Анализ линейной зависимости k-элементных сочетаний в псевдослучайной последовательности максимальной длины $n = 2^k - 1$

Analysis of Linear Dependence of k-element Combinations in a Pseudorandom Sequence of Maximum Length $n = 2^k - 1$

Когновицкий / Kognovitsky O.
Олег Станиславович
(kognovickiyo@spbgut.ru)
доктор технических наук, профессор,
заслуженный работник высшей школы РФ.
ФГБОУ ВО «Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М. А. Бонч-Бруевича» (СПбГУТ),
почетный профессор.
г. Санкт-Петербург

Владимиров / Vladimirov S.
Сергей Сергеевич
(vladimirov.opds@gmail.com)
кандидат технических наук.
СПбГУТ,
доцент кафедры сетей связи и передачи данных.
г. Санкт-Петербург

Ключевые слова: последовательность максимальной длины – maximum length sequence; М-последовательность – M-sequence; код Хэмминга – Hamming code; линейно-зависимые сочетания– linearly dependent combinations; мажоритарное декодирование – majority decoding; пересечение кодовых слов – intersection of code words.

Статья знакомит с последними результатами научных исследований авторов в рамках научной работы по изучению свойств псевдослучайных последовательностей максимальной длины (ПМД) и дуальных им циклических кодов. В работе проанализирована линейная зависимость k-элементных сочетаний в последовательности максимальной длины и показаны результаты моделирования на примере ПМД с периодом 31, уточняющие ранее вычисленные приблизительные значения. На основе результатов моделирования проведен анализ кодовых слов кода Хэмминга на примере кода (31, 26), дуального исследуемой ПМД, в рамках которого получены два новых свойства, касающихся распределения числа единичных элементов в кодовых словах кода Хэмминга, и дана оценка числа пересечений кодовых слов кода Хэмминга в единичных элементах, что позволило более точно определить число линейно-зависимых k-элементных сочетаний в ПМД с периодом 31.

The paper introduces results of the latest results of studies made by authors in the framework of scientific research of properties of the pseudorandom maximum length sequence (MLS) and their dual cyclic codes. In the paper linear dependence of k-element combinations in the sequence of maximum length was analyzed and the simulation results are shown on the example of MLS with a period of 31, specifying previously calculated approximate values. On the basis of simulation results, analysis of Hamming code words was conducted through the example of code (31, 26), dual to the MLS being studied, within the framework of which two new properties were obtained concerning distribution of unit elements in the code words of the number of unit cells in code words of the Hamming code, and was evaluated number of crossings of the Hamming code words in the unit elements, which allowed to more accurately determine number of linearly dependent k-element combinations in the MLS with period of 31.

При декодировании эквидистантных кодов, построенных на основе псевдослучайных последовательностей максимальной длины (ПМД, М-последовательностей), используется метод мажоритарного декодирования, в котором значение информационных элементов кодового слова вычисляется по начальной фазе ПМД. Начальная фаза вычисляется по любым k линейно-независимым элементам ПМД [1, 2, 3, 4]. Важной задачей при этом является поиск всех возможных линейно-независимых k-элементных сочетаний, по которым организуется мажоритарное декодирование.

Для решения этой задачи ранее был предложен аналитический способ [1, 2, 4]. В данном способе ПМД $\{\mathbf{s}\}=\{s_0,\ s_1,\ s_2,\ \ldots,\ s_{M-1}\}$ периода M над полем GF(p) рассматривается как многочлен

$$S(x)=s_0+s_1x+\ldots+s_{M-1}x^{M-1}, \qquad (1)$$

который может быть представлен, как формальный степенной ряд $\Phi(x)$ над полем GF(p) с коэффициентами $s_0,\ s_1,\ s_2,\ \ldots$ (2) [1]:

$$\Phi(x)=s_0+s_1x+\ldots+s_{M-1}x^{M-1}+0\cdot x^M+0\cdot x^{M+1}+\ldots. \qquad (2)$$

Произвольные k членов многочлена (2) могут быть записаны как многочлен

$$U(x)=s_{j_1}x^{j_1}+s_{j_2}x^{j_2}+\ldots+s_{j_k}x^{j_k}. \qquad (3)$$

Выборка из k элементов $s_{j_1}, s_{j_2}, \ldots, s_{j_k}$ линейной рекуррентной последовательности $\{\mathbf{s}\}$ будет линейно-зависимой в том случае, если среди ненулевых элементов многочлена (3) найдутся такие, что их совокупность будет представлять собой ненулевой многочлен $\varphi_1(x)$ сравнимый с нулем по модулю характеристического многочлена $p(x)$ степени k [1]. Такую выборку из k элементов удобно представлять в виде так называемой «маски», в которой k позиций $j_1, j_2, \ldots, j_k$ в ПМД с элементами $s_{j_1}, s_{j_2}, \ldots, s_{j_k}$ помечены знаком «X». Ниже приведен пример маски для позиций $j_1 = 2$, $j_2 = 4$, $j_3 = 5$, $j_4 = 12$ и $j_5 = 19$, т.е. для k-элементного сочетания s_2, s_4, s_5, s_{12}, s_{19} из ПМД длиной $n = 31$ [2]:

00X0XX000000X000000X00000000000

Так как многочлен $\varphi_1(x)$ делится без остатка на многочлен $p(x)$, то он будет соответствовать определенной разрешенной кодовой комбинации циклического кода Хэмминга, дуального ПМД [1, 5, 6]. Или, если упрощенно, знаком «X» отмечены позиции элементов k-элементного линейно-зависимого сочетания, которым будут соответствовать единичные элементы в кодовом слове кода Хэмминга, дуального ПМД. Поэтому для определения количества линейно-зависимых k-элементных сочетаний из элементов ПМД достаточно найти весовой спектр дуального ей кода Хэмминга [1].

Для двоичных циклических кодов с длиной комбинации $n = 2^k - 1$ число $A(\omega)$ кодовых слов с весом ω можно найти как коэффициент при z^ω в разложении по степеням z выражения (4) [5, 7, 8].

$$f(z)=\frac{1}{n+1}\left\{(1+z)^n+n(1+z)^{\frac{n-1}{2}}(1-z)^{\frac{n+1}{2}}\right\}. \qquad (4)$$

Число k-элементных линейно зависимых сочетаний в общем виде может быть определено выражением (5):

$$A=\sum_{\omega=\omega_{\min}}^{k} C_{n-\omega}^{k-\omega}A(\omega), \quad n=2^k-1. \qquad (5)$$

Соответственно, общее число линейно-независимых k-элементных сочетаний элементов ПМД вычисляется по формуле (6).

$$B=C_n^k-A=C_n^k-\sum_{\omega=\omega_{\min}}^{k} C_{n-\omega}^{k-\omega}A(\omega). \qquad (6)$$

Вычисления по данному методу для ПМД с периодом 15 и ПМД с периодом 31 показали, что общее число k-элементных линейно-независимых сочетаний для ПМД с периодом 15 равно $B_{15} = 840$, а для ПМД с периодом 31 – $B_{31} = 76818$ [2].

Другим вариантом определения числа линейно-независимых k-элементных сочетаний является метод моделирования, который заключается в том, что каждое k-элементное сочетание $s_{j_1}, s_{j_2}, \ldots, s_{j_k}$ проверяется на линейную независимость.

Для этого необходимо построить соответствующую этому k-элементному сочетанию матрицу Θ [1, 2] и определить, является ли она линейно-независимой, рассчитав соответствующий ей определитель $\Delta = |\Theta|$. Для линейно-независимой матрицы определитель будет отличен от нуля [9, 10].

Проведенное моделирование показало, что общее число линейно-независимых k-элементных сочетаний для ПМД с периодом 15 равно $B_{15\,\text{мод.}} = 840$, а для ПМД с периодом 31 – $B_{31\,\text{мод.}} = 83328$.

Из сравнения результатов, полученных моделированием, с результатом вычислений по формуле (6), видно, что эти результаты для ПМД с периодом 15 совпадают $B_{15\,\text{мод.}} = B_{15}$, а для ПМД с периодом 31 результаты отличаются, т.е. $B_{31\,\text{мод.}} \neq B_{31}$, количественное расхождение равно

$$\Delta B_{31} = 83328 - 76818 = 6510. \qquad (7)$$

Целью данной статьи является поиск причин данного расхождения и определение аналитических зависимостей, позволяющих определить это расхождение. Начнем с объяснения причин расхождения для случая $n = 31$.

Как было показано ранее, линейно-зависимыми будут те k-элементные сочетания, позиции которых совпадают с единичными элементами в кодовых словах веса 3, 4 и 5 кода Хэмминга, дуального рассматриваемой ПМД. Следовательно, для рассматриваемой ПМД длиной 31 при $k = 5$ линейно-зависимыми будут комбинации, позиции которых X_i:

– совпадают с кодовым словом кода Хэмминга веса 5, например

00$\boldsymbol{X_1}$0$\boldsymbol{X_2}\boldsymbol{X_3}000000\boldsymbol{X_4}000000\boldsymbol{X_5}$00000000000 – маска k-элементного сочетания в ПМД;

00**1**0**11**000000**1**000000**1**00000000000 – кодовое слово кода Хэмминга веса 5;

– либо содержат в себе кодовое слово кода Хэмминга веса 4 и еще один (любой) бит, например

00$\boldsymbol{X_1}$00$\boldsymbol{X_2}$000000$\boldsymbol{X_3}$000$\boldsymbol{X_4}$0000000$X_5$000000 – маска k-элементного сочетания в ПМД;

00**1**00**1**000000**1**000**1**00000000000000 – кодовое слово кода Хэмминга веса 4;

– либо содержат в себе кодовое слово кода Хэмминга веса 3 и еще два (любых) бита, например

00$\boldsymbol{X_1}$00$\boldsymbol{X_2}$0000000$X_3$000$X_4$00000$\boldsymbol{X_5}$0000000 – маска k-элементного сочетания в ПМД;

00**1**00**1**0000000000000000000**1**0000000 – кодовое слово веса 3.

Формула (5) объединяет в себе все эти варианты, при этом некоторые линейно-зависимые k-элементные сочетания будут учитываться несколько раз. Из-за этого и возникает расхождение между результатами вычисления по формуле (6) и результатами моделирования.

Поясним это на конкретных примерах.

Допустим, существуют два кодовых слова кода Хэмминга веса 3, которые пересекаются между собой в одной «единице». Например,

0000000000000**1**0001000001000000000 – кодовое слово 1 веса 3;

0010000010000**1**00000000000000000000 – кодовое слово 2 веса 3.

При этом получается, что одна маска k-элементного сочетания в ПМД, например

$00X_1 00000X_2 0000X_3 000X_4 00000X_5 0000000$ охватывает две линейно-зависимых комбинации, т.е. и первое и второе кодовые слова. Следовательно, каждое из этих кодовых слов учитывается в формуле (5) дважды.

Количество таких повторений будет равно числу пар различных кодовых слов кода Хэмминга веса 3, пересекающихся в одной общей для них единичной позиции. Для приведенного выше примера это будет позиция X_3 в маске.

Обозначим это число повторений функцией $Cr(w_1,w_2,l_{пер})$, где w_1 – вес кодового слова 1; w_2 – вес кодового слова 2; $l_{пер}$ – число общих единичных позиций для каждой пары кодовых слов. Тогда для рассматриваемого выше случая число пересекающихся пар кодовых слов веса $w = 3$ будет обозначаться как $Cr\{3,3,1\}$.

Аналогичная ситуация возникает в том случае, когда кодовое слово кода Хэмминга веса 4 и кодовое слово кода Хэмминга веса 3 пересекаются в двух «единицах». Например,

0000000000000**1**000**1**0000010000000 – кодовое слово веса 3;

0010000010000**1**000**1**00000000000000 – кодовое слово веса 4.

При этом получается, что маска k-элементного сочетания в ПМД с линейно-зависимыми позициями, равная

$00X_1 00000X_2 0000X_3 000X_4 00000X_5 0000000$, соответствует и одному, и другому кодовому слову, а значит, эта ситуация также учитывается в формуле (5) дважды.

Количество таких дублирований соответствует числу пар кодовых слов кода Хэмминга веса 4 и веса 3, пересекающихся в двух «единицах» ($l_{пер} = 2$). Для приведенного выше примера это позиции X_3 и X_4 маски. Обозначим это число как $Cr(4,3,2)$.

Казалось бы, аналогичной была бы ситуация при пересечении двух кодовых слов кода Хэмминга веса 4 в трех «единицах», однако такое пересечение невозможно, поскольку в этом случае кодовое расстояние между этими кодовыми словами было бы равно двум, что не совпадает с минимальным кодовым расстоянием кода Хэмминга d_{min} равным трем.

В то же время возможна ситуация, когда происходит одновременное пересечение комбинации веса 4 и двух комбинаций веса 3. Причем последние между собой пересекаются в одной «единице» ($l_{пер} = 1$), а с комбинацией веса 4 пересекаются в двух «единицах» ($l_{пер} = 2$) каждая. Например,

0000000000000**1**000**1**0000010000000 – кодовое слово A_1 веса 3;

00000100**1**00000**1**00000000000000000000 – кодовое слово A_2 веса 3;

00100000**1**00000**1**000**1**00000000000000 – кодовое слово A_3 веса 4.

При этом получается, что маска линейно-зависимого k-элементного сочетания в ПМД, равная

$00X_1 00000X_2 0000X_3 000X_4 00000X_5 0000000$,

соответствует сразу трем кодовым словам и, следовательно, в числе $Cr(4,3,2)$ учитывается дважды. То есть учитывается и пересечение слова A_3 весом 4 со словом A_1 веса 3, и пересечение того же слова A_3 веса 4 с другим словом A_2 веса 3, при том, что слова веса 3 A_1 и A_2 пересекаются между собой в одном разряде.

Обозначим это число пересечений как $Cr\{(A_1 \cap A_2)_{l=1}$ И $(A_1 \cap A_3)_{l=2}$ И $(A_2 \cap A_3)_{l=2}\}$.

Исходя из свойства линейного кода, согласно которому сумма двух кодовых слов по модулю 2 также является кодовым словом, следует, что любое пересечение двух слов веса 3 в одном разряде $Cr(3,3,1)$, будет автоматически давать вышеописанную ситуацию $Cr\{(A_1 \cap A_2)_{l=1}$ И $(A_1 \cap A_3)_{l=2}$ И $(A_2 \cap A_3)_{l=2}\}$, поскольку сумма по модулю 2 этих кодовых слов весом 3 как раз даст кодовое слово веса 4. Таким образом,

$$Cr\{(A_1 \cap A_2)_{l=1} \text{ И } (A_1 \cap A_3)_{l=2} \text{ И } (A_2 \cap A_3)_{l=2}\} \equiv Cr(3,3,1). \quad (8)$$

Учитывая изложенное выше, можно записать формулу (9), которая показывает, насколько (ΔA_{31}) рассчитываемое по формуле (5) число k-элементных линейно-зависимых комбинаций больше реального (или, что тоже самое, насколько (ΔB_{31}) рассчитываемое по формуле (6) число k-элементных линейно-независимых комбинаций меньше реального), имеет вид

$$\Delta A_{31} = \Delta B_{31} = Cr(3,3,1) + Cr(4,3,2) - Cr\{(A_1 \cap A_2)_{l=1} \text{ И } (A_1 \cap A_3)_{l=2} \text{ И } (A_2 \cap A_3)_{l=2}\} \quad (9)$$

или, с учетом равенства (8),

$$\Delta A_{31} = \Delta B_{31} = Cr(4,3,2). \quad (10)$$

Для того чтобы определить число пар различных кодовых слов, пересекающихся в l «единицах» $Cr(w_1, w_2, l)$, был проведен перебор всех кодовых слов кода Хэмминга (31, 26) соответствующих весов. Полученные числа пересечений кодовых слов приведены в табл. 1.

Как следует из полученных результатов, приведенное в табл. 1 число пар пересекающихся кодовых слов $Cr(4,3,2)$ совпадает с приведенным в формуле

Таблица 1

Число попарных различных кодовых слов весов 3, 4 и 5, пересекающихся в l «единицах», полученное методом моделирования

Cr(5,4,1)	2343600	*Cr*(5,3,1)	286440	*Cr*(4,3,1)	52080	*Cr*(3,3,1)	3255
Cr(5,4,2)	572880	*Cr*(5,3,2)	52080	***Cr*(4,3,2)**	**6510**	*Cr*(3,3,2)	0
Cr(5,4,3)	52080	*Cr*(5,3,3)	0	*Cr*(4,3,3)	0		
Cr(5,4,4)							

Таблица 2

Распределение «единиц» в кодовых словах кода Хэмминга (31, 26) веса 3, 4 и 5

Вес	Разряд						
w_i	1	2	3	4	…	30	31
3	15	15	15	15	…	15	15
4	140	140	140	140	…	140	140
5	840	840	840	840	…	840	840

Таблица 3

Распределение «единиц» во всех кодовых словах кода Хэмминга (31, 26) веса 3, 4 и 5, которые пересекаются в первом разряде длины кода

Вес	Разряд						
w_i	1	2	3	4	…	30	31
3	15	1	1	1	…	1	1
4	140	14	14	14	…	14	14
5	840	112	112	112	…	112	112

(7) значением ΔB_{31}, что подтверждает правильность формулы (10).

Число пересекающихся пар в «единицах» $Cr\{(A_1 \cap A_2)_{l=1}$ И $(A_1 \cap A_3)_{l=2}$ И $(A_2 \cap A_3)_{l=2}\}$, также полученное моделированием, равно $Cr(3,3,1) = 3255$, что соответствует равенству (8).

Следовательно, чтобы определить аналитическую зависимость для ΔB_{31}, необходимо найти аналитическое выражение для определения числа пар пересекающихся кодовых слов $Cr(4,3,2)$.

Для этого приведем ряд свойств кодовых слов кода Хэмминга (31, 26), полученных методом моделирования.

Для определения линейно-зависимых комбинаций в ПМД длиной $n = 31$ над полем степени $k = 5$, как показано выше, используются только кодовые слова кода Хэмминга (31, 26) весом $w \le k$=5, т.е. слова весом 3, 4 и 5. Количество таких слов для рассматриваемого кода (31, 26) и ПМД длиной $n = 31$ равно [2]

$$A(3) = 155;$$
$$A(4) = 1085;$$
$$A(5) = 5208.$$

Далее рассмотрим, как распределены по разрядам «единицы» в этих кодовых словах. Если поразрядно просуммировать «единицы» во всех кодовых словах каждого веса, то получится, что они распределены равномерно по всей длине кода, равной 31, как показано в табл. 2.

Таким образом получается, что в каждом разряде длины кода пересекаются по 15 слов веса 3, по 140 слов веса 4 и по 840 слов веса 5.

Теперь рассмотрим только слова, пересекающиеся в i-м $(1 \le i \le 31)$ разряде длины кода, например в первом. Их оставшиеся «единицы» распределены равномерно по всей оставшейся длине кода, как показано в табл. 3.

Таблица 4

Максимально допустимые числа пересечений l кодовых слов кода Хэмминга в «единицах» для слов веса 3, 4 и 5

w	3	4	5
3	1	2	2
4	2	2	3
5	2	3	3

Распределение для слов, пересекающихся в других разрядах, полностью аналогично.

Данные табл. 2 и 3 получены путем моделирования на компьютере. Однако вызывают интерес аналитические выражения, которые бы подтвердили полученные результаты.

Определим выражение для подсчета верхней границы числа пересечений l кодовых слов в «единицах». Исходя из того, что минимальное кодовое расстояние кода Хэмминга известно и всегда равно $d_{\min} = 3$, число пересечений l между кодовыми словами кода Хэмминга веса w_1 и w_2 должно подчиняться неравенству (11):

$$w_1 + w_2 - 2l \geq d_{\min} \;\Rightarrow\; \frac{w_1 + w_2 - d_{\min}}{2} \geq l\,. \qquad (11)$$

Максимально допустимые значения числа пересечений l кодовых слов кода Хэмминга в «единицах» для слов веса 3, 4 и 5 представлены в табл. 4.

Можно видеть, что результат расчета совпадает с результатами моделирования, представленными в табл. 1.

Далее найдем выражение для определения суммарного числа «единиц» всех кодовых слов одного веса, приходящихся на один разряд длины кода, с учётом равномерного распределения «единиц» кодовых слов по длине кода, которое было определено при моделировании и показано в табл. 2.

Всего имеется $A(w)$ кодовых слов кода Хэмминга веса w, т. е. слов, содержащих w «единиц». Эти «единицы» равномерно распределены по длине кода n (табл. 2). Таким образом, суммарное число «единиц» кодовых слов одного веса w, приходящихся на один разряд длины кода n, рассчитывается по формуле (12).

$$o(w) = \frac{w \cdot A(w)}{n}\,. \qquad (12)$$

Соответственно, для слов веса 3, 4 и 5 получим

$$o(3) = \frac{3 \cdot A(3)}{31} = \frac{3 \cdot 155}{31} = 15,$$
$$o(4) = \frac{4 \cdot A(4)}{31} = \frac{4 \cdot 1085}{31} = 140,$$
$$o(5) = \frac{5 \cdot A(5)}{31} = \frac{5 \cdot 5208}{31} = 840,$$

что соответствует результатам моделирования, приведенным в табл. 2.

Таким образом, с учетом данных моделирования, можно сформулировать следующее свойство кода Хэмминга, дуального ПМД.

Свойство 1. В коде Хэмминга, дуальном ПМД, «единицы» в кодовых словах одного w распределены равномерно, а количество таких «единиц» $o(w)$, приходящихся на один разряд длины кода n, может быть рассчитано по формуле (12).

Теперь перейдем к анализу табл. 3. Возьмем кодовые слова, пересекающиеся в одном разряде длины кода, например в первом. Как было показано проведенным моделированием (табл. 3), их оставшиеся «единицы» распределены равномерно по всей оставшейся длине кода. В этом случае для определения суммарного числа «единиц», приходящихся на один разряд оставшейся длины кода, можно использовать формулу (13):

$$o_1(w) = \frac{o(w) \cdot (w-1)}{n-1}\,. \qquad (13)$$

Таким образом, для слов веса 3, 4 и 5 по формуле (13) получим

$$o_1(3) = \frac{o(3) \cdot (3-1)}{31-1} = \frac{15 \cdot 2}{30} = 1,$$
$$o_1(4) = \frac{o(4) \cdot (4-1)}{31-1} = \frac{140 \cdot 3}{30} = 14,$$
$$o_1(5) = \frac{o(5) \cdot (5-1)}{31-1} = \frac{840 \cdot 4}{30} = 112,$$

что соответствует результатам моделирования, приведенным в табл. 3. Следовательно, можно сформулировать второе свойство кода Хэмминга, дуального ПМД.

Свойство 2. В коде Хэмминга, дуальном ПМД, оставшиеся «единицы» в кодовых словах веса w, пересекающихся в одном разряде длины кода, распределены равномерно, а количество таких «единиц» $o_1(w)$, приходящихся на один разряд оставшейся длины кода $n - 1$, может быть рассчитано по формуле (13).

Определим теперь количество пересечений в «единицах» $Cr(3,3,1)$ кодовых слов веса $w = 3$. Согласно табл. 1, табл. 4 и неравенству (11), слова веса 3 могут пересекаться только в одном разряде. Следовательно,

исходя из табл. 2 и свойства 1, в каждом единичном разряде слово веса $w = 3$ пересекается с 14 другими словами веса $w = 3$. Число таких пересечений $Cr(3,3,1)$ будет равно

$$Cr(3,3,1) = \frac{3 \cdot \left[o(3) - 1\right] \cdot A(3)}{2} = \frac{3 \cdot 14 \cdot 155}{2} = 3255,$$

что подтверждается результатом моделирования, приведенным в табл. 1. Деление на два производится для того, чтобы скомпенсировать удвоение числа пересечений, возникающее из-за учета как прямых ($K_1 \cap K_2$), так и обратных ($K_2 \cap K_1$) пересечений.

Далее определим общее число $Cr(4,3)$ пересекающихся в «единицах» пар кодовых слов веса 3 и слов веса 4. Во-первых, учитывая данные из табл. 2, определим полное число парных пересечений в «единицах» как

$$Cr(4,3) = o(4) \cdot o(3) \cdot n = 140 \cdot 15 \cdot 31 = 65100.$$

Поскольку, согласно неравенству (11), слова веса 3 и слова веса 4 могут пересекаться только в одной или в двух «единицах», составим уравнение (14).

$$Cr(4,3,1) + 2 \cdot Cr(4,3,2) = Cr(4,3), \qquad (14)$$

т.е. $Cr(4,3,1) + 2 \cdot Cr(4,3,2) = 65100$.

Теперь определим количество пар кодовых слов веса 3 и 4, пересекающихся в двух «единицах». Для этого воспользуемся табл. 3 и свойством 2. Возьмем слова веса 3 и слова веса 4, пересекающиеся в одном разряде длины кода. Выберем произвольный разряд из оставшихся. Очевидно, что в любых двух разрядах длины кода пересекаются $o_1(3) = 1$ слово веса 3 и $o_1(4) = 14$ слов веса 4. Следовательно, общее число пар кодовых слов веса 3 и 4, пересекающихся в двух «единицах», равно

$$Cr(4,3,2) = o_1(4) \cdot o_1(3) \cdot C_n^2 = 14 \cdot 1 \cdot C_{31}^2 = 6510,$$

что совпадает с результатом моделирования, приведенным в табл. 1.

Далее найдем выражение для определения числа пар кодовых слов веса 3 и 4, пересекающихся в одной «единице». Обратимся к табл. 3 и свойствам 1 и 2. Возьмем слова веса 3 и слова веса 4, пересекающиеся в одном разряде длины кода (выбранный разряд зафиксируем). Из этих слов необходимо исключить те, которые пересекаются в двух разрядах. Для этого рассмотрим одно слово веса 3. В каждом из двух оставшихся разрядов оно пересекается с $o_1(4) = 14$ словами веса 4 из $o(4) = 140$ слов, с которыми пересекается в зафиксированном разряде. Таким образом, общее число пересечений слов веса 3 и 4 в одной «единице» равно

$$Cr(4,3,1) = o(3)\left(o(4) - 2 \cdot o_1(4)\right)C_n^1 = \\ = 15 \cdot (140 - 2 \cdot 14)C_{31}^1 = 52080. \qquad (15)$$

Аналогично можно рассмотреть одно слово веса 4. В каждом из трех оставшихся разрядов оно пересекается с $o_1(3) = 1$ словом веса 3 из $o(3) = 15$ слов, с которыми пересекается в зафиксированном разряде. Таким образом, общее число пересечений слов веса 3 и 4 в одной «единице» равно

$$Cr(4,3,1) = o(4)\left(o(3) - 3 \cdot o_1(3)\right)C_n^1 = \\ = 140 \cdot (15 - 3 \cdot 1)C_{31}^1 = 52080. \qquad (16)$$

Как видно, оба выражения (15) и (16) дают один и тот же результат, совпадающий с результатом моделирования, приведенным в табл. 1. К тому же полученные результаты $Cr(4,3,1)$ и $Cr(4,3,2)$ соответствуют приведенному выше уравнению (14).

Таким образом, итоговое выражение для величины расхождения $\Delta A_{31} = \Delta B_{31}$ будет иметь вид:

$$\Delta A_{31} = \Delta B_{31} = Cr(4,3,2) = o_1(4) \cdot o_1(3) \cdot C_n^2. \qquad (17)$$

В результате работы были проанализированы кодовые слова кода Хэмминга, дуального ПМД, на примере кода (31, 26) и ПМД длиной $n = 31$. По результатам анализа сформулированы два новых свойства, которые были подтверждены моделированием и расчетами как для рассмотренного в примере кода, так и для кодов Хэмминга (15, 11) и (63, 57), дуальных ПМД длиной 15 и 63, соответственно.

Также на основании сформулированных свойств была выведена формула (17) для определения величины расхождения $\Delta A_{31} = \Delta B_{31}$ между количеством линейно-независимых комбинаций, полученным ранее представленным [1, 2] аналитическим расчетом, и количеством таких комбинаций, полученным методом моделирования, что позволяет уточнить ранее предложенную формулу (5).

Однако необходимо отметить, что выведенная формула (17) является частным случаем, верным для ПМД длиной $n = 31$ и дуального ей кода Хэмминга (31, 26). Вопрос определения формул для определения величины расхождения в случае ПМД длиной 63, и тем более общей формулы, пока остается открытым.

Уточненное значение количества линейно-независимых k-элементных комбинаций может быть использовано для более точной оценки качества мажоритарного декодирования эквидистантных кодов максимальной длины как в случае канала с ошибками, так и для канала со стираниями, на основе принципов, изложенных в работах [1–4], результаты которых были получены путем моделирования.

Литература

1. Когновицкий, О. С. Двойственный базис и его применение в телекоммуникациях / О.С. Когновицкий. – СПб. : Линк, 2009. – 424 с.

2. Владимиров, С. С. Моделирование процессов мажоритарного декодирования комбинации эквидистантного кода по К линейно-независимым элементам / С.С. Владимиров // Научно-технические ведомости СПбГПУ. Серия «Информатика. Телекоммуникации. Управление». – 2010. – № 3 (101). – С. 149–156.

3. Владимиров, С. С. Эффективность мажоритарного декодирования кода максимальной длины по k-элементным линейно-независимым комбинациям в двоичном симметричном канале / С.С. Владимиров // Информационные технологии и телекоммуникации. – 2015. – № 4 (12). – С. 108–119.

4. Владимиров, С. С. Исследование алгоритма мажоритарного декодирования комбинации эквидистантного кода по k линейно-независимым элементам / С.С. Владимиров // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IV Международная научно-техническая и научно-методическая конференция: сборник научных статей в 2 томах. Т. 1. – СПб. : Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2015. – С. 281–285.

5. Кларк, Д. К. Кодирование и исправление ошибок в системах цифровой связи. Статистическая теория связи / Д.К. Кларк, Д.Б. Кейн. – М. : «Радио и Связь», 1987. – 392 с.

6. Передача дискретных сообщений. Учебник для вузов / В.П. Шувалов [и др.] ; под ред. В.П. Шувалова. – М. : Радио и связь, 1990. – 464 с.

7. Теория электрической связи: Учебник для вузов / А.Г. Зюко [и др.] ; под ред. Д.Д. Кловского. – М. : Радио и связь, 1999. – 432 с.

8. Питерсон, У. Коды, исправляющие ошибки / У. Питерсон, Э. Уэлдон ; пер с англ. Л.Е. Филипповой. – М.: Мир, 1976. – 593.

9. Фаддеев, Д. К. Лекции по алгебре: Учебное пособие для вузов / Д.К. Фаддеев. – М. : Наука. Главная редакция физико-математической литературы, 1984. – 416 с.

10. Иберла, К. Факторный анализ / К. Иберла ; пер. с нем. В.М. Ивановой. – М.: Статистика, 1980. – 398 с.