ЭВРИСТИЧЕСКИЙ АЛГОРИТМ ПРОЕКТИРОВАНИЯ ГЕНЕРАТОРОВ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НА КЛЕТОЧНЫХ АВТОМАТАХ

И. А. Мурашко, Д. Е. Храбров
Кафедра «Информационные технологии», Гомельский государственный технический университет имени П.О. Сухого
Гомель, Республика Беларусь
E-mail: science@dexp.in, iamurashko@tut.by

Предложена методика проектирования генераторов псевдослучайных последовательностей на клеточных автоматах, основанная на эвристическом алгоритме. Алгоритм включает в себя синтез по Кателлу, эвристический выбор наборов правил и метод Монте-Карло.

Введение

Генератор псевдослучайных тестовых воздействий является одним из наиболее важных элементов встроенного самотестирования (англ. Built-in Self-test, BIST) [1]. Существует множество методов генерирования псевдослучайных последовательностей. В этой работе рассматриваются генераторы на клеточных автоматах [2,3].

Целью работы является получение программного средства для автоматизации проектирования генераторов псевдослучайных последовательностей. Программное средство должно уметь получать конфигурации клеточного автомата, который может генерировать последовательность максимальной длины. Этой проблеме и посвящена данная работа.

I. Получение конфигурации клеточного автомата

В качестве начальных исходных данных в задаче получения конфигурации клеточного автомата выступает один параметр – размерность клеточного автомата. Различные конфигурации правил приводят к различным характеристикам результирующего генератора. Далее программа предлагает пользователю варианты конфигураций правил с кратким описанием, к чему приведёт та или иная конфигурация. После этого пользователь получает код на языке VHDL, который может использовать в своих проектах.

Укрупнённая блок-схема получении конфигурации клеточного автомата показана на рис. 2. Видно, что использованы 3 основных метода синтеза: синтез по Каттеллу, эвристический синтез и метод Монте-Карло.

Первый вариант синтеза описан в [4]. Используются только правила 90 и 150, нулевые граничные условия. Генераторы на таких клеточных автоматах имеют хорошее качество генерируемой последовательности, большие межканальные сдвиги для почти всех ячеек, однако имеют значительные аппаратные затраты. Кроме того, межканальные фазовые сдвиги граничных ячеек не всегда хороши.

Эвристический синтез генераторов псевдослучайных последовательностей описан в [5]. Схема выбора оптимального набора предложена в [6]. Кроме того, рассмотрены только однонаправленные пары правил: (60, 150), (240, 90) и (240, 60). Варьируемый параметр количества перебираемых ячеек клеточного автомата изменяется от 2 до 6. Далее для каждой пары правил строятся все возможные комбинации по шаблонам: ssXYXYXY, ssXXXXXX, ssYYYYYY. Где s – варьируемый параметр; X – одно правило из пары; Y – другое правило из пары. Правила характеризуются ключами α, β и λ (рис. 1). Если предложенная конфигурация имеет примитивный характеристический полином, то она отображается пользователю как вариант для использования.

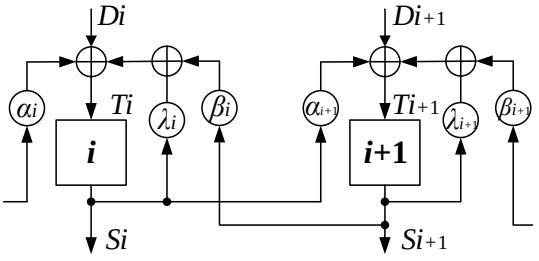

Рис. 1 – Формирование шаблона конфигурации

Исследования показали, что для чётных степеней при эвристическом синтезе более велика вероятность найти удачные вектора на правилах (240, 60). В случае же нечётной длины лучше использовать пары (60, 150) и (240, 90).

Если же не было найдено удачной конфигурации, то используется метод Монте-Карло: вектор заданной длины случайным образом заполняется правилами (240, 150, 90, 60), потом характеристический полином для этого вектора проверяется на примитивность. Если полином примитивен, то вектор отображается пользователю как вариант для использования. Недостатком данного метода является случайность получаемых характеристик.

Библиотека БГУИР

II. Реализация в Xilinx ISE

Разработанное программное средство принимает на вход единственное значение – размерность результирующего генератора. Далее задаётся уточняющий вопрос, генератор с какими именно характеристиками нужен. На выходе получается VHDL описание генератора.

Моделирование проводилось в Xilinx ISE 14.2, ПЛИС Xilinx XC3S200. Кроме того, устройства так же были реализованы на отладочной плате Digilent Spartan-3. При наличии только одного элемента XOR максимальная моделированная частота устройства была 313 МГц. Если же два элемента XOR в генераторе стояли последовательно, то частота падала до 210 МГц.

Рассмотрим реализации на клеточных автоматах и LFSR, имеющие характеристический полином $x^{13} \oplus x^{12} \oplus x^{11} \oplus x^9 \oplus x^8 \oplus x^7 \oplus x^6 \oplus x^5 \oplus x^4 \oplus x^3 \oplus x^2 \oplus x \oplus 1$. Реализация на клеточных автоматах имеет вектор правил [5557757757577] и работает на максимальной частоте 313 МГц, так как последовательно расположенных элементов XOR в такой реализации нет. Худшая реализация на LFSR имеет 11 последовательно стоящих XOR и максимальную частоту 60 МГц. Перераспределение элементов XOR так, чтобы максимальное количество последовательно соединённых элементов XOR было меньше 5, поднимает максимальную частоту до 140 МГц. Реализация на двух элементах XOR поднимает максимальную частоту до 170 МГц, что медленнее реализации на клеточных автоматах.

В общем случае быстродействие при реализации на ПЛИС зависит от числа используемых логических блоков, взаимного расположения этих блоков, оптимальности коммутации и других технологических факторов. В случае, если вся схема помещается в одном логическом блоке получается максимальная рабочая частота 317 МГц. В противном случае быстродействие снижается. Например, клеточный автомат на правилах (90, 240) и размерностью 503 триггера имеет максимальную частоту 220 МГц.

Применение эвристического алгоритма позволяет значительно упростить проектирование генераторов псевдослучайных последовательностей на клеточных автоматах. Получаемые генераторы работают быстрее LFSR-аналогов.

1. Agrawal, V. Essentials of Electronic Testing for Digital, Memory, and Mixed-Signal VLSI Circuits / V. Agrawal, M. Bushnell. – Springer, 2000. – P. 712.
2. Hortensius, P. D. Parallel random number generation for VLSI systems using cellular automata / P. D. Hortensius // IEEE Transactions on Computers. – 1989. – Vol. 38 (10). – P. 1466–1473.
3. del Reya, A. Martin. Reversibility of linear cellular automata / A. Martin del Reya, G. Rodriguez Sanchez // Applied Mathematics and Computation. – 2011. – Vol. 217. – P. 8360–8366.
4. Cattell, K. Synthesis of one-dimensional linear hybrid cellular automata / K. Cattell, J.C. Muzio // IEEE Trans. on CAD of Integrated Circuits and Systems. – 1996. – P. 325–335.
5. Мурашко, И. А. Применение клеточных автоматов с расширенным набором правил для генерирования псевдослучайных тестовых последовательностей / И. А. Мурашко, Д. Е. Храбров // Вестник московского государственного университета приборостроения и информати-ки. – 2013. – № 47. – С. 78–93.
6. Храбров, Д. Е. Применение клеточных автоматов с расширенным набором правил для генерирования псевдослучайных тестовых последовательностей / Д. Е. Храбров, И. А. Мурашко // Проблемы физики, математики и техники. – 2014. – № 1 (18). – С. 98–104.

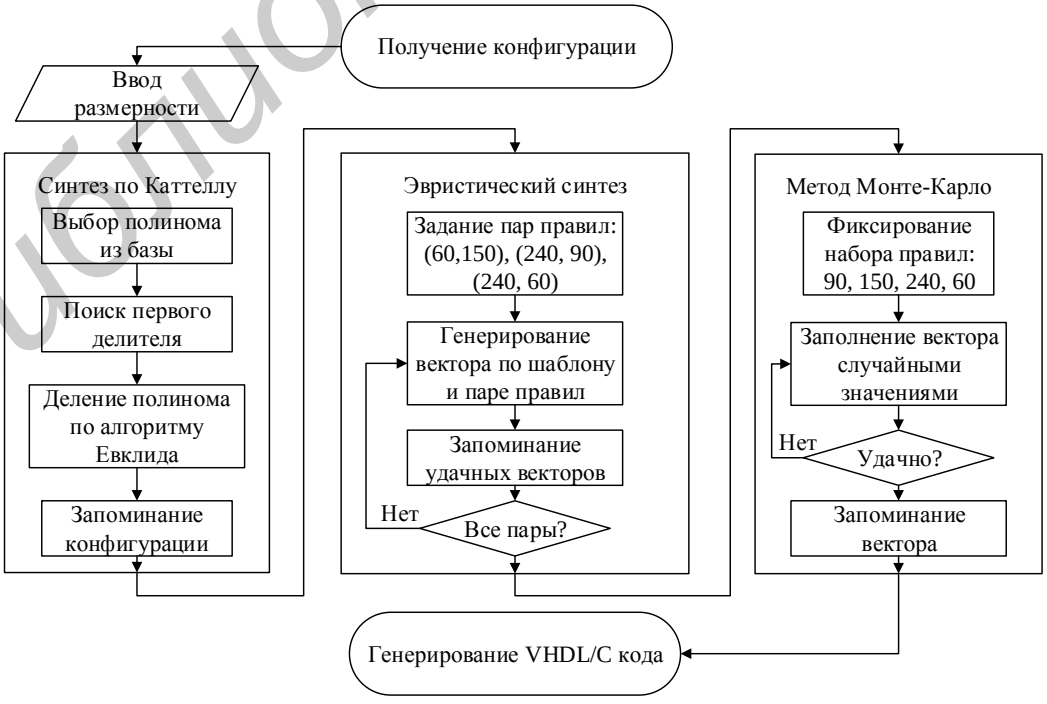

Рис. 2 – Блок-схема получении конфигурации клеточного автомата

Библиотека БГУИР