АВТОМАТИЗИРОВАННОЕ ПРОЕКТИРОВАНИЕ ГЕНЕРАТОРА ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НА КЛЕТОЧНЫХ АВТОМАТАХ

Д. Е. Храбров

Гомельский государственный технический университет имени П. О. Сухого Беларусь

Научный руководитель И. А. Мурашко

Клеточные автоматы являются дискретными динамическими системами, поведение которых полностью определяется в терминах локальных зависимостей. Пространство представлено равномерной сеткой, каждая ячейка или клетка которой содержит несколько битов данных; время идет вперед дискретными шагами, а законы мира выражаются единственным набором правил, скажем, небольшой справочной таблицей, по которой любая клетка на каждом шаге вычисляет свое новое состояние по состояниям ее близких соседей. Законы являются локальными и повсюду одинаковыми. «Локальный» означает, что для того, чтобы узнать, что произойдет здесь мгновение спустя, достаточно посмотреть на состояние ближайшего окружения: никакое дальнодействие не допускается. «Одинаковость» означает, что законы везде

одни и те же: я могу отличить одно место от другого только по форме ландшафта, а не по какой-то разнице в законах [1].

Клеточные автоматы применимы не только в математике и физике, а также в биологии, экономике, социологии, информатике и т. д. В данной работе рассмотрено автоматизированное проектирование генератора псевдослучайных последовательностей на клеточных автоматах.

Самым распространенным 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. Регистр состоит из битов, его длина – количество этих битов. Когда нужно извлечь бит, все биты регистра сдвигаются вправо на одну позицию. Новый крайний слева бит определяется функцией остальных битов. На выходе регистра оказывается один, обычно младший, значащий бит. Период регистра сдвига – длина получаемой последовательности до начала ее повторения [2].

Кроме устаревших, хорошо известных *LFSR*-генераторов, широко применявшихся в качестве аппаратных генераторов псевдослучайных чисел в XX в., к сожалению, очень мало известно о современных аппаратных генераторах (поточных шифрах), так как большинство из них разработано для военных целей и держатся в секрете. Почти все существующие коммерческие аппаратные реализации запатентованы и также держатся в секрете. Примерами аппаратных генераторов являются *Toyocrypt* и *LILI*-128, которые являются *LFSR*-генераторами, и оба были взломаны с помощью алгебраических атак.

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 итоге получается одномерный линейный клеточный автомат.

В одномерном клеточном автомате решетка представляет собой цепочку клеток, в которой для каждой из них, кроме крайних, имеется по два соседа. Для устранения краевых эффектов решетка может «заворачиваться» в тор. Это позволяет использовать следующее соотношение для всех клеток автомата:

$$y'[i] = f(y[i-1],\ \ y[i],\ y[i+1]),$$

где f – функция переходов клетки; $y'[i]$ – состояние i-й клетки в следующий момент времени; $y[i-1]$ – состояние (i – 1)-й клетки в данный момент времени; $y[i]$ – состояние i-й клетки в данный момент времени; $y[i+1]$ – состояние (i + 1)-й клетки в данный момент времени.

Правила вычисления 90 и 150 выглядят следующим образом:

– правило 90: $s_i^+ = s_{i-l} + s_{i+l}$;

– правило 150: $s_i^+ = s_{i-l} + s_i + s_{i+l}$.

В соответствии с правилом 90 значением ячейки является сумма по модулю 2 значений из двух соседних клеток на предыдущем шаге по времени t. Правило 150 также включает в себя значение ячейки i на шаг по времени t. В общем, мы используем вектор правил [d_1, d_2, … , d_N], чтобы представлять клеточный автомат размером N ячеек, где d_i равно 0, если ячейка i использует правило 90, или равно 1, если ячейка i использует правило 150.

При помощи одного и того же порождающего полинома можно построить генератор псевдослучайных последовательностей как на основе *LFSR*, так и на основе клеточных автоматов.

И клеточный автомат, и *LFSR* могут быть представлены матрицами перехода, для которых характеристические многочлены могут быть вычислены. Об отношениях между *LFSR* и клеточными автоматами известно следующее: одномерный линейный клеточный автомат и *LFSR* с тем же неприводимым или примитивным характеристическим многочленом изоморфны, и их соответствующие матрицы перехода аналогичны.

Как следствие, можно поставить задачу: для имеемого набора правил клеточного автомата нужно найти характеристический полином. В данной работе было реализовано решение поставленной задачи.

По имеемой конфигурации строится трехдиагональная матрица A, главной диагональю которой является набор правил клеточного автомата. Вспомогательные диагонали единичны. Далее находится определитель матрицы $A+Ix$, где I – единичная матрица. Определитель и является искомым полиномом.

Пускай правила построения выглядят следующим образом: [1, 1, 1, 1, 0].

Найдем матрицу A, вспомогательную матрицу и ее определитель:

$$A = \begin{vmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{vmatrix} \quad A + Ix = \begin{vmatrix} 1+x & 1 & 0 & 0 & 0 \\ 1 & 1+x & 1 & 0 & 0 \\ 0 & 1 & 1+x & 1 & 0 \\ 0 & 0 & 1 & 1+x & 1 \\ 0 & 0 & 0 & 1 & x \end{vmatrix};$$

$$det(A+Ix) = 1 - 2x - 5x^2 + 2x^3 + 4x^4 + x^5.$$

Так как вычисления проводятся в конечном поле по модулю 2, то четные коэффициенты можно считать нулевыми, а нечетные единичными. То есть

$$det(A+Ix) = 1 \oplus x^2 \oplus x^5.$$

Также можно поставить и обратную задачу. То есть у нас имеется характеристический полином, и нужно сгенерировать набор правил построения клеточного автомата.

В статье Кателла и Музио [3] предлагается метод пошагового деления на уже известный полином. То есть N-ный полином – это и есть характеристический. Предполагается, что мы знаем N–1, а из этих двух уже можно получить все остальные. Далее нужно решить полученную систему линейных алгебраических уравнений.

Загвоздка метода, предложенного Кателлом и Музио, именно в нахождении N–1 полинома. Его поиск описан математически, однако далеко не тривиален. В данной работе был предложен следующий алгоритм:

1) найти в общем виде определитель матрицы $a+Ix$ (размерность равна старшей степени характеристического полинома);

2) приравнять коэффициенты при степенях x в определителе и характеристическом полиноме;

3) решить систему нелинейных уравнений относительно a.

В данном алгоритме слабым местом является решение системы уравнений. Однако задача решение системы уравнений распространена больше, чем решение квадратного уравнения относительно полинома в бинарном поле.

При решении системы уравнений получаем минимум 2 конфигурации правил для создания клеточного автомата. Это объясняется тем, что: во-первых, найдены все конфигурации, в том числе и симметричные; во-вторых, одному полиному может соответствовать несколько конфигураций клеточных автоматов (в том числе симметричные).

В ходе данной работы был разработан генератор клеточных автоматов для *Xilinx ISE* на языке *VHDL*. Тестовая программа была скомпилирована в язык *Schematic*, близкий к аппаратной реализации. Далее была эмулирована работа аппаратного устройства, а результаты проанализированы.

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

Литература

1. Шалыто, А. От тьюрингова программирования к автоматному / А. Шалыто, Н. Туккель // Мир ПК. – 2002. – № 2.
2. Ganguly, N. Design of An On-Chip Test Pattern Generator Without Prohibited Pattern Set / N. Ganguly, B. K. Sikdar, P. P. adChaudhuri // IEEE 15th International Conference on VLSI Design, 2002.
3. Cattell, K. Synthesis of one-dimensional linear hybrid cellular automata / K. Cattell, J. C. Muzio. // To appear in IEEE Transactions on Computer-Aided Design, 1996.