Analysis of Rabin’s Irreducibility Test for Polynomials Over Finite Fields

Daniel Panario*, Boris Pittel, Bruce Richmond,
Alfredo Viola*

Abstract  We give a precise average-case analysis of Rabin’s algorithm for testing the irreducibility of polynomials over finite fields. The main technical contribution of the paper is the study of the probability that a random polynomial of degree $n$ contains an irreducible factor of degree dividing several maximal divisors of the degree $n$. We then study the expected value and the variance of the number of operations performed by the algorithm. We present an exact analysis when $n = p_1$ and $n = p_1p_2$ for $p_1, p_2$ prime numbers, and an asymptotic analysis for the general case. Our method generalizes to other algorithms that deal with similar divisor conditions. In particular, we analyze the average-case number of operations for two variants of Rabin’s algorithm, and determine the ordering of prime divisors of $n$ that minimizes the leading factor.