Информационные процессы, Том 16, № 1, 2016, стр. 41–60

ТЕОРИЯ И МЕТОДЫ ОБРАБОТКИ ИНФОРМАЦИИ

Построение и анализ кодов с расстоянием 4 и 6, минимизирующих вероятность ошибки декодера [1]

В.Б. Афанасьев, А.А. Давыдов, Д.К. Зигангиров

Институт проблем передачи информации, Российская академия наук, Москва, Россия

Поступила в редколлегию 10.03.2016

Аннотация—Рассмотрена задача минимизации вероятности ошибки декодера укороченных кодов размерности 2^m с расстоянием 4 и 6. Доказано, что укороченные коды Панченко с расстоянием 4 обеспечивают наименьшую вероятность ошибки декодирования при правильном укорочении. Тем самым показано, что коды Хэмминга не являются лучшими. В работе определены правила укорочения кодов Панченко и разработан комбинаторный метод минимизации числа слов веса 4 и 5. Для кодов $[39, 32, 4]$ и $[72, 64, 4]$ получены точные нижние границы вероятности ошибки декодера и получено полное решение задачи минимизации вероятности ошибки декодера.

Для укороченных кодов БЧХ с расстоянием 6 выведены верхние и нижние границы числа кодовых слов минимального веса. Построены $[45, 32, 4]$ и $[79, 64, 4]$ коды, у которых число слов веса 6 близко к нижней границе и вычислены значения вероятности ошибки декодера. Результаты ориентированы на применение в устройствах памяти.

КЛЮЧЕВЫЕ СЛОВА: двоичный код, вероятность ошибки декодера, спектр весов кода.

1. ВВЕДЕНИЕ

Особенностью устройств памяти большой и очень большой емкости является постепенная деградация (монотонное ухудшение) их функциональных характеристик. Необратимая деградация ячеек связана с деградацией (истощением) материала изолирующих и проводящих микроструктур. Например, в ячейке емкостного типа при многократном выполнении циклов чтения - записи может размываться ее заряд, соответствующий двоичному (или многозначному) состоянию. Логическое состояние ячейки восстанавливается при записи, однако восстановленное физическое состояние может отличаться от эталона, что приводит к постепенному росту вероятности ошибки.

В статье рассматривается задача построения наилучшего кода для исправления одной и двух ошибок в оперативной памяти вычислительных систем. Оперативная память не предназначена для длительного хранения данных и обладает максимальной скоростью изменения данных. По существу, каждая вычислительная операция завершается записью результата в оперативную память. В этих условиях ошибки не успевают накапливаться, и задачей кодирования является исправление редких ошибок, возникающих из-за импульсных помех (эффектов) в процессах записи или считывания состояния ячеек памяти. Типичная структура оперативной памяти связана со словом стандартной длины 32, 64, 128, 256 бит, к которым добавляется несколько проверочных разрядов, обеспечивающих исправление одной (или двух) ошибок и обнаружение максимально возможного количества комбинаций ошибок большего веса. Использование корректирующих кодов в оперативной памяти рассмотрено во многих работах, например, в [1–3]. Отметим, что именно коды с расстоянием 4 и 6 широко используются в оперативной памяти.

[1] Работа выполнена в ИППИ РАН за счет гранта Российского научного фонда (проект № 14-50-00150)

Вероятность ошибки декодера зависит от спектра весов кода. Асимптотические оценки спектра линейных кодов рассматривались в ряде работ, например, в [4–6]. Точные значения для отдельных весов в неукороченных линейных кодах и полный спектр неукороченного кода Хэмминга рассматривались, например, в [7–9]. Алгоритмы для вычисления полного спектра весов неукороченных циклических кодов предложены в работе [10], где даны значения малых весов для кодов БЧХ длины 63 и 127.

В данной статье, рассматриваются *точные значения* весов в *укороченных* кодах.

Рассматриваются два класса кодов: коды Панченко с расстоянием 4 и коды Боуза-Чоудхури-Хоквингема (БЧХ) с расстоянием 6. Про неукороченный код Панченко известно только, что он имеет наименьшее число слов веса 4 по сравнению с другими кодами, см. [11, 12]. Код БЧХ представляет интерес, так как его алгоритмы декодирования хорошо разработаны [7–9, 13]. Для этих кодов нерешенными до настоящего времени оставались комбинаторные задачи минимизации числа кодовых слов малого веса (4, 5, 6), определяющих, по существу, вероятность ошибки декодера.

Статья посвящена задаче минимизации вероятности ошибки декодера для укороченных кодов размерности 2^m. Формулируются правила укорочения кодов, выводятся оценки спектра весов кодовых слов и приводятся результаты расчета вероятности ошибки декодера для укороченных кодов с улучшенным спектром весов. Для кодов Панченко разрабатывается комбинаторный подход, позволяющий уменьшить число слов веса 5 при условии, что число слов веса 4 минимально. В статье находятся спектры весов неукороченных и укороченных кодов. Выводится точная формула количества слов веса 5 в неукороченном коде. Выводятся точные и достижимые нижние границы вероятности ошибки декодера для кодов с 32 и 64 информационными битами при заданной вероятности ошибки в канале. Таким образом, для укороченных кодов Панченко дается полное решение задачи минимизации вероятности ошибки декодера.

Для укороченных кодов БЧХ размерности 32 и 64 предлагаются верхние и нижние оценки минимального числа слов веса 6 и сами укороченные коды, у которых число слов веса 6 находится в промежутке между этими оценками и достаточно близко к нижней границе. Такая минимизация вероятности ошибки декодера представляется практически полезной.

Список обозначений: n – длина кода; d – минимальное кодовое расстояние; $d^\perp$ – минимальное расстояние двойственного кода; $t = \left\lfloor \frac{d-1}{2} \right\rfloor$ – число исправляемых кодом ошибок; A_w – число кодовых слов веса w; $A_w^\perp$ – число слов веса w в двойственном коде; P – вероятность ошибки в канале на символ; $[n, k, d]$ –двоичный линейный код длины n, размерности k, с расстоянием d; $[n, n-r, d]$ –двоичный линейный код длины n, избыточности r, с расстоянием d; s – число ненулевых весов в коде; $s^\perp$– число ненулевых весов в двойственном коде; важные константы –

$$D = 2^{r-4}; \quad \overline{D} = 2^{r-4} - 1; \quad E = 5 \cdot 2^{r-5}.$$

Работа организована следующим образом. В разделе 2 рассматриваются коды с расстоянием $d = 4$. Приводятся формулы для расчета вероятности ошибки декодера по спектру весов кода. Вычисляются спектры весов неукороченного и укороченного кода Панченко и двойственного ему кода. Даются алгоритмы укорочения, минимизирующие вероятность ошибки декодера. В разделе 3 рассматриваются коды с расстоянием $d = 6$. Приводятся оценки числа слов минимального веса и коды БЧХ, удовлетворяющие этим оценкам. В разделах 2 и 3 в широком диапазоне вероятностей ошибок в ячейках памяти находятся значения вероятности ошибки декодера для кодов с числом информационных символов 32 и 64. В приложения вынесены доказательства некоторых теорем.

2. КОДЫ С РАССТОЯНИЕМ 4

2.1. Вероятность ошибки декодера кода с $d = 4$

Рассмотрим декодирование двоичного кода в пределах конструктивного расстояния в двоичном симметричном канале с независимыми ошибками.

Вероятность p_c правильного (correct) декодирования $[n, k, d], d > 2t$ кода, исправляющего t ошибок, определим как

$$p_c = (1-P)^n + nP(1-P)^{n-1} + ... + \binom{n}{t} P^t (1-P)^{n-t}. \tag{2.1}$$

Введем *вероятность ошибки (error) декодера* p_e как вероятность того, что в результате исправления $\leq t$ ошибок декодер выдал ложное кодовое слово, и *вероятность отказа (reject) от декодирования* p_r как вероятность того, что декодер не нашел кодового слова на расстоянии $\leq t$ от принятого. Для любого кода справедливо равенство

$$p_c + p_e + p_r = 1. \tag{2.2}$$

Вероятностью p_{ic} неправильного (incorrect) декодирования, назовем вероятность объединения событий ошибки и отказа декодера, равную

$$p_{ic} = p_e + p_r = 1 - p_c.$$

Вероятность ошибочного декодирования линейных блоковых кодов рассмотрена в работах [8, 13, 14]. В следующей теореме приведены точные формулы, удобные для целей настоящей работы.

Теорема 2.1. *Вероятность p_e ошибки декодера двоичного* $[n, k, 4]$ *кода в симметричном канале с вероятностью P ошибки на символ равна*

$$p_e = \sum_{w=4}^{n} A_w \left(P^{w-1}(1-P)^{n-w+1} w + P^w (1-P)^{n-w} + P^{w+1}(1-P)^{n-w-1}(n-w) \right) \tag{2.3}$$

или, эквивалентно,

$$\begin{aligned} p_e = {} & P^3(1-P)^{n-3} \cdot 4A_4 + P^4(1-P)^{n-4}\left(A_4 + 5A_5\right) \\ & + \sum_{h=5}^{n} P^h (1-P)^{n-h} \left((n-h+1)A_{h-1} + A_h + (h+1)A_{h+1} \right). \end{aligned} \tag{2.4}$$

Доказательство. Для линейного кода с кодовым расстоянием $d = 4$ формулы (2.3) и (2.4) могут быть получены непосредственным комбинаторным рассмотрением ситуаций, возникающих при передаче нулевого слова. В (2.3) скобка, на которую умножается A_w, содержит 3 слагаемых, исчерпывающих все случаи неправильного декодирования кодом с $d = 4$ нулевого слова в слово веса w. Такие ситуации возникают, если кратность ошибки находится в области $\{w-1, w, w+1\}$. В (2.4) скобка, на которую умножается $P^h(1-P)^{n-h}$, содержит 3 слагаемых, исчерпывающих все случаи неправильного декодирования нулевого слова при возникновении ошибки кратности h. Такие ситуации возникают при наличии кодовых слов, имеющих веса в области $\{h-1, h, h+1\}$.

Если спектр весов кода не известен, его можно вычислить при относительно малых k или малых $n-k$. В последнем случае вычисляется перебором спектр весов $A_w^{\perp}$ двойственного кода, а затем используются тождества Мак-Вильямс [9].

Для кодов с $d = 4$, используемых для исправления ошибок в ЗУ, обычно используется $n - k = 7, 8, 9, 10$ и, следовательно, вычисление спектра весов двойственного кода реализуемо. Заметим также, что из (2.3), (2.4) следует, что для оценки вероятности ошибки декодирования p_e достаточно рассмотреть только первые компоненты спектра A_4, A_5 и, может быть, A_6.

Обозначим через $\Delta_h(r)$ отношение числа комбинаций ошибок веса h, которые обнаруживаются кодом, к общему числу ошибок веса h. Из (2.3), (2.4) вытекает, что для $[n, n-r, 4]$ кода справедливо:

$$\Delta_3(r) = 1 - \frac{4A_4}{\binom{n}{3}}, \quad \Delta_4(r) = 1 - \frac{A_4 + 5A_5}{\binom{n}{4}}. \tag{2.5}$$

Из Теоремы 2.1 и выражений (2.1), (2.2), (2.5) следует, что минимум вероятности ошибки декодирования достигается при минимизации количества кодовых слов малого веса 4, 5, 6.

2.2. Двоичный код Панченко Π_r и его основные свойства

Код Π_r был предложен В.И. Панченко в работе [11]. Неукороченный $[n, n-r, 4]$ код Π_r имеет длину $n = 5 \cdot 2^{r-4}$, избыточность $r \geq 5$ и кодовое расстояние $d = 4$. В работе [12] код Π_r обозначен через П. Радиус покрытия неукороченного кода Π_r равен 2, поэтому неукороченный код Π_r является квазисовершенным.

Введем обозначения. $B_k = [b_k \dots b_k]$ – матрица, состоящая из одинаковых столбцов b_k, где b_k – двоичное представление числа k со старшим разрядом в верхней позиции. Число строк и столбцов матрицы B_k ясно из контекста. Введем матрицу G.

$$G = \begin{bmatrix} 1\,0\,0\,0\,1 \\ 0\,1\,0\,0\,1 \\ 0\,0\,1\,0\,1 \\ 0\,0\,0\,1\,1 \end{bmatrix}. \tag{2.6}$$

Проверочная $(r \times 5 \cdot 2^{r-4})$-матрица P_r неукороченного кода Π_r имеет вид

$$P_r = \begin{bmatrix} B_0 & B_1 & B_2 & \dots & B_{\overline{D}} \\ G & G & G & \dots & G \end{bmatrix}. \tag{2.7}$$

В работе [12] предложены алгоритмы укорочения кода Π_r, направленные на уменьшение числа A_4 слов веса 4 для следующих диапазонов длин кода:

$$\max\{5 \cdot 2^{r-4} - 8, 9 \cdot 2^{r-5} - 1, 17 \cdot 2^{r-6} + 1\} \leq n \leq 5 \cdot 2^{r-4}, \tag{2.8}$$

$$\max\{5 \cdot 2^{r-4} - 25, 17 \cdot 2^{r-6} + 1\} \leq n \leq 5 \cdot 2^{r-4}. \tag{2.9}$$

Диапазон (2.8) включает $[39, 32, 4]$ и $[72, 64, 4]$ коды; диапазон (2.9) включает $[137, 128, 4]$ коды.

Алгоритм 1. *Укорочение матрицы P_r на $i \leq 8$ столбцов.* Для любого $i \leq 8$ исключаются i столбцов матрицы P_r строго в следующем порядке (слева направо):

$$\begin{bmatrix} b_\gamma \\ g_{15} \end{bmatrix}, \begin{bmatrix} b_\gamma \\ g_8 \end{bmatrix}, \begin{bmatrix} b_\gamma \\ g_4 \end{bmatrix}, \begin{bmatrix} b_\gamma \\ g_2 \end{bmatrix}, \begin{bmatrix} b_\gamma \\ g_1 \end{bmatrix}, \begin{bmatrix} b_\delta \\ g_{15} \end{bmatrix}, \begin{bmatrix} b_\nu \\ g_8 \end{bmatrix}, \begin{bmatrix} b_{\mathrm{H}} \\ g_4 \end{bmatrix}, \tag{2.10}$$

где g_u – столбец матрицы G, совпадающий с двоичным представлением числа u со старшим разрядом в верхней позиции; столбцы $b_\gamma, b_\delta, b_\nu, b_{\mathrm{H}}$ различны между собой.

Алгоритм 2. *Укорочение матрицы P_r на $i \le 25$ столбцов.* Целиком исключаются $(r \times 5)$-подматрицы $\begin{bmatrix} B_u \\ G \end{bmatrix}$, где $u = k_v$, $v = 1, \ldots, f$, $f = \lfloor \frac{i}{5} \rfloor$. Если $i \ne 5f$, одна из $(r \times 5)$-подматриц удаляется не полностью. Любые 3 и 4 столбца из множества $\{b_{k_1}, b_{k_2}, \ldots, b_{k_f}\}$ должны быть линейно независимы.

В работе [12, Теоремы 2 и 3] с использованием результатов работы [15] доказано следующее.

Теорема 2.2. [12]

(i) *В диапазоне* (2.8) *укороченный по Алгоритму* 1 $[n, n-r, 4]$ *код* Π_r *имеет минимальное число* A_4 *слов веса* 4 *и максимальную вероятность* $\Delta_3(r)$ *обнаружения тройных независимых ошибок по сравнению со всеми существующими неэквивалентными* $[n, n-r, 4]$ *кодами и их укорочениями, включая другие* (*не совпадающие с Алгоритмом* 1) *укорочения кода* Π_r.

(ii) *В диапазоне* (2.9) *укороченный по Алгоритму* 2 $[n, n-r, 4]$ *код* Π_r *имеет минимальное число* A_4 *слов веса* 4 *и максимальную вероятность* $\Delta_3(r)$ *обнаружения тройных независимых ошибок по сравнению со всеми укорочениями существующих* $[n, n-r, 4]$ *кодов, неэквивалентных коду* Π_r. *Лучшие, чем по Алгоритму* 2, *укорочения самого кода* Π_r, *в принципе, возможны.*

Алгоритм 1 допускает определенную вариативность, связанную с выбором столбцов b_γ, b_δ, b_ν, b_{H}. Для всех вариантов укорочения по Алгоритму 1 число слов веса 4 остается неизменным, но число слов других весов (5, 6 и т. д.) меняется.

Алгоритм 2 также допускает вариативность, но в этом случае число слов веса 4 может не совпадать для различных вариантов укорочения.

2.3. Спектр весов неукороченного кода Π_r

Теорема 2.3. *Число* $A_4^{\Pi}(r)$ *слов веса* 4 *в неукороченном коде* Π_r *равно*

$$A_4^{\Pi}(r) = \frac{5 \cdot 2^{r-6}(2^{r-4}-1)(2^{r-2}+5 \cdot 2^{r-5}-1)}{3}. \tag{2.11}$$

Доказательство. Из [12, формулы (8),(10)] следует $A_4^{\Pi}(r) = \frac{1}{3}\left(10D\binom{D}{2} + \overline{D}\binom{E}{2}\right)$, откуда (2.11) можно получить несложными преобразованиями.

Теорема 2.4. *Число* $A_5^{\Pi}(r)$ *слов веса* 5 *в неукороченном коде* Π_r *равно*

$$A_5^{\Pi}(r) = 2^{4r-16}. \tag{2.12}$$

Доказательство. Доказательство приведено в Приложении А.

Теорема 2.5. *Спектр весов кода* $\Pi_r^{\perp}$, *двойственного неукороченному коду* Π_r, *имеет вид*

$$A_0^{\perp} = 1, A_{2^{r-3}}^{\perp} = 10, A_{5 \cdot 2^{r-5}}^{\perp} = 2^r - 16, A_{2^{r-2}}^{\perp} = 5. \tag{2.13}$$

Доказательство. Проверочную матрицу P_r кода Π_r рассматриваем как порождающую матрицу двойственного кода $\Pi_r^{\perp}$. Легко увидеть, что линейные комбинации 4-х нижних строк этой матрицы имеют вес либо $2 \cdot 2^{r-4}$ (10 комбинаций из одной или двух строк), либо $4 \cdot 2^{r-4}$ (комбинации из 3-х или 4-х строк). Все линейные комбинации, в которые входит, по крайней мере, одна из верхних $r/2$ строк, имеют вес $5 \cdot 2^{r-5}$. Число таких комбинаций равно $2^4(2^{r-4}-1)$.

Пример 1. Из Теоремы 2.5 находим, что спектр весов неукороченного кода $\Pi_7^\perp$ имеет вид

$$A_0^\perp = 1, A_{16}^\perp = 10, A_{20}^\perp = 112, A_{32}^\perp = 5, \tag{2.14}$$

а спектр весов неукороченного кода $\Pi_8^\perp$ имеет вид

$$A_0^\perp = 1, A_{32}^\perp = 10, A_{40}^\perp = 240, A_{64}^\perp = 5. \tag{2.15}$$

Теперь спектр весов неукороченного кода Π_r может быть вычислен по формулам Мак-Вильямс [9].

Следствие 2.1. *Слова любого веса в неукороченных кодах Π_r и $\Pi_r^\perp$ образуют T-схему с $T \geq 1$.*

Доказательство. Согласно [9, Глава 6], если $d^\perp - s \geq 1$ либо $d - s^\perp \geq 1$, то кодовые слова любого веса образуют T-схему с T не меньше, чем $d^\perp - s$ или $d - s^\perp$. По Теореме 2.5 для неукороченного кода Π_r справедливо $d - s^\perp = 4 - 3 = 1$.

2.4. Спектр весов кода Π_r, укороченного на один символ

Матрицу G, см. (2.6), из которой исключен столбец, являющийся двоичным представлением числа m со старшим разрядом в верхней строке, обозначим через $G_{\setminus m}$. Например,

$$G_{\setminus 4} = \begin{bmatrix} 1\,0\,0\,1 \\ 0\,0\,0\,1 \\ 0\,1\,0\,1 \\ 0\,0\,1\,1 \end{bmatrix}, G_{\setminus 8} = \begin{bmatrix} 0\,0\,0\,1 \\ 1\,0\,0\,1 \\ 0\,1\,0\,1 \\ 0\,0\,1\,1 \end{bmatrix}, G_{\setminus 15} = \begin{bmatrix} 1\,0\,0\,0 \\ 0\,1\,0\,0 \\ 0\,0\,1\,0 \\ 0\,0\,0\,1 \end{bmatrix}. \tag{2.16}$$

Обозначим через $\Pi_{r,1}$ и $\Pi_{r,1}^\perp$ соответственно коды Π_r и $\Pi_r^\perp$, укороченные на один символ.

Теорема 2.6. *Спектр весов кода $\Pi_{r,1}^\perp$, двойственного коду Π_r, укороченному на один символ, не зависит от позиции этого символа и имеет вид*

$$A_0^\perp = 1, A_{2^{r-3}-1}^\perp = 4, A_{2^{r-3}}^\perp = 6, A_{5\cdot 2^{r-5}-1}^\perp = A_{5\cdot 2^{r-5}}^\perp = 2^{r-1} - 8, A_{2^{r-2}-1}^\perp = 4, A_{2^{r-2}}^\perp = 1. \tag{2.17}$$

Доказательство. По Следствию 2.1 при исключении любого символа число "разрушенных" и "сохраненных" слов каждого веса не зависит от исключаемой позиции. Рассмотрим вариант укорочения, заданный проверочной матрицей

$$P_{r,1} = \begin{bmatrix} B_0 & B_1 & B_2 & \dots & B_{\overline{D}} \\ G_{\setminus 15} & G & G & \dots & G \end{bmatrix}. \tag{2.18}$$

Рассмотрим три типа линейных комбинаций строк.

a) Линейная комбинация $(r-4)$-х верхних строк матрицы $P_{r,1}$.

b) Линейная комбинация 4-х нижних строк матрицы $P_{r,1}$.

c) Линейная комбинация $(r-4)$-х верхних строк и 4-х нижних строк матрицы $P_{r,1}$.

Обозначим через $L_w^{(u)}$ число линейных комбинаций строк типа u и веса w. Из непосредственного рассмотрения матрицы (2.18) легко увидеть, что все возможные варианты весов исчерпываются списком:

$$L_E^{(a)} = \overline{D}, L_{2^{r-3}-1}^{(b)} = L_{2^{r-2}-1}^{(b)} = 4, L_{2^{r-3}}^{(b)} = 6, L_{2^{r-2}}^{(b)} = 1, L_{E-1}^{(c)} = 8L_E^{(a)}, L_E^{(c)} = 7L_E^{(a)},$$

откуда следует (2.17).

Теперь спектр весов укороченного кода $\Pi_{r,1}$ может быть вычислен по формулам Мак-Вильямс [9].

Пример 2. Согласно (2.17) спектр весов кода $\Pi_{7,1}^{\perp}$, двойственного коду Π_7, укороченному на один символ, имеет вид

$$A_0^{\perp} = 1, A_{15}^{\perp} = 4, A_{16}^{\perp} = 6, A_{19}^{\perp} = 56, A_{20}^{\perp} = 56, A_{31}^{\perp} = 4, A_{32}^{\perp} = 1.$$

Спектр весов укороченного кода $\Pi_{7,1}$, вычисленный по формулам Мак-Вильямс, имеет вид

$$[A_0, A_1, \ldots, A_{10}, \ldots] = [1,\ 0,\ 0,\ 0,\ 1071,\ 3584,\ 26656,\ 118272,\ 481828,\ 1666560,\ 4935840, \ldots]$$

2.5. Спектр весов кода Π_8, укороченного на 8 символов по Алгоритму 1.

Обозначим через $\Pi_{r,8}^{(i)}$ i-й вариант кода Π_r, укороченного на 8 символов по Алгоритму 1. Соответствующую проверочную матрицу обозначим $P_{r,8}^{(i)}$.

Теорема 2.7. (i) *Спектр весов кода Π_r, укороченного на 8 символов по Алгоритму 1, зависит только от количества линейно независимых столбцов среди столбцов $b_\gamma, b_\delta, b_\nu, b_H$.*

(ii) *Код, двойственный коду, полученному укорочением кода Π_8 на 8 символов по Алгоритму 1, имеет один из трех спектров весов, указанных в таблице* 1.

Доказательство. Доказательство приведено в Приложении В. Здесь отметим, что все столбцы $b_\gamma, b_\delta, b_\nu, b_H$ различны между собой, один из них может быть нулевым. Поэтому среди этих столбцов может быть 2, 3 или 4 линейно независимых. Все эти случаи представлены в таблице 1: коды типа I (3 линейно независимых столбца); коды типа II (2 линейно независимых столбца); коды типа III (4 линейно независимых столбца).

Таблица 1. Спектры весов кодов $\Pi_{r,8}^{(i)\perp}$, двойственных кодам $\Pi_{r,8}^{(i)}$

вес (общий случай)	число слов, спектр типа I	число слов, спектр типа II	число слов, спектр типа III	вес ($r = 8$)	число слов, спектр типа I	число слов, спектр типа II	число слов, спектр типа III
$2^{r-3} - 4$	3	3	3	28	3	3	3
$2^{r-3} - 3$	6	6	6	29	6	6	6
$2^{r-3} - 2$	1	1	1	30	1	1	1
$E - 8$	0	0	2^{r-8}	32	0	0	1
$E - 7$	$5 \cdot 2^{r-7} - 2$	$2 \cdot 2^{r-6} - 2$	$8 \cdot 2^{r-8} - 2$	33	8	6	6
$E - 6$	$15 \cdot 2^{r-7} - 3$	$9 \cdot 2^{r-6} - 3$	$28 \cdot 2^{r-8} - 3$	34	27	33	25
$E - 5$	$25 \cdot 2^{r-7}$	$12 \cdot 2^{r-6}$	$56 \cdot 2^{r-8}$	35	50	48	56
$E - 4$	$35 \cdot 2^{r-7} - 3$	$15 \cdot 2^{r-6} - 3$	$70 \cdot 2^{r-8} - 3$	36	67	57	67
$E - 3$	$31 \cdot 2^{r-7} - 6$	$18 \cdot 2^{r-6} - 6$	$56 \cdot 2^{r-8} - 6$	37	56	66	50
$E - 2$	$13 \cdot 2^{r-7} - 1$	$7 \cdot 2^{r-6} - 1$	$28 \cdot 2^{r-8} - 1$	38	25	27	27
$E - 1$	$3 \cdot 2^{r-7}$	0	$8 \cdot 2^{r-8}$	39	6	0	8
E	$1 \cdot 2^{r-7} - 1$	$2^{r-6} - 1$	$1 \cdot 2^{r-8} - 1$	40	1	3	0
$2^{r-2} - 7$	2	2	2	57	2	2	2
$2^{r-2} - 6$	3	3	3	58	3	3	3

Следствие 2.2. (i) *Код, полученный укорочением кода Π_8 на 8 символов по Алгоритму 1, имеет один из трех спектров весов, первые компоненты которых указаны в таблице 2.*

(ii) *Среди кодов, полученных укорочением кода* Π_8 *на 8 символов по Алгоритму 1, наименьшее число слов веса 5 имеет код, у которого среди столбцов* $b_\gamma, b_\delta, b_\nu, b_H$ *присутствует нулевой столбец и, кроме того, имеются точно 2 линейно независимых столбца.*

Доказательство. Таблица 2 получена из таблицы 1 с помощью формул Мак-Вильямс [9]. По таблице 2 наименьшее число слов веса 5 имеет код типа II. Структура этого кода приведена в доказательстве Теоремы 2.7 в Приложении B.

Таблица 2. Спектры весов кодов $\Pi^{(i)}_{8,8}$

Вес	число слов, спектр типа I	число слов, спектр типа II	число слов, спектр типа III
4	6654	6654	6654
5	38587	38586	38588
6	695798	695799	695798
7	5350816	5350848	5350784
8	48245552	48245520	48245552
9	328360512	328360016	328361008
10	2102899496	2102899992	2102899496
11	11795458880	11795463840	11795453920

Замечание. Подход, примененный к исследованию кода Π_8, укороченного на 8 символов по Алгоритму 1, может быть использован и для изучения укорочения кода Π_9 по Алгоритму 2.

2.6. Вероятность ошибки декодирования укороченного кода Π_r

В таблицах 3 и 4 приведены результаты расчетов по формуле (2.4) для $[39, 32]$ кода $\Pi^{(1)}_{7,1}$ и $[72, 64]$ кода $\Pi^{(7)}_{8,8}$, соответственно. Для расчетов использованы спектры весов кода $\Pi^{(1)}_{7,1}$ из примера 2 и кода $\Pi^{(7)}_{8,8}$ из таблицы 2 (спектр типа II). Введем обозначение

$$p_e(h) = P^h(1-P)^{n-h}\left((n-h+1)A_{h-1} + A_h + (h+1)A_{h+1}\right).$$

Сумма $\sum_{h=3}^{8} p_e(h)$ является нижней оценкой вероятности ошибки декодирования p_e. В рассматриваемом диапазоне входных вероятностей P эта оценка является приемлемой. Запись вида e-b означает 10^{-b}.

Таблица 3. Вероятность ошибки декодирования $[39, 32]$ кода $\Pi^{(1)}_{7,1}$ при вероятности ошибки P

P	0,0001	1,0e-05	1,0e-06	1,0e-07	1,0e-08	1,0e-09	1,0e-10
$p_e(3)$	4,27e-09	4,28e-12	4,28e-15	4,28e-18	4,28e-21	4,28e-24	4,28e-27
$p_e(4)$	1,89e-12	1,90e-16	1,90e-20	1,90e-24	1,90e-28	1,90e-32	1,90e-36
$p_e(5)$	2,00e-15	2,01e-20	2,01e-25	2,01e-30	2,01e-35	2,01e-40	2,01e-45
$p_e(6)$	9,73e-19	9,76e-25	9,76e-31	9,76e-37	9,76e-43	9,76e-49	9,76e-55
$p_e(7)$	4,84e-22	4,85e-29	4,85e-36	4,85e-43	4,85e-50	4,85e-57	4,85e-64
$p_e(8)$	1,92e-25	1,92e-33	1,93e-41	1,93e-49	1,93e-57	1,93e-65	1,93e-73
$\sum_{h=3}^{8} p_e(h)$	4,27e-09	4,28e-12	4,28e-15	4,28e-18	4,28e-21	4,28e-24	4,28e-27

Таблица 4. Вероятность ошибки декодирования $[72, 64]$ кода $\Pi_{8,8}^{(7)}$ при вероятности ошибки P

P	0,0001	1,0e-05	1,0e-06	1,0e-07	1,0e-08	1,0e-09	1,0e-10
$p_e(3)$	2,64e-08	2,66e-11	2,66e-14	2,66e-17	2,66e-20	2,66e-23	2,66e-26
$p_e(4)$	1,98e-11	1,99e-15	2,00e-19	2,00e-23	2,00e-27	2,00e-31	2,00e-35
$p_e(5)$	4,63e-14	4,66e-19	4,66e-24	4,67e-29	4,67e-34	4,67e-39	4,67e-44
$p_e(6)$	4,05e-17	4,07e-23	4,07e-29	4,07e-35	4,07e-41	4,07e-47	4,07e-53
$p_e(7)$	4,34e-20	4,37e-27	4,37e-34	4,37e-41	4,37e-48	4,37e-55	4,37e-62
$p_e(8)$	3,33e-23	3,35e-31	3,35e-39	3,35e-47	3,35e-55	3,35e-63	3,35e-71
$\sum_{h=3}^{8} p_e(h)$	2,64e-08	2,66e-11	2,66e-14	2,66e-17	2,66e-20	2,66e-23	2,66e-26

Для входных вероятностей ошибок $P \le 0.0001$ из таблиц 3 и 4 видно, что сумма $\sum_{h=3}^{8} p_e(h)$ существенно меньше P. Более того, для $[39, 32]$ кода $\Pi_{7,1}^{(1)}$ справедливо следующее.

$$\sum_{h=3}^{8} p_e(h) < 4.3 \cdot 10^{-(6+3j)} = 4.3P^3 \cdot 10^3 \text{ для } P = 10^{-(3+j)} \le 10^{-4},\ j = 1, \dots, 7. \tag{2.19}$$

Для $[72, 64]$ кода $\Pi_{8,8}^{(7)}$ выполняются соотношения

$$\sum_{h=3}^{8} p_e(h) < 2.7 \cdot 10^{-(5+3j)} = 2.7P^3 \cdot 10^4 \text{ для } P = 10^{-(3+j)} \le 10^{-4},\ j = 1, \dots, 7. \tag{2.20}$$

Важно также отметить, что в случае $P \le 0.0001$ основной вклад в сумму $\sum_{h=3}^{8} p_e(h)$ вносит слагаемое $p_e(3)$. Для $[39, 32]$ кода $\Pi_{7,1}^{(1)}$ и $[72, 64]$ кода $\Pi_{8,8}^{(7)}$ справедливо следующее.

$$\frac{p_e(3)}{p_e(h)} \approx 10^{(j+2)(h-3)} \text{ для } P = 10^{-(3+j)} \le 10^{-4},\ j = 1, \dots, 7. \tag{2.21}$$

Укажем, что для кодов $\Pi_{8,8}^{(1)}$ и $\Pi_{8,8}^{(10)}$, распределение весов которых указано в таблице 2 (спектры типа I и III), вероятности неправильного декодирования практически совпадают с вероятностями для кода $\Pi_{8,8}^{(7)}$, данными в таблице 4. Следовательно, из возможных вариантов укорочения $\Pi_{8,8}^{(i)}$, следует выбирать тот, который больше подходит с точки зрения реализации.

3. КОДЫ С РАССТОЯНИЕМ 6

3.1. Оценки минимального количества слов фиксированного веса в укороченном коде БЧХ с $d = 6$

Основываясь на подходах работы [16], рассмотрим *верхние оценки* количества слов.

Теорема 3.1. *Пусть двоичный линейный $[n_0, n_0 - r, d]$ код C_{n_0} длины n_0 содержит $A_w(n_0)$ слов веса w. Тогда существует укороченный $[n, n - r, d]$ код C_n длины $n < n_0$, содержащий $A_w(n)$ слов веса w, где*

$$A_w(n) \le A_w(n_0) \frac{\binom{n_0 - w}{n - w}}{\binom{n_0}{n}}. \tag{3.1}$$

Доказательство. Проведем укорочение путем исключения столбцов из проверочной матрицы H_{n_0} кода C_{n_0}. В результате получим проверочную матрицу H_n кода C_n. Каждому слову

веса w кода C_{n_0} соответствует некоторый набор из w линейно зависимых столбцов неукороченной проверочной матрицы H_{n_0}. Этот набор остается неизменным в $\binom{n_0-w}{n-w}$ укороченных матрицах H_n. Следовательно, сумма количества слов веса w во всех укороченных кодах C_n равна $A_w(n_0)\binom{n_0-w}{n-w}$. Всего имеется $\binom{n_0}{n}$ укороченных кодов. Проведя усреднение по всем укороченным кодам, получаем (3.1).

Обозначим через $A_w^{\min}(n)$ минимально возможное число слов веса w в коде БЧХ с $d=6$ длины n.

Следствие 3.1. *Для минимума количества слов веса 6 в $[n, n-r, 6]$ коде БЧХ с $d=6$ длины $n \le n_0 = 2^m$, где $m = \frac{r-1}{2}$, имеет место верхняя оценка*

$$A_6^{\min}(n) \le \begin{cases} \binom{n}{6}\frac{2^m-8}{(2^m-3)(2^m-4)(2^m-5)}, & \text{если } m \text{ нечетное} \\ \binom{n}{6}\frac{2^m-4}{(2^m-2)(2^m-3)(2^m-5)}, & \text{если } m \text{ четное} \end{cases}. \tag{3.2}$$

Доказательство. В [7] показано, что для неукороченных кодов БЧХ длины $n_0 = 2^m$ справедливо

$$A_6(n_0 = 2^m) \le \begin{cases} \frac{2^m(2^m-1)(2^m-2)(2^m-8)}{720}, & \text{если } m \text{ нечетное} \\ \frac{2^m(2^m-1)(2^m-4)^2}{720}, & \text{если } m \text{ четное} \end{cases}. \tag{3.3}$$

Соотношение (3.2) следует из (3.1) и (3.3).

В работе [16] методами линейного программирования с использованием результатов [17] получена *нижняя оценка* величины $A_6(n)$.

Теорема 3.2. [16] *Для двоичных $[n, n-r, 6]$ кодов с расстоянием $d=6$ и четными расстояниями между кодовыми словами имеет место оценка*

$$A_6^{\min}(n) \ge \begin{cases} \frac{n(n-1)(n-2)(n^3-3n^2+8n-3\cdot 2^r)}{720(2^{r-1}-n)}, & \text{если } n \text{ четное,} \\ \frac{n(n-1)(n-2)(n^3-2n^2+3n+6-3\cdot 2^r)}{720(2^{r-1}-n-1)}, & \text{если } n \text{ нечетное} \end{cases}. \tag{3.4}$$

3.2. Проверочные матрицы укороченных кодов БЧХ с расстоянием $d=6$

Из укороченных кодов для исправления ошибок в памяти наиболее важны $[n_m, n_m - r, 6]$ коды длины

$$n_m = 2^{m-1} + 2m + 1 = \frac{n_0}{2} + r, m = \frac{r-1}{2}. \tag{3.5}$$

Число информационных символов k_m такого кода равно степени двойки

$$k_m = n_m - r = 2^{m-1} = \frac{n_0}{2}.$$

Обозначим через ℓ_i локатор i-й позиции кодового слова. Пусть F_{2^m} будет поле Галуа из 2^m элементов. Проверочная матрица $[n_m, n_m - r, 6]$ кода БЧХ с $d=6$ может быть записана в виде

$$H = \begin{bmatrix} 1 & 1 & \dots & 1 \\ \ell_1 & \ell_2 & \dots & \ell_{n_m} \\ \ell_1^3 & \ell_2^3 & \dots & \ell_{n_m}^3 \end{bmatrix} = \begin{bmatrix} J \\ H_1 \\ H_2 \end{bmatrix}, \ell_i \in F_{2^m}, n_m = 2^{m-1} + 2m + 1, m = \frac{r-1}{2}. \tag{3.6}$$

Элементы поля F_{2^m} будем обычным образом представлять в виде многочлена степени $m-1$ с двоичными коэффициентами, используя степени примитивного элемента поля.

В таблице 5 приведены десятичные эквиваленты двоичных столбцов матрицы H_1 для $m = 6, 7$ и соответствующих $[45, 32, 6]$ и $[79, 64, 6]$ кодов БЧХ. Матрицы получены с использованием компьютера. Рассмотренные коды имеют, соответственно, 2170 и 17375 слов веса 6, что меньше верхней границы и больше нижней границы, см.(3.2), (3.4).

Таблица 5. Проверочные матрицы укороченных кодов БЧХ

m	n	r	k	H_1	нижняя граница $A_6^{\min}(n) \geq$	A_6	верхняя граница $A_6^{\min}(n) \leq$
6	45	13	32	2,3,6,7,8,9,10,11,12,13,14,15,16, 17,18,19,20,21,23,24,25,26,27,30, 31,34,35,36,37,40,41, 46,47,52, 53,54,55,56,57,58,59,60, 61,62,63	1894	2170	2190
7	79	15	64	1,2,3,6,7,8,9,10,11,14,15,16,17, 18, 19,20,21,22,23,24,25, 26,27, 28,29, 30,31,32,33,34,35, 36,37, 38,39,40, 41,42,43, 48,49,50, 51, 52,53,54,55, 58,59, 62,63,68, 69, 84,85,86, 87,92 ,93,94,95,96,97,100,101,102,103, 104,105,108,109, 110,111,122,123, 124,125,126,127	16452	17375	17495

3.3. Вероятность ошибки декодирования двоичного кода с расстоянием $d = 6$

Теорема 3.3. *Вероятность ошибки декодирования p_e двоичного $[n, k, 6]$ кода в симметричном канале с вероятностью P ошибки на символ равна*

$$\begin{aligned} p_e = \sum_{w=6}^{n} A_w \Bigg(& P^{w-2}(1-P)^{n-w+2}\binom{w}{2} + P^{w-1}(1-P)^{n-w+1}w \\ & + P^w(1-P)^{n-w}(1+w(n-w)) \\ & + P^{w+1}(1-P)^{n-w-1}(n-w) + P^{w+2}(1-P)^{n-w-2}\binom{n-w}{2}\Bigg) \end{aligned} \tag{3.7}$$

или, эквивалентно,

$$\begin{aligned} p_e = \sum_{h=4}^{n} P^h(1-P)^{n-h} \Bigg(& \binom{n-h+2}{2} A_{h-2} + (n-h+1)A_{h-1} + (1+h(n-h))A_h \\ & + (n-h-1)A_{h+1} + \binom{h+2}{2} A_{h+2}\Bigg). \end{aligned} \tag{3.8}$$

Доказательство. Для линейного кода формулы (3.7) и (3.8) могут быть получены непосредственным комбинаторным рассмотрением ситуаций, возникающих при передаче нулевого слова. В (3.7) скобка, на которую умножается A_w, содержит 5 слагаемых, исчерпывающих все случаи неправильного декодирования нулевого слова в слово веса w. Такие ситуации возникают, если кратность ошибки находится в диапазоне $w-2 \ldots w+2$. В (3.8) скобка, на которую умножается $P^h(1-P)^{n-h}$, содержит 5 слагаемых, исчерпывающих все случаи неправильного декодирования нулевого слова при возникновении ошибки кратности h. Такие ситуации возникают, при наличии кодовых слов, имеющих веса диапазоне $h-2 \ldots h+2$.

Следствие 3.2. *Вероятность ошибки декодирования p_e двоичного $[n,k,6]$ кода с четными весами в симметричном канале с вероятностью P ошибки на символ равна*

$$\begin{aligned} p_e = \sum_{j=3}^{\lfloor n/2\rfloor} A_{2j} \Bigg(& P^{2j-2}(1-P)^{n-2j+2}\binom{2j}{2} \\ & + P^{2j-1}(1-P)^{n-2j+1}\cdot 2j + P^{2j}(1-P)^{n-2j}\left(1+2j(n-2j)\right) \\ & + P^{2j+1}(1-P)^{n-2j-1}(n-2j) + P^{2j+2}(1-P)^{n-2j-2}\binom{n-2j}{2}\Bigg) \end{aligned} \tag{3.9}$$

или, эквивалентно,

$$\begin{aligned} p_e = {} & P^4(1-P)^{n-4}\cdot 15A_6 + P^5(1-P)^{n-5}(n-6)A_6 + P^6(1-P)^{n-6}\left(6n-35\right)A_6 + 28A_8) \\ & + \sum_{h=7}^{n} P^h(1-P)^{n-h}\cdot \begin{cases} \binom{n-h+2}{2}A_{h-2} + (1+h(n-h))A_h + \binom{h+2}{2}A_{h+2}, & h \text{ четное} \\ (n-h+1)A_{h-1} + (n-h-1)A_{h+1}, & h \text{ нечетное} \end{cases}. \end{aligned} \tag{3.10}$$

3.4. Вероятность ошибки декодирования укороченных кодов БЧХ с расстоянием $d = 6$

В таблицах 6 и 7, соответственно, приведены результаты расчетов по формуле (3.10) для $[45, 32]$ и $[79, 64]$ кодов БЧХ. Число A_6 слов веса 6 взято из таблицы 5. Использованы обозначения $p_e(4) = P^4(1-P)^{n-4}\cdot 15A_6$, $p_e(5) = P^5(1-P)^{n-5}(n-6)A_6$. Сумма $\sum_{h=4}^{5} p_e(h)$ является нижней оценкой вероятности ошибки декодирования p_e. В рассматриваемом диапазоне входных вероятностей P эта оценка является приемлемой.

Таблица 6. Вероятность ошибки декодирования $[45, 32]$ кода

P	0,001	0,0001	0,00001	0,000001	1,0 e-7	1,0 e-8	1,0 e-9	1,0 e-10
$p_e(4)$	3,124e-08	3,241e-12	3,253e-16	3,254e-20	3,254e-24	3,254e-28	3,254e-32	3,254e-36
$p_e(5)$	8,130e-11	8,429e-16	8,459e-21	8,462e-26	8,462e-31	8,462e-36	8,462e-41	8,462e-46
$\sum_{h=4}^{5} p_e(h)$	3,132e-08	3,242e-12	3,253e-16	3,254e-20	3,254e-24	3,254e-28	3,254e-32	3,254e-36

Таблица 7. Вероятность ошибки декодирования $[79, 64]$ кода

P	0,001	0,0001	0,00001	0,000001	1,0e-7	1,0 e-8	1,0 e-9	1,0 e-10
$p_e(4)$	2,417e-07	2,588e-11	2,604e-15	2,606e-19	2,606e-23	2,606e-27	2,606e-31	2,606e-35
$p_e(5)$	1,177e-09	1,259e-14	1,267e-19	1,268e-24	1,268e-29	1,268e-34	1,268e-39	1,268e-44
$\sum_{h=4}^{5} p_e(h)$	2,429e-07	2,588e-11	2,604e-15	2,606e-19	2,606e-23	2,606e-27	2,606e-31	2,606e-35

Для входных вероятностей ошибки $P \le 0.001$ из таблиц 6 и 7 видно, что сумма $\sum_{h=4}^{5} p_e(h)$ существенно меньше P. Более того, для $[45, 32]$ кода выполняются соотношения

$$\sum_{h=4}^{5} p_e(h) < 3.26\cdot 10^{-(4+4j)} = 3.26P^4\cdot 10^4 \text{ для } P = 10^{-(3+j)} \le 10^{-3}, j = 0, 1, \ldots, 7, \tag{3.11}$$

а для $[79, 64]$ кода справедливо

$$\sum_{h=4}^{5} p_e(h) < 2.61\cdot 10^{-(3+4j)} = 2.61P^4\cdot 10^5 \text{ для } P = 10^{-(3+j)} \le 10^{-3}, j = 0, 1, \ldots, 7. \tag{3.12}$$

Важно также отметить, что в случае $P \leq 0.001$ основной вклад в сумму $\sum_{h=4}^{5} p_e(h)$ вносит слагаемое $p_e(4)$. Для $[45, 32]$ кода имеет место соотношение

$$\frac{p_e(4)}{p_e(5)} \approx 10^{j+3} \text{ для } P = 10^{-(3+j)} \leq 10^{-3}, j = 0, 1, \ldots, 7. \tag{3.13}$$

Для $[79, 64]$ кода справедливо

$$\frac{p_e(4)}{p_e(5)} \approx 10^{j+2} \text{ для } P = 10^{-(3+j)} \leq 10^{-3}, j = 0, 1, \ldots, 7. \tag{3.14}$$

4. ЗАКЛЮЧЕНИЕ

Обычно задача обеспечения высокой надежности оперативной памяти вычислительных систем решается применением помехоустойчивого кодирования с исправлением одной или двух ошибок в словах, содержащих 32, 64 или 128 информационных бит и от 6 до 14 проверочных бит с помощью укороченных кодов Хемминга и кодов Боуза-Чоудхури-Хоквингема (БЧХ).

В настоящей работе доказано, что укороченные коды Панченко с расстоянием 4 обеспечивают наименьшую вероятность ошибки декодирования при правильном укорочении. Тем самым показано, что коды Хэмминга не являются лучшими с точки зрения минимизации вероятности ошибки декодера. В работе определены правила укорочения кодов Панченко и вычислены точные вероятности ошибки декодера. Для получения этих результатов разработан специальный комбинаторный подход, который позволяет минимизировать как число слов веса 4, так и число слов веса 5. Получены спектры весов неукороченных и укороченных кодов. Выведена точная формула количества слов веса 5 в неукороченном коде. Предложенный подход применен к $[39, 32, 4]$ и $[72, 64, 4]$ кодам. Для этих кодов получены практически точные достижимые нижние границы вероятности ошибки декодера и задача минимизации вероятности ошибки декодера решена полностью. Разработанный подход представляется перспективным для дальнейшего изучения кодов Панченко, в частности, для получения эффективного укорочения $[160, 151, 4]$ кода Π_9 до $[137, 128, 4]$ кода.

Для кодов БЧХ с расстоянием 6 выведены верхние и нижние границы числа кодовых слов минимального веса. Построены $[45, 32, 4]$ и $[79, 64, 4]$ коды, у которых число слов веса 6 находится в промежутке между этими оценками достаточно близко к нижней границе. Вычислены значения вероятностей ошибки декодера для построенных кодов. Результаты являются практически полезными.

ПРИЛОЖЕНИЕ

A. ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 2.4

Рассмотрим некоторые полезные свойства двоичного $[2^m - 1, 2^m - 1 - m, 3]$ кода Хэмминга. Обозначим через $A_w^H(m)$ количество слов веса w в этом коде. Как известно [9],

$$A_3^H(m) = \frac{1}{3}\binom{2^m - 1}{2}, A_4^H(m) = \frac{1}{2^m - 3}\binom{2^m - 1}{4}, A_5^H(m) = \frac{2^m - 4}{5}\left(A_4^H(m) - A_3^H(m)\right). \tag{A.1}$$

Обозначим через $\widetilde{A}_w^H(m)$ количество слов веса w в двоичном $[2^m - 1, 2^m - 1 - m, 3]$ коде Хэмминга, укороченном на один символ путем исключения столбца проверочной матрицы.

Лемма 1. *Величина $\widetilde{A}_w^H(m)$ не зависит от исключаемого столбца. Справедливо*

$$\widetilde{A}_w^H(m) = A_w^H(m)\frac{2^m-1-w}{2^m-1}. \tag{A.2}$$

Доказательство. В соответствии с [9, Раздел 6.5, Пример (E.2)(продолжение)] слова каждого веса w неукороченного $[2^m-1, 2^m-1-m, 3]$ кода Хэмминга образуют $2-(v,k,\lambda)$-схему из b блоков. Сразу отметим, что, по определению параметров схемы, здесь $v=2^m-1$, $k=w$, $b=A_w^H(m)$. Согласно [9, Раздел 2.5, Следствие 10] в $t-(v,k,\lambda)$-схеме, состоящей из b блоков, каждый элемент встречается точно в $\frac{bk}{v}$ блоках. Следовательно, *каждый* столбец проверочной матрицы участвует в формировании точно $\frac{A_w^H(m)\cdot w}{2^m-1}$ слов веса w, которые будут разрушены, если этот столбец вычеркнуть. Таким образом, величина $\widetilde{A}_w^H(m)$ действительно не зависит от исключаемого столбца. Более того, $\widetilde{A}_w^H(m) = A_w^H(m) - \frac{A_w^H(m)\cdot w}{2^m-1} = A_w^H(m)\frac{2^m-1-w}{2^m-1}$.

Следствие 1. *Справедливо следующее:*

$$\begin{aligned}&\widetilde{A}_3^H(m) = \frac{(2^m-4)(2^{m-1}-1)}{3};\quad \widetilde{A}_4^H(m) = \frac{(2^m-2)(2^m-4)(2^m-5)}{2\cdot 3\cdot 4};\\ &\widetilde{A}_5^H(m) = \left(A_4^H(m) - A_3^H(m)\right)\frac{(2^m-4)(2^m-6)}{5(2^m-1)}.\end{aligned} \tag{A.3}$$

Доказательство. Справедливость формул в (A.3) вытекает из (A.1), (A.2).

Лемма 2. *Последние четыре строки каждой пятерки линейно зависимых столбцов проверочной матрицы P_r являются (с точностью до перестановки столбцов) матрицей G.*

Доказательство. Справедливость леммы вытекает непосредственно из (2.6), (2.7).

Введем обозначения: $A_5^{\Pi}(r)$ – количество слов веса 5 в неукороченном коде Π_r; $T_i(r)$ – количество слов веса 5 кода Π_r, имеющих i-ю структуру, где i - номер структуры; $B_k^{(i)}$ – $(r\times i)$-подматрица $(r\times 5)$-матрицы $\begin{bmatrix}B_k\\ G\end{bmatrix}$, $1\le i\le 5$; $\#B_k^{(i)}$ – количество возможных вариантов подматрицы $B_k^{(i)}$ при условии, что предыдущие подматрицы структуры заданы; $\#\left[B_{k_1}^{(i)}\dots B_{k_u}^{(j)}\right]$ – количество возможных вариантов подматрицы $\left[B_{k_1}^{(i)}\dots B_{k_u}^{(j)}\right]$ при условии, что предыдущие подматрицы структуры заданы; $\oplus$ – знак поразрядного сложения двоичных столбцов по модулю 2.

Теперь мы рассмотрим все возможные структуры слов веса 5 неукороченного кода Π_r и определим количество слов каждой структуры. Все рассуждения и подсчеты следуют непосредственно из (2.6), (2.7). Положим $k, k_i > 0$.

Структура 1. Слово вида B_0^5. $T_1(r)=1$.

Структура 2. Слова вида $\left[B_0^{(3)}B_k^{(2)}\right]$, $\forall k$. Здесь $\#B_0^{(3)}=\binom{5}{3}$, $\#B_k^{(2)}=1$, $\#\{k\}=\overline{D}$. Поэтому $T_2(r)=10\overline{D}$.

Структура 3. Слова вида $\left[B_0^{(2)}B_{k_1}^{(1)}B_{k_2}^{(1)}B_{k_3}^{(1)}\right]$, $k_1\oplus k_2\oplus k_3=0$. Здесь $\#B_0^{(2)}=\binom{5}{2}$. Для заданной тройки (k_1,k_2,k_3) и заданной пары столбцов в B_0 справедливо $\#\left[B_{k_1}^{(1)}B_{k_2}^{(1)}B_{k_3}^{(1)}\right]=3!$. Число различных троек (k_i,k_j,k_m), таких что $k_i\oplus k_j\oplus k_m=0$ равно $A_3^H(r-4)=\frac{1}{3}\binom{\overline{D}}{2}$. Поэтому $T_3(r)=\binom{5}{2}\frac{3!}{3}\binom{\overline{D}}{2}=20\binom{\overline{D}}{2}$.

Структура 4. Слова вида $\left[B_0^{(1)}B_k^{(4)}\right]$, $\forall k$. Здесь $\#B_0^{(1)}=\binom{5}{1}$, $\#B_k^{(4)}=1$, $\#\{k\}=\overline{D}$. Поэтому $T_4(r)=\binom{5}{1}\cdot 1\cdot\overline{D}=5\overline{D}$.

Структура 5. Слова вида $\left[B_0^{(1)}B_{k_1}^{(2)}B_{k_2}^{(2)}\right]$, $\forall k_1,k_2$. Здесь $\#B_0^{(1)}=\binom{5}{1}$. Кроме того, для заданной двойки (k_1,k_2) и заданного столбца в B_0 справедливо $\#\left[B_{k_1}^{(2)}B_{k_2}^{(2)}\right]=\binom{4}{2}$. Число различных двоек (k_1,k_2) равно $\binom{\overline{D}}{2}$. Поэтому $T_5(r)=\binom{5}{1}\binom{4}{2}\binom{\overline{D}}{2}=30\binom{\overline{D}}{2}$.

Структура 6. Слова вида $\left[B_0^{(1)}B_{k_1}^{(1)}B_{k_2}^{(1)}B_{k_3}^{(1)}B_{k_4}^{(1)}\right]$, $k_1\oplus k_2\oplus k_3\oplus k_4=0$. Здесь $\#B_0^{(1)}=\binom{5}{1}$. Кроме того, для заданной четверки (k_1,k_2,k_3,k_4) и заданного столбца в B_0 справедливо, $\#\left[B_{k_1}^{(1)}B_{k_2}^{(1)}B_{k_3}^{(1)}B_{k_4}^{(1)}\right]=4!$. Число различных четверок (k_i,k_j,k_m,k_u), таких что $k_i\oplus k_j\oplus k_m\oplus k_u=0$, равно $A_4^H(r-4)=\frac{1}{\overline{D}-2}\binom{\overline{D}}{4}$. Поэтому $T_6(r)=\binom{5}{1}4!A_4^H(r-4)=\binom{5}{1}\frac{4!}{\overline{D}-2}\binom{\overline{D}}{4}=\frac{120}{\overline{D}-2}\binom{\overline{D}}{4}$.

Структура 7. Слова вида $\left[B_{k_1}^{(3)}B_{k_2}^{(1)}B_{k_3}^{(1)}\right]$, $k_1\oplus k_2\oplus k_3=0$. Здесь для заданной тройки (k_1,k_2,k_3) справедливо $\#\left[B_{k_i}^{(3)}B_{k_j}^{(1)}B_{k_v}^{(1)}\right]=3\cdot\binom{5}{3}\cdot 2!$. Число различных троек (k_1,k_2,k_3), таких что $k_1\oplus k_2\oplus k_3=0$ равно $A_3^H(r-4)=\frac{1}{3}\binom{\overline{D}}{2}$. Поэтому $T_7(r)=6\binom{5}{3}\frac{1}{3}\binom{\overline{D}}{2}=20\binom{\overline{D}}{2}$.

Структура 8. Слова вида $\left[B_{k_1}^{(2)}B_{k_2}^{(1)}B_{k_3}^{(1)}B_{k_4}^{(1)}\right]$, $\forall k_1$, $k_2\oplus k_3\oplus k_4=0$. Здесь для заданной четверки (k_1,k_2,k_3,k_4) справедливо $\#\left[B_{k_1}^{(2)}B_{k_2}^{(1)}B_{k_3}^{(1)}B_{k_4}^{(1)}\right]=\binom{5}{2}\cdot 3!=60$. Кроме того, $\#\{k_1\}=\overline{D}$. Число различных троек $k_2\oplus k_3\oplus k_4=0$ при выбранном k_1 равно $\widetilde{A}_3^H(r-4)$. Следовательно, число различных четверок равно $\overline{D}\cdot\widetilde{A}_3^H(r-4)$. В результате $T_8(r)=60\overline{D}\cdot\widetilde{A}_3^H(r-4)=20\overline{D}(2^{r-4}-4)(2^{r-5}-1)$.

Структура 9. Слова вида $\left[B_{k_1}^{(1)}B_{k_2}^{(1)}B_{k_3}^{(1)}B_{k_4}^{(1)}B_{k_5}^{(1)}\right]$, $k_1\oplus k_2\oplus k_3\oplus k_4\oplus k_5=0$. Здесь для заданной пятерки (k_1,k_2,k_3,k_4,k_5) справедливо $\#\left[B_{k_1}^{(1)}B_{k_2}^{(1)}B_{k_3}^{(1)}B_{k_4}^{(1)}B_{k_5}^{(1)}\right]=5!$. Число различных пятерок (k_1,k_2,k_3,k_4,k_5), таких что $k_1\oplus k_2\oplus k_3\oplus k_4\oplus k_5=0$, равно $A_5^H(r-4)$. Поэтому $T_9(r)=120A_5^H(r-4)$.

Теперь соотношение (2.12) может быть получено суммированием величин $T_i(r)$ и простыми преобразованиями. Теорема 2.4 доказана.

В. ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 2.7

Из структуры проверочной матрицы P_r (2.7) видно, что при укорочении по Алгоритму 1 спектр весов двойственного кода зависит от того, являются ли столбцы $b_\gamma, b_\delta, b_\nu, b_H$ нулевыми или ненулевыми, а также от того есть ли среди них тройки линейно зависимых столбцов. Список вариантов укорочения по Алгоритму 1, которые, в принципе, могут дать различные

спектры весов двойственного кода, приведен ниже. Номер варианта обозначен через i.

$i=1.\ \ b_\gamma=0,\ b_\delta\oplus b_\nu\oplus b_H\neq 0.$
$i=2.\ \ b_\gamma\neq 0,\ b_\delta=0,\ b_\gamma\oplus b_\nu\oplus b_H\neq 0.$
$i=3.\ \ b_\gamma\neq 0,\ b_\nu=0,\ b_\gamma\oplus b_\delta\oplus b_H\neq 0.$
$i=4.\ \ b_\gamma,b_\delta,b_\nu,b_H\neq 0,\ b_\delta\oplus b_\nu\oplus b_H=0.$
$i=5.\ \ b_\gamma,b_\delta,b_\nu,b_H\neq 0,\ b_\gamma\oplus b_\delta\oplus b_\nu=0.$
$i=6.\ \ b_\gamma,b_\delta,b_\nu,b_H\neq 0,\ b_\gamma\oplus b_\nu\oplus b_H=0.$
$i=7.\ \ b_\gamma=0,\ b_\delta\oplus b_\nu\oplus b_H=0.$
$i=8.\ \ b_\gamma\neq 0,\ b_\delta=0,\ b_\gamma\oplus b_\nu\oplus b_H=0.$
$i=9.\ \ b_\gamma\neq 0,\ b_\nu=0,\ b_\gamma\oplus b_\delta\oplus b_H=0.$
$i=10.\ b_\gamma,b_\delta,b_\nu,b_H\neq 0,\ \ b_\gamma,b_\delta,b_\nu,b_H$ линейно независимы.

Из (2.6)–(2.10) можно увидеть, что для $r=8$ этот список является исчерпывающим.

Рассмотрим спектры весов двойственного укороченного кода для указанных вариантов. Обозначим через $W(A)$ матрицу из всех линейных комбинаций строк матрицы A. Если $A=B_iB_jB_k$, то количество строк и столбцов в подматрицах B_u, как обычно, ясно из контекста. Заметим, что матрицы $W(GGGG)$, $W\left(G_{\setminus 15}GG_{\setminus 8}G_{\setminus 4}\right)$, $W\left(GG_{\setminus 15}G_{\setminus 8}G_{\setminus 4}\right)$ одинаковы для всех кодов $\Pi^{(i)}_{r,8}$. Записи типа $B_{\setminus D}$ означают, что подматрица B вычеркивается при укорочении кода. В таблицах для спектра весов обозначим через Ai, Bi, Ci данные для следующих объектов.

Ai: линейная комбинация $(r-4)$-х верхних строк матрицы $P^{(i)}_{r,8}$.

Bi: линейная комбинация 4-х нижних строк матрицы $P^{(i)}_{r,8}$.

Ci: линейная комбинация $(r-4)$-х верхних строк и 4-х нижних строк матрицы $P^{(i)}_{r,8}$.

$i=1.\ \ b_\gamma=0,\ \ b_\delta\oplus b_\nu\oplus b_H\neq 0$. Спектр типа I.

Укорочения проверочная матрица имеет вид

$$P^{(1)}_{r,8}=\begin{bmatrix} B_0 & B_1 & B_2 & \dots & B_{\delta\neq 0} & \dots & B_{\nu\neq 0} & \dots & B_{H\neq 0} & \dots & B_{\setminus D} \\ G & G & G & \dots & G_{\setminus 15} & \dots & G_{\setminus 8} & \dots & G_{\setminus 4} & \dots & G \end{bmatrix}.$$

Условие $b_\delta\oplus b_\nu\oplus b_H\neq 0$ означает, что столбцы b_δ,b_ν,b_H линейно независимы. Учитывая (2.6)–(2.10), (2.16) и структуру матрицы $P^{(1)}_{r,8}$, можно показать, что матрица $W\left(B_{\delta\neq 0}B_{\nu\neq 0}B_{H\neq 0}\right)$ с $b_\delta\oplus b_\nu\oplus b_H\neq 0$ имеет размер $(2^{r-4}-1)\times 12$ и состоит из 2^{r-7} секций. При этом каждая из $2^{r-7}-1$ одинаковых нижних секций имеет размер 8×12 и нулевую верхнюю строку. Верхняя секция размера 7×12 этой нулевой строки не содержит. Из структуры матриц $W\left(B_{\delta\neq 0}B_{\nu\neq 0}B_{H\neq 0}\right)$, $W(GGGG)$, $W\left(GG_{\setminus 15}G_{\setminus 8}G_{\setminus 4}\right)$, $P^{(1)}_{r,8}$, $W\left(B_{\delta\neq 0}B_{\nu\neq 0}B_{H\neq 0}\right)$ вытекает таблица 8.

$i=2.\ \ b_\gamma\neq 0,\ \ b_\delta=0,\ \ b_\gamma\oplus b_\nu\oplus b_H\neq 0$. Спектр типа I.

Укороченная проверочная матрица имеет вид

$$P^{(2)}_{r,8}=\begin{bmatrix} B_{\delta=0} & B_1 & B_2 & \dots & B_{\setminus\gamma\neq 0} & \dots & B_{\nu\neq 0} & \dots & B_{H\neq 0} & \dots & B_{\setminus D} \\ G_{\setminus 15} & G & G & \dots & G & \dots & G_{\setminus 8} & \dots & G_{\setminus 4} & \dots & G \end{bmatrix}.$$

Условие $b_\gamma\oplus b_\nu\oplus b_H\neq 0$ означает, что столбцы b_γ,b_ν,b_H линейно независимы. Учитывая (2.6) – (2.10), (2.16) и структуру матрицы $P^{(2)}_{r,8}$, можно показать, что матрица $W\left(B_{\delta=0}B_{\gamma\neq 0}B_{\nu\neq 0}B_{H\neq 0}\right)$ с $b_\gamma\oplus b_\nu\oplus b_H\neq 0$ имеет размер $(2^{r-4}-1)\times 17$ и состоит из 2^{r-7} секций. При этом каждая из

Таблица 8. Спектр весов кода, двойственного коду $\Pi^{(1)}_{r,8}$. Спектр типа I.

Вес (общий случай)	A1 число слов	B1 число слов	C1 число слов	Сумма числа слов	Вес $r=8$	Сумма числа слов
$2^{r-3}-4$		3		3	28	3
$2^{r-3}-3$		6		6	29	6
$2^{r-3}-2$		1		1	30	1
$E-7$			$5\cdot 2^{r-7}-2$	$5\cdot 2^{r-7}-2$	33	8
$E-6$			$15\cdot 2^{r-7}-3$	$15\cdot 2^{r-7}-3$	34	27
$E-5$			$25\cdot 2^{r-7}$	$25\cdot 2^{r-7}$	35	50
$E-4$			$35\cdot 2^{r-7}-3$	$35\cdot 2^{r-7}-3$	36	67
$E-3$	$1\cdot 2^{r-7}$		$30\cdot 2^{r-7}-6$	$31\cdot 2^{r-7}-6$	37	56
$E-2$	$3\cdot 2^{r-7}$		$10\cdot 2^{r-7}-1$	$13\cdot 2^{r-7}-1$	38	25
$E-1$	$3\cdot 2^{r-7}$			$3\cdot 2^{r-7}$	39	6
E	$1\cdot 2^{r-7}-1$			$1\cdot 2^{r-7}-1$	40	1
$2^{r-2}-7$		2		2	57	2
$2^{r-2}-6$		3		3	58	3

$2^{r-7}-1$ одинаковых нижних секций имеет размер 8×17 и нулевую верхнюю строку. Терхняя секция размера 7×17 этой нулевой строки не содержит. Из структуры матриц $W(GGGG)$, $W\left(G_{\setminus 5}GG_{\setminus 8}G_{\setminus 4}\right)$, $P^{(2)}_{r,8}$ и $W\left(B_{\delta=0}B_{\gamma\neq 0}B_{\nu\neq 0}B_{H\neq 0}\right)$ для случая $b_\gamma\oplus b_\nu\oplus b_H\neq 0$ вытекает таблица 9.

Таблица 9. Спектр весов кода, двойственного коду $\Pi^{(2)}_{r,8}$

Вес (общий случай)	A2 число слов	B2 число слов	C2 число слов	Сумма числа слов	Вес $r=8$	Сумма числа слов $r=8$
$2^{r-3}-4$		3		3	28	3
$2^{r-3}-3$		6		6	29	6
$2^{r-3}-2$		1		1	30	1
$E-7$	$1\cdot 2^{r-7}$		$4\cdot 2^{r-7}-2$	$5\cdot 2^{r-7}-2$	33	8
$E-6$	$2\cdot 2^{r-7}$		$13\cdot 2^{r-7}-3$	$15\cdot 2^{r-7}-3$	34	27
$E-5$	$1\cdot 2^{r-7}$		$24\cdot 2^{r-7}$	$25\cdot 2^{r-7}$	35	50
$E-4$			$35\cdot 2^{r-7}-3$	$35\cdot 2^{r-7}-3$	36	67
$E-3$			$31\cdot 2^{r-7}-6$	$31\cdot 2^{r-7}-6$	37	56
$E-2$	$1\cdot 2^{r-7}$		$12\cdot 2^{r-7}-1$	$13\cdot 2^{r-7}-1$	38	25
$E-1$	$2\cdot 2^{r-7}$		$1\cdot 2^{r-7}$	$3\cdot 2^{r-7}$	39	6
E	$1\cdot 2^{r-7}-1$			$1\cdot 2^{r-7}-1$	40	1
$2^{r-2}-7$		2		2	57	2
$2^{r-2}-6$		3		3	58	3

$i=7$. $b_\gamma=0$, $b_\delta\oplus b_\nu\oplus b_H=0$. Спектр типа II.

Укороченная проверочная матрица имеет вид

$$P^{(7)}_{r,8}=\begin{bmatrix} B_0 & B_1 & B_2 & \dots & B_{\delta\neq 0} & \dots & B_{\nu\neq 0} & \dots & B_{H\neq 0} & \dots & B_{\overline{D}} \\ G & G & G & \dots & G_{\setminus 5} & \dots & G_{\setminus 8} & \dots & G_{\setminus 4} & \dots & G \end{bmatrix}.$$

Условие $b_\delta\oplus b_\nu\oplus b_H=0$ означает, что столбцы b_δ, b_ν, b_H линейно зависимы. Учитывая (2.6) –(2.10), (2.16) и структуру матрицы $P^{(7)}_{r,8}$, можно показать, что матрица $W\left(B_{\delta\neq 0}B_{\nu\neq 0}B_{H\neq 0}\right)$ с $b_\delta\oplus b_\nu\oplus b_H=0$ имеет размер $(2^{r-4}-1)\times 12$ и состоит из 2^{r-6} секций. При этом каждая из $2^{r-6}-1$ одинаковых нижних секций имеет размер 4×12 и нулевую верхнюю строку. Верхняя

секция размера 3×12 этой нулевой строки не содержит. Из структуры матриц $W\,(GGGG)$, $W\left(GG_{\setminus 15}G_{\setminus 8}G_{\setminus 4}\right)$, $P^{(7)}_{r,8}$ и $W\,(B_{\delta\neq 0}B_{\nu\neq 0}B_{H\neq 0})$ для случая $b_\delta \oplus b_\nu \oplus b_H = 0$ вытекает таблица 10.

Таблица 10. Спектр весов кода, двойственного коду $\Pi^{(7)}_{r,8}$

Вес (общий случай)	A7 число слов	B7 число слов	C7 число слов	Сумма числа слов	Вес $r=8$	Сумма числа слов $r=8$
$2^{r-3}-4$		3		3	28	3
$2^{r-3}-3$		6		6	29	6
$2^{r-3}-2$		1		1	30	1
$E-7$			$2\cdot 2^{r-6}-2$	$2\cdot 2^{r-6}-2$	33	6
$E-6$			$9\cdot 2^{r-6}-3$	$9\cdot 2^{r-6}-3$	34	33
$E-5$			$12\cdot 2^{r-6}$	$12\cdot 2^{r-6}$	35	48
$E-4$			$15\cdot 2^{r-6}-3$	$15\cdot 2^{r-6}-3$	36	57
$E-3$			$18\cdot 2^{r-6}-6$	$18\cdot 2^{r-6}-6$	37	66
$E-2$	$3\cdot 2^{r-6}$		$4\cdot 2^{r-6}-1$	$7\cdot 2^{r-6}-1$	38	27
E	$2^{r-6}-1$			$2^{r-6}-1$	40	3
$2^{r-2}-7$		2		2	57	2
$2^{r-2}-6$		3		3	58	3

$i = 10$. $b_\gamma, b_\delta, b_\nu, b_H \neq 0$, $\quad b_\gamma, b_\delta, b_\nu, b_H$ линейно независимы. Спектр типа III.

Укороченная проверочная матрица имеет вид

$$P^{(10)}_{r,8} = \begin{bmatrix} B_0 & B_1 & \dots & B_{\gamma\neq 0} & \dots & B_{\delta\neq 0} & \dots & B_{\nu\neq 0} & \dots & B_{H\neq 0} & \dots & B_{\overline{D}} \\ G & G & \dots & G & & \dots G_{\setminus 15} & \dots & G_{\setminus 8} & \dots & G_{\setminus 4} & \dots & G \end{bmatrix}.$$

Учитывая (2.6)–(2.10), (2.16) и структуру матрицы $P^{(10)}_{r,8}$, можно показать, что матрица $W\,(B_{\gamma\neq 0}B_{\delta\neq 0}B_{\nu\neq 0}B_{H\neq 0})$ для ситуации, когда $\quad b_\gamma, b_\delta, b_\nu, b_H$ линейно независимы, имеет размер $(2^{r-4}-1)\times 17$ и состоит из 2^{r-8} секций. При этом каждая из $2^{r-8}-1$ одинаковых нижних секций размер 16×17 и нулевую верхнюю строку. Верхняя секция имеет размер 15×17 и этой нулевой строки не содержит. Таблица 11 следует из структуры матриц $W\,(GGGG)$, $W\left(GG_{\setminus 15}G_{\setminus 8}G_{\setminus 4}\right)$, $P^{(10)}_{r,8}$ и $W\,(B_{\gamma\neq 0}B_{\delta\neq 0}B_{\nu\neq 0}B_{H\neq 0})$ для случая, когда $\quad b_\gamma, b_\delta, b_\nu, b_H$ линейно независимы.

Спектры кодов $\Pi^{(i)}_{r,8}$ с $i = 3, 4, 5, 6, 8, 9$ могут быть получены аналогично вышеизложенному. При этом оказывается, что спектры кодов с $i = 1, \dots, 6$ одинаковы, назовем их спектрами типа I. Спектры кодов с $i = 7, 8, 9$ одинаковы друг с другом, назовем их спектрами типа II. Наконец, код с $i = 10$ имеет тип III. Таблица 1 суммирует все результаты.

Теорема 2.7 доказана.

СПИСОК ЛИТЕРАТУРЫ

1. Fujiwara E. *Code Design for Dependable Systems Theory and Practical Applications.* USA - New Jersey: John Wiley & Sons, Inc., 2006.
2. Micheloni R., Marelli A., Ravasio R. *Error Correction Codes for Non-Volatile Memories.* Qimonda Italy: Springer, 2008.
3. Сагалович Ю.Л. Кодовая защита оперативной памяти ЭВМ от ошибок. *Автоматика и телемеханика,* 1991, т. 52, №5, стр. 3-45.
4. Сидельников В.М. О спектре весов двоичных кодов Боуза-Чоудхури-Хоквингема. *Проблемы передачи информации*, 1971, т. 7, № 1, стр. 14-22. .

Таблица 11. Спектр весов кода, двойственного коду $\Pi_{r,8}^{(10)}$

Вес (общий случай)	A10 число слов	B710 число слов	C10 число слов	Сумма числа слов	Вес $r=8$	Сумма числа слов $r=8$
$2^{r-3}-4$		3		3	28	3
$2^{r-3}-3$		6		6	29	6
$2^{r-3}-2$		1		1	30	1
$E-8$	$1\cdot 2^{r-8}$			2^{r-8}	32	1
$E-7$	$3\cdot 2^{r-8}$		$5\cdot 2^{r-8}-2$	$8\cdot 2^{r-8}-2$	33	6
$E-6$	$3\cdot 2^{r-8}$		$25\cdot 2^{r-8}-3$	$28\cdot 2^{r-8}-3$	34	25
$E-5$	$1\cdot 2^{r-8}$		$55\cdot 2^{r-8}$	$56\cdot 2^{r-8}$	35	56
$E-4$			$70\cdot 2^{r-8}-3$	$70\cdot 2^{r-8}-3$	36	67
$E-3$	$1\cdot 2^{r-8}$		$55\cdot 2^{r-8}-6$	$56\cdot 2^{r-8}-6$	37	50
$E-2$	$3\cdot 2^{r-8}$		$25\cdot 2^{r-8}-1$	$28\cdot 2^{r-8}-1$	38	27
$E-1$	$3\cdot 2^{r-8}$		$5\cdot 2^{r-8}$	$8\cdot 2^{r-8}$	39	8
E	$1\cdot 2^{r-8}-1$			$1\cdot 2^{r-8}-1$	40	0
$2^{r-2}-7$		2		2	57	2
$2^{r-2}-6$		3		3	58	3

5. Kasami T., Fujiwara T., Lin S. An approximation to the weight djstdtution uf binary linear codes. *IEEE Transactions on Information Theory*, 1985, vol. IT-31, no. 3, pp. 769-780.
6. Krasikov I., Litsyn S. On spectra of BCH codes. *IEEE Transactions on Information Theory*, 1995, vol. 41. no. 3, pp. 786-788.
7. Берлекэмп Э. *Алгебраическая теория кодирования.* М.: Мир, 1971. (Berlekamp E.R. *Algebraic Coding Theory.* New-York: McGrow-Hill Book Company, 1968)
8. Кассами Т., Токура Н., Ивадари Ё., Инагаки Я. *Теория кодирования.* М.: Мир, 1978. Перевод с японского.
9. Мак-Вильямс Ф.Дж., Слоэн Н.Дж. *Теория кодов, исправляющих ошибки.* М.: Связь, 1979. (MacWilliams F.J., Sloane N.J.A. *The Theory Error-Correcting Codes.* Amsterdam, New-York: North-Holland Publ. Company, 1977)
10. Barg A., Dumer I. On computing the weight spectrum of cyclic codes. *IEEE Transactions on Information Theory*, 1992, vol. IT-38, no. 4, pp. 1382-1386.
11. Панченко В.И. Об оптимизации линейного кода с расстоянием 4. *VIII Всесоюзная конференция по теории кодирования и передаче информации. Тезисы докладов.* М.-Куйбышев, 1981, часть II: Теория кодирования, стр. 132-134.
12. Davydov A.A., Tombak L.M. An alternative to the Hamming code in the class of SEC-DED codes in semiconductor memory. *IEEE Transactions on Information Theory*, 1991, vol. 37, no. 3, part II, pp. 897-902.
13. Блэйхут Р. *Теория и практика кодов, контролирующих ошибки.* М.: Мир, 1986. (Blahut R.E. *Theory and Practice ofError Control Codes.* Reading: Addison-Wesley Publ. Company, 1984)
14. Колесник В.Д. *Кодирование при передаче и хранении информации (алгебраическая теория блоковых кодов).* М.: Высшая школа, 2009.
15. Давыдов А.А., Томбак Л.М. Квазисовершенные линейные двоичные коды с минимальным расстоянием 4 и полные шапки в проективной геометрии. *Проблемы передачи информации*, 1989, т. 25, № 4, стр. 11-23.
16. Давыдов А.А., Дрожжина-Лабинская А.Ю., Томбак Л.М. Дополнительные корректирующие возможности кодов БЧХ, исправляющих двойные и обнаруживающих тройные ошибки. В кн.: *Вопросы кибернетики. Комплексное проектирование элементно-конструкторской базы супер-ЭВМ.* Под ред. В.А. Мельников, Ю.И. Митропольский. М.: ВИНИТИ, 1988, стр. 86-112.

17. Ашманов С.А. *Линейное программирование.* М.: Наука, 1981.

Design and Analysis of Codes with Distance 4 and 6 to Minimize the Probability of Error Decoding

Afanassiev V.B., Davydov A.A., Zigangirov D.K.

The problem of the decoder error minimizing is considered for a shortened codes of dimention 2^m and code distance 4 and 6. It is proven, that Panchenko codes of distance 4 under correct shortening achieve the minimal probability of decoding error. It follows that Hemming codes are not the best. The correct shortening rules of Panchenko codes are defined and combinatorial method is proposed that minimizes number of code words of the weight 4 and 5. The exact lower bounds of decoding error are given there for Panchenko codes $[39, 32, 4]$ and $[72, 64, 4]$.

There are given upper and lower bounds on the number of code words of minimal weight for BCH codes of distance 6. BCH codes $[45, 32, 4]$ and $[79, 64, 4]$ are constructed with the minimal number codewords of weight 6 (near the lower bound) and probabilities of decoding error are calculated. All the results are oriented for implementation with memory devices.

KEYWORDS: binary code, probability of error decoding, code weight spectrum.