Algorithms for Symbolic Polynomials (Plenary Talk)

Stephen M. Watt

Ontario Research Centre for Computer Algebra
University of Western Ontario
London Canada
watt@orcca.on.ca

Abstract. We wish to work with polynomials where the exponents are not known in advance, such as $x^{2n} - 1$. There are various operations we will want to be able to do, such as squaring the value to get $x^{4n} - 2x^{2n} + 1$, or differentiating it to get $2nx^{2n-1}$. 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.

We consider the case where multivariate polynomials can have exponents which are themselves integer-valued multivariate polynomials, and we present algorithms to compute their GCD and factorization. The algorithms fall into two families: algebraic extension methods and interpolation 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. Additionally, we also treat the case of symbolic exponents on rational coefficients (e.g. $4^{n^2+n} - 81$) and show how to avoid integer factorization.