АЛГОРИТМ ДЕЦИМАЦИИ ПОЛИНОМОВ

Ю. А. Толстогузов, И. А. Мурашко

Кафедра информационных технологий, ФАИС, Гомельский государственный технический университет имени П.О.Сухого

Гомель, Республика Беларусь

E-mail: yuriy.tolstoguzov@gmail.com, iamurashko@tut.by

Рассмотрен метод построения порождающих полиномов М-последовательностей с одинаковым периодом на основе одного заданного полинома. В основу метода положено использование свойств децимации М-последовательности. Предложенный метод пояснен примером.

Введение

М-последовательность или последовательность максимальной длины — псевдослучайная двоичная последовательность, порожденная регистром сдвига с линейной обратной связью и имеющая максимальный период. М-последовательности применяются в псевдогенераторах случайных чисел. В основу построения М-последовательностей положены порождающие полиномы, в качестве которых выступают примитивные полиномы с коэффициентами поля Галуа GF(2). Число таких полиномов зависит от их степени и вычисляется на основе функции Эйлера. Для генерации М-последовательности с периодом $M = 2^n - 1$ используется примитивный полином $h(x)$ степени n с коэффициентами GF(2), т. е.

$$h(x) = \sum_{i=0}^{n} h_i x^i, \qquad (1)$$

где $h_0 = h_n = 1$, а $h_i = \{0, 1\}$ при $0 < i < n$.

Примитивные полиномы существуют для всех $n > 1$. Известно [1], что для конкретного значения n существует точно

$$N = \frac{\Phi(M)}{n} \qquad (2)$$

различных полиномов $h(x)$, являющихся примитивными. Функция $\Phi(M)$, называемая функцией Эйлера, представляет собой количество положительных целых чисел, меньших или равных M и взаимно простых с M. Так как функция $\Phi(M)$ с увеличением n очень быстро растет, то число полиномов степени n, порождающих последовательности с максимальным периодом, с ростом n также быстро увеличивается.

Так, для $n = 10$ число примитивных полиномов равно 60, а для $n = 16$ – уже 2048. Следовательно, на основе порождающих полиномов 10-й степени можно получить 60 различных М-последовательностей, а при использовании порождающих полиномов 16-й степени – 2048. Нахождение порождающих полиномов М-последовательностей большой степени затруднительно в связи с тем, что для проверки случайного полинома на примитивность и не приводимость необходимо использование большого аппаратного и временного ресурса. В таких случаях, эффективно использовать другие способы. Одним из них является децимация М-последовательностей.

I. Метод генерации порождающих полиномов М-последовательностей

В общем случае не существует простого способа генерировать примитивные полинома заданной степени. Проще всего выбирать полином случайным образом и проверять, не является ли он примитивным. Это нелегко – и чем-то похоже на проверку, не является ли простым случайно выбранное число, но многие математические пакеты программ умеют решать такую задачу. Также стоит понимать, что с ростом степени полинома проверка быстро усложняется. Поэтому в данной статье предлагается иной метод генерации новых примитивных полиномов по одному известному, найденому любым другим способом. В основу метода положено использование свойств децимации М-последовательности.

Согласно работе [2] децимацией М-последовательности $\{a_j\}$ по индексу q_s, $s = \overline{2, 2n-2}$, называется выборка q_s-х элементов данной М-последовательности. Если период $M = 2n - 1$ исходной М-последовательности и индекс децимации q_s взаимно просты, т.е. $\gcd(M, q_s) = 1$, децимация называется собственной или нормальной. В дальнейшем под децимацией будем подразумевать только собственную (или нормальную) децимацию, в результате которой получается М-последовательность с тем же периодом, что и исходная М-последовательность. Децимацию $\{a_j\}$ по индексу q_s обозначим как $\{a_j\}^{q_s}$, а полученную в результате децимации М-последовательность – как $\{b_j\}$. Таким образом, можно записать выражение (3).

$$\{b_j\} = \{a_j\}^{q_s}. \qquad (3)$$

Опишем алгоритм получения порождающих полиномов М-последовательности:

1. Выбираем полином (1) из таблиц известных примитивных полиномов или генерируем его других известным образом. Например, алгоритм генерации примитивных полиномов заданной степени в общих чер-

тах рассмотрен в работе [4]. Однако данный алгоритм оставляет открытым вопрос о нахождении других порождающих полиномов М-последовательностей с заданным периодом

2. Представим имеющийся примитивный полином через порождающую матрицу: для этого в первую строку матрицы выпишем сам полином, а остальные строки матрицы заполним 1 по диагонали.
3. Возведем порождающую матрицу в степень соответствующую индексу децимации
4. Добавим единичную матрицу I, умноженую на x
   $A \oplus Ix$
5. Найдем определитель полученной матрицы любым удобным для нас способом (например, найдя верхную треугольную форму матрицы).
6. Полученный определитель и будет децимированным порождающим полиномом М-последовательности
7. Повторяя шаги 2-5 с примитивными числами можно генерировать новые порождающие полиномы. Их количество вычисляется по формуле (2).

II. Пример

Рассмотрим метод генерации порождающих полиномов М-последовательности на примере. Найдем все полиномы 5-й степени по одному известному.

1. Выбирается примитивный полином 5-ой. Берем $h(x) = x^5 \oplus x^2 \oplus 1$.
2. Представим примитивный полином через порождающую матрицу М:

$$M = \begin{matrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{matrix}$$

3. Возведем порождающую матрицу М в степень соответствующую индексу децимации $q_s = 3$:

$$M = \begin{matrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{matrix}$$

4. Добавляя единичную матрицу того же ранга, умноженую на x, получаем:

$$M = \begin{matrix} x\oplus 1 & 0 & 0 & 1 & 0 \\ 0 & x\oplus 1 & 0 & 1 & 0 \\ 0 & 0 & x\oplus 1 & 0 & 1 \\ 1 & 0 & 0 & x & 0 \\ 0 & 1 & 0 & 0 & x \end{matrix}$$

5. Найдем определитель матрицы $\det(M)$. Для этого, вычислим верхную треугольную форму матрицы:

$$M = \begin{matrix} x & 1 & 1 & 0 & 1 \\ 0 & 1/x & 1/x & x & 1/x \\ 0 & 0 & x\oplus 1 & x^2 & 0 \\ 0 & 0 & 0 & \frac{x^4\oplus x^2\oplus 1}{x\oplus 1} & x \\ 0 & 0 & 0 & 0 & \frac{x^6\oplus x^5\oplus x^4\oplus 1}{x^5\oplus x^4\oplus x^3\oplus x^2\oplus x\oplus 1} \end{matrix}$$

   Перемножая элементы по диагноле находим определитель $\det(M)$
   $x^5 \oplus x^3 \oplus x^2 \oplus x^1 \oplus 1$
6. Полученный определитель - порождающий полином М-последовательности при индексе децимации 3:
   $q_s = 3 : x^5 \oplus x^3 \oplus x^2 \oplus x^1 \oplus 1$
7. Повторяем шаги 2-5 с другими примитивными числами(2, 5, 7, 11) как значения индекса децимации q_s, чтобы найти все примитивные полиномы данной степени

Таблица 1 – Полученные результаты

q_s	Полученный полином
2	$x^5 \oplus x^3 \oplus 1$
3	$x^5 \oplus x^3 \oplus x^2 \oplus x^1 \oplus 1$
5	$x^5 \oplus x^4 \oplus x^3 \oplus x \oplus 1$
7	$x^5 \oplus x^4 \oplus x^3 \oplus x^2 \oplus 1$
11	$x^5 \oplus x^4 \oplus x^2 \oplus x^1 \oplus 1$

Алгоритм окончен, так как мы перебрали все возможные варианты порождающих полиномов данной степени и все последующие полиномы будет равны одному из уже полученных.

III. Заключение

Данный способ позволяет найти новые порождающие полиномы М-последовательности даже больших степеней с относительно небольшими затратами используя примитивные числа как индексы децимации.

1. Ожиганов, А. А. Использование псевдослучайных последовательностей при построении кодовых шкал для преобразователей линейных перемещений / А. А. Ожиганов, Жуань Чжипэн. – Изв. вузов. Приборостроение. 2008. Т. 51, No 7. – С. 28—33.
2. Сарвате, Д. В. Взаимно-корреляционные свойства псевдослучаийных и родственных последовательностей / Д. В. Сарвате, М. Б. Персли. – ТИИЭР. 1980. Т. 68, No 5. – С. 59—95.
3. Мурашко, И. А. Методы минимизации энергопотребления при самотестировании цифровых устройств / И. А. Мурашко, В. Н. Ярмолик. – Минск: Бестпринт, 2004. – 188 с.
4. Борисенко, Н. П. О возможности генерации примитивных полиномов заданной степени и быстрого вычисления сдвига выходной последовательности РСЛОС на заданное число тактов / Н. П. Борисенко, А. В. Гусаров, А. П. Кривонос; Сб. трудов XII Междунар. науч. конф. „Информатизация и информационная безопасность правоохранительных систем“. М. 2003. – С. 334—339.