

ФОРМИРОВАНИЕ МНОЖЕСТВ СЕМЕРИЧНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ С НИЗКИМ УРОВНЕМ ВЗАИМНОЙ КОРРЕЛЯЦИИ ДЛЯ СИСТЕМ ПЕРЕДАЧИ ЦИФРОВОЙ ИНФОРМАЦИИ

В. Г. Стародубцев, В. В. Мышко

Военно-космическая академия им. А. Ф. Можайского, Санкт-Петербург, Россия
vka@mil.ru

Аннотация. Представлены наборы векторов индексов децимации $I_S = (d_1, d_2, \dots, d_n)$ для формирования множеств семеричных последовательностей с низким уровнем взаимной корреляции в конечных полях $GF(7^S)$. На основании децимации символов базисной M -последовательности получены множества семеричных голд-подобных последовательностей с периодом $N = 7^S - 1$ ($S = 2, 3, 4, 5$). Приведены значения периодической взаимно корреляционной функции мощности формируемых множеств и числа множеств с эквивалентными свойствами.

Ключевые слова: конечные поля, корреляционная функция, M -последовательности, последовательности Голда, индексы децимации

Ссылка для цитирования: Стародубцев В. Г., Мышко В. В. Формирование множеств семеричных последовательностей с низким уровнем взаимной корреляции для систем передачи цифровой информации // Изв. вузов. Приборостроение. 2025. Т. 68, № 2. С. 105–115. DOI: 10.17586/0021-3454-2025-68-2-105-115.

FORMATION OF SETS OF SEPTENARY SEQUENCES WITH LOW CROSS-CORRELATION LEVEL FOR DIGITAL INFORMATION TRANSMISSION SYSTEMS

V. G. Starodubtsev, V. V. Myshko

A. F. Mozhaisky Military Space Academy, St. Petersburg, Russia
vka@mil.ru

Abstract. Sets of vectors of decimation indices $I_S = (d_1, d_2, \dots, d_n)$ for the formation of sets of septenary sequences with a low level of mutual correlation in finite fields $GF(7^S)$ are presented. Based on the decimation of the symbols of the basic M -sequence, sets of septenary gold-like sequences with a period $N = 7^S - 1$ ($S = 2, 3, 4, 5$) are obtained. The values of the periodic cross-correlation function, the power of the generated sets and the number of sets with equivalent properties are given.

Keywords: finite fields, correlation function, M -sequences, Gold sequences, decimation indices

For citation: Starodubtsev V. G., Myshko V. V. Formation of sets of septenary sequences with low cross-correlation level for digital information transmission systems. *Journal of Instrument Engineering*. 2025. Vol. 68, N 2. P. 105–115 (in Russian). DOI: 10.17586/0021-3454-2025-68-2-105-115.

Применение недвоичных сигналов с расширенным спектром в системах передачи цифровой информации (СПЦИ) позволяет повысить структурную скрытность передаваемых сигналов и эффективность использования частотного ресурса каналов связи [1–4]. Множества многофазных сигналов с расширенным спектром формируются на основе недвоичных псевдослучайных

последовательностей (ПСП) и обладают взаимно корреляционными свойствами, подобными свойствам ПСП [5, 6].

Вопросы разработки алгоритмов формирования множеств недвоичных ПСП рассматриваются в большом числе научных работ [7–16]. Одной из пионерских является статья Р. Голда [7], в которой получены множества двоичных последовательностей с трехуровневой взаимной корреляционной функцией. В работах [8–11] рассмотрены процедуры формирования недвоичных последовательностей с хорошими как авто-, так и взаимно корреляционными свойствами. Формированию множеств недвоичных последовательностей посвящено большое количество работ [12–16], в которых последовательности образуются путем децимации М-последовательностей (МП) и производных последовательностей по заданным индексам децимации.

Использование термина „голд-подобные“ для недвоичных последовательностей обусловлено тем, что структура проверочных полиномов, необходимых для их формирования, совпадает со структурой полиномов для формирования двоичных последовательностей Голда [7]. При этом проверочный полином формируемых последовательностей является произведением двух примитивных полиномов одинаковой степени.

Целью статьи является определение векторов индексов децимации $\mathbf{I}_S = (d_1, d_2, \dots, d_n)$ для формирования семеричных голд-подобных последовательностей (ГПП) с периодом $N = 7^S - 1 < 20\,000$ ($S = 2, 3, 4, 5$), а также вычисление их корреляционных свойств.

Формирование последовательностей выполняется в метрике Ли, то есть символами последовательностей являются элементы простого поля $GF(7)$. Вычисление периодической взаимно корреляционной функции (ПВКФ) последовательностей A_l и A_k осуществляется в метрике Евклида в соответствии с известным выражением [1, 2, 5]:

$$R_{lk}(\tau) = \sum_{i=0}^{N-1} a_{li} a_{k,i+\tau}^*,$$

где $a_{li} = \exp(j2\pi m/7)$ — символы семеричных последовательностей в комплексной форме, $m = 0, 1, \dots, 6$; „*“ — знак комплексного сопряжения; τ — циклический сдвиг.

При вычислении взаимно корреляционных функций последовательностей из формируемых множеств проводится сравнение результатов с известными граничными оценками. Например, при синтезе множеств ПСП широко применяется граничная оценка для максимального значения модуля ПВКФ в случае нечетных значений параметра S , полученная в [17, 18]:

$$|R_{\max}| = 1 + 7^{(S+1)/2}. \quad (1)$$

Для четных значений параметра S используется следующая граничная оценка [15]:

$$|R_{\max}| = -1 + k7^{S/2}, \quad k = 2, 3, \dots, p. \quad (2)$$

Для различения характеристик формируемых множеств ГПП разного типа при фиксированном значении параметра S в подстрочных индексах добавляется номер ГПП i -го типа. Например, при $S = 5$ вектор индексов децимации множества ГПП 1-го типа с периодом $N = 7^5 - 1$ обозначается как $\mathbf{I}_{5,1}$.

Зная индексы децимации d_i , возможно из символов базисной МП с полиномом $h_1(x)$ формировать произвольную ПСП с полиномом $h_i(x)$. При этом периоды формируемых ПСП совпадают с периодом базисной МП или являются его делителями. Для каждого конечного поля $GF(7^S)$ под базисной МП понимается последовательность, формируемая с помощью полинома $h_1(x)$, который используется для построения поля.

Нижний цифровой индекс при обозначении полиномов $h_i(x)$ здесь и в дальнейшем соответствует минимальным показателям степени их корней и численно равен индексу децимации d_i при формировании последовательностей из базисной МП, для которой $d_1 = 1$.

Последовательности множеств ГПП с периодом $N = 7^S - 1$ формируются на основе проверочных полиномов $h_{S,\Gamma}(x)$, вычисляемых как произведение двух примитивных полиномов степени S , соответствующих предпочтительным парам МП [1, 5]. В этом случае для полиномов выполняется условие для наибольшего общего делителя: $\text{НОД}(d_i, 7^S - 1) = 1$. Для семеричных последовательностей одним из полиномов также может быть неприводимый полином, корни которого имеют период $N_1 = N/2$ и $\text{НОД}(d_j, 7^S - 1) = 2$.

Рассмотрим пример формирования множеств ГПП с периодом $N = 7^2 - 1 = 48$, формируемых над конечным полем $\text{GF}(7^2)$ с полиномом $f(x) = h_1(x) = x^2 + x + 3$. Минимальный полином $h_i(x)$ степени $S = 2$ для произвольного элемента α^i конечного поля $\text{GF}(7^2)$ может быть представлен в виде [5]:

$$h_i(x) = x^2 - x \sum_{j=0}^1 (\alpha^i)^{7^j} + (\alpha^i)^{7^0}(\alpha^i)^{7^1} = x^2 - \text{tr}_{21}(\alpha^i)x + (\alpha^i)^8,$$

где $\text{tr}_{21}(\alpha^i)$ — функция следа примитивного элемента α^i из расширенного поля $\text{GF}(7^2)$ в простом поле $\text{GF}(7)$.

В конечном поле $\text{GF}(7^2)$ существует восемь примитивных полиномов и четыре неприводимых с периодом корней $N_1 = 24$, которые представлены в табл. 1.

Таблица 1

$N = 48$				$N_1 = 24$	
d_i	$h_i(x)$	d_i	$h_i(x)$	d_i	$h_i(x)$
1	$h_1(x) = x^2 + x + 3$	17	$h_{17}(x) = x^2 + 2x + 5$	2	$h_2(x) = x^2 + 5x + 2$
5	$h_5(x) = x^2 + 3x + 5$	19	$h_{19}(x) = x^2 + 5x + 3$	10	$h_{10}(x) = x^2 + x + 4$
11	$h_{11}(x) = x^2 + 4x + 5$	25	$h_{25}(x) = x^2 + 6x + 3$	26	$h_{26}(x) = x^2 + 2x + 2$
13	$h_{13}(x) = x^2 + 2x + 3$	41	$h_{41}(x) = x^2 + 5x + 5$	34	$h_{34}(x) = x^2 + 6x + 4$

Анализ корреляционных свойств показал, что можно выделить три типа ГПП, удовлетворяющих граничной оценке (2).

К первому типу относятся ГПП, для которых определен следующий вектор индексов децимации:

$$\mathbf{I}_{S,\Gamma i} = \mathbf{I}_{2,\Gamma 1} = (d_1, d_2) = (13, 19).$$

Данный тип ГПП обладает четырехуровневой ПВКФ с граничной оценкой вида (2) при $k = 2$:

$$R(\tau) = \{-8; -1; 6; 13\}. \quad (3)$$

Для каждого примитивного полинома может быть сформировано по два множества ГПП. Например, для $h_1(x)$ это множества ГПП с проверочными полиномами $h_{2,\Gamma 1}(x) = h_1(x)h_{13}(x)$ и $h_{2,\Gamma 2}(x) = h_1(x)h_{19}(x)$. На рис. 1 приведен график корреляционной функции множества ГПП 1-го типа с проверочным полиномом $h_{2,\Gamma 1}(x) = h_1(x)h_{13}(x) = (x^2 + x + 3)(x^2 + 2x + 3)$.

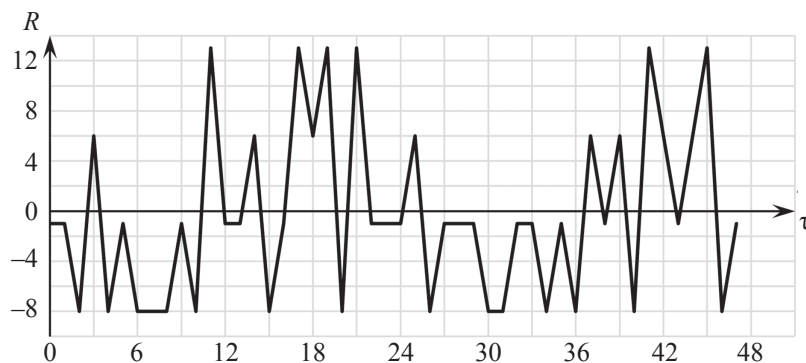


Рис. 1

Для произвольного примитивного полинома $h_i(x)$ индекс второго полинома определяется умножением на $d_1 = 13$ или $d_2 = 19$ по $\text{mod } (7^S - 1) = \text{mod } 48$ с выбором минимального p -сопряженного элемента. Например, для $h_{11}(x)$ это множества ГПП с полиномами $h_{2,\Gamma 3}(x) = h_{11}(x)h_{41}(x)$ и $h_{2,\Gamma 4}(x) = h_{11}(x)h_{17}(x)$. Всего может быть построено $M_{S,\Gamma i} = M_{2,\Gamma 1} = 16$ различных множеств мощностью $V_{S,\Gamma i} = V_{2,\Gamma 1} = 50$.

Схема устройства формирования ГПП 1-го типа с проверочным полиномом $h_{2,\Gamma 1}(x) = h_1(x)h_{13}(x)$ показана на рис. 2. Схема состоит из двух регистров сдвига с линейной обратной связью, умножители и сумматоры по $\text{mod } 7$ в цепи обратной связи которых расставляются в соответствии с обратными по сложению коэффициентами полиномов $h_1(x)$ и $h_{13}(x)$. Ячейки регистров сдвига принимают семь состояний и могут быть реализованы с помощью трех триггеров. В первом регистре сдвига, построенном по полиному $h_1(x) = x^2 + x + 3$, фиксируется некоторое ненулевое начальное состояние. Во втором регистре сдвига, построенном по полиному $h_{13}(x) = x^2 + 2x + 3$, для получения всех последовательностей множества ГПП устанавливаются все возможные начальные состояния. Для удобства сравнения с формированием множества ГПП программным способом в качестве начального состояния первого регистра сдвига выбраны символы $c_0 = \text{tr}_{21}(\alpha^0) = 2$ и $c_1 = \text{tr}_{21}(\alpha^1) = 6$. В результате формируется МП в каноническом виде. Во втором регистре сдвига для формирования первой последовательности из множества ГПП начальное состояние определяется путем децимации символов базисной МП по индексу $d_1 = 13$, то есть $c_0 = 2$ и $c_{13} = \text{tr}_{21}(\alpha^{13}) = 5$. Для формирования второй последовательности множества ГПП децимация начинается с символа c_1 , при этом начальными символами будут $c_1 = 6$ и $c_{14} = \text{tr}_{21}(\alpha^{14}) = 2$.

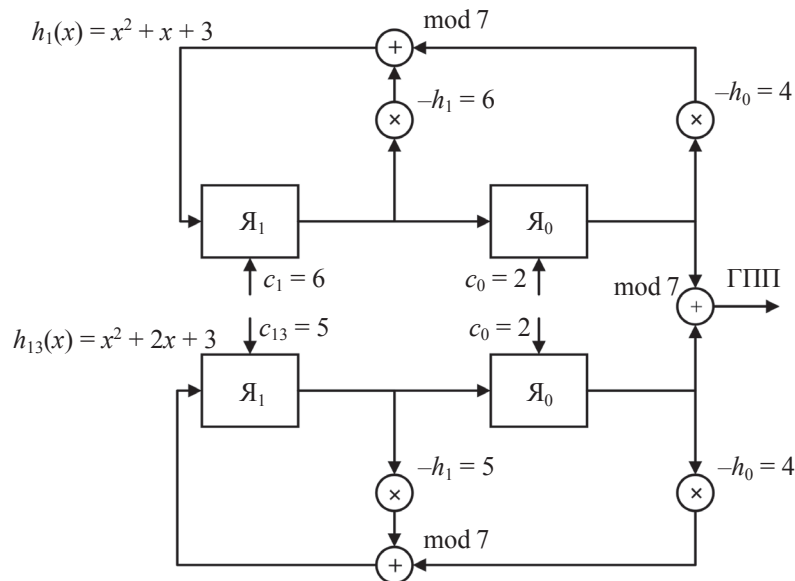


Рис. 2

При программном способе формирования последовательностей множества ГПП происходит посимвольное суммирование по $\text{mod } 7$ двух последовательностей. Первая последовательность образуется из символов c_i ($i = 0, \dots, N - 1$) базисной МП в каноническом виде с полиномом $h_1(x)$ в соответствии с выражением [5, 6]:

$$c_i = \text{tr}_{S1}(\alpha^i).$$

Вторая последовательность, также являющаяся МП, образуется путем децимации символов базисной МП по одному из индексов децимации $d_1 = 13$ или $d_2 = 19$. Например, символы e_i ($i = 0, \dots, N - 1$) МП с индексом $d_1 = 13$ определяются следующим образом:

$$e_i = c_{(d_1 \times i) \text{ mod } (7^S - 1)} = c_{13i \text{ mod } 48}.$$

В результате децимированная последовательность образуется из символов базисной МП: $c_0, c_{13}, c_{26}, c_{39}, c_4, \dots, c_{31}, c_{44}, c_9, c_{22}, c_{35}$.

Искомая последовательность множества ГПП формируется путем сложения по mod 7 символов c_i и e_i ($i = 0, \dots, N-1$).

Для формирования остальных последовательностей множества ГПП необходимо выполнить сдвиг начального символа базисной МП. Например, при сдвиге на 2 вторая из суммируемых последовательностей образуется из других символов базисной МП: $c_2, c_{15}, c_{28}, c_{41}, c_6, \dots, c_{33}, c_{46}, c_{11}, c_{35}, c_0$. При этом первая последовательность остается без изменений.

Второй тип включает ГПП с вектором индексов децимации

$$\mathbf{I}_{S,\Gamma} = \mathbf{I}_{2,\Gamma 2} = (d_3, d_4) = (2, 26).$$

Данные последовательности рассмотрены в [11], они имеют девятиуровневую ПВКФ

$$R(\tau) = \{-8; -7,31; -5,36; -2,56; -1; 0,56; 3,36; 5,31; 6\}, \quad (4)$$

максимальное значение модуля которой удовлетворяет граничной оценке, полученной В. М. Сидельниковым [18]:

$$|R_{\max}| = 1 + 7S/2. \quad (5)$$

Периоды последовательностей, формируемых с помощью полиномов $h_2(x)$ и $h_{26}(x)$, равны $N_1 = 24$, поэтому на периоде базисной МП укладывается два периода таких последовательностей. Корреляционная функция множества ГПП 2-го типа с проверочным полиномом $h_{2,\Gamma 2}(x) = h_1(x)h_2(x)$ показана на рис. 3.

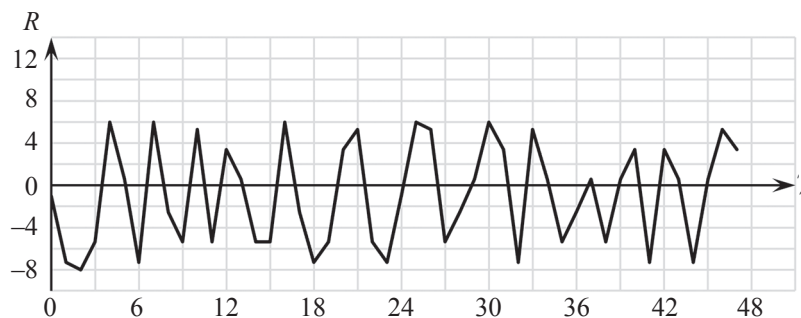


Рис. 3

Последовательности множества ГПП 2-го типа обладают более низким максимальным значением ПВКФ, что определяет предпочтительность их применения для формирования сигналов с расширенным спектром в СПЦИ.

Для последовательностей множеств ГПП 3-го типа получен следующий вектор индексов децимации:

$$\mathbf{I}_{S,\Gamma} = \mathbf{I}_{2,\Gamma 3} = (d_5, d_6) = (10, 34).$$

Периоды последовательностей, формируемых с помощью полиномов $h_{10}(x)$ и $h_{34}(x)$, равны $N_1 = N/2 = 24$.

Модуль максимального значения ПВКФ соответствует аналогичному модулю для последовательностей ГПП 1-го типа, но число уровней увеличивается до шести

$$R(\tau) = \{-8; -4,5; -1; 2,5; 6; 13\}. \quad (6)$$

В общем случае ПВКФ может быть представлена выражением

$$R(\tau) = \{(-7^{S/2} - 1); (-0,5 \times 7^{S/2} - 1); -1; (0,5 \times 7^{S/2} - 1); (7^{S/2} - 1); (2 \times 7^{S/2} - 1)\},$$

в котором добавляются два уровня $\pm 0,5 \times 7^{S/2} - 1$, по сравнению с (3).

На рис. 4 показана ПВКФ множества ГПП 3-го типа с проверочным полиномом $h_{2,\Gamma 3}(x) = h_1(x)h_{34}(x) = (x^2 + x + 3)(x^2 + 6x + 4)$.

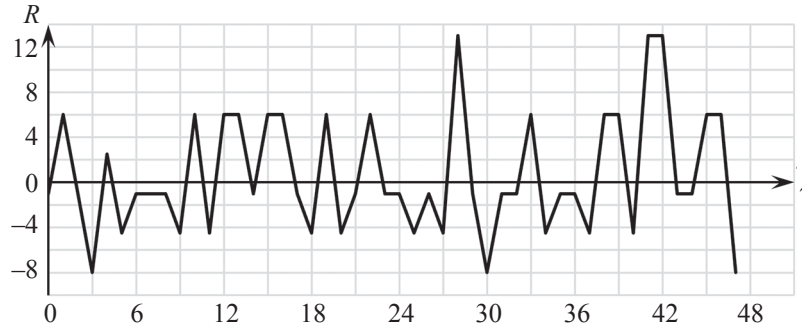


Рис. 4

Количество множеств ГПП для каждого из трех типов равно $M_{2,\Gamma} = 16$. Мощность множеств ГПП 1-го типа равна $V_{2,\Gamma 1} = 50$, а двух остальных типов $V_{2,\Gamma 2-3} = 49$, так как в данные множества не входят последовательности с периодом $N_1 = 24$.

При четном значении $S = 4$ вычисление векторов индексов децимации и анализ корреляционных свойств множеств ГПП в поле $GF(7^4)$ с полиномом $f(x) = h_1(x) = x^4 + x^2 + 3x + 5$ выполняются аналогично рассмотренному варианту при $S = 2$. В этом поле имеется 160 примитивных полиномов с периодом корней $N = 2400$ и 80 неприводимых полиномов с периодом корней $N_1 = 1200$. Некоторые полиномы с соответствующими индексами децимации, которые используются при формировании рассматриваемых множеств ГПП, приведены в табл. 2.

Таблица 2

$N = 2400$				$N_1 = 1200$	
d_i	$h_i(x)$	d_i	$h_i(x)$	d_i	$h_i(x)$
1	$h_1(x) = x^4 + x^2 + 3x + 5$	211	$h_{211}(x) = x^4 + 3x^2 + 4x + 5$	2	$h_2(x) = x^4 + x^3 + x^2 + 3x + 5$
13	$h_{13}(x) = x^4 + 4x^3 + 4x^2 + x + 5$	223	$h_{223}(x) = x^4 + x^3 + 2x^2 + 2x + 5$	14	$h_{14}(x) = x^4 + x^3 + x^2 + 3x + 5$
31	$h_{31}(x) = x^4 + 4x^3 + x^2 + 4x + 5$	403	$h_{403}(x) = x^4 + 3x^3 + 3x^2 + 4x + 5$	62	$h_{62}(x) = x^4 + x^3 + x^2 + 3x + 5$
97	$h_{97}(x) = x^4 + 6x^3 + 3x^2 + x + 5$	607	$h_{607}(x) = x^4 + x^3 + x + 5$	866	$h_{866}(x) = x^4 + x^3 + x^2 + 3x + 5$
187	$h_{187}(x) = x^4 + 6x^2 + 3x + 5$	817	$h_{817}(x) = x^4 + 5x^3 + 2x^2 + 5$	1202	$h_{1202}(x) = x^4 + x^3 + x^2 + 3x + 5$

По результатам анализа корреляционных свойств граничным оценкам (2) и (5), как и в случае $S = 2$, удовлетворяют три типа ГПП. Первый тип характеризуется следующим вектором индексов децимации:

$$\mathbf{I}_{S,\Gamma i} = \mathbf{I}_{4,\Gamma 1} = (d_1, d_2) = (97, 817).$$

Корреляционные свойства аналогичны свойствам ГПП первого типа с периодом $N = 48$, то есть ПВКФ является четырехуровневой

$$R(\tau) = \{-50; -1; 48; 97\}. \quad (7)$$

В общем виде значения функции корреляции в выражениях (3) при $S = 2$ и (7) при $S = 4$ могут быть представлены как

$$R(\tau) = \{(-7^{S/2} - 1); -1; (7^{S/2} - 1); (2 \times 7^{S/2} - 1)\}. \quad (8)$$

Формирование множеств ГПП может быть выполнено для каждого из 160 примитивных полиномов. Для базисной МП необходимо определить проверочные полиномы $h_{4,\Gamma 1}(x) = h_1(x)h_{97}(x)$ и $h_{4,\Gamma 2}(x) = h_1(x)h_{817}(x)$ (см. табл. 2). Для произвольного примитивного полинома, например $h_{31}(x)$, множества ГПП формируются с помощью $h_{4,\Gamma 3}(x) = h_{31}(x)h_{607}(x)$ и $h_{4,\Gamma 4}(x) = h_{31}(x)h_{223}(x)$.

Множества ГПП могут формироваться как аппаратным (на основании полиномов из табл. 2), так и программным способом. Множества ГПП 2-го типа определяются в соответствии с вектором индексов децимации

$$\mathbf{I}_{S,\Gamma i} = \mathbf{I}_{4,\Gamma 2} = (d_3, d_4) = (2, 1202).$$

Корреляционная функция удовлетворяет граничной оценке В. М. Сидельникова (5) и характеризуется девятью уровнями

$$R(\tau) = \{-50; -45,1; -31,6; -11,9; -1; 9,9; 29,6; 43,1; 48\}. \quad (9)$$

Общий вид выражений (4) и (9) представляется следующим образом:

$$R(\tau) = \{(-7^{S/2} - 1); (-0,9 \times 7^{S/2} - 1); (-0,6 \times 7^{S/2} - 1); (-0,2 \times 7^{S/2} - 1); -1; (0,2 \times 7^{S/2} - 1); (0,6 \times 5^{S/2} - 1); (0,9 \times 7^{S/2} - 1); (7^{S/2} - 1)\}.$$

Третий тип ГПП обладает семиуровневой ПВКФ

$$R(\tau) = \{-148; -99; -50; -1; 48; 97; 146\}$$

с граничной оценкой вида (2) при $k = 3$ и вектором индексов децимации

$$\mathbf{I}_{S,\Gamma} = \mathbf{I}_{4,\Gamma 2} = (d_5, d_6) = (13, 211).$$

Характеристики множеств ГПП при четных значениях $S = 2, 4$ приведены в табл. 3.

Таблица 3

S	Γi	N	$\mathbf{I}_{S,\Gamma i} = (d_1, \dots, d_n)$	Значения ПВКФ	$ R_{\max} $	Выражение для $ R_{\max} $	$ r_{\max} $	Число уровней ПВКФ	$V_{S,\Gamma}$	$M_{S,\Gamma}$
2	$\Gamma 1$	48	13, 19	-8; -1; 6; 13	13	$2 \cdot 7^{S/2} - 1$	0,27	4	50	16
2	$\Gamma 2$	48	2, 26	-8; -7,31; -5,36; -2,56; -1; 0,56; 3,36; 5,31; 6	8	$7^{S/2} + 1$	0,17	9	49	16
2	$\Gamma 3$	48	10, 34	-8; -4,5; -1; 2,5; 6; 13	13	$2 \cdot 7^{S/2} - 1$	0,27	6	49	16
4	$\Gamma 1$	2400	97, 817	-50; -1; 48; 97	97	$2 \cdot 7^{S/2} - 1$	0,04	4	2402	320
4	$\Gamma 2$	2400	2, 1202	-50; -45,147; -31,551; -11,904; -1; 9,904; 29,551; 43,147; 48	50	$7^{S/2} + 1$	0,02	9	2401	320
4	$\Gamma 3$	2400	13, 211	-148; -99; -50; -1; 48; 97; 146	148	$3 \cdot 7^{S/2} + 1$	0,06	7	2402	320

Таким образом, в полях $GF(7^2)$ и $GF(7^4)$ можно сформировать по три типа множеств ГПП, каждое из которых образуется с помощью двух полиномов соответствующей степени. Максимальные значения модулей ПВКФ для множеств ГПП 1-го и 2-го типов удовлетворяют граничным оценкам (2) при $k = 2$ и (5) соответственно, а для множеств ГПП 3-го типа — оценке

(2) при $k = 3$. Предпочтительными для использования в СПЦИ являются множества ГПП 2-го типа, обладающие наименьшими значениями ПВКФ.

Для нечетного значения $S = 3$ множества ГПП с периодом $N = 7^S - 1 = 7^3 - 1 = 342$ формируются в поле $GF(7^3)$ с полиномом $f(x) = h_1(x) = x^3 + 3x + 2$. В данном поле существует по 36 примитивных полиномов и неприводимых полиномов с периодом корней $N_1 = 171$.

В результате анализа взаимно корреляционных свойств последовательностей, формируемых в поле $GF(7^3)$, получены векторы индексов децимации для множеств ГПП трех типов.

Вектор индексов децимации для множеств ГПП 1-го типа имеет вид

$$\mathbf{I}_{S, \Gamma 1} = \mathbf{I}_{3, \Gamma 1} = (d_1, d_2) = (25, 43).$$

Рассматриваемые множества удовлетворяют граничной оценке (1) и характеризуются трехуровневой ПВКФ

$$R(\tau) = \{-50; -1; 48\},$$

которая в общем виде представляется следующим образом:

$$R(\tau) = \{(-7^{(S+1)/2} - 1); -1; (7^{(S+1)/2} - 1)\}. \quad (10)$$

Сегмент корреляционной функции длиной 125 символов для множества ГПП 1-го типа с проверочным полиномом $h_{3, \Gamma 1}(x) = h_1(x)h_{25}(x)$ показан на рис. 5.

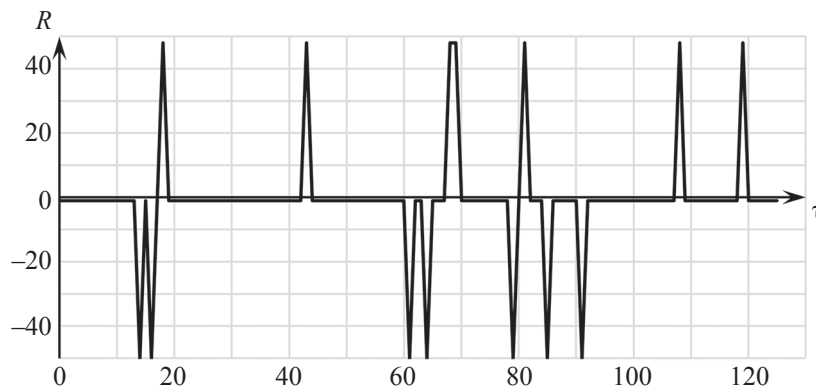


Рис. 5

Для множеств ГПП 2-го типа получен следующий вектор индексов децимации:

$$\mathbf{I}_{S, \Gamma 2} = \mathbf{I}_{3, \Gamma 2} = (d_3, d_4, d_5, d_6) = (2, 8, 86, 236).$$

Корреляционная функция последовательностей удовлетворяет граничной оценке (5) и имеет семь уровней

$$R(\tau) = \{-19,1; -15,5; -9,0; -1; 7,0; 13,5; 17,1\}.$$

В общем виде ПВКФ может быть представлена

$$R(\tau) = \{(-0,4 \times 7^{(S+1)/2} - 1); (-0,3 \times 7^{(S+1)/2} - 1); (-0,2 \times 7^{(S+1)/2} - 1); -1; (0,2 \times 7^{(S+1)/2} - 1); (0,3 \times 7^{(S+1)/2} - 1); (0,4 \times 7^{(S+1)/2} - 1)\}. \quad (11)$$

Сегмент ПВКФ последовательностей множества 2-го типа с проверочным полиномом $h_{3, \Gamma 2}(x) = h_1(x)h_{236}(x)$ показан на рис. 6.

Третий тип множеств ГПП формируется на основе вектора индексов децимации

$$\mathbf{I}_{S, \Gamma 3} = \mathbf{I}_{3, \Gamma 3} = (d_7, d_8, d_9, d_{10}, d_{11}) = (4, 10, 22, 88, 130).$$

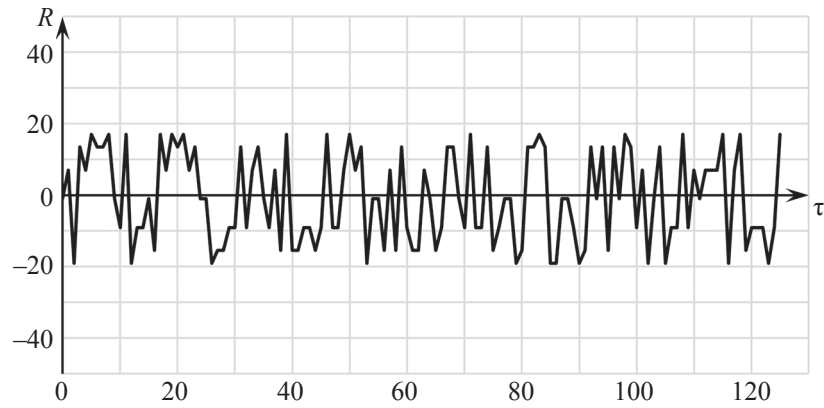


Рис. 6

Он характеризуется трехуровневой функцией взаимной корреляции $R(\tau) = \{-25,5; -1; 23,5\}$, которая в общем виде представляется как

$$R(\tau) = \{(-0,5 \times 7^{(S+1)/2} - 1); -1; (0,5 \times 7^{(S+1)/2} - 1)\}. \quad (12)$$

Сегмент корреляционной функции с полиномом $h_{3,\Gamma 3}(x) = h_1(x)h_{22}(x)$ показан на рис. 7.

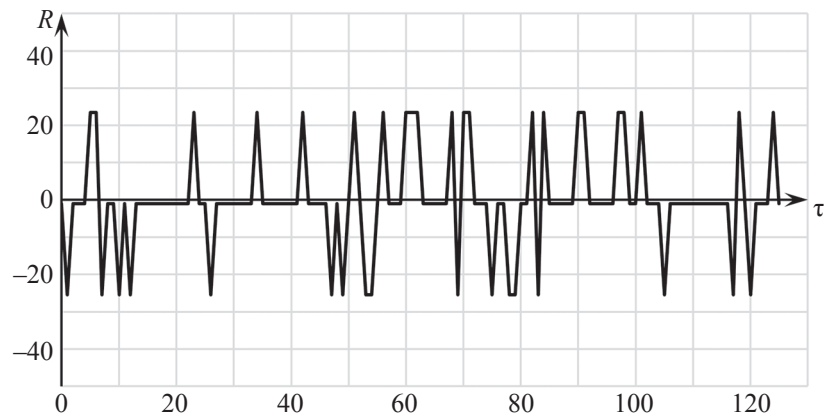


Рис. 7

Мощность множеств ГПП и их количество зависят от числа примитивных полиномов и числа индексов децимации.

При $S = 5$ в поле $GF(7^5)$ с полиномом $f(x) = h_1(x) = x^5 + 2x + 2$ существует по 1120 примитивных полиномов с периодом корней $N = 16\,806$ и неприводимых полиномов с периодом корней $N_1 = 8403$. Получены векторы индексов децимации для множеств ГПП трех типов, причем распределение уровней ПВКФ соответствует выражениям (10)–(12).

Характеристики полученных множеств ГПП для нечетных значений параметра S приведены в табл. 4.

Таким образом, в статье получены наборы векторов индексов децимации $\mathbf{I}_S = (d_1, d_2, \dots, d_n)$ для формирования в конечных полях $GF(7^S)$ множеств семеричных ГПП с периодом $N = 7^S - 1$ ($S = 2, 3, 4, 5$) с низким уровнем взаимной корреляции. Максимальные значения модуля ПВКФ последовательностей данных множеств удовлетворяют известным граничным оценкам. Формирование множеств ГПП может быть реализовано как аппаратным, так и программным способом. При аппаратном способе для формирования каждого множества требуется знать структуру двух неприводимых полиномов степени S , соответствующих заданным индексам децимации. При программном способе для каждого конечного поля $GF(7^S)$ необходимо знать структуру только одного полинома $h_1(x)$ для формирования базисной МП и набора векторов индексов децимации.

Таблица 4

S	Γ_i	N	$\mathbf{I}_{S,\Gamma_i} = (d_1, \dots, d_n)$	Значения ПВКФ	$ R_{\max} $	Выражение для $ R_{\max} $	$ r_{\max} $	Число уровней ПВКФ	$V_{S,\Gamma}$	$M_{S,\Gamma}$
3	Γ_1	342	25, 43	–50; –1; 48	50	$7^{(S+1)/2} + 1$	0,15	3	344	72
3	Γ_2	342	2, 8, 86, 236	–19,1; –15,5; –9,0; –1; 7,0; 13,5; 17,1	19,1	$0,37 \cdot 7^{(S+1)/2} + 1$	0,06	7	343	144
3	Γ_3	342	4, 10, 22, 88, 130	–25,5; –1; 23,5	25,5	$0,5 \cdot 7^{(S+1)/2} + 1$	0,07	3	343	180
5	Γ_1	16806	25, 43	–344; –1; 342	344	$7^{(S+1)/2} + 1$	0,02	3	16808	2240
5	Γ_2	16806	2, 8	–127,4; –102,4; –57,24; –1; 55,24; 100,4; 125,4	127,4	$0,37 \cdot 7^{(S+1)/2} + 1$	0,007	7	16807	2240
5	Γ_3	16806	4, 148, 172	172,5; –1; 170,5	172,5	$0,5 \cdot 7^{(S+1)/2} + 1$	0,01	3	16807	3360

Полученные множества семеричных ГПП могут найти применение при формировании сигналов с расширенным спектром в СПЦИ, к которым предъявляются повышенные требования по структурной скрытности и частотной эффективности.

СПИСОК ЛИТЕРАТУРЫ

1. Скляр Б. Цифровая связь. Теоретические основы и практическое применение: Пер. с англ. М.: Изд. дом „Вильямс“, 2003. 1104 с.
2. Вишневский В. М., Ляхов А. И., Портной С. Л., Шахнович И. В. Широкополосные беспроводные сети передачи информации. М.: Техносфера, 2005. 592 с.
3. Ипатов В. П. Широкополосные системы и кодовое разделение сигналов. Принципы и приложения. М.: Техносфера, 2007. 488 с.
4. CDMA: прошлое, настоящее, будущее / Под ред. Л. Е. Варакина и Ю. С. Шинакова. М.: МАС, 2003. 608 с.
5. Ипатов В. П. Периодические дискретные сигналы с оптимальными корреляционными свойствами. М.: Радио и связь, 1992. 152 с.
6. Golomb S. W., Gong G. Signal Design for Good Correlation for Wireless Communication, Cryptography and Radar. Cambridge Univ. Press, 2005. 438 p.
7. Gold R. Maximal recursive sequences with 3-valued recursive cross-correlation functions // IEEE Trans. Inform. Theory. 1968. Vol. 14, N 1. P. 154.
8. Helleseth T., Kumar P. V., Martinsen H. A new family of ternary sequences with ideal two-level autocorrelation function // Designs, Codes and Cryptography. 2001. Vol. 23, N 2. P. 157.
9. Boztaş S., Özbudak F., Tekin E. Generalized nonbinary sequences with perfect autocorrelation flexible alphabets and new periods // Cryptogr. Commun. 2018. Vol. 10, N 3. P. 509.
10. Cho Chang-Min, Kim Ji-Youp, No J. S. New p-ary sequence families of period $(p^n - 1)/2$ with good correlation property using two decimated m-sequences // IEICE Transactions on Communications. 2015. Vol. E98, N 7. P. 1268.
11. Стародубцев В. Г. Множества двоичных последовательностей с низким уровнем взаимной корреляции для систем передачи цифровой информации // Радиотехника и электроника. 2023. Т. 68, № 2. С. 146.
12. Choi S. T., Lim T., No J. S., Chung H. On the Cross-Correlation of a p-ary m-Sequence of Period p^{2m-1} and Its Decimated Sequences by $(p^m + 1)^2/2(p + 1)$ // IEEE Trans. Inf. Theory. 2012. Vol. 58, N 3. P. 1873.
13. Xia Y., Chen S. A new family of p-ary sequences with low correlation constructed from decimated sequences // IEEE Trans. Inf. Theory. 2012. Vol. 58, N 9. P. 6037.
14. Jang J. W., Kim Y. S., No J. S., Helleseth T. New family of p-ary sequences with optimal correlation property and large linear span // IEEE Trans. Inf. Theory. 2004. Vol. 50, N 8. P. 1839.
15. Стародубцев В. Г., Ткаченко В. В. Формирование множеств пятеричных голд-подобных последовательностей для систем передачи цифровой информации // Изв. вузов. Приборостроение. 2024. Т. 67, № 2. С. 107.
16. Seo E. Y., Kim Y. S., No J. S., Shin D. J. Cross-correlation distribution of p-ary m-sequence and its $(p + 1)$ decimated sequences with shorter period // IEICE Trans. Fund. Electron., Commun. Comput. Sci. 2007. Vol. E90-A, N 11. P. 2568.