УДК 621.323

МЕТОДИКА ПРОЕКТИРОВАНИЯ ГЕНЕРАТОРОВ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НА ОСНОВАНИИ КЛЕТОЧНЫХ АВТОМАТОВ С ЦИКЛИЧЕСКИМИ ГРАНИЧНЫМИ УСЛОВИЯМИ

Д. Е. Храбров, И. А. Мурашко

Учреждение образования «Гомельский государственный технический университет имени П. О. Сухого», Беларусь

Самым используемым методом генерации псевдослучайных последовательностей максимальной длины является регистр сдвига с линейной обратной связью (англ. *Linear feedback shift register*, *LFSR*) [1]. Однако внимание ученых направлено на использование и альтернативных методов генерации псевдослучайных последовательностей (ПСП) максимальной длины, в частности, на использование клеточных автоматов [2].

Линейный клеточный автомат представляет собой цепочку ячеек, каждая из которых функционально связана только со своими ближайшими соседями. Соотношение для всех клеток автомата: $y'[i] = f(y[i-1], y[i], y[i+1])$, где f – некоторая логическая функция; $y'[i]$ – состояние i-й клетки в следующий момент времени; $y[i-1]$, $y[i]$, $y[i+1]$ – состояние $(i-1)$, i, $(i+1)$-й клетки в данный момент времени.

Наиболее полно исследованы клеточные автоматы на основании правил 90 и 150 с нулевыми граничными условиями (ГУ) [2]. Для них созданы таблицы конфигураций, позволяющих формировать ПСП максимальной длины. Однако использование только этих правил ограничивает свободу разработчиков цифровых систем.

В ходе проведенных исследований было показано, что расширение количества используемых правил позволяет достаточно просто находить конфигурации генераторов ПСП максимальной длины. Кроме нулевых ГУ могут использоваться и циклические ГУ, для которых комбинации правил 90 и 150 не дают решения. В данной работе предложена методика проектирования генераторов ПСП на клеточных автоматах с циклическими ГУ на основании заданного полинома с расширенным набором правил.

Методика была реализована в виде программного комплекса, который формирует описание клеточных автоматов на языке *VHDL* (как функционального, так и структурного уровней) для САПР *Xilinx ISE*. Программный комплекс также позволяет получить конфигурации правил для заданного примитивного полинома. Например, для примитивного полинома пятой степени $1 + x^3 + x^5$ было найдено 136 различных конфигураций КА с циклическими граничными условиями. Примеры конфигураций: [60 60 60 240 60], [90 240 90 240 90], [240 60 240 90 60], [90 240 170 150 60], где *правило 90* – $y'[i] = y[i-1] \oplus y[i+1]$; *правило 240* – $y'[i] = y[i-1]$; *правило 170* – $y'[i] = y[i+1]$; *правило 150* – $y'[i] = y[i-1] \oplus y[i] \oplus y[i+1]$; *правило 60* – $y'[i] = y[i-1] \oplus y[i]$.

Причем программа позволяет выделять конфигурации с минимальным числом используемых правил. В примере выше первые 2 конфигурации используют правила 60 и 240, 90 и 240 соответственно.

Программный комплекс позволяет находить конфигурации КА с нулевыми и циклическими ГУ для расширенного набора правил для примитивных полиномов до 50 степени. Также формируется VHDL-описание генератора на клеточных автоматах. В дальнейшем планируется значительно увеличить степень порождающего полинома за счет использования свойств трехдиагональной матрицы и *LU*-разложения.

Литература

1. Golomb, S. W. *Shift Register Sequences* – San Francisco : Holden-Day, 1967. – 224 с.
2. Hortensius, P. D. Parallel Random Number Generation for VLSI Systems Using Cellular Automata / P. D. Hortensius, R. D. McLeod, H. C. Card – IEEE Trans. Computers 38(10), 1989. – 1466–1473 p.