УДК 519.725
DOI: 10.17586/0021-3454-2025-68-5-380-387

# ЛИНЕЙНАЯ СЛОЖНОСТЬ НЕДВОИЧНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ГОРДОНА — МИЛЛСА — ВЕЛЧА В ПРОИЗВОЛЬНЫХ КОНЕЧНЫХ ПОЛЯХ

**В. Г. Стародубцев*, Е. Б. Самойлов**

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

**Аннотация.** Представлены соотношения для определения эквивалентной линейной сложности (ЭЛС) $l_S$ недвоичных последовательностей Гордона — Миллса — Велча (ГМВП), формируемых в произвольных расширенных конечных полях GF[$(p^m)^n$]. Получены значения ЭЛС ГМВП для полей с основанием $p$ = 3–17 с учетом параметра $M_n(r_p)$, равного числу суммируемых последовательностей при формировании ГМВП. Показано, что параметр $M_n(r_p)$ зависит исключительно от степени $n$ расширения поля и значений разрядов $p$-ичного представления числа $r_p$, взаимно простого с порядком мультипликативной группы подполя GF($p^m$).

***Ключевые слова:*** *конечные поля, эквивалентная линейная сложность, М- последовательности, ГМВ-последовательности*

**Ссылка для цитирования:** *Стародубцев В. Г., Самойлов Е. Б.* Линейная сложность недвоичных последовательностей Гордона — Миллса — Велча в произвольных конечных полях // Изв. вузов. Приборостроение. 2025. Т. 68, № 5. С. 380–387. DOI: 10.17586/0021-3454-2025-68-5-380-387.

## LINEAR COMPLEXITY OF NON-BINARY GORDON – MILLS – WELCH SEQUENCES IN ARBITRARY FINITE FIELDS

**V. G. Starodubtsev*, E. B. Samoylov**

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

**The relat**ions for determining the equivalent linear complexity (ELC) $l_S$ of non-binary Gordon — Mills — Welch sequences (GMWS) formed in arbitrary extended finite fields GF[$(p^m)^n$] are presented. The values of the ELC of the GMWS for fields with a base $p$ = 3 -17 are obtained, taking into account the parameter $M_n(r_p)$ equal to the number of summable sequences during the formation of the GMWS. It is shown that the parameter $M_n(r_p)$ depends exclusively on the degree $n$ of the field expansion and the values of the digits of the $p$-ary representation of the number $r_p$, which is mutually simple with the order of the multiplicative group of the subfield GF($p^m$).

**Keywords:** finite fields, equivalent linear complexity, M-sequences, Gordon — Mills — Welch sequences

**For citation:** Starodubtsev V. G., Samoylov E. B. Linear complexity of non-binary Gordon – Mills – Welch sequences in arbitrary finite fields. *Journal of Instrument Engineering*. 2025. Vol. 68, N 5. P. 380–387 (in Russian). DOI: 10.17586/0021-3454-2025-68-5-380-387.

Одним из ключевых направлений в развитии цифровых систем радиопередачи является использование многопозиционных фазоманипулированных сигналов с расширенным спектром, формируемых на основе недвоичных псевдослучайных последовательностей (ПСП) [1–4]. В помехоустойчивых системах приоритет отдается сигналам с оптимальными корреляционными свойствами и высокой степенью структурной скрытности [5–9]. Типичным примером ПСП, одновременно удовлетворяющим предъявляемым требованиям, являются недвоичные последовательности Гордона — Миллса — Велча (ГМВП), которые представляют собой минимаксные последовательности с двухуровневой периодической корреляционной функцией. Эти последовательности характеризуются высокой степенью структурной скрытности, что определяется их эквивалентной линейной сложностью $l_S$ [10–14].

Недвоичные последовательности ГМВП создаются на основе конечных полей $\mathrm{GF}[(p^m)^n] = \mathrm{GF}(p^S)$ ($S = mn$). Символы $d_i$ недвоичных последовательностей определяются как [2, 10, 14]

$$d_i = \mathrm{tr}_{m1}[\mathrm{tr}_{mn,m}(\alpha^i))^r], \; 1 \le r_p < p^m - 1, \; \mathrm{НОД}(r_p, p^m - 1) = 1, \tag{1}$$

где $\mathrm{tr}_{a,b}(\cdot)$ — след элемента, принадлежащего полю $\mathrm{GF}(p^a)$, в поле $\mathrm{GF}(p^b)$; $\alpha \in \mathrm{GF}[(p^m)^n]$ — примитивный элемент; НОД ($a$, $b$) — наибольший общий делитель чисел $a$ и $b$; $r_p$ — $p$-ичное число.

Для двоичных ГМВП получено выражение для ЭЛС [10, 12, 13]

$$l_S = mn^{z(r_2)}, \tag{2}$$

где $z(r_2)$ — количество единиц в двоичном представлении числа $r_p = r_2$ в (1).

При проведении анализа структурной скрытности ГМВП выражение (2) представим в виде

$$l_S = mn^z M_n(r_p), \tag{3}$$

где $M_n(r_p)$ — число суммируемых последовательностей при формировании ГМВП.

Данное выражение может быть использовано как для двоичных, так и недвоичных последовательностей. Для двоичных ГМВП параметр $M_n(r_2)$ определяется как

$$M_n(r_2) = n^{z(r_2)-1}. \tag{4}$$

Соотношения (2)–(4) позволяют определить структурную скрытность двоичных ГМВП при всех допустимых значениях параметров $m$, $n$ и $r$.

Суммируемые последовательности образуются на основе примитивных или неприводимых полиномов степени $S = mn$. Таким образом, для заданного конечного поля $\mathrm{GF}[(p^m)^n]$ задача определения линейной сложности недвоичных ГМВП сводится к вычислению параметра $M_n(r_p)$.

Формула (3) применима для определения ЭЛС недвоичных ГМВП при условии вычисления $M_n(r_p)$ для допустимых значений $p \ge 3$ и степени расширения поля $n \ge 2$.

Для $n = 2$ выражение для параметра $M_n(r_p)$ получено в [15]:

$$M_2(r_p) = 0{,}5\prod_{i=1}^{p-1}(i+1)^{t_i}, \tag{5}$$

где $t_i$ — кратность разрядов (равных $i$) в $p$-ичном представлении параметра $r_p$.

Для $n \ge 3$ соотношения для вычисления параметра $M_n(r_p)$ и, соответственно, линейной сложности недвоичных ГМВП в известной литературе отсутствуют.

Таким образом, получение общих выражений для вычисления линейной сложности $l_S$ недвоичных ГМВП, формируемых в произвольных конечных полях $\mathrm{GF}[(p^m)^n]$ для значения параметра $n \ge 3$, является новой научной задачей, решение которой вносит значимый вклад в теорию передачи информации.

Определим выражение для параметра $M_n(r_p)$ при $n = 3$. Запишем в общем виде $p$-ичное представление параметра $r_p$:

$$r_p = p^k g_k + p^{k-1} g_{k-1} + \ldots + p g_1 + g_0, \tag{6}$$

где $g_i = 0, 1, \ldots, p - 1$ — коэффициенты разложения, $k$ — количество разрядов в $p$-ичном представлении параметра $r_p$.

Известно, что для различных $p \ge 3$ десятичное представление разных чисел $r_p$ может иметь одинаковое $p$-ичное представление. Например, десятичные значения $r_{10} = 11$ при $p = 3$ и $r_{10} = 23$ при $p = 11$ имеют одинаковые $p$-ичные представления $r_3 = r_{11} = 21$, т. е. $g_1 = 2$, $g_0 = 1$.

С учетом разложения (6) выражение (5) для параметра $M_n(r_p)$ может быть представлено в виде

$$M_2(r_p) = 0{,}5\prod_{i=0}^{k}(g_i + 1). \quad (7)$$

Рассмотрим значения параметра $M_n(r_p)$ при одноразрядном и двухразрядном представлении $r_p = pg_1 + g_0$, которые приведены в табл. 1. Будем использовать запись $M_3(g_1, g_0)$ для обозначения зависимости параметра от коэффициентов разложения. Данные в таблице получены с помощью программы вычисления индексов децимации [16] для различных сочетаний параметров $p \le 13$, $m \le 4$, $n = 3$ и допустимых значений параметра $r_p$, удовлетворяющих условию НОД $(r_p, p^m - 1) = 1$. В скобках в таблице приведены значения $M_3(g_1, g_0)$, полученные аналитическим способом на основе анализа выявленных закономерностей.

*Таблица 1*

| $g_1, g_0$ | $M_3(g_1, g_0)$ | $g_1, g_0$ | $M_3(g_1, g_0)$ | $g_1, g_0$ | $M_3(g_1, g_0)$ | $g_1, g_0$ | $M_3(g_1, g_0)$ |
|---|---|---|---|---|---|---|---|
| 0,1 | 1 | 1,2 | 6 = 1·2·3 | 2,1 | 6 = 2·1·3 | 3,2 | 20 = 2·5·2 |
| 0,3 | 4 | 1,4 | 15 = 1·3·5 | 2,3 | 20 = 2·2·5 | 3,4 | 50 = 2·5·5 |
| 0,5 | 7 | 1,6 | 28 = 1·4·7 | 2,5 | 42 = 2·3·7 | 3,6 | |
| 0,7 | 12 | 1,8 | 45 = 1·5·9 | 2,7 | 72 = 2·4·9 | 3,8 | 150 = 2·5·15 |
| 0,9 | 19 | 1,10 | 66 = 1·6·11 | 2,9 | 110 = 2·5·11 | 3,10 | 220 = 2·5·22 |
| 0,11 | 26 | 1,12 | (91 = 1·7·13) | 2,11 | 156 = 2·6·13 | 3,12 | |
| 0,13 | (35) | 1,14 | (120 = 1·8·15) | 2,13 | 210 = 2·7·15 | 3,14 | (400 = 2·5·40) |
| 0,15 | (46) | 1,16 | (153 = 1·9·17) | 2,15 | (272 = 2·8·17) | 3,16 | (510 = 2·5·51) |
| | | | | | | | |
| 4,1 | 15 = 5·1·3 | 5,2 | 42 = 7·2·3 | 6,1 | 28 = 4·7·1 | 7,2 | 72 = 12·2·3 |
| 4,3 | 50 = 5·2·5 | 5,4 | 105 = 7·3·5 | 6,3 | | 7,4 | 180 = 12·3·5 |
| 4,5 | 105 =5·3·7 | 5,6 | 196 = 7·4·7 | 6,5 | 196 = 4·7·7 | 7,6 | 336 = 12·4·7 |
| 4,7 | 180 = 5·4·9 | 5,8 | 315 = 7·5·9 | 6,7 | 336 = 4·7·12 | 7,8 | (540 = 12·5·9) |
| 4,9 | 275 = 5·5·11 | 5,10 | | 6,9 | | 7,10 | 792 = 12·6·11 |
| 4,11 | (390 = 5·6·13) | 5,12 | (637 = 7·7·13) | 6,11 | 728 = 4·7·26 | 7,12 | 1092 = 12·7·13 |
| 4,13 | (525 = 5·7·15) | 5,14 | (840 = 7·8·15) | 6,13 | (980 = 4·7·35) | 7,14 | (1440 = 12·8·15) |
| 4,15 | (680 = 5·8·17) | 5,16 | (1071 = 7·9·17) | 6,15 | | 7,16 | (1836 = 12·9·17) |
| | | | | | | | |
| 8,1 | 45 = 15·1·3 | 9,2 | 110 = 5·11·2 | 10,1 | 66 = 22·1·2 | 11,2 | 156 = 26·2·3 |
| 8,3 | 150 = 15·2·5 | 9,4 | 275 = 5·11·5 | 10,3 | 220 = 22·2·5 | 11,4 | (390 = 26·3·5) |
| 8,5 | 315 = 15·3·7 | 9,6 | | 10,5 | | 11,6 | (728 = 26·4·7) |
| 8,7 | (540 = 15·4·9) | 9,8 | 825 = 5·11·15 | 10,7 | (792 = 22·4·9) | 11,8 | 1170 = 26·5·9 |
| 8,9 | 825 = 15·5·11 | 9,10 | 1210 = 5·11·22 | 10,9 | 1210 = 22·5·11 | 11,10 | (1716 = 26·6·11) |
| 8,11 | 1170 = 15·6·13 | 9,12 | | 10,11 | (1716 = 22·6·13) | 11,12 | 2366 = 26·7·13 |
| 8,13 | (1575 = 15·7·15) | 9,14 | (2200 = 5·11·40) | 10,13 | (2310 = 22·7·15) | 11,14 | (3120 = 26·8·15) |
| 8,15 | (2040 = 15·8·17) | 9,16 | (2805 = 5·11·51) | 10,15 | | 11,16 | (3978 = 26·9·17) |

Анализ данных, приведенных в табл. 1, показал, что число $M_3(g_1, g_0)$ зависит исключительно от параметра $r_p$, а именно от значений разрядов его $p$-ичного представления. Линейная сложность ГМВП в соответствии с (3) дополнительно определяется параметром $m$, т. е. степенью расширения подполя GF($p^m$).

Например, для полей GF[$(3^3)^3$] с $r_p = 5_{10} = 12_3$ и GF[$(5^2)^3$] с $r_p = 7_{10} = 12_5$ параметр $M_3(g_1, g_0) = 6$, а ЭЛС соответственно равны $l_S = 54$ и $l_S = 36$. Для полей GF[$(5^2)^3$] с $r_p = 19_{10} = 34_5$ и GF[$(7^2)^3$] с $r_p = 25_{10} = 34_7$ параметр $M_3(g_1, g_0) = 50$, а ЭЛС равны $l_S = 300$.

Для допустимых значений параметра $r_p$ значения разрядов $g_1$ и $g_0$ имеют разную четность, так как в противном случае не будет выполняться условие НОД($r_p$, $p^m - 1$) = 1.

На основе выявленных закономерностей для значений $M_3(g_1, g_0)$, приведенных в табл. 1, получим

$$M_3(g_1, g_0) = 0{,}5L_3(g_1)(g_0 + 1)(g_0 + 2), \tag{8}$$

где $L_3(g_1) = (g_1 + 2)!/(6g_1!)$ — коэффициент для старшего разряда $p$-ичного разложения параметра $r_p$.

Для одноразрядных нечетных значений $r_p = g_0$ (см. табл. 1) параметр $M_3(g_0)$ вычисляется округлением коэффициента $L_3(g_0)$ до ближайшего большего целого:

$$M_3(g_0) = \lfloor L_3(g_0) \rfloor. \tag{9}$$

При вычислениях необходимо учитывать ограничение

$$\text{НОД}(g_1, g_0) = 1, \tag{10}$$

вследствие которого отсутствуют данные в соответствующих ячейках табл. 1.

Для допустимых значений параметра $r_p$ выполняется равенство

$$M_3(g_1, g_0) = M_3(g_0, g_1). \tag{11}$$

Например, $M_3(4, 7) = M_3(7, 4) = 180$, $M_3(8, 9) = M_3(9, 8) = 825$.

При $p = 3$ для трех и более разрядных представлений параметра $r_p$ были получены значения $M_3(r_p)$, приведенные в табл. 2 [16].

*Таблица 2*

| $r_p$ | $M_3(r_p)$ | $r_p$ | $M_3(r_p)$ | $r_p$ | $M_3(r_p)$ |
|---|---|---|---|---|---|
| 111 | 9 | 1112 | 54 | 11122 | 324 |
| 122 | 36 | 1222 | 216 | 12222 | 1296 |

Из сравнения выражений (7) для $n = 2$ и (8) для $n = 3$ следует, что число множителей пропорционально возрастает с увеличением как параметра $n$, так и числа разрядов $p$-ичного представления параметра $r_p$. Для трехразрядных значений число $M_3(g_2, g_1, g_0)$ определяется следующим образом:

$$M_3(g_2, g_1, g_0) = 0{,}25L_3(g_2)(g_1 + 1)(g_1 + 2)(g_0 + 1)(g_0 + 2). \tag{12}$$

Например, число $M_3(1, 2, 2) = 0{,}25L(1)(2 + 1)^2(2 + 2)^2 = 36$, что соответствует значению в табл. 2.

В общем случае для $k$-разрядных значений параметра $r_p$ число $M_3(r_p)$ имеет следующий вид:

$$M_3(g_k, g_{k-1}, \ldots, g_1, g_0) = 2^{-k}L_3(g_k)\prod_{i=1}^{k}(g_{k-i} + 1)(g_{k-i} + 2). \tag{13}$$

Например, $M_3(1, 1, 1, 2, 2) = 2^{-4}L_3(1)(1 + 1)^2(1 + 2)^2(2 + 1)^2(2 + 2)^2 = 324$.

Перейдем к рассмотрению случая $n = 4$. Для отдельных значений параметра $r_p$ результаты вычисления числа $M_4(r_p)$ приведены в табл. 3 [16].

Экстраполяция (7), (8), (12), (13), а также результатов, представленных в табл. 1–3, позволила получить общее выражение для вычисления параметра $M_n(r_p)$ при произвольном значении $n$ и общем ограничении НОД($g_k$, $g_{k-1}$, …, $g_1$, $g_0$) = 1:

$$M_3(g_k, g_{k-1}, \ldots, g_1, g_0) = L_n(g_k)[(n-1)!]^{-k}\prod_{i=1}^{k}\prod_{j=1}^{n-1}(g_{k-i} + j). \tag{14}$$

*Таблица 3*

| $r_p$ | $M_4(r_p)$ | $r_p$ | $M_4(r_p)$ | $r_p$ | $M_4(r_p)$ | $r_p$ | $M_4(r_p)$ |
|---|---|---|---|---|---|---|---|
| 3 | 5 | 5 | 14 | 7 | 30 | 9 | 55 |
| 1,2 | 10 | 1,4 | 35 | 1,6 | 84 | 2,1 | 10 |
| 2,3 | 50 | 2,5 | 140 | 3,2 | 50 | 1,2,2 | 100 |

Значения коэффициента $L_n(g_k)$ были получены на основании (14) с учетом того, что $L_n(1) = 1$ для всех значений $n$, и приведены в табл. 4. В этой таблице некоторые значения параметра $L_n(g_k)$ могут быть нецелыми. В этом случае знаменатели дробей определяются через НОД($g_k$, $n$) > 1: например, $L_6(12) = 1031\frac{1}{3}$; $L_7(7) = 245\frac{1}{7}$.

*Таблица 4*

| $L_n(g_k)$ | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| $g_k$ | $n$ | | | | | | | | |
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 2 | 1 | 1,5 | 2 | 2,5 | 3 | 3,5 | 4 | 4,5 | 5 |
| 3 | 1 | 2 | 3,33 | 5 | 7 | 9,33 | 12 | 15 | 18,33 |
| 4 | 1 | 2,5 | 5 | 8,75 | 14 | 21 | 30 | 41,25 | 55 |
| 5 | 1 | 3 | 7 | 14 | 25,2 | 42 | 66 | 99 | 143 |
| 6 | 1 | 3,5 | 9,33 | 21 | 42 | 77 | 132 | 214,5 | 333,67 |
| 7 | 1 | 4 | 12 | 30 | 66 | 132 | 245,14 | 429 | 715 |
| 8 | 1 | 4,5 | 15 | 41,25 | 99 | 214,5 | 429 | 804,38 | 1430 |
| 9 | 1 | 5 | 18,33 | 55 | 143 | 333,67 | 715 | 1430 | 2701,11 |
| 10 | 1 | 5,5 | 22 | 71,5 | 200,2 | 500,5 | 1144 | 2431 | 4862 |
| 11 | 1 | 6 | 26 | 91 | 273 | 728 | 1768 | 3978 | 8398 |
| 12 | 1 | 6,5 | 30,33 | 113,75 | 364 | 1031,33 | 2652 | 6298,5 | 13996,67 |
| 13 | 1 | 7 | 35 | 140 | 476 | 1428 | 3876 | 9690 | 22610 |
| 14 | 1 | 7,5 | 40 | 170 | 612 | 1938 | 5537,14 | 14535 | 35530 |
| 15 | 1 | 8 | 45,33 | 99 | 775,2 | 2584 | 7752 | 21318 | 54479,33 |
| 16 | 1 | 8,5 | 51 | 242,25 | 969 | 3391,5 | 10659 | 30644,63 | 81719 |
| 17 | 1 | 9 | 57 | 285 | 1197 | 4389 | 14421 | 43263 | 120175 |
| 18 | 1 | 9,5 | 63,33 | 332,5 | 1463 | 5608,17 | 19228 | 60087,5 | 173586,11 |

Для перехода к целым числам умножим элементы каждой $g_k$-й строки на значение параметра $g_k$:

$$L_n^*(g_k) = g_k L_n(g_k). \tag{15}$$

Модифицированные значения коэффициентов представлены в табл. 5.

Анализ модифицированных значений коэффициентов показал, что элементы столбцов матрицы представляют собой последовательности $n$-угольных пирамидальных чисел, определяемых следующим образом:

$$L_n^*(g_k) = \frac{(g_k + n - 1)!}{(g_k - 1)!n!}.$$

*Таблица 5*

| $L_n^*(g_k)$ | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| $g_k$ | $n$ | | | | | | | | |
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 2 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 3 | 3 | 6 | 10 | 15 | 21 | 28 | 36 | 45 | 55 |
| 4 | 4 | 10 | 20 | 35 | 56 | 84 | 120 | 165 | 220 |
| 5 | 5 | 15 | 35 | 70 | 126 | 210 | 330 | 495 | 715 |
| 6 | 6 | 21 | 56 | 126 | 252 | 462 | 792 | 1287 | 2002 |
| 7 | 7 | 28 | 84 | 210 | 462 | 924 | 1716 | 3003 | 5005 |
| 8 | 8 | 36 | 120 | 330 | 792 | 1716 | 3432 | 6435 | 11440 |
| 9 | 9 | 45 | 165 | 495 | 1287 | 3003 | 6435 | 12870 | 24310 |
| 10 | 10 | 55 | 220 | 715 | 2002 | 5005 | 11440 | 24310 | 48620 |
| 11 | 11 | 66 | 286 | 1001 | 3003 | 8008 | 19448 | 43758 | 92378 |
| 12 | 12 | 78 | 364 | 1365 | 4368 | 12376 | 31824 | 75582 | 167960 |
| 13 | 13 | 91 | 455 | 1820 | 6188 | 18564 | 50388 | 125970 | 293930 |
| 14 | 14 | 105 | 560 | 2380 | 8568 | 27132 | 77520 | 203490 | 497420 |
| 15 | 15 | 120 | 680 | 1485 | 11628 | 38760 | 116280 | 319770 | 817190 |
| 16 | 16 | 136 | 816 | 3876 | 15504 | 54264 | 170544 | 490314 | 1307504 |
| 17 | 17 | 153 | 969 | 4845 | 20349 | 74613 | 245157 | 735471 | 2042975 |
| 18 | 18 | 171 | 1140 | 5985 | 26334 | 100947 | 346104 | 1081575 | 3124550 |

Для обратного перехода к коэффициентам $L_n(g_k)$ необходимо элементы каждой строки таблицы разделить на значения $g_k$, что соответствует соотношению

$$L_n(g_k) = \frac{(g_k + n - 1)!}{g_k! n!}. \tag{16}$$

После подстановки (16) в (14) получим окончательное выражение для числа суммируемых последовательностей $M_n(r_p)$ при формировании ГМВП:

$$M_n(r_p) = M_n(g_k, g_{k-1}, \ldots, g_0) = \frac{(g_k + n - 1)!}{g_k! n! [(n-1)!]^k} \prod_{i=1}^{k} \prod_{j=1}^{n-1} (g_{k-i} + j). \tag{17}$$

Вследствие того что все суммируемые последовательности формируются на основании неприводимых полиномов степени $mn$, линейная сложность ГМВП в соответствии с (3) будет определяться как

$$l_S = mnM_n(r_p) = \frac{m(g_k + n - 1)!}{g_k! [(n-1)!]^{k+1}} \prod_{i=1}^{k} \prod_{j=1}^{n-1} (g_{k-i} + j). \tag{18}$$

Легко показать, что выражения (2) и (3) являются частным случаем выражений (17) и (18) для двоичных последовательностей при $p = 2$ и $g_k = 1$. Например, для ГМВП с периодом $N = 4095$, формируемой в поле $\mathrm{GF}[(2^4)^3]$ с параметрами $r_{10} = 7$, $r_2 = 111$, $m = 4$, $n = 3$, число $M_4(1, 1, 1)$ в соответствии с выражением (3) равно $M_4(1, 1, 1) = 3^{z(111)-1} = 3^2 = 9$, а в соответствии с (17) оно также равно $M_4(1, 1, 1) = \dfrac{(1 + 3 - 1)!}{1!3![(2)!]^2} \prod_{i=1}^{2} \prod_{j=1}^{2} (g_{2-i} + j) = 2^{-2}(1 + 1)^2(1 + 2)^2 = 9$.

Определим значения ЭЛС для различных значений параметров $p$, $m$, $n$ и $r_p$. Например, пусть требуется найти ЭЛС для пятеричной ГМВП, сформированной в поле $GF[(5^4)^3]$ с периодом $N = p^{mn} - 1 = 5^{4\cdot3} - 1 = 244\,140\,625$ и параметром $r_{10} = 449$, $r_5 = 3244$.

Параметр $r_{10} = 449$ удовлетворяет условию НОД(449; 244140625) = 1. Число суммируемых последовательностей и, соответственно, выигрыш в структурной скрытности по сравнению с М- последовательностями определяется как

$$M_3(3, 2, 4, 4) = \frac{(3 + 3 - 1)!}{3!3!2^3} \prod_{i=1}^{3} \prod_{j=1}^{2} (g_{3-i} + j) = \frac{5!}{3!3!2^3}(2 + 1)(2 + 2)(4 + 1)^2(4 + 2)^2 = 4500.$$

Тогда ЭЛС пятеричной ГМВП с периодом $N = 244\,140\,625$ при $r_{10} = 449$ равна

$$l_S = mnM_n(r_p) = 4\cdot3\cdot4500 = 5400.$$

Таким образом, представлены формулы для расчета линейной сложности $l_S$ недвоичных ГМВП, создаваемых в произвольных конечных полях $GF[(p^m)^n]$, а также для числа $M_n(r_p)$ суммируемых последовательностей. Параметр $M_n(r_p)$ численно соответствует приросту структурной скрытности по сравнению с широко применяемыми М-последовательностями. Представленные формулы являются обобщением известных выражений для расчета ЭЛС двоичных последовательностей. Полученные результаты могут быть использованы при разработке последовательностей с заданными структурными и корреляционными характеристиками, а также для формирования требований к структурной скрытности сигналов с расширенным спектром при проектировании помехозащищенных систем передачи цифровой информации по радиоканалам.

## СПИСОК ЛИТЕРАТУРЫ


1. *Ипатов В. П.* Широкополосные системы и кодовое разделение сигналов. Принципы и приложения / Пер. с англ.; Под ред. *В. П. Ипатова.* М.: Техносфера, 2007. 488 с.
2. *Golomb S. W., Gong G.* Signal Design for Good Correlation for Wireless Communication, Cryptography and Radar. Cambridge Univ. Press, 2005. 438 p.
3. CDMA: прошлое, настоящее, будущее / Под ред. *Л. Е. Варакина* и *Ю. С. Шинакова.* М.: МАС, 2003. 608 с.
4. *Скляр Б.* Цифровая связь. Теоретические основы и практическое применение: Пер. с англ. М.: Изд. дом „Вильямс“, 2003. 1104 с.
5. *Gold R.* Maximal recursive sequences with 3-valued recursive cross-correlation functions // IEEE Trans. Inform. Theory. 1968. Vol. 14. N 1. P. 154.
6. *Liang H., Chen W., Luo J., Tang Y.* A new nonbinary sequence family with low correlation and large size // Advances in Mathematics of Communications. 2017. Vol. 11. P. 671.
7. *Wang Q.* The Linear Complexity of Some Binary Sequences With Three-Level Autocorrelation // IEEE Trans. on Information Theory. 2010. Vol. 56, N 8. P. 4046.
8. *Shi X., Zhu X., Huang X., Yue Q.* A Family of M-Ary σ-Sequences With Good Autocorrelation // IEEE Communications Letters. 2019. Vol. 23, N 7. P. 1132.
9. *Cho C. M., Kim J. Y., No J. S.* New p-ary sequence families of period (p↑n-1)/2 with good correlation property using two decimated m-sequences // IEICE Trans. on Com. 2015. Vol. E98, N 7. P. 1268.
10. *No J. S.* Generalization of GMW sequences and No sequences // IEEE Trans. on Information Theory. 1996. Vol. 42, N 1. P. 260–262.
11. *Chung H. B., No J. S.* Linear span of extended sequences and cascaded GMW sequences // IEEE Trans. Inform. Theory. 1999. Vol. 45, N 6. P. 2060.
12. *Кренгель Е. И.* О числе псевдослучайных последовательностей Гордона, Милза, Велча // Техника средств связи, серия ТРС. 1979. Вып. 3. С. 17–30.
13. *Мешковский К. А., Кренгель Е. И.* Генерация псевдослучайных последовательностей Гордона, Милза, Велча // Радиотехника. 1998. № 5. С. 25–28.
14. *Стародубцев В. Г.* Метод формирования недвоичных последовательностей Гордона — Миллса — Велча для систем передачи цифровой информации // Радиотехника и электроника. 2023. Т. 68, № 7. С. 676–682.

15. *Стародубцев В. Г.* Линейная сложность недвоичных последовательностей Гордона — Миллса — Велча // Радиотехника и электроника. 2021. Т. 66, № 8. С. 810–814.
16. Свид. о гос. рег. прогр. № 2021616735. Программа вычисления индексов децимации для суммируемых последовательностей при формировании недвоичных последовательностей Гордона — Миллса — Велча / *В. Г. Стародубцев, В. В. Ткаченко, А. С. Леонов, Е. Ю. Подолина, А. Х. Келоглян*. 26.04.2021 г.

## 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; преподаватель; E–mail: vgstarod@mail.ru

***Евгений Борисович Самойлов*** — канд. техн. наук, доцент; ВКА им. А. Ф. Можайского, кафедра технологий и средств автоматизации обработки и анализа информации космических средств; E–mail: vka@mil.ru

Поступила в редакцию 13.05.24; одобрена после рецензирования 12.07.24; принята к публикации 27.02.25.

**REFERENCES**

1. Ipatov V.P. *Spread Spectrum and CDMA. Principles and Applications*, NY, John Wiley and Sons Ltd., 2005, 488 p.
2. Golomb S.W., Gong G. *Signal Design for Good Correlation for Wireless Communication, Cryptography and Radar*, Cambridge University Press, 2005, 438 p.
3. Varakin L.E. and Shinakov Yu.S., ed., *CDMA: proshloye, nastoyashcheye, budushcheye* (CDMA: Past, Present, Future), Moscow, 2003, 608 p. (in Russ.)
4. Sklar B. *Digital Communications: Fundamentals and Applications*, Prentice Hall, 2001, 1079 p.
5. Gold R. *IEEE Trans. Inf. Theory*, 1968, no. 1(14), pp. 154.
6. Liang H., Chen W., Luo J., Tang Y. *Advances in Mathematics of Communications*, 2017, vol. 11, pp. 671.
7. Wang Q. *IEEE Trans. Inform. Theory*, 2010, no. 8(56), pp. 4046.
8. Shi X., Zhu X., Huang X., Yue Q. *IEEE Communications Letters*, 2019, no. 7(23), pp. 1132.
9. Cho C.M., Kim J.Y., No J.S. *IEICE Trans. on Com.*, 2015, no. 7(E98), pp. 1268.
10. No J.S. *IEEE Trans. Inform. Theory*, 1996, no. 1(42), pp. 260–262.
11. Chung H.B., No J.S. *IEEE Trans. Inform. Theory*, 1999, no. 6(45), pp. 2060.
12. Krengel E.I. *Communication Equipment, TRS series*, 1979, no. 3, pp. 17–30. (in Russ.)
13. Meshkovsky K.A., Krengel E.I. *Radioengineering*, 1998, no. 5, pp. 25–28. (in Russ.)
14. Starodubtsev V.G. *Journal of Communications Technology and Electronics*, 2023, no. 2(67), pp. 676–682. (in Russ).
15. Starodubtsev V.G. *Journal of Communications Technology and Electronics*, 2023, no. 8(66), p. 810–814. (in Russ).
16. Certificate on the state registration of the computer programs 2021616735, *Programma vychisleniya indeksov detsimatsii dlya summiruyemykh posledovatel'nostey pri formirovanii nedvoichnykh posledovatel'nostey Gordona-Millsa-Velcha* (A Program for Calculating Decimation Indices for Summable Sequences when Forming Non-binary Gordon-Mills-Welch Sequences), V.G. Starodubtsev, V.V. Tkachenko, A.S. Leonov, E.Yu. Podolina, A.Kh. Keloglyan, 26.04.2021. (in Russ.)

**DATA ON AUTHORS**

***Victor G. Starodubtsev*** — PhD., Associate Professor; A. F. Mozhaisky Military Space Academy, Department of Technologies and Automation of Processing and Analysis of Spacecraft Information; Senior Lecturer; E–mail: vgstarod@mail.ru

***Evgeny B. Samoylov*** — PhD, Associate Professor; A. F. Mozhaisky Military Space Academy, Department of Technologies and Automation of Processing and Analysis of Spacecraft Information; E–mail: vka@mil.ru

Received 13.05.24; approved after reviewing 12.07.24; accepted for publication 27.02.25.