

Pseudo-random numbers generators test for CAS

M. N. Gevorkyan (RUDN University, Moscow)

A. V. Demidova (RUDN University, Moscow)

A. V. Korolkova (RUDN University, Moscow)

D. S. Kulyabov (RUDN University, Moscow; LIT JINR, Dubna)

E-mail address: `gevorkyan-mn@rudn.ru`, `kulyabov-ds@rudn.ru`,
`demidova-av@rudn.ru`, `korolkova-av@rudn.ru`

For a long time the implementation of pseudo-random number sequence generators in standard programming language libraries and mathematical packages was of poor quality. The situation has started to improve relatively recently. Even nowadays a large number of libraries and poorly supported mathematical packages utilize the old algorithms of pseudo-random numbers generation. We describe four actual sets of statistical tests that can be used to test the generator that is used in a particular software system. The emphasis is on the use of command-line utilities, to avoid low-level programming.

Тестирование генераторов случайных чисел для систем компьютерной алгебры

М. Н. Геворкян (РУДН, Москва)

А. В. Демидова (РУДН, Москва)

А. В. Королькова (РУДН, Москва)

Д. С. Кулябов (РУДН, Москва; ЛИТ ОИЯИ, Дубна)

А.А. Петрова (МГУ, Москва)

E-mail address: `gevorkyan-mn@rudn.ru`, `kulyabov-ds@rudn.ru`,
`demidova-av@rudn.ru`, `korolkova-av@rudn.ru`

Долгое время реализации генераторов последовательностей псевдослучайных чисел в стандартных библиотеках языков программирования и математических пакетов были плохо проработаны. Ситуация начала улучшаться сравнительно недавно. До сих пор большое количество библиотек и слабо поддерживаемых математических пакетов используют в своем составе старые алгоритмы генерации псевдослучайных чисел. Описывается четыре актуальных набора статистических тестов, которые можно применить для проверки генератора, который используется в той или иной программной системе. Упор делается на использование утилит командной строки, что позволяет избежать довольно низкоуровневого программирования.