УДК 621.3.085

И. Д. Захаров, А. А. Ожиганов

ИСПОЛЬЗОВАНИЕ ПОРОЖДАЮЩИХ ПОЛИНОМОВ М-ПОСЛЕДОВАТЕЛЬНОСТЕЙ ПРИ ПОСТРОЕНИИ ПСЕВДОСЛУЧАЙНЫХ КОДОВЫХ ШКАЛ

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

Ключевые слова: *порождающий полином, М-последовательность, децимация, псевдослучайная кодовая шкала.*

Введение. Среди приборов, используемых в устройствах вычислительной техники и систем управления, особое место занимают преобразователи угловых и линейных перемещений (ПП), построенные по методу параллельного считывания. Основным элементом таких преобразователей является кодовая шкала (КШ). Классический подход к построению ПП базируется на использовании КШ с числом информационных кодовых дорожек, равным, как правило, разрядности преобразователей.

В работах [1—3] предложен новый тип более простых в реализации однодорожечных псевдослучайных кодовых шкал (ПСКШ). Для формирования структуры информационной кодовой дорожки таких шкал используются псевдослучайные двоичные последовательности максимального периода (М-последовательности), причем для построения n-разрядной ПСКШ могут быть использованы различные М-последовательности с одинаковым периодом. Таким образом, n-разрядная ПСКШ может иметь множество реализаций. В свою очередь, 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.

В настоящее время при разработке преобразователей перемещения на основе ПСКШ применяются системы автоматизированного проектирования (САПР ПСКШ) [4], что позволяет с использованием эффективного алгоритма вычислять необходимые порождающие полиномы во избежание сохранения в памяти ЭВМ всей базы данных о полиномах.

В настоящей работе приводятся необходимые для понимания сути статьи базовые положения теории М-последовательностей, основные сведения о принципах построения ПСКШ для преобразователей перемещений, а также рассматривается метод синтеза порождающих полиномов М-последовательностей с заданным периодом, предназначенный для использования в САПР ПСКШ.

Теоретические основы построения псевдослучайных кодовых шкал. ПСКШ имеют всего одну информационную кодовую дорожку, выполненную в соответствии с символами $\{a_j\}=a_0, a_1, ..., a_{M-1}$ М-последовательности, и n считывающих элементов (СЭ), размещенных вдоль дорожки. Наличие считывающих элементов позволяет получить при полном перемещении шкалы $M=2^n-1$ различных n-разрядных кодовых комбинаций.

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 $n > 1$. В табл. 1 приведены полиномы $h(x)$ для n =1…16, которые имеют минимальное число ненулевых коэффициентов h_i и могут быть использованы для генерации соответствующих М-последовательностей [5].

Таблица 1

n	$h(x)$	$M=2^n-1$	n	$h(x)$	$M=2^n-1$
1	$x+1$	1	9	x^9+x^4+1	511
2	x^2+x+1	3	10	$x^{10}+x^3+1$	1023
3	x^3+x+1	7	11	$x^{11}+x^2+1$	2047
4	x^4+x+1	15	12	$x^{12}+x^6+x^4+x+1$	4095
5	x^5+x^2+1	31	13	$x^{13}+x^4+x^3+x+1$	8191
6	x^6+x+1	63	14	$x^{14}+x^{10}+x^6+x+1$	16383
7	x^7+x^3+1	127	15	$x^{15}+x+1$	32787
8	$x^8+x^4+x^3+x^2+1$	255	16	$x^{16}+x^{12}+x^3+x+1$	65535

Известно [6], что для конкретного значения n существует точно

$$N = \frac{\Phi\left(M = 2^n - 1\right)}{n} \tag{2}$$

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 очень быстро растет, то число полиномов степени n, порождающих последовательности с максимальным периодом, с ростом n также быстро увеличивается. В табл. 2 приведены расчетные значения N для n =2…16.

Таблица 2

n	N	n	N
2	1	10	60
3	2	11	176
4	2	12	144
5	6	13	630
6	6	14	756
7	18	15	1800
8	16	16	2048
9	48		

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.

Символы a_{n+j} М-последовательности удовлетворяют рекуррентному выражению

$$a_{n+j} = \bigoplus_{i=0}^{n-1} a_{i+j} h_i, \; j = 0, 1, \ldots, \tag{3}$$

где знак $\oplus$ — суммирование по модулю два, а индексы при символах М-последовательности берутся по модулю M; начальные значения символов a_0, a_1, ..., a_{n-1} М-последовательности могут выбираться произвольно, за исключением нулевой комбинации.

Известно, что М-последовательности относятся к классу циклических кодов и могут задаваться с помощью полинома $g(x) = (x^M + 1)/h(x)$. Для каждой М-последовательности с периодом M существует ровно M различных циклических сдвигов, которые могут быть получены путем умножения полинома $g(x)$ на x^j, где $j = 0, 1, ..., M-1$.

Поскольку ПСКШ строятся в соответствии с символами М-последовательности, можно путем циклических сдвигов определить порядок размещения на шкале n считывающих элементов, т.е. m-му СЭ, $m = 1, 2, ..., n$, ставится в соответствие j_m-й циклический сдвиг $x^{j_m} g(x)$ М-последовательности.

Тогда полином, определяющий порядок размещения n СЭ на шкале, имеет вид

$$r(x) = \sum_{m=1}^{n} x^{j_m}, \quad j_m \in \{0, 1, ..., M-1\}. \tag{4}$$

Приняв $j_1 = 0$, согласно полиному (4) получим положения 2-го, 3-го, ..., n-го СЭ, смещенные относительно 1-го СЭ на $j_2, j_3, ..., j_n$ позиций соответственно.

Размещение считывающих элементов в соответствии с полиномом (4) должно обеспечивать получение при полном перемещении шкалы M различных n-разрядных кодовых комбинаций. В общем виде задача размещения СЭ на ПСКШ решена в работе [7].

Метод синтеза порождающих полиномов М-последовательностей. В основу метода положено использование свойств децимации М-последовательности и алгоритма Берлекемпа — Мэсси.

Согласно работе [8] децимацией М-последовательности $\{a_j\}$ по индексу q_s, $s = \overline{2, 2^n - 2}$, называется выборка q_s-х элементов данной М-последовательности. Если период $M = 2^n - 1$ исходной М-последовательности и индекс децимации q_s взаимно просты, т.е. НОД(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

$$\{b_j\} = \{a_j\}^{q_s}. \tag{5}$$

Алгоритм генерации примитивных полиномов заданной степени в общих чертах рассмотрен в работе [9]. Однако данный алгоритм оставляет открытым вопрос о нахождении всего множества порождающих полиномов М-последовательностей с заданным периодом и не оптимизирован для использования в САПР ПСКШ.

Рассмотрим метод синтеза порождающих полиномов М-последовательностей, свободный от указанного недостатка. Реализация метода предусматривает выполнение следующих шагов.

1. Из табл. 1 выбирается примитивный полином вида (1) определенной степени n.

2. На основе полинома (1) строится рекуррентное выражение (3).

3. Посредством рекуррентного выражения (3) генерируются символы $\{a_j\}$ М- последовательности с периодом $M = 2^n - 1$.

4. В соответствии с выражением (2) определяется число примитивных полиномов $h(x)$ степени n.

5. Осуществляется поиск значений индексов децимации q_l, $l = \overline{1, N-1}$, $\{q_l\} \subset \{q_s\}$, позволяющих сформировать все нормальные децимации М-последовательности $\{a_j\}$, на основе которых могут быть получены N–1 различных М-последовательностей $\{b_j\}$ с периодом M.

6. Производится нормальная децимация М-последовательности $\{a_j\}$ по индексу q_l. Результатом такой децимации является M_l-последовательность (5) с периодом M.

7. Далее, с использованием алгоритма Берлекемпа — Мэсси и предварительной выборки $2n$ символов из полученной M_l -последовательности определяется полином $h_l(x)$, который также будет примитивным.

8. Шаги 6 и 7 повторяются для всех нормальных децимаций, найденных на шаге 5.

Результатом применения метода являются N–1 порождающих полиномов степени n.

Эффективность разработанного метода в основном определяется результатом выполнения шага 5. Для оптимизации поиска значений индексов децимации рассмотрим алгоритм, в котором: $\{q_s\}$ — множество всех значений индексов децимации; $\{q_k\} \subset \{q_s\}$ — множество нечетных значений индексов децимации; REG[n] — n-разрядный двоичный циклический регистр сдвига; REG_z, $z = 0,...,n-1$, — значение z-го разряда регистра; SHIFT[p] — p-разрядный двоичный счетчик числа сдвигов, где p=[lb n]; C_k — флаг децимации с индексом q_k, причем

$$C_k = \begin{cases} 0, \text{ если децимация с индексом } q_k \text{ не позволяет} \\ \quad \text{получить необходимую М-последовательность;} \\ 1, \text{ в противном случае.} \end{cases}$$

Алгоритм содержит следующие шаги:

1. $q_k := 1$; $C_k := 1$, $k = 2e+1, e = \overline{1, 2^{n-1}-1}$.

2. $q_k := q_k + 2$.

3. Если $q_k \geq 2^n - 1$, переход к шагу 13.

4. Если $C_k = 0$, переход к шагу 2.

5. Запись q_k в REG[n]; обнуление счетчика SHIFT [p].

6. Если SHIFT [p]≥n–1, переход к шагу 10.

7. Циклический сдвиг регистра REG[n] на один разряд влево. SHIFT [p]:= SHIFT [p]+1.

8. Если REG_0=1, $k := REG[n], C_k := 0$.

9. Возврат к шагу 6.

10. Если НОД$\left(q_k, 2^n - 1\right)$=1, переход к шагу 12.

11. $C_k := 0$, переход к шагу 2.

12. Сохранение полученного значения q_k в массив результатов. Переход к шагу 2.

13. Вывод массива результатов.

Таким образом, используя рассмотренный алгоритм, можно найти все значения индексов, позволяющие сформировать нормальные децимации М-последовательности $\{a_j\}^{q_l}$, $l = \overline{1, N-1}$, на основе которых могут быть получены N–1 различных М-последовательностей $\{b_j\}$ с периодом M.

Пример. Рассмотрим метод синтеза порождающих полиномов М-последовательности на примере, ограничившись получением всех полиномов 5-й степени.

1. Из табл. 1 выбирается примитивный полином $h(x) = x^5 + x^2 + 1$.

2. На основе выбранного полинома строится рекуррентное выражение $a_{5+j} = a_{2+j} \oplus a_j$.

3. Посредством полученного рекуррентного выражения генерируются символы $\{a_j\} = (0,0,0,0,1,0,0,1,0,1,1,0,0,1,1,1,1,1,0,0,0,1,1,0,1,1,1,0,1,0,1)$ М-последовательности с периодом $M = 2^5 - 1$=31.

4. В соответствии с выражением (2) вычисляется количество примитивных полиномов $h(x)$ степени 5, т.е.

$$N = \frac{\Phi\left(M = 2^n - 1\right)}{n} = \frac{\Phi\left(M = 2^5 - 1\right)}{5} = \frac{\Phi(31)}{5} = \frac{30}{5} = 6.$$

5. Осуществляется поиск значений индексов децимации q_l, позволяющих сформировать нормальные децимации М-последовательности $\{a_j\}^{q_l}, l = \overline{1,5}$. В соответствии с приведенным выше алгоритмом используются только нечетные значения индекса $q_k \in \left[\overline{3, 2^5 - 1}\right)$. Каждое значение q_k заносится в регистр REG[5] и вычисляются все возможные значения, получаемые при его циклическом сдвиге влево. Например, при занесении в REG[5] значения q_1=3 получается следующий результат:

$$\begin{aligned}
&\mathrm{REG}[5] \leftarrow 3 \quad \Rightarrow \quad \mathrm{REG}[5]: 0\,0\,0\,1\,1; \\
&\text{сдвиг } 1: \quad \mathrm{REG}[5]: 0\,0\,1\,1\,0 \quad (6); \\
&\text{сдвиг } 2: \quad \mathrm{REG}[5]: 0\,1\,1\,0\,0 \quad (12); \\
&\text{сдвиг } 3: \quad \mathrm{REG}[5]: 1\,1\,0\,0\,0 \quad (24); \\
&\text{сдвиг } 4: \quad \mathrm{REG}[5]: 1\,0\,0\,0\,1 \quad (17).
\end{aligned}$$

С учетом того [8], что $\left\{a_j\right\}^{2^d q_s} = \left\{a_j\right\}^{(2^d q_s) \bmod M}$, полученные значения индексов децимации $q_1(0)$=3, $q_1(1)$=6, $q_1(2)$=12, $q_1(3)$=24 и $q_1(4)$=17 (где значение (*) определяет число сдвигов содержимого регистра) позволяют сформировать одинаковые (с точностью до циклического сдвига) М-последовательности. Следовательно, для синтеза необходимой М-последовательности достаточно использовать один из пяти индексов децимации, например $q_1(0)$=3.

Аналогичным образом вычисляем:

$$\begin{aligned}
&q_2(0) = 5 \quad \Rightarrow \quad q_2(1) = 10,\ q_2(2) = 20,\ q_2(3) = 9,\ q_2(4) = 18; \\
&q_3(0) = 7 \quad \Rightarrow \quad q_3(1) = 14,\ q_3(2) = 28,\ q_3(3) = 25,\ q_3(4) = 19; \\
&q_4(0) = 11 \quad \Rightarrow \quad q_4(1) = 22,\ q_4(2) = 21,\ q_4(3) = 13,\ q_4(4) = 26; \\
&q_5(0) = 15 \quad \Rightarrow \quad q_5(1) = 30,\ q_5(2) = 29,\ q_5(3) = 27,\ q_5(4) = 23.
\end{aligned}$$

Далее осуществляется проверка, являются ли полученные децимации q_l, $l = 1, ..., 5$, нормальными. Для этого определяется наибольший общий делитель значения каждого из полученных индексов q_l и периода M М-последовательности, т.е.

НОД(3, 31)=1; НОД(5, 31)=1; НОД(7, 31)=1; НОД(11, 31)=1; НОД(15, 31)=1.

Данный результат свидетельствует о нахождении пяти индексов децимации, использование которых дает возможность получения пяти различных М-последовательностей.

6. Производятся нормальные децимации полученной на шаге 3 М-последовательности $\{a_j\}$ по индексам q_l, $l = 1, ..., 5$. Например, первые $2n$=10 символов M_1-последовательности, полученные в результате децимации по индексу 3, равны $\left\{a_j\right\}_{10}^{3} = (0,0,0,0,1,1,0,0,1,0)$.

7. Далее, составляется система линейных алгебраических уравнений, решаемая с использованием алгоритма Берлекемпа — Мэсси, т.е.

$$\left.\begin{aligned} a_5 &= a_4h_4 \oplus a_3h_3 \oplus a_2h_2 \oplus a_1h_1 \oplus a_0h_0;\\ a_6 &= a_5h_4 \oplus a_4h_3 \oplus a_3h_2 \oplus a_2h_1 \oplus a_1h_0;\\ a_7 &= a_6h_4 \oplus a_5h_3 \oplus a_4h_2 \oplus a_3h_1 \oplus a_2h_0;\\ a_8 &= a_7h_4 \oplus a_6h_3 \oplus a_5h_2 \oplus a_4h_1 \oplus a_3h_0;\\ a_9 &= a_8h_4 \oplus a_7h_3 \oplus a_6h_2 \oplus a_5h_1 \oplus a_4h_0 \end{aligned}\right\} = \left\{\begin{aligned} 1 &= 1\cdot h_4 \oplus 0\cdot h_3 \oplus 0\cdot h_2 \oplus 0\cdot h_1 \oplus 0\cdot h_0;\\ 0 &= 1\cdot h_4 \oplus 1\cdot h_3 \oplus 0\cdot h_2 \oplus 0\cdot h_1 \oplus 0\cdot h_0;\\ 0 &= 0\cdot h_4 \oplus 1\cdot h_3 \oplus 1\cdot h_2 \oplus 0\cdot h_1 \oplus 0\cdot h_0;.\\ 1 &= 0\cdot h_4 \oplus 0\cdot h_3 \oplus 1\cdot h_2 \oplus 1\cdot h_1 \oplus 0\cdot h_0;\\ 0 &= 1\cdot h_4 \oplus 0\cdot h_3 \oplus 0\cdot h_2 \oplus 1\cdot h_1 \oplus 1\cdot h_0. \end{aligned}\right.$$

В результате получаем значения $h_0 = 1; h_1 = 0; h_2 = 1; h_3 = 1; h_4 = 1; h_5 = 1$, по которым находим искомый порождающий полином

$$h_1(x) = h_5x^5 + h_4x^4 + h_3x^3 + h_2x^2 + h_1x^1 + h_0 = 1\cdot x^5 + 1\cdot x^4 + 1\cdot x^3 + 1\cdot x^2 + 0\cdot x^1 + 1\cdot x^0 =$$
$$= x^5 + x^4 + x^3 + x^2 + 1.$$

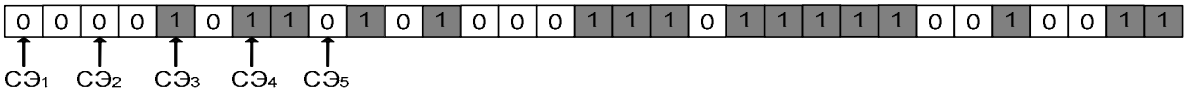
8. Шаги 6 и 7 повторяются для остальных нормальных децимаций, найденных на шаге 5; в результате получаем еще четыре порождающих полинома 5-й степени.

Все порождающие полиномы 5-й степени, соответствующие М-последовательности и значения индексов децимации приведены в табл. 3.

Таблица 3

Индекс децимации q	Порождающий полином $h(x)$	М-последовательность
0	$h(x) = x^5 + x^2 + 1$	00001001011001111100011011101 01
3	$h_1(x) = x^5 + x^4 + x^3 + x^2 + 1$	00001100100111110111000101011 01
5	$h_2(x) = x^5 + x^4 + x^2 + x + 1$	00001110011011111010001001010 11
7	$h_3(x) = x^5 + x^3 + x^2 + x + 1$	00001011010100011101111100100 11
11	$h_4(x) = x^5 + x^4 + x^3 + x + 1$	00001101010010001011111011001 11
15	$h_5(x) = x^5 + x^3 + 1$	00001010111011000111110011010 01

Отметим, что любая из приведенных в табл. 3 М-последовательностей пригодна для построения 5-разрядной ПСКШ. Например, линейная развертка круговой ПСКШ, выполненной с использованием М-последовательности, полученной на основе порождающего полинома $h_3(x) = x^5 + x^3 + x^2 + x + 1$, приведена на рисунке. Размещение на шкале пяти считывающих элементов задано в соответствии с полиномом $r(x) = 1 + x^2 + x^4 + x^6 + x^8$.



Последовательно с использованием считывающих элементов фиксируя кодовую комбинацию при перемещении шкалы на один квант, например справа налево, получаем 31 различную 5-разрядную кодовую комбинацию. Эти кодовые комбинации, соответствующие 31 различному угловому положению ПСКШ, приведены в табл. 4.

Таблица 4

Номер сдвига ПСКШ	Кодовая комбинация		Номер сдвига ПСКШ	Кодовая комбинация	
	Двоичный псевдослучайный код	Десятичный эквивалент		Двоичный псевдослучайный код	Десятичный эквивалент
0	00110	6	16	10110	22
1	00011	3	17	11110	30
2	01100	12	18	01101	13
3	00111	7	19	11100	28
4	11000	24	20	11010	26
5	01110	14	21	11001	25
6	10000	16	22	10101	21

Продолжение табл. 4

Номер сдвига ПСКШ	Кодовая комбинация		Номер сдвига ПСКШ	Кодовая комбинация	
	Двоичный псевдослучайный код	Десятичный эквивалент		Двоичный псевдослучайный код	Десятичный эквивалент
7	11101	29	23	10010	18
8	00001	1	24	01010	10
9	11011	27	25	00100	4
10	00010	2	26	10100	20
11	10111	23	27	01001	9
12	00101	5	28	01000	8
13	01111	15	29	10011	19
14	01011	11	30	10001	17
15	11111	31			

Заключение. Предложенный в настоящей статье метод построения порождающих полиномов М-последовательностей наиболее целесообразно использовать в системах автоматизированного проектирования псевдослучайных кодовых шкал для преобразователей перемещений.

СПИСОК ЛИТЕРАТУРЫ

1. *Ожиганов А. А.* Псевдослучайные кодовые шкалы // Изв. вузов СССР. Приборостроение. 1987. Т. 30, № 2. С. 40—43.

2. *Ожиганов А. А.* Псевдослучайные кодовые шкалы для преобразователей линейных перемещений // Изв. вузов. Приборостроение. 1995. Т. 38, № 11—12. С. 37—39.

3. *Ожиганов А. А., Чжипэн Жуань.* Использование псевдослучайных последовательностей при построении кодовых шкал для преобразователей линейных перемещений // Там же. 2008. Т. 51, № 7. С. 28—33.

4. *Ожиганов А. А., Коробейников А. Г., Климанов В. А.* Структура системы автоматизированного проектирования рекурсивных кодовых шкал // Науч.-техн. вестн. СПбГУ ИТМО. 2006. Вып. 32. С. 237—245.

5. *Макуильямс Ф. Д., Слоан Н. Д.* Псевдослучайные последовательности и таблицы // ТИИЭР. 1976. Т. 64, № 12. С. 80—95.

6. *Муттер В. М.* Основы помехоустойчивой телепередачи информации. Л.: Энергоатомиздат, 1990. 288 с.

7. *Ожиганов А. А.* Алгоритм размещения считывающих элементов на псевдослучайной кодовой шкале // Изв. вузов. Приборостроение. 1994. Т. 37, № 2. С. 22—27.

8. *Сарвате Д. В., Персли М. Б.* Взаимно-корреляционные свойства псевдослучайных и родственных последовательностей // ТИИЭР. 1980. Т. 68, № 5. С. 59—95.

9. *Борисенко Н. П., Гусаров А. В., Кривонос А. П.* О возможности генерации примитивных полиномов заданной степени и быстрого вычисления сдвига выходной последовательности РСЛОС на заданное число тактов // Сб. трудов XII Междунар. науч. конф. „Информатизация и информационная безопасность правоохранительных систем“. М., 2003. С. 334—339.

Сведения об авторах

Илья Дмитриевич Захаров — аспирант; Санкт-Петербургский государственный университет информационных технологий, механики и оптики, кафедра вычислительной техники; E-mail: zakharov_ilya@hotmail.com

Александр Аркадьевич Ожиганов — д-р техн. наук, профессор; Санкт-Петербургский государственный университет информационных технологий, механики и оптики, кафедра вычислительной техники; E-mail: ojiganov@mail.ifmo.ru

Рекомендована кафедрой вычислительной техники

Поступила в редакцию 18.01.11 г.