ВЫБОР КОНФИГУРАЦИИ ГЕНЕРАТОРА НА КЛЕТОЧНЫХ АВТОМАТАХ С МИНИМАЛЬНЫМИ АППАРАТНЫМИ ЗАТРАТАМИ

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

В статье рассматриваются вопросы классификации правил функционирования клеточных автоматов в контексте генерирования псевдослучайной последовательности максимально возможной длины. Проведен анализ возможных наборов правил, выявлены заведомо неудачные конфигурации. Предложена методика выбора конкретного набора правил по критериям быстродействия, качества и аппаратных затрат.

Введение

Важнейшим элементом встроенного самотестирования (англ. Built-in Self-test, BIST) является генератор псевдослучайных тестовых воздействий [1]. Самым используемым методом генерации тестовых воздействий максимальной длины является регистр сдвига с линейной обратной связью (англ. Linear feedback shift register, LFSR). Основным достоинством LFSR является его изученность и простота аппаратной реализации, для которой требуется лишь регистр сдвига и многовходовой сумматор по модулю два [2]. Однако использование LFSR не всегда оправдано для схем встроенного самотестирования ввиду сильной корреляции между последовательностями, формируемыми на различных разрядах генератора. Так что в последнее время внимание учёных направлено на использование альтернативных методов генерации псевдослучайных последовательностей максимальной длины, так же называемых М-последовательностями. В частности, в качестве генераторов М-последовательностей рассматриваются генераторы на клеточных автоматах (КА) [3,4].

В работе рассматриваются вопросы классификации правил функционирования клеточных автоматов в контексте генерирования псевдослучайной последовательности максимально возможной длины. Проведен анализ возможных наборов правил, выявлены заведомо неудачные конфигурации. Предложена методика выбора конкретного набора правил по критериям быстродействия, качества и аппаратных затрат..

I. Клеточные автоматы

В общем случае клеточный автомат может быть рассмотрен как простая модель пространственно протяжённого устройства, состоящего из ряда ячеек. Связи между ячейками ограничены локальным взаимодействием, то есть каждая ячейка находится в каком-либо состоянии, которое изменяется с течением времени в зависимости от предыдущего значения самой ячейки и значений её ближайших соседей [5].

В данной работе использован набор правил: 0, 170, 204, 102, 240, 90, 60, 150. Эти 8 правил представляют из себя все вариации одной клетки и двух соседей при использовании только сумматоров по модулю два.

В наборе правил есть закономерность: если есть правило с зависимостью только от левого соседа, то будет правило с зависимостью только от правого. Назовём это инвертированием правила, или обращением. На рисунке 1 показана общая идея инвертирования правил.

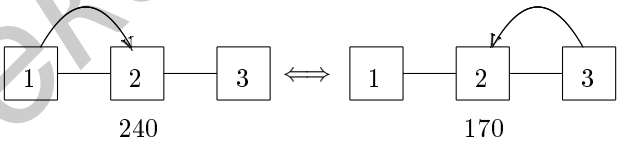

Рис. 1 – Иллюстрация процесса инвертирования

При инвертировании всех правил одного и того же автомата с примитивным характеристическим полиномом может получится тот же самый полином, другой примитивный или другой не примитивный. Причём, замена всего одной ячейки может существенно изменить результат.

Отдельное место в расширенном наборе занимают правила 0 и 204, так как по сути сводят циклический клеточный автомат к автомату с нулевыми граничными условиями, но меньшей размерности.

II. Правила функционирования клеточных автоматов

Для классификации было проведено моделирование всех конфигураций клеточных автоматов на различных наборах правил. Для каждой из степеней были найдены все удачные конфигурации.

Для пар правил авторами предлагается следующая классификация:

- Дающие корректный примитивный характеристический полином
  1. Прямые: 60-240, 60-150, 90-240

2. Инвертированные: 102-170, 102-150, 90-170

- Не дающие корректный полином
  1. Симметричные сами себе: 60-102, 90-150, 170-240
  2. Сдвигающие, противоположно направленные: 60-170, 102-240
  3. Другие: 60-90, 90-102, 150-170, 150-240

Как видно из классификации, корректные порождающие вектора могут давать наборы как чисто сдвигающих правил (60-240), так и комбинации сдвигающих с суммирующими (60-150). Инвертировав правила из корректного набора так же получим правила, дающие корректные порождающие вектора: 60-240 и 102-170, 60-150 и 102-150.

Были найдены конфигурации из трёх и четырёх правил, которые позволяют генерировать М-последовательность: 60,90,240 / 102,90,170; 60,90,150 / 102,90,150; 90,150,240 / 90,150,170; 60,150,240 / 102,150,170; 60,90,150,240 / 90,102,150,170.

В ходе исследования было выявлено, что при наличии в наборе противоположно направленных правил (рисунок 2) невозможно получить корректную конфигурацию. На рисунке знаком “>” обозначены правила, сдвигающие значение вправо, “<” – влево, “+” – суммирующие правила, “0” – ячейка, в которую собираются все значения.

>>+>>0<<<

Рис. 2 – Противоположная направленность правил

Из рисунка видно, что левая и правая части автомата по сути сдвигают все свои значения в ячейку “0”. Так как значения оттуда не берутся, то получается “дыра”, место куда значения уходят. В то же время крайняя левая и крайняя правая ячейки новых значений ниоткуда не берут. Даже если на начальном этапе в этих ячейках было значение 1, то уже через 2 хода это значение будет перемещено далее и более никогда не появится.

Основа методики выбора набора правил для создания оптимального генератора псевдослучайных последовательностей показана на рисунке 3.

III. Практические результаты

Поиск по предложенному методу был реализован в виде программного средства. В качестве примера можно привести порождающий вектор $[666(4)^{500}]$ с характеристическим полиномом $1 \oplus x^{500} \oplus x^{501} \oplus x^{502} \oplus x^{503}$, главным критерием которого является быстродействие, а вторым критерием – аппаратные затраты.

Выигрыш по аппаратным затратам можно получить при использовании не разреженных полиномов. Уже на пентаномиалах можно получить реализацию генератора на клеточных автоматах, которая будет требовать меньше аппаратных затрат, чем LFSR. Таким примером является $1 \oplus x^4 \oplus x^5 \oplus x^6 \oplus x^7$, генератор на клеточных автоматах требует два сумматора по модуля два вместо трёх при LFSR-реализации.

1. Agrawal, V. Essentials of Electronic Testing for Digital, Memory, and Mixed-Signal VLSI Circuits / V. Agrawal, M. Bushnell. – Springer, 2000. – P. 712.
2. Golomb, S. W. Shift register sequences / S. W. Golomb // San Francisco: Holden-Day. – 1967. – P. 224.
3. 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.
4. 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.
5. Мурашко, И. А. Встроенное самотестирование. Методы минимизации энергопотребления (монография) / И. А. Мурашко, В. Н. Ярмолик. – Saarbrucken: LAP Lambert Academic Publishing, 2012. – С. 348.

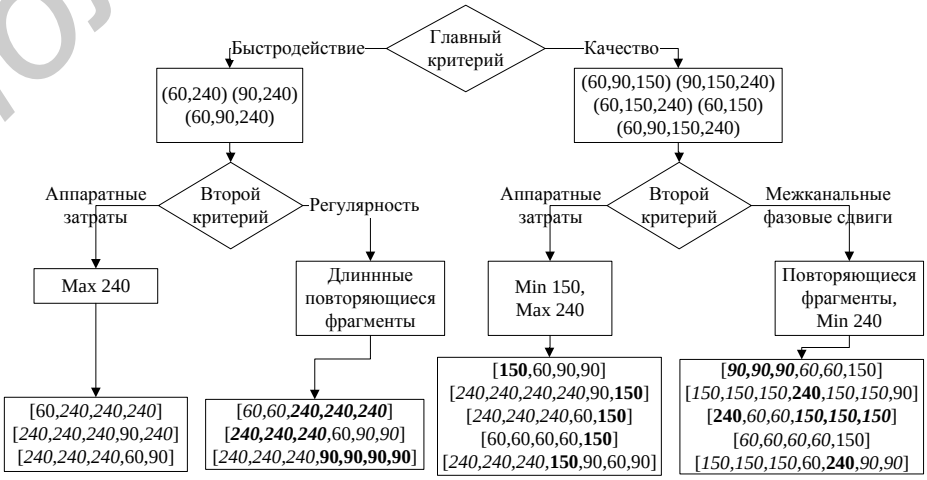

Рис. 3 – Схема выбора набора правил