**УДК** 004.5

О.В. Иванцов, И.А. Саитов

# ГРАНИЦЫ МИНИМАЛЬНОГО КОДОВОГО РАССТОЯНИЯ ДЛЯ НЕКОТОРОЙ БЛОКОВОЙ ДЛИНЫ СЕГМЕНТА ДВОИЧНОГО КОДА ЛИНЕЙНОЙ РЕКУРРЕНТНОЙ ПОСЛЕДОВАТЕЛЬНОСТИ

*Иванцов О.В., Саитов И.А.* **Границы минимального кодового расстояния для некоторой блоковой длины сегмента двоичного кода линейной рекуррентной последовательности.**

**Аннотация.** Решение научной проблемы по использованию линейных рекуррентных последовательностей (ЛРП) в помехоустойчивом кодировании информации требует разработки быстрых способов вычисления максимальной исправляющей способности для выбранного в качестве кодового слова сегмента произвольной длины на ЛРП. Количественной оценкой исправляющей способности таких кодеров является минимальное кодовое расстояние. В работе предложен нестандартный подход к быстрому и сравнительно точному определению границ минимального кодового расстояния для некоторых длин сегментов двоичного кода ЛРП на основе применения гипотетической $M_r$-последовательности.

**Ключевые слова:** линейная рекуррентная последовательность, гипотетическая $M_r$-последовательность, сегмент двоичного кода, границы минимального кодового расстояния.

*Ivantsov O.B., Saitov I.A.* **Minimum distance border for random block length binary code segment of linear recurring sequence.**

**Abstract.** The decision of scientific problem on using linear recurring sequence (LRS) in antinoise coding requires the development the fast ways calculate of maximum correcting ability for the selected for the selected segment of arbitrary LRS segment length. Quantitative correcting ability assessment of such coders is minimum code distance. In this paper unconventional approach to rapid and relatively precise definition of the boundaries of the minimum code distance for random segment length of binary LRS code by applying the hypothetical $M_r$-sequence is proposed.

**Keywords:** linear recurring sequence, hypothetical $M_r$-sequence, binary code segment, minimum distance code border.

**1. Введение.** Для любого линейного ($n$; $k;d$) двоичного кода, к которому относятся отрезки линейной рекуррентной последовательности (ЛРП), включая и код максимальной длины (КМД), определение минимального кодового расстояния $d_{\min}$ для $n < 2^k-1$ является актуальной и сложной задачей. Актуальность решения задачи в настоящее время заключается в достаточно активной разработке способов применения ЛРП не только в системах синхронизации [4], но и помехозащищенном кодировании информации. Сложность решаемой задачи объясняется влиянием на значение $d_{\min}$ вида примитивного полинома обратных связей, по закону которого формируется участок (отрезок) ЛРП длиной $n$. Участки ЛРП длиной $n < 2^k-1$ по отношению КМД являются усеченными линейными двоичными кодами. Далее усеченный линейный двоичный код длиной $n < 2^k–1$ будем называть сегментом КМД.

Существует два основных пути по увеличению $d_{\min}$ для сегментов КМД любой длины $n$: увеличение числа ненулевых коэффициентов примитивного полинома $h(x)$ и увеличение $m$ – избыточной части участка $n$ линейной рекуррентной последовательности при заданной длине $k$ – информационной части участка [1].

Можно доказать, что если примитивный полином $h(x)$ является триномом, то минимально кодовое расстояние любого сегмента КМД $d_{\min}=2$ при $m< n$ и $d_{\min}=3$ при $m=n$ [1].

Вычисление же значений $d_{\min}$ сегментов КМД для примитивных полиномов $h(x)$, которые не являются триномами, возможно только путем полного перебора участков длиной $n$ на КМД. Для определения нижней и верхней границы минимального кодового расстояния необходимо осуществить полный перебор всех сегментов на КМД, которые образованы всеми существующими примитивными полиномами с разрядностью $k$, что является сложной вычислительной задачей, особенно для больших значений $k$ и $n$.

Получение аналитических выражений для нижней верхней границы минимального кодового расстояния для некоторых длин сегментов КМД [3], значения которой необходимо учитывать при расчетах по проектированию систем синхронизации и кодирования информации, позволит избавиться от необходимости проведения сложных вычислений. Перед тем как перейти к решению задачи, необходимо выяснить закономерные особенности влияния веса примитивного полинома $h(x)$ и его распределения на значение минимального кодового расстояния для выбранного сегмента КМД длиной $n$, так как полученные сведения могут повлиять на ход дальнейших решений.

**2. Анализ закономерностей влияния вида образующего полинома на минимальное кодовое расстояние сегмента двоичного кода ЛРП.** Для определения случаев нарушения зависимости увеличения $d_{\min}$ от сегмента КМД длиной $n$ и вида примитивного полинома $h(x)$ были использованы экспериментальные значения для всех сегментов при разрядности ЛРР $k=7$.

В таблице 1 приведены значения $d_{\min}$ для сегментов КМД на М-последовательности, произведенных линейными рекуррентными регистрами (ЛРР) длиной $k=7$ по закону обратных связей $h(x)$ при различных значениях $n$. Источниками М-последовательностей являются ЛРР с обратными связями с включенными в них схемами сложения по mod 2. ЛРР такого вида получили название простых (ПГРС) или модулярных генераторов на регистрах сдвига (МГРС).

Нетрудно заметить, что при длине участка на М-последовательности $n$=15 значения $d_{\min}$=3, полученные по закону полиномов $h_1(x)=x^7+ x^5+x^3+x^2+x+1$ и $h_2(x)=x^7+x+1$, равны и уступают значению $d_{\min}$=5 с использованием полинома $h_3(x) = x^7+x^6+x^3+x+1$, причем вес последнего примитивного полинома $h_3(x)$ меньше веса полинома $h_1(x)$ и больше $h_3(x)$.

Таблица 1. Экспериментальные значения $d_{\min}$ сегментов КМД-кодов ($k$=7)

| $h(x)$ / $n$ | 10011101 | 10000011 | 10100111 | 10111111 | 11000001 | 11001011 |
|---|---|---|---|---|---|---|
| 7 | 1 | 1 | 1 | 1 | 1 | 1 |
| 8 | 1 | 1 | 1 | 1 | 1 | 1 |
| 9 | 1 | 1 | 1 | 2 | 1 | 1 |
| 10 | 2 | 1 | 2 | 2 | 1 | 2 |
| 11 | 2 | 1 | 3 | 2 | 1 | 2 |
| 12 | 3 | 1 | 3 | 2 | 1 | 2 |
| 13 | 3 | 2 | 3 | 3 | 2 | 3 |
| 14 | 3 | 3 | 4 | 3 | 3 | 4 |
| 15 | 3 | 3 | 4 | 3 | 3 | 5 |
| 16 | 4 | 3 | 4 | 4 | 3 | 5 |
| 17 | 4 | 3 | 4 | 4 | 3 | 5 |
| 18 | 4 | 3 | 4 | 4 | 3 | 6 |
| 19 | 5 | 4 | 5 | 5 | 4 | 6 |
| 20 | 6 | 4 | 6 | 5 | 4 | 7 |
| 21 | 7 | 5 | 7 | 6 | 5 | 7 |
| 22 | 7 | 5 | 7 | 7 | 5 | 7 |
| 23 | 7 | 5 | 8 | 7 | 5 | 8 |
| 24 | 7 | 5 | 8 | 7 | 5 | 9 |
| 25 | 8 | 6 | 8 | 8 | 6 | 9 |
| 26 | 8 | 7 | 8 | 9 | 7 | 10 |
| 27 | 8 | 8 | 9 | 9 | 8 | 11 |
| 28 | 9 | 9 | 10 | 9 | 9 | 11 |

Из этого следует, что сегменты КМД одной длины $n$ и соответствующие им значения $d_{\min}$, полученные по закону примитивных полиномов $h(x)$, не имеют пропорциональной зависимости увеличения минимального кодового расстояния от уменьшения числа нулевых коэффициентов полиномов.

Следовательно, необходимо определить закономерность, по которой изменяется значение $d_{\min}$ в зависимости от длины любого сегмента КМД длиной $n$ с учетом выбранного образующего полинома $h(x)$.

Отсутствие прямой зависимости увеличения $d_{\min}$ для некоторых сегментов КМД от числа ненулевых коэффициентов примитивного полинома $h(x)$ можно объяснить тем, что вид примитивного полинома, прежде всего, влияет на размещение серий из нулей или единиц на М-последовательности, т.е. насколько пропорционально рассеяны (разнесены) друг от друга по отношению к размеру серии на М-последовательности, начиная с серий большой длины, настолько возможно увеличение $d_{\min}$ с учетом выбранных величины сегмента КМД $n$ и примитивного полинома $h(x)$.

Для проверки выдвинутого предположения в качестве примера, на рисунках 1 и 2 представлены М-последовательности, полученные с помощью примитивных полиномов $x^7 + x^6 + x^5 + x^3 + x^2 + x + 1$ и $x^7 + x + 1$. Все места расположения серий из нулей и единиц длиной $l \geq 3$ на М-последовательности выделены серым фоном.

001100111011101001011000110111101101101100100100011100001011111
001010111001101000100111100010100001100000100000011111111010101

Рис. 1. Порядок распределения серий на М-последовательности с использованием примитивного полинома $x^7 + x + 1$

001110001100101100110001011110111001000100001101011010001111О
000010011011000010100000011101101111100111111101001001010111О
10101

Рис. 2. Порядок распределение серий на М-последовательности с использованием примитивного полинома $x^7 + x^6 + x^5 + x^3 + x^2 + x + 1$

Взаимное расположение выделенных серий на М-последовательности, изображенные на рисунках 1 и 2, указывает на то, что вид образующего полинома влияет на распределение этих серий. Количество и размер серий остаются неизменными на основании известного свойства "серий" ЛРР.

*Свойство "серий"*. Любая двоичная последовательность максимальной длины ($2^k - 1$) содержит серии как "единиц", так и "нулей" длины $l$ точно $2^{k-(l+2)}$ раз, где $1 \leq l \leq k$-2. Во всех этих случаях число серий "единиц" длины $l$ равно числу серий "нулей" такой же длины. Исключение составляют серии длиной ($k$–1) и $k$, а именно, серия из ($k$–1) "нулей" встречается в замкнутом периоде М-последовательности только один раз, а серия из $k$ "нулей" отсутствует. Напротив, серия из ($k$–1) "единиц" отсутствует, а серия из $k$ "единиц" появляется только один раз [3].

Если пропорциональное рассеивание больших серий на М-последовательности дает положительный результат по повышению значения $d_{\min}$ для заданного сегмента КМД длиной $n$, то можно предположить, что "склеивание" серий, начиная с серии величиной $k$ и далее по убыванию, должно дать прямо противоположный результат для сегмента любой длины.

**3. Математическое описание вычислительного эксперимента по определению нижней границы $d^{\text{н}}_{\min}$ для некоторых длин сег-**

**ментов КМД.** Важность обнаружения "склеенных" больших серий из нулей и единиц на М-последовательности, начиная с серии максимальной длины, совпадающие с размером сегмента КМД длиной $n$, заключается в том, что при сдвиге на один бит, оба участка будут иметь максимальное количество совпадающих разрядов, между собой, что соответствует минимальному кодовому расстоянию. В этом случае необходимость полного перебора сегментов на М-последовательности длиной $n$ отпадает, так как найти значение меньше обнаруженного уже невозможно независимо от того, каким из примитивных полиномов эта последовательность сформирована.

Но у М-последовательностей, полученных, например, от ПГРС, не может быть большого количества, "склеенных" между собой больших серий из нулей и единиц, и при выборе определенных значений участков М-последовательности длиной $n$, сравнимые с длиной этого "склеенного" участка, $d_{\min}$ не всегда будет достигать нижней границы минимальных значений.

Это дает возможность теоретически предположить существование такой М-последовательности, у которой все значения $d_{\min}$ сегментов КМД длиной $n$ являются элементами нижней границы.

Введем абстрактную модель генератора на регистре сдвига, вырабатывающую гипотетическую М-последовательность ($М_г$), у которой все серии "склеены" между собой, начиная с серии максимальной длины с учетом убывания до одиночных серий включительно. Действительно, $М_г$-последовательности такого вида, с одной стороны, присущи все свойства линейной рекуррентной последовательности, с другой – она не может быть получена ни одним из генераторов на регистре сдвига, следовательно, данную последовательность можно отнести к гипотетической. Для примера на рисунке 3 изображена $М_г$-последовательность при $k$=7.

Очевидно, что при выборе сегмента длиной $n$, необходимо выбрать, такую же, комбинацию, начиная с серии максимальной длины, как и в гипотетической $М_г$-последовательности. Затем сравнить между собой эти комбинации, при сдвиге их на один разряд по отношению друг к другу и получить самое минимальное значение $d^{\text{н}}_{\min a}$. Дальнейшее сравнение и перебор остальных участков на $М_г$-последовательности меньший результат, чем был получен ранее, не даст.

1111111000000111110000011110000111100001110001110001110001110
0011001100110011001100110011001010101010101010101010101
01010

Рис. 3. $М_г$-последовательность для ЛРР разрядностью $k$=7

Соответственно все значения $d_{\min}$, полученные на гипотетической последовательности при различных значениях $n$, будут определять нижнюю границу всех сегментов КМД, полученных ПГРС с разрядностью $k$=7.

Полученная закономерность распространяется на все возвратные М-последовательности, полученные ПГРС любой разрядности, так как им присуще свойство "серий".

После введения $М_г$-последовательности необходимо проверить на одном или нескольких примерах, согласуются ли ее новые абстрактные свойства и применяемые правила вычисления с предшествующим опытом определения нижней границы минимального кодового расстояния.

Правило вычисления $d^{н}_{\min a}$ заключается в том, что при сдвиге на один шаг сравниваются два сегмента длиной $n$ $М_г$-последовательности и М-последовательности. М-последовательность не должна содержать больше двух подряд склеенных серий, начиная с самой большой по убыванию, так как она не является гипотетической.

*Пример.*

*Дано*: Пусть ПГРС величиной $k$=7 вырабатывает М-последовательность по закону примитивного полинома $h(x)= x^7+x+1$ (рисунок 1). Размер сегмента КМД: *а)* $n$=7; б) $n$=13=7+6; в) $n$=18=7+6+5; г) $n$=23=7+6+5+5; д) $n$=27=7+6+5+5+4; е) $n$=31=7+6+5+5+4+4.

*Найти*: значения нижней границы $d_{\min}$ , для $n$=7, 13, 18, 23, 27, 31.

*Решение*:

Используя гипотетическую последовательность (рисунок 3), определим значения нижней границы $d_{\min}$:

а) Сегмент КМД длиной $n$=7 на $М_г$-последовательности вмещает в себя одну полную серию длиной 7 бит. При сдвиге на один бит полученные два сегмента отличаются друг от друга 1 разрядом. Применяя правило вычисления $d_{\min}$=1:

$$\oplus\begin{array}{l|l} \;1111111 & \\ 01111111 & \\ \hline 1 & d_{\min}=1 \end{array}$$

б) Сегмент КМД длиной $n$=13 на $М_г$-последовательности вмещает в себя две серии длиной 7 и 6 бит соответственно. При сдвиге на один бит (рисунок 5) два сегмента одной длины отличаются друг от друга 2 разрядами. Применяя правило вычисления $d_{\min}$=2:

$$\begin{array}{l|l} \oplus\ 111111100000011111 & \\ \phantom{\oplus\ }01111111000000 & \\ \hline 1 \qquad\qquad 1 & d_{\min} = 2 \end{array}$$

в) Сегмент КМД $n$=18 на $М_г$-последовательности вмещает в себя три серии длиной 7, 6 и 5 бит соответственно. При сдвиге на один бит два сегмента одной длины отличаются друг от друга 3 разрядами. Применяя правило вычисления $d_{\min}$=3:

$$\begin{array}{l|l} \oplus\ 11111110000001111100000 & \\ \phantom{\oplus\ }0111111100000011111 & \\ \hline 1 \qquad\qquad 1 \qquad\qquad 1 & d_{\min} = 3 \end{array}$$

г) В верхней строке сегмент КМД длиной $n$=23 на $М_г$-последовательности вмещает в себя четыре серии длиной 7, 6 и две серии по 5 бит соответственно. Во второй строке представлен реальный сегмент М-последовательности длиной $n$=23, который отличается на минимальное количество разрядов, при условии, что сегмента с тремя и более склеенными сериями не существует. Для этого необходимо в один из разрядов сегмента внести изменения. В серии из пяти единиц значение тетьего разряда изменено на противоположный и обозначено как "$\underline{0}$". При сдвиге на один бит два сегмента одной длины отличаются друг от друга 5 разрядами ($d_{\min}$=5). Применяя правило вычисления получим:

$$\begin{array}{l|l} \oplus\ 111111100000011111000001 & \\ \phantom{\oplus\ }011111110000001\underline{0}1100000 & \\ \hline 1 \qquad\quad 1 \qquad\quad 1 \quad 1 \qquad\qquad 1 & d^{\text{н}}_{\min} = 5 \end{array}$$

д) В верхней строке сегмент КМД длиной $n$=27 на $М_г$-последовательности вмещает в себя пять серий длиной 7, 6, две серии по 5 бит и одна серия 4 бита соответственно. В нижней строке необходимо внести минимальные изменения, чтобы в сегменте не было больше двух больших склеенных серий. Для этого в каждой из трех серий необходимо изменить как минимум по одному разряду. При сдвиге на один бит два сегмента одной длины отличаются друг от друга 8 разрядами ($d_{\min}$=8). Применяя правило вычисления, получим значение $d_{\min}$ в виде:

$$\begin{array}{l|l} \oplus\ 1111111000000111110000011110 & \\ \phantom{\oplus\ }011111110000001\underline{0}1100\underline{1}001\underline{0}11 & \\ \hline 1 \qquad\quad 1 \qquad\quad 1 \quad 1\ 1 \quad 1\ 1\ 1 & d^{\text{н}}_{\min} = 8 \end{array}$$

е) Сегмент КМД длиной $n$=31 на $М_г$-последовательности вмещает в себя шесть серий длиной 7, 6, две серии по 5 бит и две серия 4 бита соответственно. Таким образом, во второй строке необходимо внести минимальные изменения в четыре серии. В этом случае при сдвиге на один бит два сегмента одной длины отличаются друг от друга 10 разрядами. $d_{\min}$=10. Порядок вычисления можно представить в виде:

$$\begin{array}{l|l} \oplus \begin{array}{l} 11111110000001111100000111100001 \\ 01111111000000110\underline{0}1100\underline{1}001\underline{0}110\underline{1}00 \end{array} & \\ \hline 1 \quad\quad 1 \quad\quad 1 \quad 1\,1 \quad 1\;1\;1\;1\;1 & d^{н}_{\min} = 10 \end{array}$$

Подчеркнутые значения (таблица 2), вычисленные по выше предложенному правилу, не попадают в ряд чисел, составляющих арифметическую прогрессию.

Таблица 2. Вычисленные значения $d^{н}_{\min}$ сегментов КМД-кодов ($k$=7)

| Длина сегмента $n$ | 7 | 18 | 27 | 35 | 42 | 48 | 54 | 60 |
|---|---|---|---|---|---|---|---|---|
| Нечетное количество серий $b_n$ | 1 | 3 | 5 | 7 | 9 | 11 | 13 | 15 |
| Вычисленное аналитически $d^{н}_{\min\,a}$ | 1 | $\underline{3}$ | 8 | 11 | 14 | 17 | 20 | 23 |
| Эсприментальное значение $d^{н}_{\min\,э}$ | 1 | 3 | 8 | 11 | 15 | 18 | 20 | 23 |
| Длина сегмента $n$ | 13 | 23 | 31 | 39 | 45 | 51 | 57 | 62 |
| Четное количество серий $b_n$ | 2 | 4 | 6 | 8 | 10 | 12 | 14 | 16 |
| Вычисленное аналитически $d^{н}_{\min\,a}$ | 2 | $\underline{5}$ | 10 | 13 | 16 | 19 | 22 | 25 |
| Эсприментальное значение $d^{н}_{\min\,э}$ | 2 | 5 | 10 | 13 | 16 | 19 | 22 | 26 |

*Вывод:*

Вычисленные значения $d_{\min}$ с использованием гипотетической последовательности в большинстве случаев совпадают с экспериментальными значениями минимального кодового расстояния, а это значит, что ее новые абстрактные свойства согласуются с предшествующим опытом машинного вычисления нижней границы минимального кодового расстояния.

Вычисленные значения $d_{\min}$, за некоторым исключением (таблица 2), сегментов КМД длиной $n$, которые вмещают целое четное или нечетное количество серий по убыванию, образуют два ряда с арифметической прогрессией с шагом $d$=3 для четного и нечетного количества серий соответственно.

Для получения аналитического выражения в общем виде для полного количества серий, умещающихся на заданной длине $n$ КМД-кода необходимо $М_г$-последовательность представить в виде суммы слагаемых $a_{ji}$, например при $k$=7 (таблица 3), где $a_{ji}$ – длина $ji$-ой серии гипотетической М-последовательности.

Таблица 3. Нумерация членов гипотетической последовательности (к=7)

| Длина серии ($k$=7) | $K$ | $k$-1 | $k$-2 | $k$-2 | $k$-3 | $k$-3 | $k$-3 | $k$-3 | $k$-4 | $k$-4 | ... | $k$-4 | $k$-5 | ... | $k$-5 | $k$-6 | $k$-6 | ... | $k$-6 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 7 | 6 | 5 | 5 | 4 | 4 | 4 | 4 | 3 | 3 | ... | 3 | 2 | ... | 2 | 1 | 1 | ... | 1 |
| Вид серии | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | ... | 0 | 1 | ... | 0 | 1 | 0 | ... | 0 |
| № вид серии ($j$) | 0 | 1 | 2 | 2 | 3 | 3 | 3 | 3 | 4 | 4 | ... | 4 | 5 | ... | 5 | 6 | 6 | ... | 6 |
| № серии одного вида ($i$) | 0 | 1 | 1 | 2 | 1 | 2 | 3 | 4 | 1 | 2 | ... | 8 | 1 | ... | 16 | 1 | 2 | ... | 32 |
| $a_{ji}$ | $a_{00}$ | $a_{11}$ | $a_{21}$ | $a_{22}$ | $a_{31}$ | $a_{32}$ | $a_{33}$ | $a_{34}$ | $a_{41}$ | $a_{42}$ | ... | $a_{48}$ | $a_{51}$ | ... | $a_{516}$ | $a_{61}$ | $a_{62}$ | ... | $a_{632}$ |

$M_г$-последовательность в соответствии со свойством "серий" ЛРР и длиной $k$ может быть представлена в виде суммы длин $a_{ji}$ равной длине КМД:

$$S_k = a_{00} + a_{11} + a_{21} + a_{22} + a_{31} + a_{32} + \ldots + a_{41} + a_{42} + \ldots + a_{48} +,$$
$$a_{52} + \ldots + a_{516} + \ldots + a_{(k-1)1} + a_{(k-1)2} + \ldots + a_{(k-1)2^{k-2}} = 2^k - 1 \qquad (1)$$

В результате этого уравнение (2) позволяет в общем виде выразить количество серий, начиная с серии максимальной длины, помещающихся на сегменте КМД длиной $n$:

$$n = a_{00} + \sum_{j=1}^{k-1} \sum_{i=1}^{\frac{2^{k-1}}{2^{k-j}}} a_{ji}, \qquad (2)$$

где $a_{00}$ – длина максимальной серии $k$ разрядов; $a_{ji}$ – длина $j$-ой серии; $\frac{2^{k-1}}{2^{k-j}}$ – количество серий одной длины на М-последовательности; $k$ – количество видов серий разной длины, определяемая длиной ЛРР.

Равенство (2) выполняется только лишь в том случае, если выбранная длина сегмента КМД $n$ равна сумме длин полных серий $M_г$-последовательности, начиная с серии максимальной длины $k$.

Исходя из выражения (2), если количество полных серий $b_n$ разного вида, помещается одна, две, три серии на выбранной длине сегмента $n$, то можно записать как:

$$b_7 = a_{00} = 1;$$
$$b_{13} = a_{00} + a_{11} = 2;$$
$$b_{18} = a_{00} + a_{11} + a_{21} = 3;$$
......................................
$$b_n = a_{00} + a_{11} + a_{21} + a_{22} + ... + a_{ji} = 2^{j-1} + i.$$

Таким образом, количество полных серий $b_n$ разного вида, помещающихся на выбранной длине сегмента $n$ определяется выражением:

$$b_n = 2^{j-1} + i. \tag{3}$$

Нахождение $d_{min}$ КМД-кодов длиной $n$, которые вмещают в себя нечетное или четное количество серий, можно представить в виде выражения, описывающего две арифметические прогрессии:

$$d^{\text{н}}_{\min a} \geq \begin{cases} a_0 + \dfrac{b_n - 1}{2} d, & a_0 = 1, d = 3, b = 3,5,7,...,2^k - 1; \\ a_0 + \dfrac{b_n - 2}{2} d, & a_0 = 2, d = 3, b = 4,6,8,...,2^k - 2. \end{cases} \tag{4}$$

Чтобы проверить точность полученных значений $d^{\text{н}}_{\min a}$ с помощью аналитического выражения (4), необходимо провести сравнение со значениями $d^{\text{н}}_{\min \text{э}}$, полученными экспериментальным путем.

В ходе сравнения экспериментальных и аналитических значений $d_{min}$, выяснилось, что показатель $d^{\text{н}}_{\min \text{э}}$ имеет значительные выходы за пределы двух рядов арифметической прогрессии при $b_n$=3 ($n$=18) и $b_n$=4 ($n$=23). С целью повышения точности вычисления $d^{\text{н}}_{\min \text{э}}$ и компенсации этих выбросов в выражение (4) введены дополнительные слагаемые.

$$d^{\text{н}}_{\min a} \geq \begin{cases} a_0 + \dfrac{b_n - 1}{2} d + \left\lceil \dfrac{b_n - 4}{b_n - 2} \right\rceil, a_0 = 1, d = 3, b = 3,5,7,...,2^k - 1; \\ a_0 + \dfrac{b_n - 2}{2} d + 2\left\lceil \dfrac{b_n - 4}{b_n - 3} \right\rceil, a_0 = 2, d = 3, b = 4,6,8,...,2^k - 2. \end{cases} \tag{5}$$

На графике (рисунок 4) произведено сравнение $d^{\text{н}}_{\min \text{э}}$ и $d^{\text{н}}_{\min a}$ всех сегментов КМД при $k$=7 длиной $k \leq n \leq 2^{k-1}+11$.

*Вывод*:

1) Графики на рисунке 4, полученные экспериментальным и аналитическим путем и описывающие нижние границы всех сегментов КМД на примере ПГРС при $k$=7 в точках, где длина $n$ равна сумме длин серий $М_г$-последовательности, в основном совпадают, а в некоторых точках погрешность Δ не превышает $\Delta = |d^{\text{н}}_{\min \text{э}} - d^{\text{н}}_{\min a}| \leq 1$.

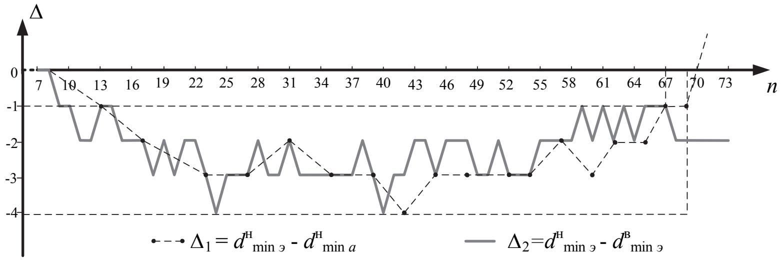


Рис. 4. Нижняя граница сегментов КМД при $k$=7, полученных экспериментальным и аналитическим способом

2) Начиная с участка $n > 2^{k-1}+4$ возрастание $d^{\text{н}}_{\min a}$ по закону арифметической прогрессии, полученное с помощью выражения (5), нарушается и расходится с экспериментальными значениями $d^{\text{н}}_{\min \text{э}}$.

Полученная граница арифметической прогрессии соответствует сегменту КМД длиной $n = 2^{k-1}+4$ на $М_г$-последовательности. Величина этого сегмента равна сумме длин всех серии $l \geq 3$ по убыванию и примыкающей к ним двух серий из двух единиц и нулей (рисунок 3) с учетом сдвига на один разряд вправо, при которой еще наблюдается на участке последней серии совпадение в одном разряде и сохраняется шаг арифметической прогрессии $d = 3$. В силу этого количество серий $b_n$, помещающихся на участке $2^{k-1}+1$, составит $2^{k-3}+2$.

После уточнения верхнего предела длины сегмента $n$ КМД выражение (5) примет окончательный вид:

$$d^{\text{н}}_{\min a} \geq \begin{cases} a_0 + \dfrac{b_n - 1}{2} d + \left\lceil \dfrac{b_n - 4}{b_n - 2} \right\rceil, a_0 = 1, d = 3, b = 3,5,7,\ldots,2^{k-3}+1; \\ a_0 + \dfrac{b_n - 2}{2} d + 2\left\lceil \dfrac{b_n - 4}{b_n - 3} \right\rceil, a_0 = 2, d = 3, b = 4,6,8,\ldots,2^{k-3}+2. \end{cases} \quad (6)$$

**4. Математическое описание вычислительного эксперимента по определению аналитического выражения верхней границы $\boldsymbol{d}^{\text{в}}_{\mathbf{min}}$ для некоторых длин сегментов КМД.** Не менее интересной, а может быть, и более важной задачей является определение аналитического выражения верхней границы $d^{\text{в}}_{\min}$ для некоторых длин сегментов КМД на участке $k \leq n \leq 2^k-1$.

Возвращаясь к гипотетической $М_г$-последовательности (рисунок 3), так же как и при определении нижней границы минимального кодового расстояния необходимо проверить на одном или нескольких примерах, согласуются ли ее новые абстрактные свойства и применяемые правила вычисления с предшествующим опытом вычисления минимального кодового расстояния для определения верхней границы.

Правило вычисления верхней границы минимального кодового расстояния заключается в том, что при сдвиге на один шаг сравниваются два сегмента длиной $n$ $М_г$-последовательности и $М'_г$-последовательности. $М'_г$-последовательность представляет из себя неполную гипотетическую последовательность, которая составлена из оставшихся больших серий по убыванию, не поместившихся на участке сегмента длиной $n$.

*Пример.*

*Дано*: Пусть ПГРС величиной $k$=7 вырабатывает М-последовательность по закону примитивного полинома $h(x)= x^7+x+1$ (рисунок 1). Размер сегмента КМД: *а)* $n$=7; б) $n$=13=7+6; в) $n$=18=7+6+5; г) $n$=23=7+6+5+5; д) $n$=27=7+6+5+5+4; е) $n$=31=7+6+5+5+4+4; ж) $n$=35=7+6+5+5+4+4+3.

*Найти*: значения верхней границы $d_{\min}$ , для $n$=7, 13, 18, 23, 27, 31.

*Решение*:

Используя гипотетическую последовательность (рисунок 3), определим значения верхней границы $d_{\min}$:

а) Сегмент КМД длиной $n$=7 на $М_г$-последовательности вмещает в себя одну полную серию длиной 7 бит. При сдвиге на один бит полученные два сегмента отличаются друг от друга 1 разрядом, таким образом $d_{\min}$=1.

б) Сегмент КМД длиной $n$=13 на $М_г$-последовательности вмещает в себя две серии длиной 7 и 6 бит соответственно. Этот сегмент сравнивается с сегментом, который уже не имеет серии длиной 7 и 6 бит, а составлен из оставшихся больших серии длиной по 5 бит. Два сегмента отличаются друг от друга 3 разрядами. Порядок вычисления $d_{\min}$ можно представить в виде:

$$\begin{array}{l|l} \oplus\begin{matrix}111111100000011111\\0111110100000\phantom{00000}\end{matrix} & \\ \hline 1\phantom{00000}11 & d_{\min}= 3 \end{array}$$

в) Сегмент КМД $n$=18 на $М_г$-последовательности вмещает в себя три серии длиной 7, 6 и 5 бит соответственно. Этот сегмент сравнивается с другим сегментом, который составлен из оставшихся больших серий длиной 5 и три серии по 4 бита. Два сегмента отличаются друг от друга 6 разрядами. Вычисление $d_{\min}$ можно представить в виде:

```
 1111111000000111110 |
⊕000011110000011110  |
 ---------------------------
 1111   1          1 | dmin= 6
```

г) Сегмент КМД длиной $n$=23 на $М_г$-последовательности вмещает в себя четыре серии длиной 7, 6 и две серии по 5 бит соответственно. Этот сегмент сравнивается с другим сегментом, который составлен из оставшихся больших серий длиной 4 и 3 бита. Два сегмента отличаются друг от друга 8 разрядами и вычисление $d_{\min}$ можно представить в виде:

```
 111111100000011111000001|
⊕111101110000011110000111|
 ---------------------------------
     1  1    1    11  111| dmin= 8
```

д) Сегмент КМД длиной $n$=27 на $М_г$-последовательности вмещает в себя пять серий длиной 7, 6, две серии по 5 бит и одна серия 4 бита соответственно. Этот сегмент сравнивается с другим сегментом, который составлен из оставшихся больших серий длиной 4 и 3 бита. Два сегмента отличаются друг от друга 11 разрядами и вычисление $d_{\min}$ можно представить в виде:

```
 111111100000011111000001111 0|
⊕000111100000111000111000011 10|
 -----------------------------------------
 111          11 111 11    1   | dmin= 11
```

е) Сегмент КМД длиной $n$=31 на $М_г$-последовательности вмещает в себя шесть серий длиной 7, 6, две серии по 5 бит и две серии 4 бита соответственно. Этот сегмент сравнивается с другим сегментом, который составлен из оставшихся больших серий длиной 4 и 3 бита. Два сегмента отличаются друг от друга 12 разрядами и вычисление $d_{\min}$ можно представить в виде:

```
 11111110000001111100000111100001|
⊕1111001110001110001110001110000 |
 ------------------------------------------
     11 1 1   1  1 11111   1     | dmin= 12
```

ж) Сегмент КМД длиной $n$=35 на $М_г$-последовательности вмещает в себя семь серий длиной 7, 6, две серии по 5 бит, три серии по 4 бита соответственно. Этот сегмент сравнивается с другим сегментом, который составлен из оставшихся больших серий длиной 4, 3 и 2 бита.

Два сегмента отличаются друг от друга 14 разрядами и вычисление $d_{\min}$ можно представить в виде:

```
 1111111000000011111000000111100001111 |
⊕001110001100011100011100011000011100  |
---------------------------------------+----------
 11    11111        11  111  11        | dmin= 14
```

Подчеркнутые значения (таблица 4), вычисленные по выше предложенному правилу, не попадают в ряд чисел, составляющих арифметическую прогрессию.

Таблица 4. Вычисленные значения $d^{в}_{\min}$ сегментов КМД-кодов ($k$=7)

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Длина сегмента $n$ | 7 | 18 | 27 | 35 | 42 | 48 | 54 | 60 |
| Нечетное количество серий $b_n$ | 1 | 3 | 5 | 7 | 9 | 11 | 13 | 15 |
| Вычисленное аналитически $d^{в}_{\min a}$ | 1 | $\underline{6}$ | 11 | 14 | 17 | 20 | 23 | 26 |
| Эсприментальное значение $d^{в}_{\min э}$ | 1 | 6 | 11 | 14 | 18 | 20 | 23 | 26 |
| Длина сегмента $n$ | 13 | 23 | 31 | 39 | 45 | 51 | 57 | 62 |
| Четное количество серий $b_n$ | 2 | 4 | 6 | 8 | 10 | 12 | 14 | 16 |
| Вычисленное аналитически $d^{в}_{\min a}$ | 3 | $\underline{8}$ | $\underline{12}$ | 16 | 19 | 22 | 25 | 28 |
| Эсприментальное значение $d^{в}_{\min э}$ | 3 | 8 | 12 | 16 | 19 | 21 | 24 | 27 |

*Вывод:*

1) Вычисленные значения $d_{\min}$ с использованием гипотетической последовательности в большинстве случаев совпадают с экспериментальными значениями минимального кодового расстояния, а это значит, что ее новые абстрактные свойства согласуются с предшествующим опытом вычисления верхней границы минимального кодового расстояния.

2) Вычисленные значения $d_{\min}$ сегментов КМД длиной $n$, которые вмещают целое четное или нечетное количество серий по убыванию, образуют два ряда с арифметической прогрессией с шагом $d$=3 для четного и нечетного количества серий соответственно.

$$d^{в}_{\min a} \le \begin{cases} a_0 + \dfrac{b_n+1}{2}d + \left\lceil \dfrac{b_n-4}{b_n-2} \right\rceil, a_0 = 1, d = 3, b = 3,5,7,\ldots,2^{k-3}+1; \\ a_0 + \dfrac{b_n}{2}d + \left\lceil \dfrac{b_n-6}{b_n-2} \right\rceil, a_0 = 3, d = 3, b = 4,6,8,\ldots,2^{k-3}+2. \end{cases} \qquad (7)$$

*Вывод*:

1) Графики на рисунке 5, полученные экспериментальным и аналитическим путем и описывающие верхние границы сегментов КМД на примере ПГРС при $k$=7 в точках, где длина $n$ равна сумме длин серий $М_г$-последовательности, в основном совпадают, а в некоторых точках погрешность Δ не превышает $\Delta = |d^{в}_{\min э} - d^{в}_{\min a}| \le 1$.

2) Начиная с участка $n>2^{k-1}+4$ возрастание и $d^{\text{в}}_{\min\alpha}$ по закону арифметической прогрессии, полученное с помощью выражения (7), нарушаются и расходятся с их экспериментальными значениями.

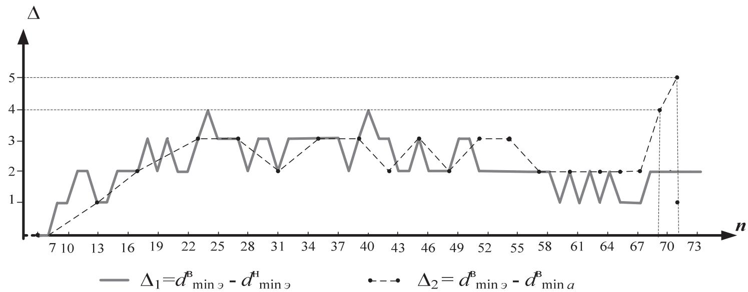


Рис. 5. Верхняя граница сегментов КМД при $k$=7, полученных экспериментальным и аналитическим способом

Экспериментальные значения $d^{\text{н}}_{\min э}$ и $d^{\text{в}}_{\min э}$получены путем полного перебора всего множества сегментов КМД (для $k$=7) на М-последовательностях, образованных ПГРС с использованием восемнадцати примитивных полиномов, и выбора для каждого сегмента длиной $n$ минимального и максимального значений соответственно.

**5. Заключение.** Применение аналитических выражений по нахождению нижней и верхней границ $d_{min}$ для сегментов КМД на М-последовательности, образованной ПГРС или МГРС для любых $k$, значительно упрощает процесс их вычисления по сравнению с машинным способом полного перебора.

Полученные аналитические выражения для некоторых блоковых длин сегментов КМД, составляющих полную сумму серий, определяют нижние и верхние границы $d_{\min}$ с минимальной погрешностью. Для остальных блоковых длин сегментов, размер которых составляет немногим больше половины длины М-последовательности, полученные значения являются ориентировочными.

Ограничение длины $n$ в полученных выражениях для применения в телекоммуникационных системах не снижает их значения, так как наибольшее практическое применение из всего возможного спектра сегментов простой возвратной М-последовательности получили коды, равные ее длине или не превышающие одной трети ее длины, часто применяемые в системах цикловой синхронизации синхронных систем передачи данных, в системах кодирования адреса корреспондента и в помехоустойчивом кодировании информации [4].

## Литература

1. *Когновицкий О.С.* Теория, методы и алгоритмы решения задач в телекоммуникациях на основе двойственного базиса и рекуррентных последовательностей. Монография // СПбГУТ. 2011.

2. *Гладких А. А.* Основы теории мягкого декодирования избыточных кодов в стирающем канале связи // Ульяновск :УлГТУ. 2010. 379 с.
3. Гребенев С. В., Дроздов И. А., Семкин С. Н. и др. Системы документальной связи: учебное пособие. В 3 ч. Ч. 1. Основы построения сетей специальной документальной связи / под. общ. ред. И. А. Дроздова // Орел.: Академия ФСО России. 2008. 196 с.
4. Радыгин В.М., Иванцов О.В., Бочков П.В. Применение полиномиальной системы классов вычетов для коррекции ошибок в системах передачи сигналов времени // Ученые записки Орловского государственного университета. Серия "Естественные, технические и медицинские науки". Орел: ФГБОУ ВПО "Орловский Государственный университет". 2013. Вып. (53). С.65–69.

## References

1. Kognovitsky O.S. *Teorija, metody i algoritmy reshenija zadach v telekommunikacijah na osnove dvojstvennogo bazisa i rekurrentnyh posledovatel'nostej. Monografija* [Theory, methods and algorithms for solving problems in telecommunications based on the dual basis and recurrent sequences. Monograph]. SUT. 2011. (In Russ.).
2. Gladkih A.A. *Osnovy teorii mjagkogo dekodirovanija izbytochnyh kodov v stirajushhem kanale svjazi* [Fundamentals of the theory of soft decoding of redundant codes in the erasing communication channel]. Ulyanovsk: Ulyanovsk State Technical University. 2010. 379 p. (In Russ.).
3. Grebenev S. V., Drozdov I. A., Semkin S. N. et al. *Sistemy dokumental'noj svjazi: uchebnoe posobie. V 3 ch. Ch. 1. Osnovy postroenija setej special'noj dokumental'noj svjazi / pod. obshh. red. I. A. Drozdova* [Systems of documentary communication: a tutorial. In 3 p. Part 1. Bases of creation of networks of special documentary communication. Edited by I. Drozdov]. Orel: Academy FSO of Russia. 2008. 196 p. (In Russ.).
4. Radygin V. M., Ivantcov O. V., Bochkov P. V. [Application of polynomial systems of residue classes for error correction in systems transmitting signals of time]. *Uchenye zapiski Orlovskogo gosudarstvennogo universiteta. Serija "Estestvennye, tehnicheskie i medicinskie nauki" – The researchers notes of Orel State University. Series"Natural, technical and medical science".* Orel: Orel State University". 2013. vol. 3(53). pp. 65–69. (In Russ.).

**Иванцов Олег Владимирович** — к-т техн. наук, доцент, сотрудник Академии ФСО России. Область научных интересов: помехоустойчивое кодирование и синхронизация линейными рекуррентными последовательностями Число научных публикаций — 65. iowwaa@mail.ru; Академия ФСО России, Приборостроительная, 35, г. Орел, 302034, РФ; р.т. (4862)549934.

**Ivantsov Oleg Vladimirovich** — Ph.D. associate professor, employee of Academy Federal Agency of protection of Russian Federation. Research interests: the antinoise coding and synchronization by linear recurring sequence. Number of scientific publications — 65. iowwaa@mail.ru; Academy of Federal Agency of protection of Russian Federation, Priborostroitelnaya Street, 35, Orel, 302034, Russia, office phone (4862)549934.

**Саитов Игорь Акрамович** — д-р техн. наук, профессор, сотрудник Академии ФСО России. Область научных интересов: анализ и синтез инфокоммуникационных сетей и систем. Число научных публикаций — 160. Akramovish@mail.ru; Академия ФСО России, Приборостроительная, 35, г. Орел, 302034, РФ; р.т. (4862)549801.

**Saitov Igor Akramovich** — Ph.D., Dr. Sci., professor, employee of Academy Federal Agency of protection of Russian Federation. Research interests: analysis and synthesis of infocommunicational networks and systems. The number of publications — 160. Akramovish@mail.ru; Academy of Federal Agency of protection of Russian Federation, Priborostroitelnaya Street, 35, Orel, 302034, Russia, office phone (4862)549801.

# РЕФЕРАТ

*Иванцов О.В., Саитов И.А.* **Границы минимального кодового расстояния для некоторой блоковой длины сегмента двоичного кода линейной рекуррентной последовательности.**

В статье рассматриваются сегменты линейных двоичных кодов максимальной длины, в качестве которых выступают участки разной блоковой длины, выделяемые на семействе линейных рекуррентных последовательностей, образованных по закону примитивных полиномов. Доказывается, что нижняя и верхняя границы минимального кодового расстояния зависят от количества полных серий гипотетической М-последовательности (начиная с серий максимальной длины k), помещающихся на участке длиной k ≤n≤ 2k-1+4.

Статья состоит из частей: 1)Введение 2) Анализ закономерностей влияния вида образующего полинома на минимальное кодовое расстояние сегмента двоичного кода ЛРП 3) Математическое описание вычислительного эксперимента по определению нижней границы $d_{\min}^{\text{н}}$ для некоторых длин сегментов КМД 4) Математическое описание вычислительного эксперимента по определению аналитического выражения верхней границы $d_{\min}^{\text{в}}$ для некоторых длин сегментов КМД 5) Заключение. Во введении указывается пути повышения, наличие некоторых теоретических проблем по вычислению минимального кодового расстояния для сегментов ЛРП, актуальность наличия быстрого и простого способа вычисления. Во второй части проводится анализ влияния вида и размерности образующего полинома на минимальное кодовое расстояние сегмента двоичного кода ЛРП. Выявленные закономерности определили необходимость применения в вычислительной системе гипотетической ЛРП. В третьей и четвертой частях авторами проведены вычислительные эксперименты по определению нижней и верхней границ соответственно с использованием гипотетической $М_г$-последовательности. Проведен сравнительный анализ полученных значений границ минимального кодового расстояния с машинным способом вычислений. Пятая часть ставит вопрос о возможности применения результатов быстрого вычисления при проектировании систем помехоустойчивого кодирования и синхронизации.

## SUMMARY


*Ivantsov O.B., Saitov I.A.* **Minimum distance border for random block length binary code segment of linear recurring sequence.**

The article considers the segments maximum length linear binary codes, such as different sections of the block length allocated on the family of linear recurring sequences, formed under the law of primitive polynomials. It is proved that the lower and upper bounds of the minimum distance of the code depends on the hypothetical M-sequence full series number (starting with a series of maximum length *k*), locate on the k ≤n≤ 2k-1 + 4 length.

The paper consists of parts: 1) Introduction 2) Analysis of the influence the forming polynomial type on the minimum binary LRS code segment distance 3) The mathematical description of the computational experiment to determine the lower border $d_{\min}^{\text{н}}$ for some segment lengths MLC 4) The mathematical description of the computational experiment to determine the upper border analytical expression $d_{\min}^{\text{в}}$ for some segment lengths MLC 5) Conclusion. The introduction indicates ways to improve some theoretical problems in a minimum distance calculating for the LRS code segment and showing availability a quick and easy calculating way. The second part is showing the impact analyzes of the form and the influence the forming polynomial type on the minimum binary LRS code segment distance. The revealed regularities identified the need to applying a hypothetical LRS in a computer system. In the third and fourth parts the authors carried out the computational experiments, to determine, lower and upper bounds, using a hypothetical $M_r$-sequence. A comparative analysis the obtained values of the minimum code distance boundaries with machine method is carried. The fifth part examines the opportunity of fast evaluation of the results of in antinoise coding and synchronize systems on design.