MARK GIESBRECHT, University of Waterloo, Waterloo, Ontario, Canada

New Algorithms for Lacunary Polynomials

Some of the most compelling theoretical work in computer algebra of the past decade has been on computations with lacunary or super-sparse polynomials. Computer algebra systems (and mathematicians!) are good at representing multivariate polynomials of very high degree but only a few terms in the form of a linked list of coefficient/exponent tuples. However, the repertoire of algorithms for computing with polynomials in this representation is limited, and the area is fraught with intractable problems. Recent work of Lenstra, Kaltofen and Koiran has extended the reach of fast algorithms. We seek here to further augment the available toolkit.

We give new algorithms for two important problems. First, we give an algorithm to interpolate an unknown integer polynomial in the sparsest shifted power basis. We assume that we are given a function or "black box" for evaluating that polynomial at a point modulo a prime or at a (complex) root of unity. Second, the question of functionally decomposing a univariate polynomial is investigated when the input is lacunary. A new algorithm is proposed to compute sparse decompositions. Some interesting connections are noted to long-standing open problems studied by Erdős, Schinzel and others.

This is work with Daniel Roche (Waterloo).