Методика синтеза генератора псевдослучайных последовательностей по заданному полиному на клеточных автоматах

Мурашко И.А.; Храбров Д.Е.
Кафедра «Информационные технологии», ФАИС
Гомельский государственный технический университет им. П. О. Сухого
Гомель, Беларусь
e-mail: science@dexp.in

***Аннотация* — В работе исследуется проблема синтеза генераторов псевдослучайных последовательностей на клеточных автоматах по заданному полиному. Получен алгоритм синтеза генераторов для порождающих полиномов определённой степени, реализованный программно.**

Ключевые слова: псевдослучайная последовательность; генератор псевдослучайных последовательностей; автоматизированное проектирование; клеточные автоматы; информационное обеспечение

I. Введение

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, небольшой справочной таблицей, по которой любая клетка на каждом шаге вычисляет своё новое состояние по состояниям её близких соседей.

Самым распространённым методом генерации псевдослучайных последовательностей 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 бит. 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 значащий бит. Период регистра сдвига – длина получаемой последовательности до начала её повторения [1].

Кроме устаревших, хорошо известных *LFSR*-генераторов, широко применявшихся в качестве аппаратных генераторов псевдослучайных чисел в XX веке, 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 два входа и два 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 соотношение для всех клеток автомата, показанное в (1)

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

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;

$y[i]$ – состояние i-й клетки в данный момент времени;

$y[i+1]$ – состояние $(i+1)$-й клетки в данный момент.

Правила вычисления 90 и 150 выглядят следующим образом:

1) правило 90: $s_i^+ = s_{i-1} \oplus s_{i+1}$;

2) правило 150: $s_i^+ = s_{i-1} \oplus s_i \oplus s_{i+1}$.

В соответствии с правилом 90, значением ячейки является сумма по модулю два значений из двух соседних клеток на предыдущем шаге по времени t. Правило 150 включает в себя еще и значение ячейки i на предыдущем шаге. В общем случае, будем использовать вектор правил $[d_1, d_2, \ldots, d_N]$ для описания N-разрядного клеточного автомата, где d_i равно 0, если ячейка i использует правило 90, или равно 1, если ячейка i использует правило 150.

II. Математический аппарат

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 следующее решение поставленной задачи:

По имеемой конфигурации строится трёхдиагональная матрица A, главной диагональю которой является набор правил клеточного автомата. Вспомогательные диагонали единичны. Далее находится определитель матрицы $A \oplus Ix$, где I –

единичная матрица. Определитель и является искомым полиномом.

Пусть правила построения выглядят следующим образом – [1, 1, 1, 1, 0]. Порождающая матрица для данных правил имеет вид:

$$A \oplus Ix = \begin{vmatrix} 1 \oplus x & 1 & 0 & 0 & 0 \\ 1 & 1 \oplus x & 1 & 0 & 0 \\ 0 & 1 & 1 \oplus x & 1 & 0 \\ 0 & 0 & 1 & 1 \oplus x & 1 \\ 0 & 0 & 0 & 1 & x \end{vmatrix}$$

Вычислив определитель порождающей матрицы, получим:

$$\det (A \oplus I \cdot x) = 1 \oplus x2 \oplus x5 \quad GF(2). \qquad (2)$$

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 [2] 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 $A \oplus Ix$ (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 две 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).

III. Полученные результаты

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 методами, описанными в [3].

Одним из результатов работы приложения является таблица порождающих полиномов седьмой степени, дающих максимальную длину генерируемой последовательности (таблица 1).

Табл. 1. Все порождающие полиномы седьмой степени, дающие максимальную длину генерируемой последовательности

Полином	Конфигурация
$1 \oplus x \oplus x^3 \oplus x^5 \oplus x^7$	1, 1, 1, 1, 0, 1, 1
$1 \oplus x \oplus x^4 \oplus x^6 \oplus x^7$	1, 1, 1, 0, 1, 1, 0
$1 \oplus x^4 \oplus x^7$	1, 1, 1, 0, 1, 0, 0
$1 \oplus x \oplus x^2 \oplus x^3 \oplus x^7$	1, 1, 1, 0, 0, 0, 1
$1 \oplus x \oplus x^3 \oplus x^6 \oplus x^7$	1, 1, 0, 1, 1, 0, 1
$1 \oplus x^2 \oplus x^3 \oplus x^4 \oplus x^7$	1, 1, 0, 1, 0, 1, 0
$1 \oplus x \oplus x^2 \oplus x^3 \oplus x^5 \oplus x^6 \oplus x^7$	1, 1, 0, 1, 0, 0, 0
$1 \oplus x^2 \oplus x^4 \oplus x^6 \oplus x^7$	1, 0, 1, 1, 1, 1, 0
$1 \oplus x \oplus x^3 \oplus x^6 \oplus x^7$	1, 0, 1, 1, 0, 1, 1
$1 \oplus x \oplus x^7$	1, 0, 1, 1, 0, 0, 1
$1 \oplus x^2 \oplus x^5 \oplus x^6 \oplus x^7$	1, 0, 1, 0, 1, 0, 0
$1 \oplus x^4 \oplus x^5 \oplus x^6 \oplus x^7$	1, 0, 1, 0, 0, 0, 1
$1 \oplus x^3 \oplus x^4 \oplus x^5 \oplus x^7$	1, 0, 0, 1, 0, 0, 0
$1 \oplus x \oplus x^2 \oplus x^3 \oplus x^4 \oplus x^5 \oplus x^7$	1, 0, 0, 0, 0, 1, 0
$1 \oplus x^3 \oplus x^7$	0, 1, 1, 1, 0, 1, 0
$1 \oplus x \oplus x^2 \oplus x^5 \oplus x^7$	0, 1, 0, 0, 1, 0, 0
$1 \oplus x^6 \oplus x^7$	0, 0, 1, 0, 0, 0, 0
$1 \oplus x \oplus x^2 \oplus x^4 \oplus x^5 \oplus x^6 \oplus x^7$	0, 0, 0, 1, 1, 1, 0

Пока реализованный алгоритм не способен вычислять список полиномов для степеней больше 30, но учитывая успешный опыт оптимизации [4] в будущем эту цифру удастся значительно улучшить.

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

[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] K. Cattell, J.C. Muzio. Synthesis of one-dimensional linear hybrid cellular automata. IEEE Transactions on Computer-Aided Design, 1996.

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

[4] 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