Исследование модификаций конгруэнтного генератора псевдослучайных чисел

Трачева Наталья Валерьевна
Институт вычислительной математики и математической геофизики СО РАН (Новосибирск
e-mail: tnv@osmf.sscc.ru

В данной работе рассматривается линейный конгруэнтный генератор вида:

$$u_0 = 1,\ u_n \equiv u_{n-1}M (\mathrm{mod}\ 2^r),\ \alpha_n = u_n 2^{-r}.$$

Здесь r, как правило, число двоичных разрядов, используемых для представления числа, M – множитель генератора, достаточно большое число, взаимно-простое с 2^r, α_n – псевдослучайное число. Для данного генератора длина периода последовательности $\{\alpha_n\}$ равна 2^{r-2}.

В течение многих лет в расчетах методами Монте-Карло использовался конгруэнтный генератор с параметрами $M = 5^{17}$ и $r = 40$ (см., например, [1]). Однако, поскольку период данного генератора ограничен $L = 2^{38} \approx 2,7 \cdot 10^{11}$ случайных чисел, а возможности вычислительных систем в последние годы значительно возрасли, возникла необходимость в использовании генераторов с бóльшим периодом, например, линейного конгруэнтного генератора с параметрами $M = 5^{100109} (\mathrm{mod}\ 2^{128})$ и $r = 128$, т.е. с длиной периода $L = 2^{126} \approx 10^{38}$ (см., например, [2, 3]). Реализация алгоритма для данного генератора обладает высокой вычислительной сложностью и традиционно использует 32-битные целые типы данных и операции с ними.

В данной работе рассматривается 64-битная реализация линейного конгруэнтного генератора с параметрами $M = 5^{100109} (\mathrm{mod}\ 2^{128})$ и $r = 128$, которая позволяет достичь ускорения вычислений на процессорах, архитектура которых поддерживает быструю 64-битную арифметику. Исследован вопрос о возможности "векторизации" данного генератора псевдослучайных чисел. Численно показано, что процедуры "векторного" типа более эффективны, чем их скалярные аналоги. Предложены и численно исследованы модификации рассматриваемого генератора "сдвиг влево на 32 бита" и "нарезка по 52 бита", позволяющие ускорить генерирование последовательности псевдослучайных чисел в 1.5 раза. Исследована возможность использования комбинации генераторов псевдослучайных чисел с параметрами $M = 5^{100109} (\mathrm{mod}\ 2^{128})$ и $r = 128$ и $M = 5^{17}$, $r = 40$. Многомерные распределения последовательностей псевдослучайных чисел, полученных с использованием модифицированных алгоритмов, тестировались на равномерность для размерностей $k = 1, 2, \ldots, 9$ по критерию Пирсона χ^2. Учитывая большой объем статистических выборок и состоятельность критерия, тестирование можно считать успешным.

Список литературы

[1] Михайлов Г.А., Войтишек А.В. Численное статистическое моделирование. М.: Учебно-издательский центр "Академия", 2006.

[2] Dyadkin I.G., Hamilton K.G. A study of 128-bit multipliers for congruential pseudorandom number generators// Comp. Phys. Comm., 2000, Vol. 125, pp.239-258.

[3] Марченко М.А. Михайлов Г.А. Распределенные вычисления по методу Монте-Карло// Автоматика и телемеханика. 2007, № 5. С. 157–170.