

ИССЛЕДОВАНИЕ ГЕНЕРАТОРОВ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ, ФУНКЦИОНИРУЮЩИХ В ПОЛЕ GF(3)

Рысованый А.Н., Зыков Д.В., Сильченко С.А., Нежурина И.И.

Национальный технический университет

"Харьковский политехнический институт", г. Харьков

Генераторы псевдослучайных последовательностей (ПСП) применяются в различных областях науки и техники, например, в космической связи; в кодах, обнаруживающие и исправляющие ошибки; в встроенных самотестуемых СБИС; в защите информации и др.

Некоторый класс ПСП обладает свойствами случайных последовательностей и может их заменять.

В работе для исследования ПСП применяются две группы тестов.

Графические тесты. Статистические свойства последовательностей отображаются в виде графических зависимостей, по виду которых делают выводы о свойствах исследуемой последовательности.

Оценочные тесты. Статистические свойства последовательностей определяются числовыми характеристиками. На основе оценочных критериев делаются заключения о степени близости свойств анализируемой и истинно случайной последовательностей.

В работе рассмотрены графические тесты:

- гистограмма распределения элементов последовательности (для оценки равномерности распределения);
- распределение на плоскости (для определения зависимостей между элементами);
- проверка серий (анализ частоты появления символов);
- проверка на монотонность (анализа длин участков невозрастания и неубывания элементов);
- автокорреляционная функция (корреляции между сдвинутыми копиями последовательности);
- профиль сложности (от длины последовательности);
- графический спектральный тест (равномерность распределения 0 и 1 в исследуемой последовательности на основе анализа высоты выбросов преобразования Фурье).

В работе сформулированы требования, предъявляемые к системе оценки качества нелинейных генераторов ПСП и проведен анализ существующих систем аналогичного назначения.