Вычисление фазовых сдвигов М-последовательности

Морозов В.В.; Мурашко И.А.
Кафедра «Информационные технологии», Факультет Автоматизированных и Информационных Систем
Учреждение Образования «Гомельский Государственный Технический Университет имени П. О. Сухого»
Гомель, Республика Беларусь
e-mail: lordscorpio.gml@gmail.com

***Аннотация* – В работе представлен анализ фазовых сдвигов М-последовательности, формируемой на основе свойства децимации. Предложена программа, которая позволяет автоматизировать расчет фазовых сдвигов при децимации М-последовательности.**

Ключевые слова: LFSR, М-последовательность, фазовый сдвиг, децимация

I. Введение

Ключевым элементом любой системы встроенного самотестирования СБИС является источник тестовых воздействий. Большинство подобных систем используют для этой цели псевдослучайные последовательности максимальной длины (М-последовательности) [1]. В качестве генератора М-последовательности используется, как правило, линейный сдвиговый регистр с сумматорами по модулю два в цепи обратной связи (LFSR – Linear Feedback Shift Register). Функционирование LFSR определяется характеристическим полиномом $\varphi(x)$, который должен быть примитивным и неприводимым [2]. Период формируемой М-последовательности определяется старшей степенью порождающего полинома.

Недостатком LFSR является то, что фазовый сдвиг М-последовательностей, формируемых на соседних разрядах, равен единице. Для увеличения межразрядных фазовых сдвигов предлагается использовать свойство децимации М-последовательности. Разработана программа, которая позволяет автоматизировать вычисление фазовых сдвигов М-последовательности при децимации по произвольному индексу.

II. Термины и определения

Для удобства изложения применим следующие обозначения из [3]. Пусть a_i – i-й символ М-последовательности, определяемой порождающим полиномом $\varphi(x)$ степени m. Саму М-последовательность, начинающуюся с k-го символа, будем обозначать $\{a_k\}=a_k, a_{k+1}, a_{k+2},\ldots,a_{L-1}, a_0, a_1, \ldots, a_{k-1}$, где $L = 2^m - 1$ это период М-последовательности. Будем считать, что порождающий полином является примитивным.

На рис.1 представлена стандартная реализация LFSR с внешними сумматорами и формируемые на его выходах фазовые сдвиги М-последовательности.

В общем случае для порождающего полинома $\varphi(x)$ степени m существует $L = 2^m - 1$ различных М-последова-тельностей, отличающихся фазовым сдвигом: $\{a_0\}$, $\{a_1\}$, $\{a_2\}$, …, $\{a_{L-1}\}$. Среди этих последовательностей существует характеристическая последовательность, для которой справедливо выражение $a_i=a_{2i}$, где i=0,1,2,…,L–1. Обозначим ее через $\{a_0\}$.

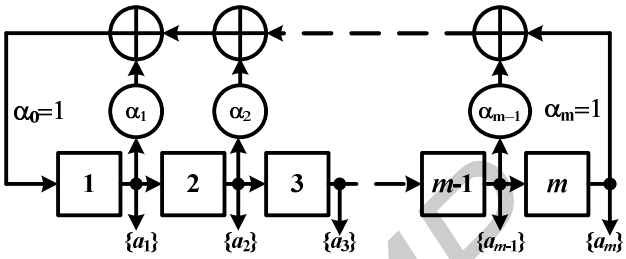

Рис. 1. Пример LFSR с произвольным порождающим полиномом

Децимацией М-последовательности $\{a_i\}$ по индексу q (q = 1,2,3,…) называется выборка q-х элементов данной М-последовательности. В результате децимации формируется некоторая последовательность $\{b_j\}$. Если период исходной М-последовательности L и коэффициент децимации q взаимно просты, то децимация называется собственной или нормальной. Формируемая последовательность является М-последовательностью, определяемой примитивным полиномом той же самой степени. В дальнейшем под децимацией будем подразумевать только собственную (или нормальную) децимацию, в результате которой получается М-последовательность того же самого периода. Децимацию $\{a_i\}$ по индексу q будем обозначать через $\{a_i\}^q$. Формируемую последовательность будем обозначать $\{b_j\}$. Таким образом, можно записать:

$$\{b_j\}=\{a_i\}^q. \qquad (1)$$

На рис.2 приведен пример децимации М-последовательности $\{a_3\}$, определяемой порождающим полиномом $\varphi(x)= x^4 \oplus x^3 \oplus 1$, по индексу q=2 и q=4. При децимации по индексу два формируется девятый фазовый сдвиг исходной М-последовательности, то есть $\{a_3\}^2=\{a_9\}$. Во втором случае формируется 12-й фазовый сдвиг исходной, то есть $\{a_3\}^4=\{a_{12}\}$. Если в качестве индекса децимации взять q=2, то результирующая последовательность не является М-последовательностью. Это вызвано тем, что коэффициент децимации и период М-последовательности не являются взаимно простыми числами, то есть (15,3)=3.

N	0	1	2	3	4	5	6	7	8	9	10	11	12
$\{a_3\}$	1	1	0	1	0	1	1	0	0	1	0	0	0
$\{a_3\}^2$	1		0		0		1		0		0		0
$\{a_3\}^4$	1				0				0				0

Рис.2 Пример децимации М-последовательности по индексу 2 и 4

Порождающий полином $\psi(x)$, которым определяется формируемая в результате собственной децимации М=последовательность, в общем случае может быть найден из следующего выражения [3]:

$$\psi(x) = \det (V^q \oplus I), \qquad (2)$$

Библиотека БГУИР

где V – порождающая матрица исходной последовательности, I – единичная диагональная матрица ранга m.

III. Методика расчета фазовых сдвигов

Значение фазового сдвига сформированной последовательности может быть определено на основании следующего выражения [3]:

$$\{a_i\}^q = \{b_{i/q \bmod L}\}, \quad (3)$$

где $\{a_i\}$ – i-й сдвиг исходной М-последовательности, q=2,3,4,… – коэффициент децимации, $(q, L) = 1$.

На основании (1) и (3) можно записать:

$$j = i/q \bmod L. \quad (4)$$

При программной реализации наибольшую сложность вызывает целочисленное деление в кольце целых чисел по модулю для больших значений L [4]. Для упрощения вычислений преобразуем (4) следующим образом:

$$j = i\cdot (1/q \bmod L) \bmod L. \quad (5)$$

Обозначим

$$k = 1/q \bmod L. \quad (6)$$

Тогда

$$j = i\cdot k \bmod L, \quad (7)$$

Таким образом, для вычисления фазовых сдвигов М-последовательности, определяемой порождающим полиномом степени m при фиксированном коэффициенте децимации q, требуется определение взаимной простоты q и L и однократное вычисление k по (6). Программная реализация умножения по модулю проблем не представляет.

IV. Программная реализация

На основании методики, рассмотренной в предыдущем разделе, была разработана программа для быстрого вычисления фазовых сдвигов при децимации М-последовательности. Укрупненный алгоритм работы программы можно записать следующим образом.

1) Ввод исходных данных – коэффициента децимации q, порождающего полинома $\varphi(x)$ и номеров фазового сдвига исходной последовательности (по умолчанию – от единицы до m, где $m = \deg \varphi(x)$).

2) Проверка взаимной простоты $(q, 2^m–1) = 1$. Для проверки используется алгоритм Эвклида [5].

3) Вычисление k на основании (6).

4) Вычисление значений фазовых сдвигов новой М-последовательности на основании (7) для заданных номеров фазовых сдвигов исходной М-последовательности. Вычисление порождающего полинома новой М-последовательности на основании (2).

5) Вывод результатов на экран.

Рассмотрим пример работы алгоритма. Пусть необходимо определить номера фазовых сдвигов М-последовательности, полученной в результате децимации по индексу три фазовых сдвигов М-последовательности, определяемой порождающим полиномом $\varphi(x)=x^7\oplus x^6\oplus 1$ с номерами 7, 11, 20.

1) Ввод исходных данных: q=3, m = deg $\varphi(x)$ = 7, i={7, 11, 20}.

2) Проверка взаимной простоты $(q, 2^m–1) = (3, 127) =1$.

3) Вычисление k на основании (6):

k = 1/3 mod 127 = 85.

4) Вычисление значений фазовых сдвигов новой М-последовательности на основании (7):

i=7: j=7·85 mod 127 = 87;

i=11: j=11·85 mod 127 = 46;

i=20: j=20·85 mod 127 = 49.

Вычисление порождающего полинома для новой М-последовательности на основании (2):

$$\psi(x) = \det(V \oplus Ix) = \begin{vmatrix} x & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & x & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & x & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & x & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & x & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & x & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & x \end{vmatrix} = x^7 \oplus x \oplus 1.$$

5) Вывод результатов на экран – j={87, 46, 49} и $\psi(x)=x^7\oplus x\oplus 1$.

V. Программная реализация

Предложенная программа позволяет автоматизировать расчет фазовых сдвигов при децимации М-последовательности по произвольному индексу. Максимальная степень порождающего полинома не должна превышать 60.

[1] M.L Bushnell, V.D. Agrawal, «Essentials of Electronic Testing». – Boston: Kluwer Academic Publishers, 2002. – 690 p.

[2] В. Н. Ярмолик, «Контроль и диагностика цифровых устройств ЭВМ». – Мн.: Наука и техника, 1988. – 240 с.

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

[4] Н.Коблиц «Курс теории чисел и криптографии». – М., ТВП, 2001

[5] Ronald L. Graham, Donald E. Knuth, Oren Patashnik. Concrete mathematics: a foundation for computer science. – Addison-Wesley Publishing Company, 1989. – 625 p.

Библиотека БГУИР