

ФОРМИРОВАНИЕ МНОЖЕСТВ ТРОИЧНЫХ КАСАМИ-ПОДОБНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ
ДЛЯ СИСТЕМ ПЕРЕДАЧИ ЦИФРОВОЙ ИНФОРМАЦИИ

В. Г. Стародубцев*, Е. А. Четвериков

Военно-космическая академия им. А. Ф. Можайского, Санкт-Петербург, Россия,
*vgstarod@mail.ru

Аннотация. Представлены наборы векторов индексов децимации $I_S(i_{d1}, i_{d2}, \dots, i_{dn})$ базисных троичных M -последовательностей, на основании которых в конечных полях $GF(3^S)$ ($S = 4, 6, 8$) формируются малые и большие множества касами-подобных последовательностей (КПП) с периодами $N = 3^S - 1 < 20\,000$. Показано, что для четных значений S периодическая взаимно корреляционная функция малого множества КПП является трехуровневой с максимальным значением модуля периодической взаимно корреляционной функции $|R_{\max}| = (3^{S/2} + 1)$. Корреляционная функция большого множества при $S = 4$ является восьмиуровневой с $|R_{\max}| = (2 \times 3^{S/2} + 1)$, а при $S = 6, 8$ — десятиуровневой с $|R_{\max}| = (3^{S/2+1} + 1)$. Приведены значения объемов малого и большого множеств троичных КПП.

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

Ссылка для цитирования: Стародубцев В. Г., Четвериков Е. А. Формирование множеств троичных касами-подобных последовательностей для систем передачи цифровой информации // Изв. вузов. Приборостроение. 2023. Т. 66, № 10. С. 807—817. DOI: 10.17586/0021-3454-2023-66-10-807-817.

FORMATION OF SETS OF TERNARY KASAMI-LIKE SEQUENCES
FOR DIGITAL INFORMATION TRANSMISSION SYSTEMS

V. G. Starodubtsev*, E. A. Chetverikov

A.F. Mozhaisky Military Space Academy, St. Petersburg, Russia
vgstarod@mail.ru

Abstract. Sets of vectors of decimation indices $I_S(i_{d1}, i_{d2}, \dots, i_{dn})$ of ternary M -sequences are presented, on the basis of which small and large sets of Kasami-similar sequences (KSS) with periods $N = 3^S - 1 < 20\,000$ are formed in finite fields $GF(3^S)$ ($S = 4, 6, 8$). It is shown that for even values of S , the periodic cross-correlation function of a small set of KSS is three-level with the maximum value of the module of the mutual correlation function $|R_{\max}| = (3^{S/2} + 1)$. The correlation function of a large set at $S = 4$ is eight-level with $|R_{\max}| = (2 \cdot 3^{S/2} + 1)$, and at $S = 6, 8$ is ten-level with $|R_{\max}| = (3^{S/2+1} + 1)$. The values of the volumes of small and large sets of ternary KSS are given.

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

For citation: Starodubtsev V. G., Chetverikov E. A. Formation of sets of ternary Kasami-like sequences for digital information transmission systems. *Journal of Instrument Engineering*. 2023. Vol. 66, N 10. P. 807—817 (in Russian). DOI: 10.17586/0021-3454-2023-66-10-807-817.

В системах передачи цифровой информации (СПЦИ) защищенность от преднамеренных помех повышается за счет применения сигналов с расширенным спектром, формируемых на основе псевдослучайных последовательностей [1—4]. В различных режимах работы

СПЦИ могут использоваться как отдельные последовательности, так и множества последовательностей с заданными корреляционными и структурными свойствами [5].

В системах передачи цифровой информации при формировании фазоманипулированных сигналов с расширенным спектром в основном применяются двоичные псевдослучайные последовательности (ПСП), такие как М-последовательности (МП), последовательности Голда, Касами [2, 4, 6]. Эти последовательности обладают хорошими авто- и взаимно корреляционными свойствами.

Одним из направлений развития СПЦИ является переход от двоичных сигналов к многопозиционным, в частности — многофазным. Многофазные сигналы с расширенным спектром формируются на основе недвоичных ПСП и обеспечивают повышение помехозащищенности СПЦИ в условиях воздействия узкополосных и широкополосных помех. Например, в системах спутниковой связи с кодовым многостанционным доступом множества троичных ПСП могут применяться в виде фазоманипулированных на 120° сигналов, которые представляют собой эквидистантную систему сигналов [7—9].

Вопросам разработки алгоритмов формирования недвоичных ПСП с хорошими корреляционными и структурными свойствами посвящено большое число публикаций [10—18]. В работах [10—13] проанализированы методы формирования множеств троичных последовательностей, синтезируемых на основе децимации МП по различным индексам. В статьях [14—18] синтезированы множества недвоичных последовательностей с низким уровнем взаимной корреляции.

При формировании множеств троичных последовательностей, у которых порядок вычисления проверочных полиномов аналогичен порядку вычисления полиномов для двоичных последовательностей Касами и Голда [5, 6, 19], будем использовать термины „касами-подобные последовательности“ (КПП) и „голд-подобные последовательности“ (ГПП). Необходимость введения термина определяется тем, что при совпадении структуры проверочных полиномов троичных КПП и ГПП их корреляционные свойства отличаются от двоичного случая.

Целью статьи является определение в полях $GF(3^S)$ при $S = 4, 6, 8$ векторов индексов децимации $\mathbf{I}_S(i_{d1}, i_{d2}, \dots, i_{dn})$ для формирования малого и большого множеств КПП с низким уровнем взаимной корреляции.

По аналогии с двоичным случаем возможно формирование как малого, так и большого множества троичных КПП. Эти последовательности формируются путем сложения по $\text{mod}3$ базисной МП и одной (для малого множества) или двух (для большого множества) последовательностей, полученных на основе децимации базисной МП по индексам i_{di} , равным показателям степени корней α^i минимальных полиномов поля $GF(3^S)$. При формировании больших множеств троичных КПП используются полиномы, участвующие в образовании предпочтительных пар МП и соответственно троичных голд-подобных последовательностей.

При выполнении вычислений будем использовать подстрочные индексы „МК“ для характеристик малого множества троичных КПП, „БК“ — для большого множества КПП, „Г“ — для множества ГПП, „ПП“ — для предпочтительных пар МП. Например, в статье применяются следующие обозначения: $\mathbf{I}_{S,МК}(i_{d1}, i_{d2}, \dots, i_{dn})$ — для векторов индексов децимации малого множества троичных КПП, $\mathbf{I}_{S,БК}(i_{d1}, \dots, i_{dl})$ — для большого множества КПП, $\mathbf{I}_{S,Г}(i_{d1}, \dots, i_{dk})$ — для множества ГПП.

Символы c_i ($i = 0, \dots, N-1$) базисной МП с периодом $N = 3^S - 1$, представленной в каноническом виде, определяются выражением [2, 6]:

$$c_i = \text{tr}_{S1}(\alpha^i), \quad (1)$$

где $\text{tr}_{S1}(\alpha^i)$ — функция следа примитивного элемента α из расширенного поля $GF(3^S)$ в простом поле $GF(3)$.

Троичные последовательности малого множества КПП с периодом $N = 3^S - 1$ формируются в конечном поле $GF(3^S)$ на основании проверочного полинома $h_{МК}(x)$, являющегося произведением примитивного полинома степени S и неприводимого полинома степени $S/2$. При этом модуль максимального значения периодической взаимно корреляционной функции (ПВКФ) и объем малого множества КПП определяются выражениями [5, 6]:

$$|R_{\max}|_{МК} = 3^{S/2} + 1, \tag{2}$$

$$V_{МК} = 3^{S/2}. \tag{3}$$

Троичные КПП малого множества с периодом $N = 3^4 - 1 = 80$ формируются в конечном поле $GF(3^4)$ с полиномом $f(x) = x^4 + 2x^3 + 2$, в котором имеется восемь примитивных полиномов и два неприводимых полинома степени 2, период корней которых равен $N = 8$ (табл. 1).

Таблица 1

Неприводимые полиномы в поле $GF(3^4)$, $f(x) = x^4 + 2x^3 + 2$

α^i	Полиномы $h_i(x)$	Корни полиномов (показатели степени)	Периоды корней
α^1	$h_1(x) = x^4 + 2x^3 + 2$	$\alpha^1, \alpha^3, \alpha^9, \alpha^{27}$	80
α^7	$h_7(x) = x^4 + x^3 + x^2 + 2x + 2$	$\alpha^7, \alpha^{21}, \alpha^{63}, \alpha^{29}$	80
α^{11}	$h_{11}(x) = x^4 + 2x^3 + 2x^2 + x + 2$	$\alpha^{11}, \alpha^{33}, \alpha^{19}, \alpha^{57}$	80
α^{13}	$h_{13}(x) = x^4 + 2x + 2$	13, 39, 37, 31	80
α^{17}	$h_{17}(x) = x^4 + x^3 + 2x^2 + 2x + 2$	17, 51, 73, 59	80
α^{23}	$h_{23}(x) = x^4 + 2x^3 + x^2 + x + 2$	23, 69, 47, 61	80
α^{41}	$h_{41}(x) = x^4 + x^3 + 2$	41, 43, 49, 67	80
α^{53}	$h_{53}(x) = x^4 + x + 2$	53, 79, 77, 71	80
α^{10}	$h_{10}(x) = x^2 + 2x + 2$	10, 30	8
α^{50}	$h_{50}(x) = x^2 + x + 2$	50, 70	8

Нижние индексы в полиномах $h_i(x)$ здесь и в дальнейшем соответствуют минимальным показателям степени корней данных полиномов и равны индексам децимации i_{di} базисной МП с $h_{МП}(x) = h_1(x)$ при формировании других МП или ПСП с проверочными полиномами $h_i(x)$.

Анализ ПВКФ МП с проверочным полиномом $h_1(x)$ (период $N = 80$) и МП с полиномами $h_{10}(x)$ и $h_{50}(x)$ (период $N = 8$) показал, что взаимно корреляционная функция $R(\tau)$ является двухуровневой и принимает следующие значения: $R(\tau) = [-10; 3, 5]$.

Для полинома $h_1(x)$ малые множества КПП с периодом $N = 3^4 - 1 = 80$ формируются на основании следующих проверочных полиномов:

$$h_{МК1}(x) = h_1(x)h_{10}(x) = (x^4 + 2x^3 + 2)(x^2 + 2x + 2);$$

$$h_{МК2}(x) = h_1(x)h_{50}(x) = (x^4 + 2x^3 + 2)(x^2 + x + 2).$$

Анализ корреляционных свойств показал, что ПВКФ последовательностей малого множества КПП $R_{S,МК}$ с $h_{МК}(x)$ и периодом $N = 80$ является трехуровневой и принимает следующие значения: $R_{S,МК}(\tau) = R_{4,МК}(\tau) = [-10; -1; 3, 5]$.

В общем виде ПВКФ троичных КПП малого множества в полях $GF(3^S)$ определяется выражением

$$R_{S,МК}(\tau) = [(-3^{S/2} - 1); -1; (0, 5 \times 3^{S/2} - 1)]. \tag{4}$$

Таким образом, при $S = 4$ вектор индексов децимации для формирования малых множеств троичных КПП имеет вид

$$\mathbf{I}_{S,МК}(i_{d1}, i_{d2}) = \mathbf{I}_{4,МК}(10, 50). \tag{5}$$

В поле $GF(3^4)$ имеется восемь примитивных полиномов, поэтому всего можно сформировать $M_{S,МК} = M_{4,МК} = 16$ малых множеств троичных КПП с периодом $N = 80$, максимальным значением $|R_{\max}|_{МК} = 3^{S/2} + 1 = 10$ и объемом $V_{4,МК} = 3^{S/2} = 9$.

Троичные последовательности большого множества КПП с периодом $N=3^S - 1$ (S — четное) формируются в конечном поле $GF(3^S)$ на основании проверочного полинома $h_{BK}(x)$, являющегося произведением двух примитивных полиномов степени S , образующих предпочтительную пару (ПП) МП, и неприводимого полинома степени $S/2$, определяемого на основании проверочного полинома малого множества КПП. При $S = 4$ модуль максимального значения ПВКФ и объем большого множества КПП определяются аналогично двоичному случаю [5, 6]:

$$|R_{\max}|_{BK} = 2 \times 3^{S/2} - 1 = 17,$$

$$V_{4,BK} = 3^{S/2}(3^S + 1) - 1 = 737.$$

Последовательности большого множества с периодом $N = 3^4 - 1 = 80$ также формируются в конечном поле $GF(3^4)$ с полиномом $f(x) = x^4 + 2x^3 + 2$. Для формирования больших множеств троичных КПП сначала необходимо определить ПП МП.

Анализ результатов вычисления ПВКФ МП с периодом $N = 80$ показал, что для базисной МП с $h_1(x)$ можно выделить две предпочтительные пары МП, ПВКФ которых принимает четыре значения в интервале от -10 до $+17$, на основании этих пар формируются множества троичных ГПП с аналогичной функцией корреляции

$$R_{4,ПП}(\tau) = R_{4,Г}(\tau) = [-10; -1; 8; 17]. \quad (6)$$

Это пары МП с полиномами: $h_1(x)$ и $h_{11}(x)$; $h_1(x)$ и $h_{17}(x)$. Тогда при $S = 4$ вектор индексов децимации для формирования множеств троичных ГПП определяется выражением

$$\mathbf{I}_{S,Г}(i_{d1}, i_{d2}) = \mathbf{I}_{4,Г}(11, 17). \quad (7)$$

Для произвольного примитивного полинома $h_i(x)$ полиномы, с помощью которых формируются ПП, образуются путем умножения индексов полиномов на 11 или 17 по mod80. При этом выбираются минимальные индексы, соответствующие показателям степени корней данных полиномов.

Например, МП с $h_{41}(x)$ образует ПП с МП с $h_{41 \times 11 \bmod 80}(x) = h_{51}(x) = h_{17}(x)$ и с МП с $h_{41 \times 17 \bmod 80}(x) = h_{57}(x) = h_{11}(x)$. А МП с $h_{23}(x)$ образует ПП с МП при $h_{23 \times 11 \bmod 80}(x) = h_{13}(x)$ и с МП при $h_{23 \times 17 \bmod 80}(x) = h_{71}(x) = h_{53}(x)$. Всего можно получить $M_{4,ПП} = 8$ предпочтительных пар МП.

На рис. 1 показана ПВКФ $R_{4,ПП}(\tau)$ ПП МП с $h_1(x)$ и $h_{11}(x)$, причем МП формируется в каноническом виде в соответствии с (1).

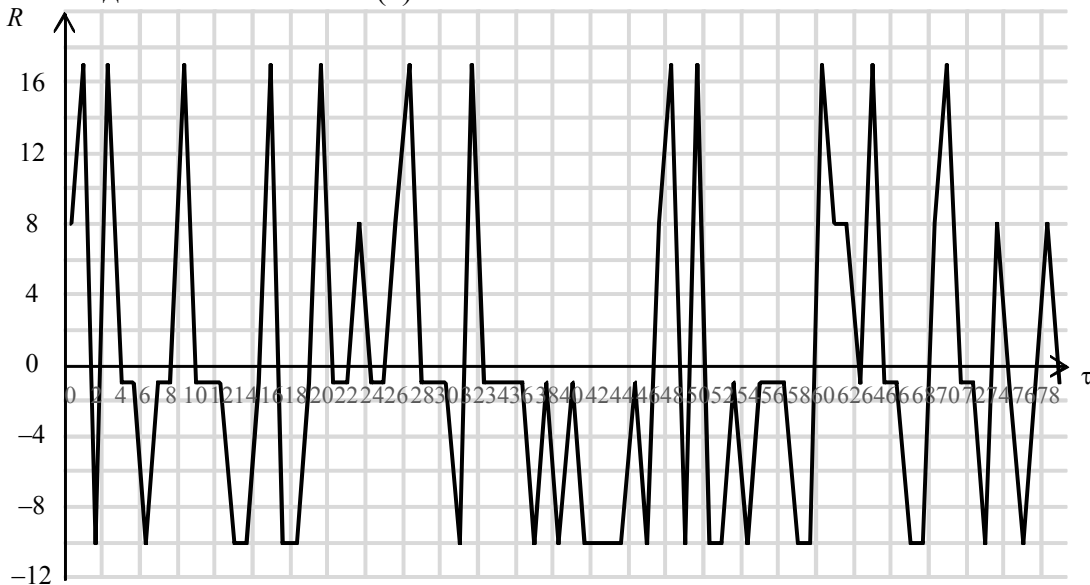


Рис. 1

Для полинома $h_1(x)$ множества ГПП с периодом $N = 3^4 - 1 = 80$ и объемом $V_{4,\Gamma} = 3^4 + 1 = 82$ формируются на основании следующих проверочных полиномов:

$$h_{\Gamma 1}(x) = h_1(x)h_{11}(x) = (x^4 + 2x^3 + 2)(x^4 + 2x^3 + 2x^2 + x + 2);$$

$$h_{\Gamma 2}(x) = h_1(x)h_{17}(x) = (x^4 + 2x^3 + 2)(x^4 + x^3 + 2x^2 + 2x + 2).$$

Тогда для восьми примитивных полиномов поля $GF(3^4)$ число множеств троичных ГПП $M_{4,\Gamma} = 8$.

Выражение для ПВКФ ПП троичных МП и последовательностей множества ГПП в общем виде при $S = 0 \pmod{2}$ определяется выражением

$$R_{S,\text{ПП}}(\tau) = R_{S,\Gamma}(\tau) = [(-3^{S/2} - 1); -1; (3^{S/2} - 1); (2 \times 3^{S/2} - 1)]. \quad (8)$$

На рис. 2 показана ПВКФ $R_{4,\Gamma}(\tau)$ двух последовательностей из множества ГПП с $h_{\Gamma 3}(x) = h_{23}(x)h_{53}(x)$, удовлетворяющая (6) и (8).

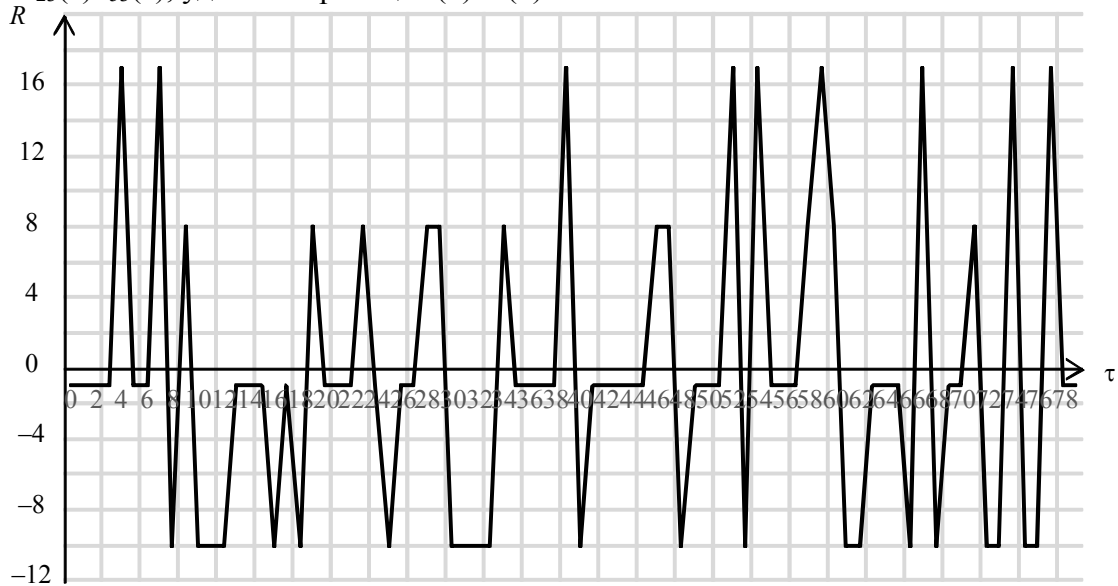


Рис. 2

С учетом предпочтительных пар МП и проверочных полиномов для последовательностей малого множества были получены проверочные полиномы последовательностей большого множества КПП для полинома $h_1(x)$:

$$h_{\text{БК1}}(x) = h_1(x)h_{10}(x)h_{11}(x) = (x^4 + 2x^3 + 2)(x^2 + 2x + 2)(x^4 + 2x^3 + 2x^2 + x + 2);$$

$$h_{\text{БК2}}(x) = h_1(x)h_{10}(x)h_{17}(x) = (x^4 + 2x^3 + 2)(x^2 + 2x + 2)(x^4 + x^3 + 2x^2 + 2x + 2);$$

$$h_{\text{БК3}}(x) = h_1(x)h_{50}(x)h_{11}(x) = (x^4 + 2x^3 + 2)(x^2 + x + 2)(x^4 + 2x^3 + 2x^2 + x + 2);$$

$$h_{\text{БК4}}(x) = h_1(x)h_{50}(x)h_{17}(x) = (x^4 + 2x^3 + 2)(x^2 + x + 2)(x^4 + x^3 + 2x^2 + 2x + 2). \quad (9)$$

Так как проверочный полином при формировании большого множества КПП содержит три множителя, включая $h_1(x)$, вектор индексов децимации становится двумерным и определяется выражением

$$\mathbf{I}_{S,\text{БК}}[i_{d1}, \dots, i_{dn}] = \mathbf{I}_{4,\text{БК}}[(10, 11), (10, 17), (50, 11), (50, 17)]. \quad (10)$$

Для произвольного примитивного полинома $h_i(x)$ проверочные полиномы большого множества КПП образуются путем умножения индексов полиномов из (9) на значение i по $\pmod{80}$. При этом выбираются минимальные индексы, соответствующие показателям степени корней данных полиномов.

Например, для примитивного полинома $h_{13}(x)$ выражения (9) преобразуются к виду

$$h_{\text{БК5}}(x) = h_{13}(x)h_{10 \times 13 \pmod{80}}(x)h_{11 \times 13 \pmod{80}}(x) = h_{13}(x)h_{50}(x)h_7(x);$$

$$h_{\text{БК6}}(x) = h_{13}(x)h_{10 \times 13 \pmod{80}}(x)h_{17 \times 13 \pmod{80}}(x) = h_{13}(x)h_{50}(x)h_{23}(x);$$

$$h_{\text{БК7}}(x) = h_{13}(x)h_{50 \times 13 \pmod{80}}(x)h_{11 \times 13 \pmod{80}}(x) = h_{13}(x)h_{10}(x)h_7(x);$$

$$h_{\text{БК8}}(x) = h_{13}(x)h_{50 \times 13 \pmod{80}}(x)h_{17 \times 13 \pmod{80}}(x) = h_{13}(x)h_{10}(x)h_{23}(x).$$

Всего можно сформировать $M_{4,БК} = 16$ больших множеств троичных КПП. Каждое большое множество составляет $V_{4,БК} = 737$ последовательностей.

Анализ корреляционных свойств большого множества троичных КПП показал, что ПВКФ в общем случае является восьмиуровневой:

$$R_{4,БК}(\tau) = [-14,5; -10; -5,5; -1; 3,5; 8; 12,5; 17].$$

Представим в общем виде выражение для ПВКФ большого множества троичных КПП

$$R_{4,БК}(\tau) = [(-1,5 \times 3^{S/2} - 1); (-3^{S/2} - 1); (-0,5 \times 3^{S/2} - 1); -1; (0,5 \times 3^{S/2} - 1); (3^{S/2} - 1); (1,5 \times 3^{S/2} - 1); (2 \times 3^{S/2} - 1)]. \quad (11)$$

На рис. 3 показана ПВКФ $R_{4,БК}(\tau)$ двух последовательностей из большого множества КПП с $h_{БК7}(x) = h_{13}(x)h_{10}(x)h_7(x)$.

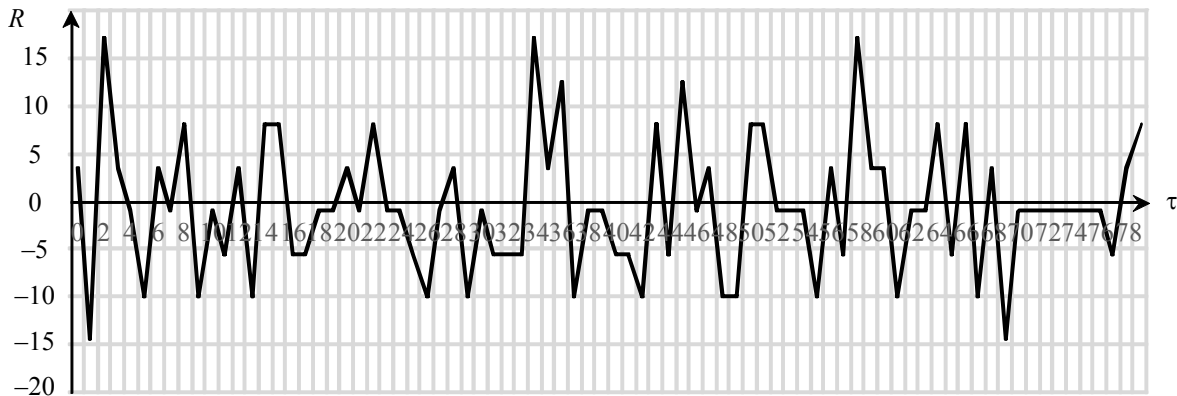


Рис. 3

Рассмотрим формирование множеств троичных ГПП и КПП с периодом $N = 3^6 - 1 = 728$. Троичные ГПП и КПП с периодом $N = 3^6 - 1 = 728$ формируются в конечном поле $GF(3^6)$ с полиномом $f(x) = x^6 + x + 2$, в котором имеется сорок восемь примитивных полиномов с индексами децимации 1, 5, 11, 17, 19, 23, 25, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 95, 97, 101, 103, 107, 113, 115, 121, 125, 131, 149, 151, 155, 157, 185, 187, 197, 205, 211, 215, 229, 233, 239, 241, 365, 395, 401, 485 базисной МП с $h_1(x)$ и четыре неприводимых полинома с периодом $N = 26$ и индексами децимации 28, 140, 196, 476.

Анализ корреляционных свойств МП с проверочным полиномом $h_1(x)$ (период $N = 728$) и МП с полиномами $h_{28}(x)$, $h_{140}(x)$, $h_{196}(x)$ и $h_{476}(x)$ (период $N = 26$) показал, что все ПВКФ отличаются друг от друга. Можно выделить четыре типа функции корреляции

$$R_{1-28}(\tau) = [-28(224); 12,5(504)];$$

$$R_{1-140}(\tau) = [-14,5(336); -1(168); 12,5(168); 53(56)];$$

$$R_{1-196}(\tau) = [-28(168); -1(336); 12,5(56); 26(168)];$$

$$R_{1-476}(\tau) = [-28(56); -14,5(336); 12,5(168); 26(168)],$$

три из которых удовлетворяют граничным оценкам (2).

При этом вектор индексов децимации при формировании малого множества КПП имеет вид

$$\mathbf{I}_{S,МК}(i_{d1}, i_{d2}, i_{d3}) = \mathbf{I}_{6,МК}(28, 196, 476). \quad (12)$$

Соответственно можно сформировать три типа малых множеств КПП с проверочными полиномами

$$h_{МК1}(x) = h_1(x)h_{28}(x) = (x^6+x+2)(x^3+2x^2+1);$$

$$h_{МК2}(x) = h_1(x)h_{196}(x) = (x^6+x+2)(x^3+2x^2+x+1);$$

$$h_{\text{МКЗ}}(x) = h_1(x)h_{476}(x) = (x^6+x+2)(x^3+2x+1).$$

Взаимно корреляционная функция данных множеств является трех-, четырех- и пяти-уровневой и определяется выражениями

$$R_{6,\text{МК1}}(\tau) = [-28; -1; 12,5];$$

$$R_{6,\text{МК2}}(\tau) = [-28; -1; 12,5; 26];$$

$$R_{6,\text{МК3}}(\tau) = [-28; -14,5; -1; 12,5; 26].$$

Всего можно сформировать по $M_{6,\text{МК}} = 48$ малых множеств КПП каждого типа с $V_{6,\text{МК}} = 27$. На рис. 4 показан сегмент длиной в сто символов ПВКФ $R_{6,\text{МК1}}(\tau)$ последовательностей малого множества КПП 1-го типа, $h_{\text{МК1}}(x) = h_1(x)h_{28}(x)$.

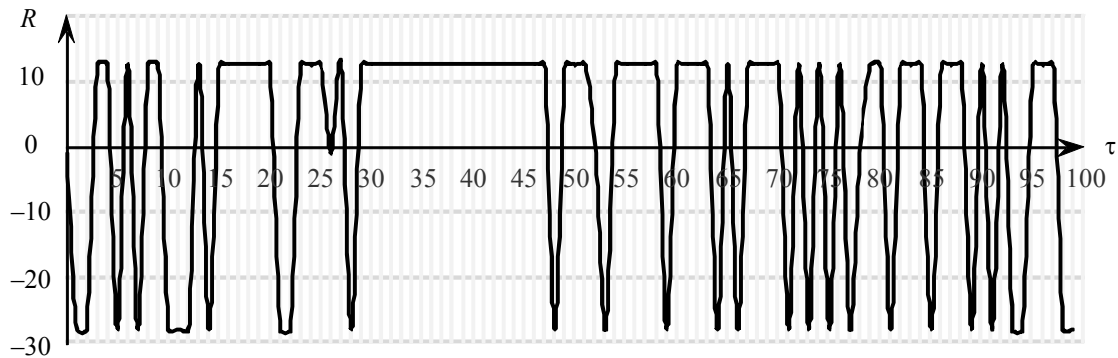


Рис. 4

Для формирования большого множества КПП с периодом $N = 728$ в конечном поле $\text{GF}(3^6)$ сначала определим ПП МП. Анализ корреляционных свойств всевозможных пар МП показал, что для полинома $h_1(x)$ существует всего два примитивных полинома $h_{29}(x)$ и $h_{53}(x)$, на основании которых можно построить две ПП МП и ГПП с четырехуровневой ПВКФ, удовлетворяющей (8):

$$R_{4,\text{ПП}}(\tau) = R_{4,\text{Г}}(\tau) = [-28; -1; 26; 53].$$

Вектор индексов децимации при формировании множеств троичных ГПП определяется выражением

$$\mathbf{I}_{S,\text{Г}}(i_{d1}, i_{d2}) = \mathbf{I}_{6,\text{Г}}(29, 53). \quad (13)$$

На основании ПП МП и малых множеств КПП для полинома $h_1(x)$ можно сформировать проверочные полиномы большого множества КПП. Анализ корреляционных свойств последовательностей показал, что ПВКФ больших множеств КПП является десятиуровневой с модулем максимального значения корреляционной функции $|R_{\text{max}}|_{\text{БК}} = 3^{S/2+1} - 1 = 80$.

Проверочные полиномы больших множеств КПП определяются выражениями

$$h_{\text{БК1}}(x) = h_1(x)h_{28}(x)h_{29}(x);$$

$$h_{\text{БК2}}(x) = h_1(x)h_{28}(x)h_{53}(x);$$

$$h_{\text{БК3}}(x) = h_1(x)h_{196}(x)h_{29}(x);$$

$$h_{\text{БК4}}(x) = h_1(x)h_{196}(x)h_{53}(x).$$

Вектор индексов децимации при формировании больших множеств КПП имеет вид

$$\mathbf{I}_{S,\text{БК}}[i_{d1}, \dots, i_{dn}] = \mathbf{I}_{6,\text{БК}}[(28, 29), (28, 53), (196, 29), (196, 53)]. \quad (14)$$

Последовательностям данного множества соответствует десятиуровневая ПВКФ

$$R_{6,\text{БК}}(\tau) = [-41,5; -28; -14,5; -1; 12,5; 26; 39,5; 53; 66,5; 80].$$

Всего можно сформировать $M_{6,БК} = 98$ больших множеств КПП с $V_{6,БК} = 19\ 655$. На рис. 5 показан сегмент длиной в сто символов ПВКФ $R_{6,БК}(\tau)$ последовательностей большого множества КПП с периодом $N = 728$, $h_{БК1}(x) = h_1(x)h_{28}(x)h_{29}(x)$.

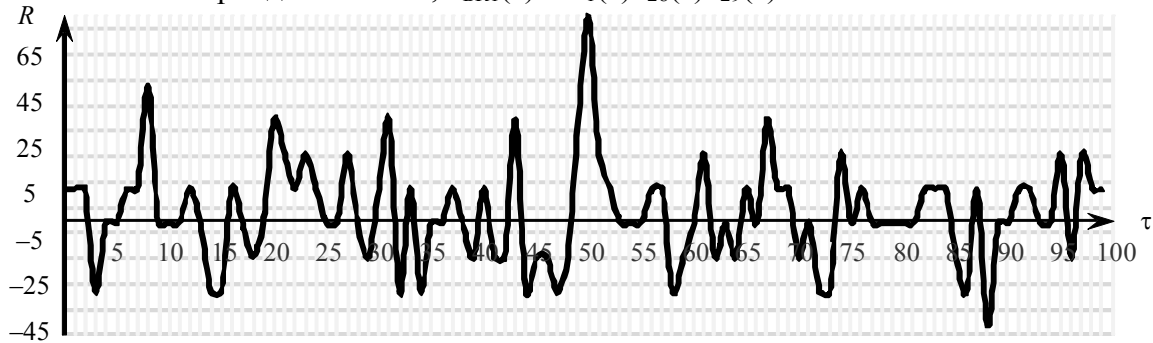


Рис. 5

В общем виде ПВКФ большого множества троичных КПП с периодом $N = 728$ определяется выражением

$$R_{6,БК}(\tau) = [(-1,5 \times 3^{S/2} - 1); (-3^{S/2} - 1); (-0,5 \times 3^{S/2} - 1); -1; (0,5 \times 3^{S/2} - 1); (3^{S/2} - 1); (1,5 \times 3^{S/2} - 1); (2 \times 3^{S/2} - 1); (2,5 \times 3^{S/2} - 1); (3 \times 3^{S/2} - 1)]. \quad (15)$$

Троичные ГПП и КПП с периодом $N = 3^8 - 1 = 6560$ формируются в конечном поле $GF(3^8)$ с полиномом $f(x) = x^8 + 2x^3 + 2$, в котором имеется триста двадцать примитивных полиномов с индексами децимации 1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 43, 47, 49, 53, 59, 61, 67, 71, ..., 3317, 3371, 3389, 3401, 3533, 3563, 3617, 3641, 4103, 4121, 4373 базисной МП с $h_1(x)$ и восемь неприводимых полиномов с периодом $N = 80$ и индексами децимации 82, 574, 902, 1066, 1394, 1886, 3362, 4346.

Анализ ПВКФ МП с периодом $N = 6560$ и ПСП с периодом $N = 80$ показал, что можно сформировать два малых множества КПП в соответствии с вектором индексов децимации

$$\mathbf{I}_{S,МК}(i_{d1}, i_{d2}) = \mathbf{I}_{8,МК}(82, 3362). \quad (16)$$

Корреляционная функция малых множеств КПП является трехуровневой и удовлетворяет (4):

$$R_{8,МК}(\tau) = [-82; -1; 39,5].$$

Множества ГПП с периодом $N = 6560$ образуются на основании ПП МП. Вектор индексов децимации содержит всего два из трехсот двадцати возможных индексов децимации

$$\mathbf{I}_{S,Г}(i_{d1}, i_{d2}) = \mathbf{I}_{8,Г}(83, 161).$$

Периодическая взаимно корреляционная функция множества троичных ГПП является четырехуровневой и удовлетворяет (8):

$$R_{8,Г}(\tau) = [-82; -1; 80; 161].$$

Большие множества КПП формируются на основании векторов индексов децимации $\mathbf{I}_{8,МК}(82, 3362)$ и $\mathbf{I}_{8,Г}(83, 161)$.

Проверочные полиномы больших множеств КПП задаются выражениями

$$h_{БК1}(x) = h_1(x)h_{82}(x)h_{83}(x);$$

$$h_{БК2}(x) = h_1(x)h_{82}(x)h_{161}(x);$$

$$h_{БК3}(x) = h_1(x)h_{3362}(x)h_{83}(x);$$

$$h_{БК4}(x) = h_1(x)h_{3362}(x)h_{161}(x).$$

Вектор индексов децимации при формировании больших множеств КПП имеет вид

$$\mathbf{I}_{S,БК}[i_{d1}, \dots, i_{dn}] = \mathbf{I}_{8,БК}[(82, 83), (82, 161), (3362, 83), (3362, 161)]. \quad (17)$$

Последовательностям данного множества соответствует десятиуровневая ПВКФ, которая удовлетворяет (15):

$$R_{8, \text{БК}}(\tau) = [-122,5; -82; -41,5; -1; 39,5; 80; 120,5; 161; 201,5; 242].$$

Таким образом, для каждого примитивного полинома можно синтезировать по четыре больших множества КПП с десятиуровневой ПВКФ.

Основные корреляционные и структурные характеристики больших и малых множеств КПП, а также множеств ГПП, формируемых в конечных полях $\text{GF}(3^S)$, для четных значений параметра S приведены в табл. 2—4.

Таблица 2

Характеристики малых множеств троичных КПП

S	N	$\mathbf{I}_{S, \text{МК}}[i_{d1}, i_{dn}]$	Значения ПВКФ	$ R_{\text{max}} $	Число уровней ПВКФ	$V_{S, \text{МК}}$	$M_{S, \text{МК}}$
4	80	10, 50	-10; -1; 3,5	10	3	9	16
6	728	28	-28; -1; 12,5	28	3	27	48
6	728	196	-28; -1; 12,5; 26	28	4	27	48
6	728	476	-28; -14,5; -1; 12,5; 26	28	5	27	48
8	6560	82, 3362	-82; -1; 39,5	82	3	81	640

Таблица 3

Характеристики множеств троичных ГПП

S	N	$\mathbf{I}_{S, \Gamma}[i_{d1}, i_{d2}]$	Значения ПВКФ	$ R_{\text{max}} $	Число уровней ПВКФ	$V_{S, \Gamma}$	$M_{S, \Gamma}$
4	80	10, 50	-10; -1; 8; 17	17	4	82	8
6	728	29, 53	-28; -1; 26; 53	53	4	730	48
8	6560	83, 161	-82; -1; 80; 161	161	4	6562	320

Таблица 4

Характеристики больших множеств троичных КПП

S	N	$\mathbf{I}_{S, \text{БК}}[i_{d1}, \dots, i_{dn}]$	Значения ПВКФ	$ R_{\text{max}} $	Число уровней ПВКФ	$V_{S, \text{БК}}$	$M_{S, \text{БК}}$
4	80	(10, 11), (10, 17), (50, 11), (50, 17)	-14,5; -10; -5,5; -1; 3,5; 8; 12,5; 17	17	8	737	16
6	728	(28, 29), (28, 53), (196, 29), (196, 53)	-41,5; -28; -14,5; -1; 12,5; 26; 39,5; 53; 66,5; 80	80	10	19656	96
8	6560	(82, 83), (82, 161), (3362, 83), (3362, 161)	-122,5; -82; -41,5; -1; 39,5; 80; 120,5; 161; 201,5; 242	242	10	524959	640

Таким образом, в статье получены полные наборы векторов индексов децимации $\mathbf{I}_S(i_{d1}, \dots, i_{dn})$ для формирования малого и большого множеств троичных КПП, а также множеств троичных ГПП в полях $\text{GF}(3^S)$ при $S = 4, 6, 8$. Определены основные характеристики данных множеств: значения и число уровней ПВКФ, максимальные значения модуля взаимной корреляционной функции $|R_{\text{max}}|$, а также объемы множеств и число множеств с эквивалентными корреляционными свойствами.

Полученные результаты могут быть использованы при организации кодового много-станционного доступа в СПЦИ с большим числом абонентов на основе троичных фазоманипулированных сигналов с расширенным спектром.

СПИСОК ЛИТЕРАТУРЫ

1. Вишневецкий В. М., Ляхов А. И., Портной С. Л., Шахнович И. В. Широкополосные беспроводные сети передачи информации. М.: Техносфера, 2005. 592 с.
2. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. М.: Вильямс, 2003. 1104 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: Cambridge Univ. Press, 2005.
7. 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.
8. 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.
9. 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.
10. Dobbertin H., Hellesteth T., Kumar P. V., Martinsen H. Ternary M-sequences with three-valued cross-correlation function: New decimations of Welch and Niho type // IEEE Trans. Inf. Theory. 2001. Vol. 47, N 4. P. 1473.
11. Hellesteth 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.
12. Hu Z., Li X., Mills D., Muller E., Sun W., Williams W., Yang Y., Zhang Z. On the cross-correlation of sequences with the decimation factor $d=(p^n+1)/(p+1)-(p^n-1)/2$ // Applicable Algebra Eng. Commun. Comput. 2001. Vol. 12. P. 255.
13. Seo E. Y., Kim Y. S., No J. S., Shin D. J. Cross-correlation distribution of p-ary m-sequence of period $p^{4k} - 1$ and its decimated sequences by $((p^{2k}+1)/2)$ // IEEE Trans. Inf. Theory. 2008. Vol. 54, N 7. P. 3140.
14. Jang J. W., Kim Y. S., No J. S., Hellesteth 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. Liang H., Tang Y. The cross correlation distribution of a p-ary m-sequence of period $p^m - 1$ and its decimated sequences by $(p^k+1)(p^m+1)/4$ // Finite Fields and Their Applications. 2015. Vol. 31. P. 137.
16. Lee W. J., Kim J. Y., No J. S. New families of p-ary sequence of period $(p^n - 1)/2$ with low maximum correlation magnitude // IEICE Transactions on Communications. 2014. Vol. E97-B, N 1. P. 2311.
17. Muller E. N. On the cross-correlation of sequences over GF(p) with short periods // IEEE Trans. Inf. Theory. 1999. Vol. 45, N 1. P. 289.
18. Song M. K., Song H. Y. A construction of odd length generators for optimal families of perfect sequences // IEEE Trans. Inf. Theory. 2018. Vol. 64, N 4. P. 2901.
19. Gold R. Maximal recursive sequences with 3-valued recursive cross-correlation functions // IEEE Trans. Inf. Theory. 1968. Vol. 14, N 1. P. 154.

Сведения об авторах

- Виктор Геннадьевич Стародубцев** — канд. техн. наук, доцент; ВКА им. А. Ф. Можайского, кафедра технологий и средств автоматизации обработки и анализа информации космических средств; E-mail: vgstarod@mail.ru
- Евгений Александрович Четвериков** — ВКА им. А. Ф. Можайского, кафедра технологий и средств автоматизации обработки и анализа информации космических средств; слушатель; E-mail: vka@mil.ru

Поступила в редакцию 19.05.23; одобрена после рецензирования 25.05.23; принята к публикации 28.08.23.

REFERENCES

1. Vishnevskij V.M., Lyahov A.I., Portnoj S.L., Shahnovich I.V. *Shirokopolosnye besprovodnye seti peredachi informacii* (Broadband Wireless Data Transmission Network), Moscow, 2005, 592 p. (in Russ.)
2. Sklar B. *Digital Communications: Fundamentals and Applications*, Prentice Hall, 2001, 1079 p.
3. Ipatov V.P. *Spread Spectrum and CDMA. Principles and Applications*, NY, John Wiley and Sons Ltd., 2005, 488 p.
4. Varakin L.E. and Shinakov Yu.S., ed., *CDMA: proshloe, nastoyashchee, budushchee* (CDMA: Past, Present, Future), Moscow, 2003, 608 p. (in Russ.)
5. Ipatov V.P. *Periodicheskie diskretnye signaly s optimal'nymi korrelyacionnymi svoystvami* (Periodic Discrete Signals with Optimum Correlation Properties), Moscow, 1992, 152 p. (In Russ.).

6. Golomb S.W., Gong G. *Signal Design for Good Correlation for Wireless Communication, Cryptography and Radar*, Cambridge, Cambridge Univ. Press, 2005.
7. Boztaş S., Özbudak F., Tekin E. *Cryptogr. Commun.*, 2018, no. 3(10), pp. 509.
8. Cho Chang-Min, Kim Ji-Youp, No J.S. *IEICE Transactions on Communications*, 2015, no. 7(E98), pp. 1268.
9. Choi S.T., Lim T., No J.S., Chung H. *IEEE Trans. Inf. Theory.*, 2012, no. 3(58), pp. 1873.
10. Dobbertin H., Hellesteth T., Kumar P.V., Martinsen H. *IEEE Trans. Inf. Theory*, 2001, no. 4(47), pp. 1473.
11. Hellesteth T., Kumar P.V., Martinsen H. *Designs, Codes and Cryptography*, 2001, no. 2(23), pp. 157.
12. Hu Z., Li X., Mills D., Muller E., Sun W., Williams W., Yang Y., Zhang Z. *Applicable Algebra Eng. Commun. Comput.*, 2001, vol. 12, pp. 255.
13. Seo E.Y., Kim Y.S., No J.S., Shin D.J. *IEEE Trans. Inf. Theory*, 2008, no. 7(54), pp. 3140.
14. Jang J.W., Kim Y.S., No J.S., Hellesteth T. *IEEE Trans. Inf. Theory*, 2004, no. 8(50), pp. 1839.
15. Liang H., Tang Y. *Finite Fields and Their Applications*, 2015, vol. 31, pp. 137.
16. Lee W.J., Kim J.Y., No J.S. *IEICE Transactions on Communications*, 2014, no. 1(E97-B), pp. 2311.
17. Muller E.N. *IEEE Trans. Inf. Theory*, 1999, no. 1(45), pp. 289.
18. Song M.K., Song H.Y. *IEEE Trans. Inf. Theory*, 2018, no. 4(64), pp. 2901.
19. Gold R. *IEEE Trans. Inf. Theory*, 1968, no. 1(14), pp. 154.

Data on authors

- Victor G. Starodubtsev** — PhD, Associate Professor; A. F. Mozhaisky Military Space Academy, Department of Technologies and means for Automating the Processing and Analysis of Spacecraft Information; E-mail: vgstarod@mail.ru
- Evgeny A. Chetverikov** — A. F. Mozhaisky Military Space Academy, Department of Technologies and Means for Automating the Processing and Analysis of Spacecraft Information; Student; E-mail: vka@mail.ru

Received 19.05.23; approved after reviewing 25.05.23; accepted for publication 28.08.23.