1077-68-906 **Daniel S Roche*** (`roche@usna.edu`). *Finding a polynomial multiple that is sparse.*

Recent work is presented on the problem of computing sparse multiples of polynomials over the rational numbers or a finite field. Specifically, given a (dense) polynomial $f \in \mathsf{F}[x]$, we look for another polynomial $g \in \mathsf{F}[x]$ with $f|g$, such that g has higher degree but fewer nonzero terms than f. Depending on the field F, a bound on the degree of the multiple g, or on the coefficient sizes, is also required.

This problem has important applications in cryptography and extension field arithmetic. Though a few heuristic approaches have previously been developed, our interest is in the existence or nonexistence of polynomial-time algorithms in the *size* of the polynomials (that is, the number of nonzero terms, the logarithm of degree, and the size of the coefficients). We provide such polynomial-time algorithms for certain cases, and prove NP-hardness in other cases.

This is joint work with Mark Giesbrecht and Hrushikesh Tilak at the University of Waterloo. (Received September 14, 2011)