Письма в ЭЧАЯ. 2025. Т. 22, № 5(262). С. 986

КОМПЬЮТЕРНЫЕ ТЕХНОЛОГИИ В ФИЗИКЕ

QUALITY RANDOM NUMBER GENERATOR

M. Dima [a, 1], *M.-T. Dima* [a], *S. Dima* [a], *M. Mihailescu* [b]

[a] Joint Institute for Nuclear Research, Dubna, 141980, Russia

[b] Hyperion University, Bucharest, RO-030615, Romania

Numerous applications in physics and technology rely on random number generation: for Monte Carlo purposes, key distribution, and other tasks. Accordingly, elaborate hash functions with carefully studied and tuned algorithms have been developed, giving pseudo-random numbers. Depending on the complexity and quality of their output, they vary from very good quality (such as RANLUX with a 10^{171} repetition period) to fast algorithms, however of lesser period (such as the Mersenne Twister, a factor of ca. $\times 40$ faster). We present the implementation of a true-random number "multiplier" algorithm. It relies on a finite set of true-random numbers from a physical source (in our case 0.2 million random numbers of atmospheric noise in the range of 0–9999). The algorithm produces new numbers by combining pairs of two random numbers from the list, situated at random distance apart. The random offset is calculated by a shift register structure involving both the local rand() generator and numbers from the list itself, whereby it produces "non-repetitive repetitions", i.e., our multiplier has no known period. The tests, performed with the DieHarder test suite, show good quality.

Многочисленные приложения в физике и технике используют генерацию случайных чисел: для методов Монте-Карло, распределения ключей и других задач. Для этих целей были разработаны сложные хеш-функции с тщательно изученными и настроенными алгоритмами, дающие псевдослучайные числа. В зависимости от сложности и качества выходных данных они варьируются от алгоритмов с очень хорошим качеством (например, RANLUX с периодом повторения 10^{171}) до быстрых, однако с меньшим периодом (например, Mersenne Twister, примерно в 40 раз быстрее). Мы представляем реализацию алгоритма «умножения» истинно случайных чисел. Алгоритм опирается на конечный набор истинно случайных чисел из физического источника (в нашем случае 0,2 млн случайных чисел атмосферного шума в диапазоне 0–9999). Алгоритм выдает новые числа путем объединения пар из двух случайных чисел из списка, находящихся на случайном расстоянии друг от друга. Случайное смещение вычисляется структурой сдвигового регистра, включающей как локальный генератор rand(), так и числа из самого списка, посредством чего он производит «неповторяющиеся повторения» — т. е. наш множитель не имеет известного периода. Тесты, проведенные с помощью тестового набора DieHarder, показывают высокое качество.

PACS: 07.05.Tp

Received on April 7, 2025.

[1] E-mail: mmdima@jinr.ru