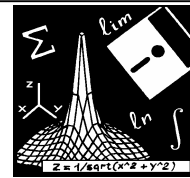


ИНФОРМАТИКА И ПРИКЛАДНАЯ МАТЕМАТИКА



УДК 621.391

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТИ СИНТЕЗА БИНАРНЫХ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ С ПЕРИОДОМ $P = 6R + 1$ ПРИ ФОРМИРОВАНИИ НА ОСНОВЕ ШЕСТИ КЛАССОВ СТЕПЕННЫХ ВЫЧЕТОВ ПО ПРОСТОМУ МОДУЛЮ

В.Е.Гантмахер, С.Ю.Кравцов

Институт электронных и информационных систем НовГУ, Kravcov_sergei@mail.ru

Проведено исследование возможности синтеза бинарных псевдослучайных последовательностей с простым периодом $P \equiv 1 \pmod{6}$ на основе шести классов степенных вычетов по простому модулю. Доказано, что кроме последовательностей Холла и Лежандра других бинарных последовательностей с указанными ограничениями не существует. Найдено новое правило кодирования псевдослучайных последовательностей Холла.

Ключевые слова: синтез, бинарные последовательности, периодическая корреляционная функция, правило кодирования, циклотомические числа

We carried out an investigation of possibility of the binary pseudorandom sequences synthesis with ordinary period $P \equiv 1 \pmod{6}$ based on six classes of power residue by prime module. It is proven that besides the Holl and Legendre sequences no other binary sequences with mentioned contingencies exist. The new rule of Holl pseudorandom sequence coding is found out.

Keywords: synthesis, binary sequences, periodic correlation function, code rule, cyclotomic rationals

Одними из наиболее известных, хорошо исследованных и широко востребованных псевдослучайных последовательностей (ПСП) являются последовательности Холла (ПХ) [1-4]. Они формируются на основе разностного множества Холла [5]. Необходимые и достаточные условия существования ПХ:

1. Период — простое число

$$P = 4u^2 + 27. \quad (1)$$

2. Первообразный корень θ простого поля Гауля $GF(P)$, по которому осуществляется формирование классов степенных вычетов, должен удовлетворять условию:

$$\text{ind}_{\theta} 3 \equiv 1 \pmod{6}. \quad (2)$$

3. Правило кодирования ПХ $Y = \{y_i\}$, $y_i = \{\pm 1\}$, $i = \overline{0, P-1}$

$$U(i) = \begin{cases} +1, & \text{ind}_{\theta} i \equiv 0, 1, 3 \pmod{6}, \\ -1, & \text{ind}_{\theta} i \equiv 2, 4, 5 \pmod{6}, \\ U(0) = -1. \end{cases} \quad (3)$$

ПХ имеют одноуровневую периодическую автокорреляционную функцию (ПАКФ)

$$r_y(\tau) = \sum_{i=1}^{P-1} y_i y_{i+\tau} = -1, \tau = \overline{1, P-1}. \quad (4)$$

Причиной возврата к исследованию ПХ явилась публикация [6], в которой показано, что существуют ПСП с периодами $P = 1471$ и $P = 16927$ при $\text{ind}_{\theta} 3 \not\equiv 1 \pmod{6}$, что противоречит (2), и с периодом $P = 1051$ при $\text{ind}_{\theta} i \equiv 0, 1, 4 \pmod{6}$, что противоречит (3).

Все три периода удовлетворяют условию (1). Поэтому целью настоящей работы является исследование возможности синтеза ПСП с периодом $P = 6R + 1$ и корреляционной функцией (4), частным случаем которых являются ПСП Холла.

Обобщенное правило кодирования (ПК) рассматриваемого семейства бинарных последовательностей (БП)

$$U(i) = \begin{cases} U(0), \\ +1, K(i) \in I_+, \\ -1, K(i) \in I_-. \end{cases} \quad (5)$$

Здесь $K(i)$ — функция, определяющая номер класса степенных вычетов, которому принадлежит число i , I_+ и I_- ($|I_+| + |I_-| = 6$) — непересекающиеся множества классов степенных вычетов, занятых символами «+» и «-» соответственно.

Прежде всего определим необходимые условия существования искомых последовательностей. Так как не существует бинарных последовательностей, неуровновешенность которых превышает по модулю единицу: $\Delta m = |m_+ - m_-| \leq 1$ (m_+ и m_- — число символов «+» и «-» на периоде БП соответственно), то $|I_+| = |I_-| = 3$. Это означает, что число допустимых комбинаций классов в (5) равно $C_6^3 = \frac{6 \cdot 5 \cdot 4}{2 \cdot 3} = 20$.

Ниже приведены все двадцать комбинаций возможных правил кодирования с учетом их циклической зависимости:

«А»						«В»						«С»						«D»					
0	1	2	3	4	5	0	1	2	3	4	5	0	1	2	3	4	5	0	1	2	3	4	5
+	+	+	-	-	-	+	+	-	+	-	-	+	+	-	-	+	-	+	-	+	-	+	-
-	+	+	+	-	-	-	+	+	-	+	-	-	+	+	-	-	+	-	+	-	+	-	+
-	-	+	+	+	-	-	-	+	+	-	+	+	-	+	+	-	-	-	+	+	-	+	-
-	-	-	+	+	+	+	-	-	+	+	-	-	+	+	+	-	-	-	+	+	+	-	-
+	-	-	-	+	+	-	+	-	-	+	+	-	-	+	-	+	+	-	-	+	+	+	-
+	+	-	-	-	+	+	-	+	-	+	-	+	-	-	+	-	+	+	-	-	+	+	-

Так как циклически связанные последовательности имеют одинаковый рельеф ПАКФ относительно ПК (5) [6], то нам понадобится вычислить четыре рельефа ПАКФ для каждой из групп «А», «В», «С», «D». Для этого рассчитаем таблицу циклотомических чисел для $P = dR + 1$, $d = 6$ [7]. Предварительно заметим, что простые числа $P = dR + 1$ однозначно представляются в виде суммы квадратов двух целых чисел $P = A^2 + 3B^2$. Сравнивая это равенство с (1) получим $A = 2u$, $B = 3$.

Таблица 1
Спектры циклотомических чисел порядка $d = 6$

	0	1	2
$36S(0,0)$	$p - 16u - 11$	$P + 8u + 13$	$P + 8u - 23$
$36S(0,1)$	$2P + 4u + 50$	$2P + 4u - 58$	$2P - 8u + 2$
$36S(0,2)$	$2P + 4u + 14$	$2P - 8u + 2$	$2P + 4u - 22$
$36S(0,3)$	$2P + 16u - 10$	$2P - 8u + 2$	$2P - 8u + 2$

В табл. 1 принято обозначение $S(0,k) = S(0,k) + S(k,0)$ и приведены значения циклотомических чисел лишь для $d/2$, так как при $R \equiv 1 \pmod{2}$ таблица спектров симметрична относительно $d/2$. С помощью табл. 1 были рассчитаны все четыре рельефа ПАКФ. Ниже в таблицах 2-4 приведен расчет ПАКФ двоичных последовательностей (ДП) $X = \{x_i\}$, $x_i = \{0,1\}$, $i = \overline{0, P-1}$, соответствующих распределению символов «+» в бинарной последовательности Y .

Таблица 2
Расчет спектров ДП $X_B \{0,1,3\}$ и БП Y_B

	0	1	2
$36S(0,0)$	$P - 16u - 11$	$P + 8u + 13$	$P + 8u - 23$
$36DS(0,0)$	$P + 8u - 23$	$P - 16u - 11$	$P + 8u + 13$
$36D^3S(0,0)$	$P - 16u - 11$	$P + 8u + 13$	$P + 8u - 23$
$36S(0,1)$	$2P + 4u + 50$	$2P + 4u - 58$	$2P - 8u + 2$
$36S(0,3)$	$2P + 16u - 10$	$2P - 8u + 2$	$2P - 8u + 2$
$36DS(0,2)$	$2P + 4u - 22$	$2P + 4u + 14$	$2P - 8u + 2$
$36S_{X_B}$	$9P - 27$	$9P - 27$	$9P - 27$
S_{X_B}	$(P - 3)/4$	$(P - 3)/4$	$(P - 3)/4$
S_{Y_B}	-1	-1	-1

Здесь D — оператор циклического сдвига Хаффмена, $S(0,k) = D^{k-d/2} S(0, -k)_d \Rightarrow S(0,4) = D^{4-3} S(0,1)_d = D S(0,2)$.

Как видно из результатов расчета, все гармоники спектра S_{X_B} имеют одинаковую амплитуду $s = (P - 3)/4$. Двоичная последовательность X_B имеет одноуровневую ПАКФ, значение которой зависит только от периода. ПАКФ соответствующей бинарной последовательности $Y = 2X - 1$ будет равна

$$r_{Y_B}(\tau) = P - 4(m_+ - r_{X_B}(\tau)) = -1.$$

Таким образом, все шесть последовательностей, правила кодирования которых представлены в группе «В», являются псевдослучайными последовательностями Холла. Результаты расчета трех остальных групп представлены в табл. 3, 4.

Таблица 3
Расчет спектров ДП $X_A \{0,1,2\}$, $X_C \{0,1,4\}$,

$X_D \{0,2,4\}$ и БП Y_A, Y_C, Y_D

	0	1	2
S_{X_A}	$(P + 5)/4$	$(P - 3)/4$	$(P - 11)/4$
S_{Y_A}	7	-1	-9
S_{X_C}	$(P - 3)/4$	$(P - 7)/4$	$(P + 1)/4$
S_{Y_C}	-1	-5	3
S_{X_D}	$(P - 3)/4$	$(P - 3)/4$	$(P - 3)/4$
S_{Y_D}	-1	-1	-1

Таблица 4
Расчет спектров БП Y_C при $U(0) = +1$

	0	1	2
S_{Y_C}	-1	-5	3
ΔS_{Y_C}	0	4	-4
$(S_{Y_C})_{U(0)=+1}$	-1	-1	-1

Как видно из результатов расчетов, две из рассматриваемых групп правил кодирования формируют максимально трансортгоналичные последовательности $(r_Y(\tau) = -1, \tau = \overline{1, P-1})$. По ПК группы «В» формируются шесть последовательностей Холла. А по ПК

группы «D» формируются две последовательности символов Лежандра. Однако если в группе «C» преобразование $U(0) = -1$ заменить на $U(0) = +1$, то БП, полученная по ПК

$$U(i) = \begin{cases} +1, \text{ ind}_\theta i \equiv 0, 1, 4 \pmod{6}, \\ -1, \text{ ind}_\theta i \equiv 2, 3, 5 \pmod{6}, \\ U(0) = +1, \end{cases} \quad (6)$$

также окажется максимально трансортгональной. При этом в отличие от (2) первообразный корень θ простого поля Галуа $GF(P)$ должен удовлетворять условию

$$\text{ind}_\theta 3 \equiv -1 \pmod{6}. \quad (7)$$

Правило кодирования $\begin{cases} (6) \\ (7) \end{cases}$ отличается от пра-

вила кодирования последовательностей Холла $\begin{cases} (2) \\ (3) \end{cases}$.

Однако двумя преобразованиями, инвариантными к рельефу автокорреляционной функции, — инверсией символов и циклическим сдвигом номеров классов на D^4 , — последовательности, построенные по новому правилу кодирования, преобразуются в последовательности Холла:

«C»						Инверсия символов					
0	1	2	3	4	5	0	1	2	3	4	5
+	+	-	-	+	-	-	-	+	+	-	+
-	+	+	-	-	+	+	-	-	+	+	-
+	-	+	+	-	-	-	+	-	-	+	+
-	+	-	+	+	-	+	-	+	-	-	+
-	-	+	+	-	+	+	+	-	+	-	-
+	-	-	+	-	+	-	+	+	-	+	-

Из сравнения двух последних столбцов видно, что после выполнения указанных выше преобразований правила кодирования «C» и «B» полностью совпадают.

Заключение

По результатам проведенных исследований можно сделать следующие выводы.

1. Среди последовательностей с простым периодом $P \equiv 1 \pmod{6}$, формируемых на основе шести классов степенных вычетов, не существует бинарных псевдослучайных максимально трансортгональных

последовательностей кроме последовательностей Холла и последовательностей символов Лежандра.

2. Найденное новое правило кодирования является лишь новым способом формирования последовательностей Холла.

1. Свердлик М.Б. Оптимальные дискретные сигналы. М.: Сов. радио, 1975. 200 с.
2. Ипатов В.П. Периодические дискретные сигналы с оптимальными корреляционными свойствами. М.: Радио и связь, 1992. 162 с.
3. Fan Pinghi, Darnel Michael. Sequence Design for communication Applications. UK, Hertfordshire: Research Studies Press Ltd., 1996. 487 p.
4. <http://signalslab.marstu.net/>
5. Холл М. Комбинаторика. М.: Мир, 1970. 423 с.
6. Гантмахер В.Е., Быстров Н.Е., Чеботарев Д.В. Шумоподобные сигналы. Анализ, синтез, обработка. СПб.: Наука и техника, 2005. 400 с.
7. Едемский В.А., Гантмахер В.Е. Синтез двоичных и троичных последовательностей с заданными ограничениями на их характеристики. В. Новгород: НовГУ, 2009. 189 с.

Bibliography (Transliterated)

1. Sverdlik M.B. Optimal'nye diskretnye signaly. M.: Sov. radio, 1975. 200 s.
2. Ipatov V.P. Periodicheskie diskretnye signaly s optimal'nymi korreljacionnymi svojstvami. M.: Radio i svjaz', 1992. 162 s.
3. Fan Pinghi, Darnel Michael. Sequence Design for communication Applications. UK, Hertfordshire: Research Studies Press Ltd., 1996. 487 p.
4. <http://signalslab.marstu.net/>
5. Khol M. Kombinatorika. M.: Mir, 1970. 423 s.
6. Gantmakher V.E., Bystrov N.E., Chebotarev D.V. Shumopodobnye signaly. Analiz, sintez, obrabotka. SPb.: Nauka i tekhnika, 2005. 400 s.
7. Edemskij V.A., Gantmakher V.E. Sintez dvoichnykh i troichnykh posledovatel'nostej s zadannymi ogranichenijami na ikh kharakteristiki. V. Novgorod: NovGU, 2009. 189 s.