Functional Decomposition of Sparse Polynomials (Short Talk Abstract)

Mark Giesbrecht

Cheriton School of Computer Science, University of Waterloo, Canada

Keywords
Computer algebra, sparse polynomials, complexity.

We consider the algorithmic problem of functionally decomposing sparse polynomials. For example, given a (ridiculously) high degree ($5 \cdot 2^{100}$) and very sparse (7 terms) polynomial such as:

$$f(x) = x^{5\cdot 2^{100}} + 15 \cdot x^{2^{102}+2^{47}} + 90 \cdot x^{3\cdot 2^{100}+2^{48}} + 270 \cdot x^{2^{101}+3\cdot 2^{47}} + 405 \cdot x^{2^{100}+2^{49}} + 243 \cdot x^{5\cdot 2^{47}} + 1,$$

we ask how to determine quickly whether it can be written as a composition of lower degree polynomials such as

$$f(x) = g(h(x)) = g \circ h = (x^5 + 1) \circ (x^{2^{100}} + 3x^{2^{47}}),$$

and if so, to generate such a decomposition.

That such decompositions remain sparse was first conjectured for perfect powers in 1949 by Erdős [3], but not proven until 1987 by Schinzel [9]. Zannier [10] then generalized this theory to functional decompositions.

Computationally, we have had algorithms for functional decomposition of (dense) polynomials since Barton & Zippel [2] in 1976. The first polynomial-time (in the degree) algorithms appeared in 1986 by [7], at least in the "tame" case, where the characteristic of the underlying field does not divide the degree, and an almost linear time algorithm was shown later in [4]. In fact, we can now show that, except for a very specific class of polynomials, Barton & Zippel's algorithm runs in polynomial time in the degree [5]. Polynomial-time algorithms for the (dense) "wild" case and rational functions have now been been developed, most completely in [1].

Algorithms for polynomial decomposition that exploit sparsity have remained elusive until recently (see [6, 8]). We want algorithms that run in time polynomial in the *representation size* – the length/logarithm of the exponents and coefficients of the non-zero terms of the input (and output). In this talk I will present some new algorithms which meet this goal, and provide very fast and simple solutions to some polynomial decomposition problems, such as the example above. These new methods require time quadratic in the number of non-zero terms in the input and output, and in the logarithm of the degree and coefficients.

Many open algorithmic problems remain for sparse polynomials, including detecting indecomposability, the "wild" case, and rational functions. We show connections to the well-known open (and possibly intractable) problems of sparse polynomial divisibility and irreducibility. There is also considerable room to tighten bounds in the underlying mathematics (and thereby improve the cost), as well as to explore a broader class of sparsely represented functions [8].

This is ongoing work with Saiyue Liu (UBC) and Daniel S. Roche (USNA).

References

[1] L. Allem, J. Capaverde, M. van Hoeij, J. Szutkoski, Functional decomposition using principal subfields, in: Proc. 2017 ACM International Symposium on Symbolic and Algebraic Computation, Association for Computing Machinery, New York, NY, USA, 2017, pp. 421–428.

SCSS 2024: 10th International Symposium on Symbolic Computation in Software Science, August 28–30, 2024, Tokyo, Japan
mwg@uwaterloo.ca (M. Giesbrecht)
https://uwaterloo.ca/~mwg (M. Giesbrecht)

[2] D. Barton, R. Zippel, A polynomial decomposition algorithm, in: Proceedings of the third ACM symposium on symbolic and algebraic computation, SYMSAC '76, 1976, pp. 356–358.
[3] P. Erdős, On the number of terms of the square of a polynomial, Nieuw Arch. Wiskunde (2) 23 (1949) 63–65.
[4] J. von zur Gathen, D. Kozen, S. Landau, Functional decomposition of polynomials, in: Proc. 28th Ann. IEEE Symp. Foundations of Computer Science, Los Angeles CA, 1987, pp. 127–131.
[5] M. Giesbrecht, J. May, New algorithms for exact and approximate polynomial decomposition, in: Proc. International Workshop on Symbolic-Numeric Computation (SNC), 2005, pp. 99–112.
[6] M. Giesbrecht, D. S. Roche, Detecting lacunary perfect powers and computing their roots, Journal of Symbolic Computation 46 (2011) 1242–1259.
[7] D. Kozen, S. Landau, Polynomial Decomposition Algorithms, Technical Report 86–773, Department of Computer Science, Cornell University, Ithaca NY, 1986.
[8] S. Lyu, Faster algorithms for sparse decomposition and sparse series solutions to differential equations, Master's thesis, U. Waterloo, Waterloo, ON, Canada, 2022.
[9] A. Schinzel, On the number of terms of a power of a polynomial, Acta Arith. 49 (1987) 55–70.
[10] U. Zannier, On composite lacunary polynomials and the proof of a conjecture of Schinzel, Inventiones Mathematicae 174 (2008) 127–138.