DANIEL S. ROCHE, University of Waterloo, 300 University Ave. W., Waterloo, ON N2L 3G1

Sparse interpolation and small primes in arithmetic progressions

In recent work, we have developed the first polynomial-time algorithm to interpolate an unknown univariate rational polynomial $f \in \mathbb{Q}[x]$ into the sparsest shifted power basis. That is, we find the "sparsest shift" α such that $f(x+\alpha)$ has the fewest number of nonzero terms, and then explicitly compute the terms of f in the shifted power basis $[1, (x-\alpha), (x-\alpha)^2, \ldots]$. Both steps in the algorithm work by computing over a series of fields $\mathbb{Z}/p\mathbb{Z}$ for many small primes p. In order to guarantee that the crucial information about f is not lost by working modulo p, certain equalities must not hold in both the additive and multiplicative groups of $\mathbb{Z}/p\mathbb{Z}$. Our method for finding primes p that satisfy these conditions involves finding small primes in certain arithmetic progressions, which fortunately is a well-studied problem in number theory. Since the efficiency of the algorithm depends heavily on the size of the chosen primes, we need good bounds on their size. We examine the various approaches and results used to construct these small primes, and discuss some open problems and areas for further refinement.

This is joint work with Mark Giesbrecht.