating-point computation with rigorous guarantees by enclosing exact solutions in certified intervals. We aim to develop validated numerical homotopy methods for decomposable systems. Building on recent approaches based on Krawczyk’s method [20] and validated Newton–Puiseux techniques for singularities [5], we aim to address the multiple roots and singularities that naturally arise in decomposable systems. A key objective is to combine structural information on singularities with validated numerical methods, while deriving explicit bounds on the required floating-point precision and, ultimately, a complete bit-complexity analysis.

b. Applications to Demanding Problems

Apply the algorithms developed in Section a to accelerate performance in polynomial optimization and real algebraic geometry.

Polynomial Optimization. Polynomial optimization problems (POPs) provide a flexible framework for modeling nonlinear systems but are, in general, NP-hard. The Moment-SOS approach of Lasserre [24] solves POPs through a hierarchy of semidefinite relaxations, but the resulting SDPs grow rapidly with the number of variables and typically provide only approximate certificates. Structural properties can significantly reduce this complexity [31, 38].

This part will investigate how decomposable structures can be exploited to construct smaller primal-dual relaxations and improve the scalability and numerical stability of polynomial optimization. We will also develop hybrid symbolic-numeric methods combining efficient first-order SDP solvers with Newton/homotopy techniques, with the goal of computing high-precision and ultimately exact certificates for global optima.

Real Algebraic Geometry. Real algebraic geometry involves computationally demanding problems such as deciding the existence of real solutions, computing sample points, and determining connectivity of semi-algebraic sets. Classical approaches, including cylindrical algebraic decomposition and critical-point methods, have been progressively improved to achieve singly exponential complexity in the number of variables [10, 19, 28, 8, 2]. Recent work has shown that exploiting structural properties such as symmetry can significantly improve these bounds [22, 29, 30].

In this part of the thesis, we will investigate how decomposable structures $F = G \circ H$ can similarly be exploited to accelerate algorithms for real root detection and connectivity. The key idea is to analyze the geometry of the outer system G and lift its solutions through the inner map H , thereby reducing computational costs and enabling the treatment of larger, structured instances.

c. Implementation, Software, and Reproducibility

We will develop an open-source software platform enabling researchers to experiment with decomposition-based methods and reproduce the project's results. Open-source software libraries interfaced with JULIA¹ and MAPLE², together with documentation, tutorials, and benchmark datasets. Implementations will combine the strengths of JULIA for high-performance numerical algebraic geometry, MAPLE for symbolic computation and certification, and MSOLVE³ for efficient solving of zero-dimensional polynomial systems.

III. Supervision Team and PhD Candidate

This research proposal is supported by guaranteed Ph.D. funding as part of the ANR JCJC project **ANR-26-CE48-6773-01 – DECOMPASS**. The Ph.D. thesis will be carried out within the CFHP (Computer Algebra and HPC) team at the CRISTAL research unit, Université de Lille, France.

The thesis will be primarily supervised by Thi Xuan Vu (Université de Lille / CRISTAL, France), in collaboration with Florent Bréhard (CNRS, France) and Josué Tonelli-Cueto (CUNEF Universidad, Spain), whose complementary expertise covers symbolic computation, validated numerics, and numerical complexity.

- **Thi Xuan Vu** works on solving multivariate polynomial systems using symbolic homotopy techniques, exploiting structural properties to design faster algorithms, and computational real algebraic geometry.
- **Florent Bréhard** works at the intersection of computer algebra, validated numerics, and formal proof, with the goal of combining the efficiency of floating-point computation with rigorous guarantees.
- **Josué Tonelli-Cueto** focuses on the design and analysis of numerical methods for nonlinear problems, using condition numbers, algebraic geometry, and probability to develop theoretical complexity guarantees.

Student required skills. A background in algebra, algorithms, and/or numerical analysis, as well as basic programming skills, would be useful but is not mandatory. An interest in computational mathematics and computer algebra is expected.

IV. References

- [1] D. Barton and R. Zippel. Polynomial decomposition algorithms. *Journal of Symbolic Computation*, 1(2):159–168, 1985.
- [2] S. Basu, R. Pollack, and M.-F. Roy. On the combinatorial and algebraic complexity of quantifier elimination. *Journal of the ACM (JACM)*, 43(6):1002–1045, 1996.
- [3] D. J. Bates, A. J. Sommese, J. D. Hauenstein, and C. W. Wampler. *Numerically solving polynomial systems with Bertini*. SIAM, 2013.
- [4] F. Bréhard. *Certified numerics in function spaces*. PhD thesis, École Normale Supérieure de Lyon, 2019.
- [5] F. Bréhard, F. Corinaldesi, and A. Poteaux. Validated numerical Newton–Puisseux algorithm. In *Proceedings of the 2026 International Symposium on Symbolic and Algebraic Computation*, pages 58–67, 2026.
- [6] P. Bürgisser and F. Cucker. *Condition: The geometry of numerical algorithms*, volume 349. Springer Science & Business Media, 2013.
- [7] P. Bürgisser, F. Cucker, and P. Lairez. Rigid continuation paths II. Structured polynomial systems. In *Forum of Mathematics, Pi*, volume 11, page e12. Cambridge University Press, 2023.
- [8] J. Canny. *The complexity of robot motion planning*. MIT Press, 1987.
- [9] E.-W. Chionh, X.-S. Gao, and L.-Y. Shen. Inherently improper surface parametric supports. *Computer Aided Geometric Design*, 23(8):629–639, 2006.
- [10] G. E. Collins. Quantifier elimination for real closed fields by cylindrical algebraic decomposition: a synopsis. *ACM SIGSAM Bulletin*, 10(1):10–12, 1976.

¹<https://julialang.org/>

²<https://www.maplesoft.com/>

³<https://msolve.proj.lip6.fr/>

- [11] M. T. Dickerson. General polynomial decomposition and the $(s-1)$ -decomposition are NP-hard. *International Journal of Foundations of Computer Science*, 4(2):147–156, 1993.
- [12] J. Ding and D. Schmidt. Rainbow, a new multivariable polynomial signature scheme. In *ACNS 2005*, volume 3531 of *LNCS*, pages 164–175. Springer, 2005.
- [13] T. Duff, V. Korotynskiy, T. Pajdla, and M. Regan. Using monodromy to recover symmetries of polynomial systems. In *Proceedings of the 2023 International Symposium on Symbolic and Algebraic Computation*, pages 251–259, 2023.
- [14] C. Ebenbauer, T. Faulwasser, and F. Allgöwer. Analysis and design of polynomial control systems. *Automatica*, 42(10):1717–1727, 2006.
- [15] J.-C. Faugère and A. Joux. Algebraic cryptanalysis of hidden field equation (HFE) cryptosystems using Gröbner bases. In *CRYPTO 2003*, volume 2729 of *LNCS*, pages 44–60. Springer, 2003.
- [16] J.-C. Faugère and L. Perret. An efficient algorithm for decomposing multivariate polynomials and its applications to cryptography. *Journal of Symbolic Computation*, 44(12):1676–1689, 2009.
- [17] M. R. Garey and D. S. Johnson. *Computers and Intractability: A Guide to the Theory of NP-Completeness*, volume 29 of *Series of Books in the Mathematical Sciences*. W. H. Freeman and Company, New York, 2002.
- [18] M. Giusti, G. Lecerf, and B. Salvy. A Gröbner free alternative for polynomial system solving. *Journal of complexity*, 17(1):154–211, 2001.
- [19] D. Y. Grigor’ev and N. N. Vorobjov Jr. Solving systems of polynomial inequalities in subexponential time. *Journal of Symbolic Computation*, 5(1-2):37–64, 1988.
- [20] A. Guillemot and P. Lairez. Validated numerics for algebraic path tracking. In *Proceedings of the 2024 International Symposium on Symbolic and Algebraic Computation*, pages 36–45, 2024.
- [21] D. Kozen and S. Landau. Polynomial decomposition algorithms. *Journal of Symbolic Computation*, 7(5):445–456, 1989.
- [22] G. Labahn, C. Riener, M. Safey El Din, É. Schost, and T. X. Vu. Faster real root decision algorithm for symmetric polynomials. In *Proceedings of the 2023 International Symposium on Symbolic and Algebraic Computation*, pages 452–460, 2023.
- [23] P. Lairez. Rigid continuation paths I. Quasilinear average complexity for solving polynomial systems. *Journal of the American Mathematical Society*, 33(2):487–526, 2020.
- [24] J. B. Lasserre. Global optimization with polynomials and the problem of moments. *SIAM Journal on optimization*, 11(3):796–817, 2001.
- [25] R. E. Moore, R. B. Kearfott, and M. J. Cloud. *Introduction to interval analysis*. SIAM, 2009.
- [26] A. Ovchinnikov, I. Pérez Verona, G. Pogudin, and M. Tribastone. CLUE: exact maximal reduction of kinetic models by constrained lumping of differential equations. *Bioinformatics*, 37(12):1732–1738, 2021.
- [27] J. Patarin. Hidden field equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms. In *EUROCRYPT 1996*, volume 1070 of *LNCS*, pages 33–48. Springer, 1996.
- [28] J. Renegar. On the computational complexity and geometry of the first-order theory of the reals. part I: Introduction. preliminaries. the geometry of semi-algebraic sets. the decision problem for the existential theory of the reals. *Journal of symbolic computation*, 13(3):255–299, 1992.
- [29] C. Riener, R. Schabert, and T. X. Vu. Connectivity in symmetric semi-algebraic sets. In *Proceedings of the 2024 International Symposium on Symbolic and Algebraic Computation*, pages 162–169, 2024.
- [30] C. Riener, R. Schabert, and T. X. Vu. Deciding connectivity in symmetric semi-algebraic sets. *Journal of Symbolic Computation*, page 102599, 2027.
- [31] C. Riener, T. Theobald, L. J. Andrén, and J. B. Lasserre. Exploiting symmetries in SDP-relaxations for polynomial optimization. *Mathematics of Operations Research*, 38(1):122–141, 2013.
- [32] S. M. Rump. Verification methods: rigorous results using floating-point arithmetic. *Acta numerica*, 19:287–449, 2010.
- [33] G. Su. *Polynomial decomposition algorithms in signal processing*. PhD thesis, Massachusetts Institute of Technology, 2013.
- [34] W. Tucker. *Validated numerics: a short introduction to rigorous computations*. Princeton University Press, 2011.
- [35] J. von zur Gathen, J. Gutierrez, and R. Rubio. Multivariate polynomial decomposition. *Applicable Algebra in Engineering, Communication and Computing*, 14(1):11–31, 2003.
- [36] T. X. Vu. Computing polynomial representation in subrings of multivariate polynomial rings. In *Proceedings of the 2025 International Symposium on Symbolic and Algebraic Computation*, pages 284–292, 2025.
- [37] T. X. Vu. A symbolic homotopy algorithm for solving composable polynomial systems. In *Proceedings of the 2026 International Symposium on Symbolic and Algebraic Computation*, pages 379–387, 2026.
- [38] J. Wang, V. Magron, and J.-B. Lasserre. TSSOS: A moment-SOS hierarchy that exploits term sparsity. *SIAM Journal on optimization*, 31(1):30–58, 2021.