Interval Partitions and Polynomial Factorization

Joachim von zur Gathen, Daniel Panario, Bruce Richmond

February 9, 2009

Abstract

The average cost of baby-step/giant-step polynomial factorization algorithms is studied. It depends on the distribution of the degrees of the irreducible factors of a random polynomial of degree n in subintervals of a given partition of the interval $[1 \ldots n]$. When factoring polynomials over finite fields, the presence of more than one irreducible factor degree in a subinterval is of particular interest; we called this a *multi-factor interval.* For each partition, we study several parameters of random polynomials such as the expected number of multi-factor intervals, the expected number of irreducible factors with degrees lying in multi-factor intervals, the number of gcds executed in the factoring process, and the expected total degree among the irreducible factors with degrees in multi-factor intervals. We also study the probability of a polynomial to have no multi-factor intervals for a given partition. Our studies are general for partitions with growing interval sizes, and we also specialize to specific partitions. We provide, among the partitions considered, the one that minizes the the expected number of gcds computed when the polynomial to be factored is taken uniformly at random.