УДК 004.021

АЛГОРИТМ ГЕНЕРАЦИИ ПОРОЖДАЮЩИХ ПОЛИНОМОВ *М*-ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Ю. А. Толстогузов

Учреждение образования «Гомельский государственный технический университет имени П. О. Сухого», Республика Беларусь

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.

$$h(x) = \sum_{\mathrm{i}=0}^{\mathrm{n}} h_{\mathrm{i}} x^{i}, \tag{1}$$

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

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

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 быстро растет, то число полиномов степени n, порождающих *М*-последовательности, также быстро увеличивается.

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. $\text{НОД}(M, q_s) = 1$, децимация называется собственной или нормальной. Собственную 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

$$\{b_j\} = \{a_j\}^{q_s}. \tag{3}$$

Опишем алгоритм получения порождающих полиномов *М*-последовательности:

1. Выбираем полином вида (1) из таблиц известных примитивных полиномов или генерируем его других известным образом.
2. Представим имеющийся примитивный полином через порождающую матрицу *A* [3].
3. Вычислим матрицу $M' = A^n \oplus Ix$, где и взаимно простое число с периодом полинома.
4. Найдем определитель полученной матрицы M'.

Полученный определитель и будет децимированным по индексу q_s порождающим полиномом *М*-последовательности.

Литература

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, № 7. – С. 28–33.
2. Сарвате, Д. В. Взаимно-корреляционные свойства псевдослучайных и родственных последовательностей / Д. В. Сарвате, М. Б. Персли // ТИИЭР. – 1980. – Т. 68, № 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.