ГЕНЕРАЦИЯ ПАРАЛЛЕЛЬНЫХ ПОТОКОВ СЛУЧАЙНЫХ ЧИСЕЛ: РЕШЕНИЕ ПРОБЛЕМЫ КОРРЕЛЯЦИИ

Л.Н. Щур, Л.Ю. Бараш

В работе приводится обзор текущего состояния исследований по генерации параллельных потоков случайных чисел. Формулируется проблема генерации псевдослучайных чисел для проведения расчетов Монте-Карло на параллельных вычислительных системах. Необходимо обеспечить отсутствие корреляций между параллельными потоками псевдослучайных чисел. Также необходимо обеспечить быстрый и эффективный способ получения начальных значений для большого числа параллельных потоков. Обсуждаются способы реализации для различных архитектур параллельных компьютеров, в том числе для гибридных суперкомпьютерных систем. Работа выполнена при поддержке грантов РФФИ 11-07-00471, 12-07-13121 и 13-07-00999 и программы РАН «Высокопроизводительные вычислительные системы и телекоммуникации». Компьютерные ресурсы были выделены Суперкомпьютерным центром МГУ.

Введение.

При проведении моделирования и расчетов методом Монте-Карло используются последовательности случайных чисел. Такие последовательности генерируются с помощью специальных программ, которые называются генераторами псевдослучайных чисел (ГПСЧ). Они основаны на алгоритмах, что и выражает приставка «псевдо». Последовательность псевдослучайных чисел выглядит случайной с точки зрения заданных требований и/или тестирующих ее методов. Не доказано существование алгоритмов, генерирующих истинно случайные числа.

Эффективная реализация метода Монте-Карло на параллельных компьютерных системах накладывает дополнительные требования на способ генерации случайных чисел. Например, при моделировании параллельно нескольких независимых реализаций, необходимо использование нескольких псевдослучайных последовательностей. При этом, необходимы основания для того, чтобы эти последовательности не обладали корреляциями.

Нами развит подход по построению эффективных генераторов псевдослучайных чисел. Подход использован для разработки библиотек программ. Библиотека RNGSSELIB использует процессоры Intel и AMD и дополнительный набор команд SSE2. Языки программирования C и Fortran. Библиотека PRAND использует графические ускорители Nvidia и опробована на суперкомпьютерах «К-100» и «Ломоносов».

ЛИТЕРАТУРА:

1. L. Barash, L.N. Shchur, Periodic orbits of the ensemble of Sinai-Arnold cat maps and pseudorandom number generation, Phys. Rev. E. 73. 2006. 036701.
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, Europhys. Lett. 95. 2011. 10003.
3. L.Yu. Barash, Geometric and statistical properties of pseudorandom number generators based on multiple recursive transformations, Springer Proceedings in Mathematics and Statistics. 23. 2012. 265-280.
4. Л.Ю. Бараш, Л.Н. Щур, Генерация случайных чисел и параллельных потоков случайных чисел для расчетов Монте-Карло, Моделирование и анализ информационных систем. 19. 2012. 145-162.
5. Л.Ю. Бараш, Л.Н. Щур, О генерации параллельных потоков псевдослучайных чисел, Программная инженерия. 1. 2013. 24-32.
6. L.Yu. Barash, L.N. Shchur, RNGSSELIB: Program library for random number generation, SSE2 realization, Comput. Phys. Commun. 182. 2011. 1518-1527.
7. L.Yu. Barash, L.N. Shchur, RNGSSELIB: Program library for random number generation. More generators, parallel streams of random numbers and Fortran compatibility. Comput. Phys. Commun. 184. 2013. Nd.
8. L.Yu. Barash, L.N. Shchur, PRAND: GPU accelerated parallel random number generation library: Using most reliable algorithms and applying parallelism of modern GPUs and CPUs. 184. 2013. Accepted.