Предельные совместные распределения статистик, используемых при проверке качества генераторов случайных двоичных последовательностей

М. П. Савелов*

Тезисы

Пусть $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n$ — последовательность независимых случайных величин, имеющих распределение Бернулли $Bern(p)$, $p \in (0,1)$. Для проверки гипотезы о том, что $p = \frac{1}{2}$, в пакете NIST [1] предлагается использовать 15 статистических критериев. Пусть $T_{mon}, T_{fr}, T_{serial}$ — статистики критериев «Monobit Test», «Frequency Test within a Block» и «Serial Test» соответственно. Предположим, что в критерии «Frequency Test within a Block» используется N блоков, а в критерии «Serial Test» рассматриваются подпоследовательности длин m и $m-1$. Нас будет интересовать случай, когда $N, m \geq 2$ фиксированы и n стремится к бесконечности.

Теорема 1. *Пусть $\varepsilon_1, \varepsilon_2, \ldots$ — последовательность независимых случайных величин, имеющие распределение $Bern(\frac{1}{2})$. Тогда статистики $T_{mon}, T_{fr}, T_{serial}$ попарно асимптотически зависимы. Статистики T_{mon} и (T_{fr}, T_{serial}) асимптотически некоррелированы, статистики T_{fr} и T_{serial} асимптотически положительно коррелированы.*

В докладе будет предъявлено предельное совместное распределение статистик $T_{mon}, T_{fr}, T_{serial}$, а также предельные совместные распределения других статистик критериев пакета NIST.

Список литературы

[1] Rukhin A., Soto J., Nechvatal J., Smid M., Barker E., Leigh S., Levenson M., Vangel M., Banks D., Heckert A., Dray J., Vo S., "A statistical test suite for random and pseudorandom number generators for cryptographic applications", *NIST Special Publication 800-22 Revision 1a, ed. L. E. Bassham III, NIST*, April 2010.

*Место работы: МГУ им. М. В. Ломоносова, МФТИ; e-mail: savelovmp@gmail.com