SPARSE EXPONENTS IN SYMBOLIC POLYNOMIALS

MATTHEW MALENFANT AND STEPHEN M. WATT

Abstract. We consider multivariate polynomials with coefficients in an arbitrary ring and exponents that are themselves integer-valued multivariate polynomials. These are known as *symbolic polynomials* because they may be used to model families of polynomials with parametric exponents. These objects have a natural group ring structure and for suitable choices of coefficient ring form a unique factorization domain. Earlier work has shown algorithms to compute GCD and to factor such symbolic polynomials. These algorithms are of limited utility, however, because they have at least exponential computational complexity. The current work improves on this using sparse techniques on the exponent polynomials.

We wish to work with polynomials where the exponents are not known in advance, such as $x^{2n}-1$. There are various operations we want to be able to do, such as squaring the value to get $x^{4n}-2x^{2n}+1$, or differentiating it to get $2nx^{2n-1}$. This is far from a purely academic problem — expressions of this sort arise frequently in practice, for example in the analysis of algorithms, and it is very difficult to work with them effectively in current computer algebra systems.

These objects may be viewed as representing parameteric families of polynomials or as elements of a group ring structure. In either case there is a rich algebraic structure and one is naturally led to examine algorithms for their arithmetic. We view symbolic polynomials as formal polynomials in some base variables $x_1, ..., x_v$ with coefficients from an arbitrary ring and with exponents as multivariate integer-valued polynomials over some domain [2, 3]. Symbolic polynomials are related to exponential polynomials [1, 5] and algorithms relating to families of polynomials with parametric exponents have also been studied in other contexts [6, 7, 8].

In earlier work [9, 10] we have shown that, for suitable coefficient rings and exponent domains, symbolic polynomials form a unique factorization domain and have given algorithms for their GCD and factorization. For example, we are able to compute GCDs such as $\gcd(p,q) = 2x^{n^2+4n}+3$ for

$$\begin{aligned} p = {} & 8x^{n^2+6n+4+m^2-m} - 2x^{2n^2+7n+2mn}y^{n^2+3n} \\ & - 3x^{n^2+3n+2mn}y^{n^2+3n} + 12x^{4+m^2-m+2n} \end{aligned}$$

$$\begin{aligned} q = {} & 4x^{n^2+4n+m^2+6m} - 28x^{n^2+8n+m^2+6m+2}y^{4n^2-4n} \\ & + 2x^{n^2+4n} - 14x^{n^2+8n+2}y^{4n^2-4n} + 6x^{m^2+6m} \\ & - 42x^{m^2+6m+4n+2}y^{4n^2-4n} - 21y^{4n^2-4n}x^{4n+2} + 3. \end{aligned}$$

The algorithms fall into two families: algebraic extension methods and projection methods. The first family of algorithms uses the algebraic independence of x, x^n, x^{n^2}, x^{nm}, etc, to solve related problems with more indeterminates. Some subtlety is needed to avoid problems with fixed divisors of the exponent polynomials. The second family of algorithms uses evaluation and interpolation of the exponent polynomials. While these methods can run into unlucky evaluation points, in many cases they can be more appealing. Neither of these two families of algorithms, however, are attractive from a complexity point of view: The extension methods work in polynomial rings with a number of variables exponential in the number of the symbolic polynomial exponent variables. The projection methods require a number of evaluations exponential in the number of the exponent variables.

This paper presents probabalistic algorithms for the GCD and factorization of symbolic polynomials. These algorithms are projection methods that exploit the sparsity of exponent polynomials to reduce the number of required evaluations. We adapt the ideas of Zippel's sparse interpolation [4] and apply them to limit the number of evaluations in the symbolic polynomial exponent domain, potentially reducing the number of required image computations by an exponential factor.

References

[1] Baron Gaspard Riche de Prony, Essai éxperimental et analytique: sur les lois de la dilatabilité de fluides élastique et sur celles de la force expansive de la vapeur de l'alkool, à différentes températures. Journal de l'École Polytechnique, volume 1, cahier 22, 24-76 (1795).

[2] G. Pólya, Über ganzwertige Polynome in algebraischen Zahlköpern, J. Reine Angew. Math., 149 (1919), 97-116.

[3] A. Ostrowski, Über ganzwertige Polynome in algebraischen Zahlköpern, J. Reine Angew. Math., 149 (1919), 117-124.

[4] R. Zippel, Probabalistic algorithms for sparse polynomials. Proc EUROSAM '79, Volume 2 Lecture Notes in Computer Science, Springer Verlag 1979, 216-226.

[5] C.W. Henson, L. Rubel and M. Singer, Algebraic Properties of the Ring of General Exponential Polynomials. Complex Variables Theory and Applications, **13**, 1989, 1-20.

[6] K. Yokoyama, On Systems of Algebraic Equations with Parametric Exponents. pp 312-319, ISSAC '04, July 4-7, 2004, Santander, Spain, ACM Press.

[7] V. Weispfenning, Gröbner bases for binomials with parametric exponents. Technical report, Universität Passau, Germany, 2004.

[8] W. Pan and D. Wang., Uniform Gröbner bases for ideals generated by polynomials with parametric exponents. Proc ISSAC 2006, ACM, 269–276.

[9] S.M. Watt, Two Families of Algorithms for Symbolic Polynomials, Proc Waterloo Workshop on Computer Algebra: Devoted to the 60th birthday of Sergei Abramov, April 10-12, 2006, Waterloo, Canada, World Scientific (in press).

[10] S.M. Watt, Making Computer Algebra More Symbolic, Proc TC 2006: A conference in honor of Jean Della Dora, April 24-26, 2006, Granada, Spain, 43–49.

Dept of Computer Science, U. Western Ontario, London Ontario, Canada N6A 5B7
E-mail address: watt@csd.uwo.ca
URL: http://www.csd.uwo.ca/~watt