

УДК 621.391

# ОБ ОДНОМ СЕМЕЙСТВЕ ЧЕТЫРЕХФАЗНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ С ИДЕАЛЬНОЙ ПЕРИОДИЧЕСКОЙ АВТОКОРРЕЛЯЦИОННОЙ ФУНКЦИЕЙ

М.В.Залешин, В.Е.Гантмахер

## ON THE FAMILY OF FOUR-PHASE SEQUENCES WITH IDEAL PERIODIC AUTOCORRELATION FUNCTION

M.V.Zaleshin, V.E.Gantmakher

*Институт электронных и информационных систем НовГУ, mikhailzaleshin@gmail.com*

Предложено новое правило кодирования четырехфазных последовательностей с идеальной периодической автокорреляционной функцией, которые обладают следующей совокупностью основных характеристик: период —  $6(q^m-1)/(q-1)$ , пик-фактор стремится к значению 1,2 с ростом периода, простота формирования.

**Ключевые слова:** *четырефазная последовательность, идеальная ПАКФ, анализ, расширенное поле Галуа, M-последовательность*

A new coding rule of four-phase sequences with ideal periodic autocorrelation function is offered. This sequences possess following set of properties: the period is  $6(q^m-1)/(q-1)$ , the limit of peak factor is 1.2 as the period approaches infinity, ease of formation.

**Keywords:** *four-phase sequence, ideal PACF, analysis, extended Galois field, M-sequence*

### 1. Введение

В основе радиолокационных, навигационных, акустических, спутниковых, мобильных и многих других информационно-технических комплексов лежат различные шумоподобные сигналы. Содержательная часть сигнала определяется с помощью периодических последовательностей, для которых одним из требований является идеальность их периодической автокорреляционной функции (ПАКФ) [1].

Известно немало работ, в которых представлены семейства последовательностей с идеальной ПАКФ, напр., [2-6]. Общим для большинства из этих

последовательностей является лишь условие идеальности ПАКФ. При этом они различаются целым набором характеристик, в частности:

- алфавитом, над которым осуществляется их формирование;
- периодом и плотностью сетки периодов;
- пик-фактором;
- мощностью правила кодирования;
- простотой формирования.

Спрос на последовательности с идеальной ПАКФ и различными совокупностями характеристик из числа приведенных выше в прикладных областях опережает предложение, поскольку конкретные на-

боры требований, предъявляемые к последовательностям, зависят от области применения и особенностей задач, которые решают с их помощью. Объектом нашего исследования являются четырехфазные последовательности.

В связи с вышесказанным, целью работы является синтез семейства четырехфазных последовательностей с идеальной ПАКФ.

## 2. Семейство четырехфазных последовательностей с идеальной ПАКФ

Построим правило кодирования над расширенным полем Галуа  $GF(q^m)$ , где  $q=p^s$ ,  $p$  — простое число, а  $m>1$  и  $s\geq 1$ . При этом  $GF(q)$  может быть как простым, так и расширенным полем Галуа без уменьшения общности дальнейших выкладок. Таким образом, определим правило кодирования семейства четырехфазных последовательностей следующей формулой:

$$y_n = i^n \begin{cases} 1, & \text{если } d_n \in H_0 \cup H_3 \cup H_8 \cup H_{10} \cup H_{11}; \\ -1, & \text{если } d_n \in H_2 \cup H_4 \cup H_5 \cup H_6 \cup H_9; \\ 0, & \text{в противном случае.} \end{cases} \quad (*)$$

В приведенном правиле кодирования приняты следующие обозначения:  $i=\sqrt{-1}$  — мнимая единица;  $\{d_n\}$  — М-последовательность периода  $q^m-1$  над расширенным полем Галуа  $GF(q^m)$ ;  $H_r = \{\theta^{12k+r} | k=0,1,\dots,\frac{q-1}{12}-1\}$ , где  $r=0,1,\dots,11$  — классы степенных вычетов над полем Галуа  $GF(q)$  с первообразным элементом  $\theta$ .

Найдем необходимые и достаточные условия, при выполнении которых последовательности, формируемые на основе правила кодирования (\*), имеют идеальную ПАКФ.

**Теорема 1.** Четырехфазная последовательность  $\{y_n\}$ , формируемая на основе правила кодирования (\*), имеет идеальную ПАКФ тогда и только тогда, когда характеристика  $q$  и степень расширения  $m$  поля Галуа  $GF(q^m)$  являются нечетными числами.

**Доказательство.** По построению  $q-1$  должно делиться без остатка на 12. Отсюда вытекает условие нечетности  $q$ .

Покажем, что  $m$  должно быть нечетным числом. Для этого сначала найдем ПАКФ последовательности, определяемой следующим правилом кодирования:

$$y'_n = \begin{cases} 1, & \text{если } d_n \in H_0 \cup H_3 \cup H_8 \cup H_{10} \cup H_{11}; \\ -1, & \text{если } d_n \in H_2 \cup H_4 \cup H_5 \cup H_6 \cup H_9; \\ 0, & \text{в противном случае.} \end{cases}$$

По свойствам М-последовательностей [7]:

$$R_{y'}(\tau) = 10R_x(\tau) + \sum_{j_1, j_2 \in I_1} R_x(\tau - \Delta j h) + \sum_{j_1, j_2 \in I_2} R_x(\tau - \Delta j h) - \sum_{j_1 \in I_1, j_2 \in I_2} R_x(\tau - \Delta j h) - \sum_{j_1 \in I_2, j_2 \in I_1} R_x(\tau - \Delta j h),$$

где  $h = \frac{q^m-1}{q-1}$ ;  $\Delta j = j_2 - j_1$ ;  $I_1 = \{0, 3, 8, 10, 11\}$ ;  $I_2 = \{2, 4, 5, 6, 9\}$ ;

$$R_x(\tau) = q^{m-2} \begin{cases} q, & \text{если } \tau \equiv 0 \pmod{q^m-1}; \\ 0, & \text{если } \tau \equiv 0 \pmod{h}; \\ 1, & \text{в противном случае.} \end{cases}$$

Выполнив подстановку  $R_x(\tau)$  и проведя необходимые преобразования, получаем ПАКФ последовательности  $\{y'_n\}$ :

$$R_{y'}(\tau) = 10q^{m-1} \begin{cases} 1, & \text{если } \tau \equiv 0 \pmod{12h}; \\ -1, & \text{если } \tau \equiv 0 \pmod{6h}; \\ 0, & \text{в противном случае.} \end{cases}$$

Отсюда следует, что ПАКФ последовательности  $\{y'_n\}$  определяется формулой:

$$R_{y'}(\tau) = [i^\tau]^* R_{y'}(\tau).$$

Поскольку для каждого  $\tau$ , кратного двум, но не кратного четырем, значение  $[i^\tau]^* = -1$ , то  $\{y'_n\}$  имеет идеальную ПАКФ тогда и только тогда, когда выполнено сравнение  $2 \equiv 6h \pmod{4}$ . Следовательно, необходимо, чтобы  $3h \equiv 1 \pmod{2}$ , т. е.  $h$  должно быть нечетным числом. Согласно принятым обозначениям:

$$h = \frac{q^m-1}{q-1} = \sum_{n=0}^{m-1} q^n.$$

Для каждого  $n=0,1,\dots,m-1$  величина  $q^n$  является нечетной. Представленная сумма является нечетной тогда и только тогда, когда число слагаемых  $m$  также нечетно, т. е. степень расширения поля Галуа  $GF(q^m)$  должна быть нечетным числом. Что и требовалось доказать.

Из доказанной теоремы следует, что для нечетных значений  $q$  и  $m$  ПАКФ четырехфазных последовательностей из семейства, сформированного по предложенному правилу кодирования, является идеальной и имеет вид:

$$R_y(\tau) = \begin{cases} 5q^{m-1}, & \text{если } \tau \equiv 0 \pmod{6h}; \\ 0, & \text{в противном случае.} \end{cases}$$

## 3. Свойства предложенного семейства четырехфазных последовательностей с идеальной ПАКФ

Определим период четырехфазных последовательностей  $\{y_n\}$ , формируемых на основе предложенного в предыдущем разделе правила кодирования.

**Теорема 2.** Период четырехфазных последовательностей  $\{y_n\}$  с идеальной ПАКФ, формируемых с помощью (\*), определяется формулой  $6h$ ,

где  $h = \frac{q^m-1}{q-1}$ .

**Доказательство.** Достаточно показать, что выполняется равенство  $y_{n+6h} = y_n$ . Истинность этого равенства напрямую вытекает из формулы правила кодирования (\*) и свойств циклической структуры М-последовательностей [7].

Заметим, что полученный период отличается от периодов известных семейств четырехфазных последовательностей с идеальной ПАКФ, например:

- последовательности Ли [4] имеют период, определяемый формулой  $q+1$ ;
- последовательности Ким-Джанг-Ким-Но [5] имеют период  $2p$ ;
- последовательности Лим-Но [6] имеют период  $2N$ .

Кроме того, известно, что произведение двух последовательностей с идеальной ПАКФ также имеет идеальную ПАКФ, если периоды перемножаемых последовательностей — взаимно-простые числа [8]. Поскольку существуют правила кодирования троичных последовательностей с идеальной ПАКФ и периодом вида  $h$  (напр., [9]), то умножая их на четырехфазную последовательность периода шесть, получим семейство четырехфазных последовательностей периода  $6h$ . ПАКФ последовательностей из этого семейства будет идеальной, если выполнено  $(6, h)=1$ . Покажем, что это возможно не для всех значений  $m$ , т. е. полученное в настоящей работе семейство расширяет сетку периодов четырехфазных последовательностей по сравнению с известными.

**Теорема 3.** Четырехфазные последовательности, формируемые по правилу кодирования (\*), отличаются от произведения последовательностей с идеальной ПАКФ периода шесть и  $h$  тогда, когда степень расширения поля Галуа  $GF(q^m)$  делится на три без остатка.

**Доказательство.** Делители числа шесть — двойка и тройка. Достаточно проверить делимость  $h = \frac{q^m - 1}{q - 1}$  на эти же числа. Поскольку  $h$  — нечетное число, то  $h$  не делится на два, но может быть кратно трем.

Найдем такие степени расширения  $m$ , что  $h \equiv 0 \pmod{3}$ . По построению  $q \equiv 1 \pmod{12}$ , т. е. имеет вид  $q = 12c + 1$ , где  $c$  — произвольное натуральное число. Отсюда в результате преобразований получаем:

$$\frac{q^m - 1}{q - 1} = \frac{(12c + 1)^m - 1}{12c} = m + 3 \sum_{n=2}^m C_m^n 3^{n-2} (4c)^{n-1}.$$

Из разложения видно, что  $h \equiv 0 \pmod{3}$  для каждой степени расширения  $m$ , которая кратна трем. Что и требовалось доказать.

Из теоремы следует, что при формировании четырехфазных последовательностей с идеальной ПАКФ по правилу кодирования (\*) необходимо использовать такие поля Галуа  $GF(q^m)$ , степень расширения которых делится на три без остатка.

Зная период и значение главного лепестка ПАКФ последовательности  $\{y_n\}$ , рассчитаем ее пик-фактор:

$$pf_y = 1, 2 \left[ \frac{q}{q-1} - \frac{1}{q^{m-1}(q-1)} \right].$$

Отсюда следует, что с ростом значения характеристики расширенного поля Галуа  $q$  значение пик-фактора  $pf_y$  стремится к 1,2.

Поскольку предложенное правило кодирования семейства четырехфазных последовательностей с идеальной ПАКФ определяется над расширенными полями Галуа на основе М-последовательности, то его мощность совпадает с мощностью правила кодирования самих М-последовательностей и равняется:

$$\frac{\phi(q^m - 1)}{2m}, \text{ где } \phi(n) \text{ — фи-функция Эйлера.}$$

Аналогичным образом объясняется простота формирования представленного семейства последовательностей, поскольку М-последовательности обладают оптимально малой линейной сложностью и для них существуют эффективные устройства-генераторы.

#### 4. Примеры

Проиллюстрируем работу предложенного правила кодирования четырехфазных последовательностей с идеальной ПАКФ (\*) на нескольких примерах.

**Пример 1.** Положим в качестве параметров расширенного поля Галуа  $q=13$  и  $m=3$ . Для формирования последовательностей найдем необходимые классы степенных вычетов над  $GF(13)$ , первообразный элемент которого  $\theta=2$ :

$$H_0 = \{1\}; H_3 = \{8\}; H_8 = \{9\}; H_{10} = \{10\}; H_{11} = \{7\}; \\ H_2 = \{4\}; H_4 = \{3\}; H_5 = \{6\}; H_6 = \{12\}; H_9 = \{5\}.$$

Для таких классов степенных вычетов правило кодирования принимает вид:

$$y_n = i^n \begin{cases} 1, & \text{если } d_n \in \{1, 7, 8, 9, 10\}; \\ -1, & \text{если } d_n \in \{3, 4, 5, 6, 12\}; \\ 0, & \text{в противном случае.} \end{cases}$$

Тогда для произвольной М-последовательности  $\{d_n\}$  над расширенным полем Галуа  $GF(13^3)$  четырехфазная последовательность  $\{y_n\}$ , формируемая с помощью полученного правила кодирования:

- по теореме 1 имеет идеальную ПАКФ;
- по теореме 2 имеет период 1098;
- обладает пик-фактором  $pf_y \approx 1,3$ .

**Пример 2.** Выберем в качестве параметров расширенного поля Галуа  $q=25$  и  $m=3$ . Поскольку  $q=5^2$ , то  $GF(q)$  является расширенным полем Галуа. Пусть его первообразный элемент  $\theta=\alpha$ , а примитивный многочлен  $f(\alpha)=\alpha^2+\alpha+2$ . В этом случае необходимые классы степенных вычетов над  $GF(5^2)$  имеют следующий вид:

$$H_0 = \{1, 4\}; H_3 = \{4\alpha + 2, \alpha + 3\}; H_8 = \{3\alpha + 1, 2\alpha + 4\}; \\ H_{10} = \{\alpha + 4, 4\alpha + 1\}; H_{11} = \{3\alpha + 3, 2\alpha + 2\}; \\ H_2 = \{4\alpha + 3, \alpha + 2\}; H_4 = \{3\alpha + 2, 2\alpha + 3\}; H_5 = \{4\alpha + 4, \alpha + 1\}; \\ H_6 = \{2, 3\}; H_9 = \{3\alpha + 4, 2\alpha + 1\}.$$

Для таких классов степенных вычетов правило кодирования принимает вид:

$$y_n = i^n \begin{cases} 1, & \text{если } d_n \in \{1, 4, \alpha+3, \alpha+4, 2\alpha+2, 2\alpha+ \\ & +4, 3\alpha+1, 3\alpha+3, 4\alpha+1, 4\alpha+2\}; \\ -1, & \text{если } d_n \in \{2, 3, \alpha+1, \alpha+2, 2\alpha+1, 2\alpha+ \\ & +3, 3\alpha+2, 3\alpha+4, 4\alpha+3, 4\alpha+4\}; \\ 0, & \text{в противном случае.} \end{cases}$$

Тогда для произвольной М-последовательности  $\{d_n\}$  над расширенным полем Галуа  $GF(25^3)$  четырехфазная последовательность  $\{y_n\}$ , формируемая с помощью полученного правила кодирования:

- по теореме 1 имеет идеальную ПАКФ;
- по теореме 2 имеет период 3906;
- обладает пик-фактором  $pf_y \approx 1,25$ .

Аналогичным образом выполняется формирование последовательностей для расширенных полей Галуа с произвольными параметрами, удовлетворяющими необходимым и достаточным условиям из теоремы 1.

### 5. Заключение

Предложено новое семейство четырехфазных последовательностей с идеальной ПАКФ. Эти последовательности обладают следующей совокупностью характеристик:

- период определяется формулой  $6 \frac{q^m - 1}{q - 1}$ , где  $q \equiv 1 \pmod{12}$  и  $m \equiv 0 \pmod{3}$ ;
- значение пик-фактора стремится к 1,2 с ростом  $q$ ;
- мощность правила кодирования равняется  $\frac{\varphi(q^m - 1)}{2m}$ ;
- простота формирования обусловлена тем, что правило кодирования основано на М-последовательностях с оптимально малой линейной сложностью.

Апробация правила кодирования полученного семейства последовательностей проведена на многочисленных примерах с использованием вычислитель-

ной техники, что гарантирует достоверность приведенных результатов.

1. Ипатов В.П. Периодические дискретные сигналы с оптимальными корреляционными свойствами. М.: Радио и связь, 1992. 152 с.
2. Luke H.D. BTP-transform and perfect sequences with small phase alphabet // IEEE Trans. Aerosp. Electron. Syst. 1996. V.32. P.497-499.
3. Krengel E.I. New polyphase perfect sequences with small alphabet // Electron. Lett. 2008. V.44. №17. P.1013-1014.
4. Lee C.E. Perfect  $q$ -ary sequences from multiplicative characters over  $GF(p)$  // Electron. Lett. 1992. V.28. №9. P.833-835.
5. Kim Y.S., Jang S.H., Kim S.H., No J.S. New construction of quaternary sequences with ideal autocorrelation from Legendre sequences. Seoul: ISIT, 2009. P.282-285.
6. Lim T., No J.S. New construction of quaternary sequences with ideal autocorrelation and balance property // ICTC. 2010. V.1. P.395-396.
7. Цирлер Н. Линейные возвратные последовательности // Кибернетический сборник. 1963. №6. С.55-79.
8. Ipatov V.P. Spread spectrum and CDMA: principles and applications. N.Y.: Wiley, 2005. 400 p.
9. Ipatov V.P. Ternary sequences with ideal periodic autocorrelation properties // Radio Engineering and Electronic physics. 1979. №24. P.75-79.

### References

1. Ipatov V.P. Periodicheskie diskretnye signaly s optimal'nymi korrelyatsionnymi svoystvami [Periodic discrete signals with optimal correlation properties]. Moscow, "Radio i svyaz" Publ., 1992. 152 p.
2. Luke H.D. BTP-transform and perfect sequences with small phase alphabet. IEEE Trans. Aerosp. Electron. Syst., 1996, vol. 32, pp. 497-499.
3. Krengel E.I. New polyphase perfect sequences with small alphabet. Electron. Lett., 2008, vol. 44, no. 17, pp. 1013-1014.
4. Lee C.E. Perfect  $q$ -ary sequences from multiplicative characters over  $GF(p)$ . Electron. Lett., 1992, vol. 28, no. 9, pp. 833-835.
5. Kim Y.S., Jang S.H., Kim S.H., No J.S. New construction of quaternary sequences with ideal autocorrelation from Legendre sequences. Seoul: ISIT, 2009, pp. 282-285.
6. Lim T., No J.S. New construction of quaternary sequences with ideal autocorrelation and balance property. ICTC, 2010, vol. 1, pp. 395-396.
7. Zierler N. Lineinye vozvratnye posledovatel'nosti [Linear recursive sequences]. Kiberneticheskii sbornik, 1963, no. 6, pp.55-79.
8. Ipatov V.P. Spread spectrum and CDMA: principles and applications. New York, Wiley, 2005. 400 p.
9. Ipatov V.P. Ternary sequences with ideal periodic autocorrelation properties. Radio Engineering and Electronic physics, 1979, no. 24, pp. 75-79.