Д. Е. Храбров, И. А. Мурашко
(ГГТУ им. П. О. Сухого, Гомель)

АВТОМАТИЗАЦИЯ ПОСТРОЕНИЯ ГЕНЕРАТОРОВ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НА КЛЕТОЧНЫХ АВТОМАТАХ ПО ЗАДАННОМУ ПОЛИНОМУ

Самым распространённым методом генерации псевдослучайных чисел является регистр сдвига с линейной обратной связью (англ. *Linear feedback shift register, LFSR*). Он состоит из двух частей: собственно регистра сдвига и функции обратной связи [1].

Ячейки памяти *LFSR* можно заменить на похожие, но имеющие по 2 входа и 2 выхода. Это даст возможность создавать генераторы без линейной обратной связи, на которой при аппаратной реализации идут максимальные потери.

В одномерном клеточном автомате решетка представляет собой цепочку клеток, в которой для каждой из них, имеется по два соседа. Соотношение для всех клеток автомата: $y'[i] = f(y[i\text{-}1], y[i], y[i\text{+}1])$, где f – функция переходов клетки; $y'[i]$ – состояние i-й клетки в следующий момент времени; $y[i\text{-}1]$, $y[i]$, $y[i\text{+}1]$ – состояние (i-1), i, (i+1)-й клетки в данный момент времени.

Разработан генератор клеточных автоматов для *Xilinx ISE* на языке *VHDL*. Тестовая программа была скомпилирована в язык *Schematic*. Так же была эмулирована работа аппаратного устройства, а результаты проанализированы методами, описанными в [2].

Одним из результатов является таблица порождающих полиномов седьмой степени, дающих максимальную длину последовательности.

Пока реализованный алгоритм не способен вычислять список полиномов для степеней больше 30, но учитывая успешный опыт оптимизации [3] в будущем эту цифру удастся значительно улучшить.

Аналогов данной разработке нет. Однако использованное подмножество клеточных автоматов довольно узкое, при расширении которого могут быть аналогичные программные продукты.

Литература

1 N. Ganguly, B. K. Sikdar, P. P. adChaudhuri. Design of An On-Chip Test Pattern Generator Without Prohibited Pattern Set. IEEE 15th International Conference on VLSI Design, 2002.

2 Мурашко, И. А. Методы минимизации энергопотребления при самотестировании цифровых устройств / И. А. Мурашко, В. Н. Ярмолик. – Минск: Бестпринт, 2004. – 188 с.

3 Пат. 7437 РБ. МПК H 03 K 3/80. Формирователь синусоиды на основе широтно-импульсной модуляции. / Е.А. Храбров, Ю.Е. Котова, Д.Е. Храбров (РБ).– № 20101084; Заявлено 30.12.2010; Опубл. 18.04.2011