МОДЕЛИ И ИНСТРУМЕНТАЛЬНЫЕ СРЕДСТВА ФОРМИРОВАНИЯ И АНАЛИЗА СВОЙСТВ СЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Ставицкая Е.С., Саранча С.Н.
Научный руководитель: д-р техн. наук, проф. Руженцев И.В.
Харьковский национальный университет радиоэлектроники,
Кафедра электронных вычислительных машин
пр. Ленина, 14, г. Харьков, 61166, Украина
Тел.: +38 0963534292; e-mail: spro@mail.ru

Abstract — The three methods of random and pseudorandom numbers generation are considered and software means for random sequence logging and analysis are proposed.

1. Введение

Случайные и псевдослучайные последовательности имеют широкий спектр практического применения — в задачах криптографии, моделирования сложных систем и игровых приложениях. При этом в ряде случаев могут применяться достаточно простые генераторы с относительно «слабыми» статистическими характеристиками, а в других областях (например, криптографии) к генераторам предъявляются достаточно серьезные требования.

Основными требованиями к генератору случайной последовательности можно отнести вычислительную простоту, большую длину периода последовательности (в идеальном случае она должна быть бесконечной), строгое соответствие заданному закону распределения.

Целью данной работы является построение программного обеспечения для формирования и анализа свойств случайных (и псевдослучайных) последовательностей.

2. Основная часть

В настоящее время принято выделять три способа формирования случайных (и псевдослучайных) последовательностей [1].

Алгоритмический способ предполагает воспроизведение случайных чисел на компьютере с помощью программной реализации специальных алгоритмов. Каждое случайное число вычисляется с помощью соответствующей программы по мере возникновения потребностей при моделировании системы на компьютере. Способ обеспечивает получение периодических числовых последовательностей с большим периодом. В пределах периода эти последовательности обладают заданными свойствами и называются псевдослучайными или квазислучайными. Основное достоинство способа — возможность получения на компьютере последовательности случайных чисел без внешних устройств и приставок при малых затратах памяти. В области алгоритмического способа формирования псевдослучайной последовательности можно выделить мультипликативный генератор, генератор на основе линейного рекуррентного регистра и т.д. [2].

Табличный способ предполагает тщательное формирование и хранение реализаций случайных чисел, функций и их систем в запоминающих устройствах с последующим считыванием и воспроизведением. Основной недостаток способа состоит в том, что необходима память большой емкости. Основное достоинство — высокая точность вероятностных характеристик моделируемых случайных чисел.

Аппаратный или физический способ предполагает применение специальных электронных генераторов случайных сигналов. Действие их основано на некоторых физических случайных явлениях, например шумах в электронных и полупроводниковых приборах. Выходное напряжение генератора, получаемое усилением шума, представляет собой случайную функцию S(t) с определенными вероятностными характеристиками. В частном случае этот закон может быть равномерным. Основными недостатками способа являются нестабильность вероятностных характеристик случайной функции S(t) и невозможность повторного получения одной и той же реализации.

Аппаратный способ генерации случайных чисел на базе программируемых интегральных микросхем с архитектурой FPGA в качестве источника случайности использует либо разброс временных параметров задержки логических элементов (таблиц подстановки — LUT) с цепями коммутации сигналов, либо нестабильность внешнего источника синхроимпульсов.

Макет аппаратного генератора случайных последовательностей выполнен на ПЛИС Altera Stratix II и подключается к рабочей станции по последовательному интерфейсу.

Разработанный пакет программного обеспечения включает в себя средства формирования vhdl-описаний макета по его параметрам — количеству колец и числу инвертирующих логических элементов в каждом кольце и средства алгоритмической генерации и анализа свойств последовательностей. При этом пользователь может выбрать тип генератора (алгоритмический мультипликативный, на основе линейного рекуррентного регистра или аппаратный генератор на базе ПЛИС) и провести статистический анализ на соответствие требованиям NIST [3].

3. Заключение

В работе осуществлен анализ существующих способов формирования и анализа свойств случайных последовательностей с целью получения оптимального по аппаратным затратам генератора на базе ПЛИС, удовлетворяющего требованиям NIST.

4. Список литературы

[1] Горбачев В.А. Моделирование систем / В.А. Горбачев. — Харьков: СМИТ. — 2006. — 320 с.
[2] Кнут Д. Искусство программирования для ЭВМ / Д. Кнут. СПб: Вильямс. — 2000. — 720 с.
[3] Статистические тесты генераторов случайных и псевдослучайных чисел / Википедия. — http://ru.wikipedia.org/wiki/Статистические_тесты_генераторов_случайных_и_псевдослучайных_чисел. — 10.02.2010.