Randomness and Complexity of Sequences over Finite Fields

Harald Niederreiter

RICAM Linz and University of Salzburg
E-mail: ghnied@gmail.com

Abstract

Random sequences of bits, and more generally of elements of a finite field, are needed for simulation methods and cryptography. The assessment of the randomness of such a sequence proceeds by complexity-theoretic and statistical methods. We first survey complexity measures that are relevant for cryptography and then investigate the relationship between these complexity measures and equidistribution properties of sequences. Probabilistic results on the behavior of complexity measures for random sequences will also be discussed.