ID: P1.14

Title: Pseudorandom number generators for Monte Carlo simulations: equidistribution property, statistical independence of bits and effective implementations using SIMD parallelism of modern CPUs

Name: Barash, Lev

Affiliation: Landau Institute for Theoretical Physics, 142432, Chernogolovka, Russia

New algorithms for generating uniform pseudorandom numbers are proposed and studied. The theory of the generators, which includes proofs of periodic properties and of statistical independence of bits at distances up to logarithm of mesh size, is presented. Extensive statistical testing using available test packages demonstrates excellent results, while SIMD parallelism of modern Intel and AMD processors results in increasing of the speed of the new generators which becomes comparable to other modern generators. We present the library RNGSSELIB for pseudorandom number generators based on SIMD parallelism of modern Intel and AMD processors. The library contains realization of a number of modern and most reliable generators, including the proposed new generators. Usage of SIMD parallelism allows to substantially improve performance of the generators. [1] L.Yu. Barash, L.N. Shchur, RNGSSELIB: Program library for random number generation, SSE2 realization, Computer Physics Communications 182 (2011) 1518-1527. [2] L.Yu. Barash, Applying dissipative dynamical systems to pseudorandom number generation: Equidistribution property and statistical independence of bits at distances up to logarithm of mesh size, Europhysics Letters 95 (2011) 10003.