Информационные процессы, Том 16, № 4, 2016, стр. 382–404

Оценка доли стираний, исправляемых линейными кодами [1]

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

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

Поступила в редколлегию 02.12.2016

Аннотация—Исследуется условная вероятность (доля) успешного исправления комбинаций стираний большого веса (больше кодового растояния) линейным кодом с частично известным или неизвестным спектром весов кодовых слов. Полученные оценки условных вероятностей и методы их вычисления относятся к произвольным двоичным линейным кодам и двоичным кодам Хэмминга, Панченко и БЧХ, включая их расширения и укорочения. Выводятся оценки вероятности обнаружения ошибок при исправлении стираний. Предлагаются алгоритмы декодирования кода-произведения с исправлением стираний большого веса компонентными кодами Хэмминга, Панченко, БЧХ и дается оценка сверху вероятности отказа от декодирования.

КЛЮЧЕВЫЕ СЛОВА: линейный код, исправление стираний, код-произведение

1. ВВЕДЕНИЕ

Задача исправления стираний в стирающем канале исследуется давно. Известна пропускная способность для канала с независимыми ошибками и стираниями. Известны экспоненциальные границы вероятности ошибки для схем кодирования – декодирования, включающих стирания, списки переменной длины, обратную связь [1]. Известны алгоритмы и границы для декодирования по обобщенному расстоянию и многие другие результаты. Список работ огромен! Тем не менее, для двоичных линейных кодов остались недостаточно исследованными многие задачи. Например, следующие: *доля исправляемых комбинаций стираний веса больше или равного кодовому расстоянию для произвольных и конкретных классов кодов, вероятность отказа декодера при исправлении только стираний или ошибок и стираний.* В настоящее время весьма активно исследуется корректирующая способность LDPC кодов в стирающем канале. Имеется длинный список работ в этой области. Например, в работе [2] исследуется исправление стираний композицией LDPC кодов с кодом Хэмминга, при этом выводятся и используются (в каскадной схеме декодирования) точные оценки доли исправляемых стираний большого веса для двоичного кода Хэмминга. Отметим также работу [3], где рассматривается доля стираний, исправляемых недвоичными кодами. Для оценки доли исправляемых комбинаций стираний полезны результаты, связанные с исследованием минимальных слов в линейных кодах [4].

Оценка доли исправляемых стираний большого веса необходима для оптимизации декодирования в канале со стираниями и ошибками и декодирования произведения кодов или каскадных кодов. Интерес представляет зависимость между снижением вероятности отказа и ошибки декодера и расширением области декодирования.

Вопросы сложности исправления стираний большого веса активно исследовались в период 1963 – 1980 в условиях очень низкой производительности вычислительных устройств. Например, в работах [5, 6] исследуются алгоритмы и схемы исправления стираний большого веса и обнаружения ошибок для линейных и некоторых циклических кодов. В настоящее время вопрос сложности не является настолько критическим, хотя остается важным.

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

Теоретическая часть работы, относящаяся к исправлению стираний большого веса, содержит оценки (точные или снизу) доли исправляемых комбинаций стираний заданного веса (от кодового расстояния до числа проверок кода) для произвольных и конкретных блоковых кодов с известным спектром весов, с частично известным и полностью неизвестным спектром весов кодовых слов. В ряде случаев эти оценки являются точными. Доказано, что при укорочении кода доля исправляемых конфигураций не уменьшается и, в принципе, может возрастать. Показано также, что при определенных (часто выполняемых) условиях доли исправляемых конфигураций не меняются при расширении кода. Это относится, в частности, к неукороченным кодам Хэмминга с $d = 3$ и БЧХ с $d = 5$. В качестве объектов подробного исследования выбраны коды Хэмминга и Панченко с расстоянием 4 и БЧХ с расстоянием 6.

В прикладном аспекте данная работа является продолжением работы [7] в направлении повышения надежности устройств долговременной памяти типа твердотельных накопителей (SSD) или их модификаций. В устройствах памяти этого типа деградация канала (ячеек памяти) успевает проявиться в виде накопления ошибок. Однако скорость накопления ошибок относительно мала, а каждый цикл записи запускает процесс накопления ошибок заново. С целью оптимизации процесса чтения и записи файла подкачки обмен данными между оперативной и долговременной памятью происходит в виде блоков достаточно большого объема (десятки или сотни и даже тысячи стандартных слов). Естественный компромисс между сложностью и надежностью состоит в использовании каскадной конструкции кодирования, сохраняющей кодирование стандартных слов и дополненной общим кодированием набора слов. В качестве такой компромиссной конструкции рассматривается произведение компонентных кодов из работы [7].

Нерешенной задачей для произведения двоичных кодов остается, например, задача наилучшего декодирования с исправлением частично зависимых конфигураций ошибок в “соседних” (в каком-либо конструктивном смысле) словах. Часто такие “пятна” ошибок возникают при внешнем облучении микросхем памяти или критическом температурном режиме. Исправление стираний большого веса позволяет расширить область декодирования произведения кодов (Хэмминга, Панченко и БЧХ) с кодовым расстоянием 4 и 6. В результате, размер исправляемых *почти всех* “пятен” ошибок может существенно превышать размер порядка 4×4 и 6×6.

В работе приводится оценка доли исправляемых конфигураций ошибок большого веса для компонентных кодов и оценка вероятности правильного декодирования и отказа для произведения кодов. Строго говоря, оценки делаются в предположении независимости ошибок и стираний из-за отсутствия адекватной (области применения) модели зависимых событий. На самом деле, это не является существенным “минусом” для данной работы, так как все исправляемые комбинации стираний располагаются в некотором (ограниченном) количестве строк или столбцов и, следовательно, любая конфигурация “пятна” является их подмножеством. Оценка вероятности отказа для “расширенного” декодирования произведения кодов Панченко и БЧХ с исправлением комбинаций стираний большого веса показывает радикальное снижение вероятности отказа по сравнению с “нерасширенным” декодером кода-произведения (ограниченным весом меньше кодового расстояния) даже при увеличении веса на единицу.

На самом деле, понятие “пятно” ошибок (или двумерный пакет ошибок) появилось давно. Оно связано с теорией Марковских процессов в каналах связи. В прикладных задачах это понятие связано с кодированием для жестких дисков, ленточных и дискетных носителей, для оптических дисков (CD, DVD) [8]. В области кодирования для твердотельных накопителей доступный ресурс жестко ограничен, прежде всего, по допустимой задержке. По этой причине в качестве объектов подробного исследования выбраны коды Хэмминга и Панченко с расстоянием 4 и БЧХ с расстоянием 6.

Обозначим через $[n, n-r, d]$ линейный двоичный код длины n, избыточности r с минимальным расстоянием d. Введем обозначения величин, связанных с этим кодом:

n – длина кода; r – число проверочных символов; d – минимальное расстояние кода;

A_w – число кодовых слов веса w;

ρ – вес стираний, исправление которых анализируется (рассматриваются только ситуации $\rho \le r$);

S_ρ – число исправляемых кодом конфигураций стираний веса ρ (эквивалентно, количество различных наборов из ρ линейно независимых столбцов проверочной матрицы кода или количество в проверочной матрице различных $r \times \rho$-подматриц полного ранга);

δ_ρ – доля исправляемых кодом стираний веса ρ, определяемая соотношением

$$\delta_\rho = \frac{S_\rho}{\binom{n}{\rho}} \le 1. \tag{1.1}$$

Очевидно, что для любого $[n, n-r, d]$ кода справедливо

$$S_\rho = \binom{n}{\rho}, \quad \delta_\rho = 1, \quad \text{если и только если } \rho \le d-1. \tag{1.2}$$

Для двоичного неукороченного $[2^r-1, 2^r-1-r, 3]$ кода Хэмминга обозначим:

$S^H_{\rho,r}$ – число исправляемых конфигураций стираний веса ρ;

$\delta^H_{\rho,r}$ – доля исправляемых стираний веса ρ, где $\delta^H_{\rho,r} = \frac{S^H_{\rho,r}}{\binom{2^r-1}{\rho}} \le 1$ в соответствии с (1.1).

Для двоичного неукороченного $\left[2^{r-1}, 2^{r-1}-r, 4\right]$ расширенного кода Хэмминга, полученного из $[2^{r-1}-1, 2^{r-1}-r, 3]$ кода добавлением проверки на четность, обозначим:

$S^{H\bullet}_{\rho,r}$ – число исправляемых конфигураций стираний веса ρ;

$\delta^{H\bullet}_{\rho,r}$ – доля исправляемых стираний веса ρ, где $\delta^{H\bullet}_{\rho,r} = \frac{S^{H\bullet}_{\rho,r}}{\binom{2^{r-1}}{\rho}} \le 1$ в соответствии с (1.1).

Работа организована следующим образом. В разделе 2 рассмотрен метод вычисления числа S_ρ наборов линейно независимых столбцов проверочной матрицы кода с известным спектром весов. Выводятся соответствующие асимптотические оценки. Предложен рекурсивный подход к оценке величины δ_ρ. В разделе 3 даны рекуррентные оценки S_ρ, δ_ρ для произвольных кодов и кодов с четными весами. Показана связь и совместное использование весового и рекуррентного подходов. Для кода Хэмминга с $d = 3$ и его расширения получены точные значения $S^H_{\rho,r}$, $\delta^H_{\rho,r}$, $S^{H\bullet}_{\rho,r}$, $\delta^{H\bullet}_{\rho,r}$. В разделе 4 исследованы соотношения между величинами S_ρ, δ_ρ в укороченных и неукороченных кодах и выколотых и расширенных кодах. В разделе 5 получены формулы для вычисления S_ρ, δ_ρ для кодов Хэмминга, Панченко и БЧХ, основанные на результатах предыдущих разделов, приведены соответствующие графики и таблицы. В разделе 6 рассмотрено исправление стираний с обнаружением ошибок. В разделах 7, 8 предложены алгоритмы декодирования кода-произведения с использованием исправления стираний большого веса и даны формулы вычисления вероятности успешного декодирования. Приведен ряд примеров.

2. ДОЛЯ СТИРАНИЙ, ИСПРАВЛЯЕМЫХ ЛИНЕЙНЫМИ КОДАМИ С ИЗВЕСТНЫМ СПЕКТРОМ ВЕСОВ

2.1. Число наборов линейно независимых столбцов проверочной матрицы кода с известным спектром весов

Необходимым условием исправления стираний веса ρ является полный ранг подматрицы, составленной из столбцов проверочной матрицы кода, соответствующих стертым позициям. В этом разделе оценивается число и доля таких подматриц.

Далее для $[n, n-r, d]$ кода со спектром весов $A_0, A_1, \ldots, A_n$ используется функция

$$\Psi(n, d, \rho) = \binom{n}{\rho} - \sum_{w=d}^{\rho} A_w \binom{n-w}{\rho-w}, \quad d \le \rho \le r, \tag{2.1}$$

значение которой является нижней оценкой количества S_ρ конфигураций стираний веса ρ, исправляемых рассматриваемым кодом. (В ряде случаев эта оценка точная.) Если необходимо подчеркнуть, что функция $\Psi(n, d, \rho)$ вычисляется для некоторого $[n, n-r, d]$ кода C, записывается $\Psi(n, d, \rho, C)$.

Теорема 2.1. *Доля δ_ρ стираний веса ρ, исправляемых $[n, n-r, d]$ кодом, и число S_ρ различных наборов из ρ линейно независимых столбцов проверочной матрицы этого кода удовлетворяют следующим оценкам снизу:*

$$\delta_\rho \ge \frac{\Psi(n, d, \rho)}{\binom{n}{\rho}}, \quad S_\rho \ge \Psi(n, d, \rho), \quad d \le \rho \le r. \tag{2.2}$$

В частности, справедливы равенства

$$\delta_\rho = \frac{\Psi(n, d, \rho)}{\binom{n}{\rho}}, \quad S_\rho = \Psi(n, d, \rho), \tag{2.3}$$

если выполняется условие

$$\rho - d \le \frac{d-1}{2}. \tag{2.4}$$

Доказательство. Величина S_ρ равна разности между общим числом наборов из ρ столбцов проверочной матрицы $\binom{n}{\rho}$ и числом конфигураций из ρ линейно зависимых столбцов. Любая конфигурация из ρ линейно зависимых столбцов проверочной матрицы может быть получена добавлением $\rho - w$ столбцов к набору из w столбцов с нулевой суммой, соответствующему кодовому слову веса w (поэтому $\rho \ge w$). Для фиксированного набора из w столбцов число способов выбора указанных $\rho - w$ столбцов равно $\binom{n-w}{\rho-w}$. Сказанное объясняет структуру выражения (2.1). Подматрица проверочной матрицы размера $r \times \rho$, где $d \le \rho \le r$, в принципе, может содержать более одного подмножества из $\ge d$ столбцов, имеющих нулевую сумму. Это ведет к тому, что в (2.1) некоторые линейно зависимые конфигурации столбцов подсчитываются (и затем вычитаются из $\binom{n}{\rho}$) более одного раза. Поэтому в (2.2) появляется знак "$\ge$". При условии (2.4) все линейно зависимые конфигурации столбцов подсчитываются (и вычитаются из $\binom{n}{\rho}$) однократно, откуда следует равенство в (2.3). Теорема доказана.

Замечание 1. Насколько известно авторам, впервые оценка вида (2.1) появилась в работе О.В. Попова 1967 года [5].

Замечание 2. Из (2.1), (2.3), (2.4) следует, что для всех $[n, n-r, d]$ кодов число S_d различных наборов из d линейно независимых столбцов проверочной матрицы составляет $S_d = \binom{n}{d} - A_d$, откуда $\max\{S_d(n, r)\} = \binom{n}{d} - \min\{A_d(n, r)\}$, где $\max\{S_d(n, r)\}$ – максимально возможное значение величины S_d при фиксированных n, r, d, $\min\{A_d(n, r)\}$ – минимально возможное число слов минимального веса при фиксированных n, r, d. Границы для $\min\{A_d(n, r)\}$ и коды, достигающие границ, можно найти в [9–13].

Спектры весов кодов и их асимптотика изучались (и продолжают изучаться) многочисленными авторами, см. например, работы [7, 9–21] и ссылки в них.

Оценки теоремы 2.1 могут быть улучшены с помощью следующей очевидной леммы.

Лемма 2.1. *Любой набор из ρ линейно зависимх столбцов проверочной матрицы является объединением набора из w столбцов с нулевой суммой, соответствующего кодовому слову веса w, и набора из $\rho - w$ линейно независимых столбцов, где $d \le w \le \rho$.*

Используя рекурсивным образом функцию типа (2.1), на основе леммы 2.1 построим *рекурсивную схему* включения-исключения, которая, в принципе, улучшает оценку (2.2):

$$\tilde{\Psi}(n,d,\rho) = \binom{n}{\rho} - \sum_{w=d}^{\rho} A_w(n)\tilde{\Psi}(n-w,d,\rho-w),$$

где $A_w(n)$ - число слов веса w в коде длины n. Оценка доли исправляемых стираний для одного и двух шагов рекурсии имеет вид, соотвественно,

$$\tilde{\delta}\,(n,d,\rho) = \frac{\tilde{\Psi}(n,d,\rho)}{\binom{n}{\rho}} = 1 - \sum_{w=d}^{\rho} A_w(n)\tilde{\delta}(n-w,d,\rho-w)\frac{\binom{n-w}{\rho-w}}{\binom{n}{\rho}};$$

$$\tilde{\delta}\,(n,d,\rho) = 1 - \sum_{w_1=d}^{\rho} A_{w_1}(n)\frac{\binom{n-w_1}{\rho-w_1}}{\binom{n}{\rho}}\left[1 - \sum_{w_2=d}^{\rho-w_1} A_{w_2}\,(n-w_1)\,\frac{\binom{n-w_1-w_2}{\rho-w_1-w_2}}{\binom{n-w_1}{\rho-w_1}}\right].$$

2.2. Асимптотическая оценка доли исправляемых стираний

Мотивацией включения в процесс декодирования стираний большого веса может служить следующее наблюдение. Если воспользоваться известным биномиальным приближением спектра весов линейного кода [15,17,18,20] $A_w \approx 2^{-z}\binom{n}{w},\ r-1 < z \le r,\ w \ge d$, где z- вещественное число, учитывающее (в принципе) поправочный член в упомянутых приближениях и ограничение диапазона весов $w \ge d$, то можно получить следующую приближенную оценку поведения функции S_ρ для интервала $d \le \rho < r$.

$$S_\rho \ge \binom{n}{\rho} - \sum_{w=d}^{\rho} A_w\binom{n-w}{\rho-w} \approx \binom{n}{\rho} - 2^{-z}\sum_{w=d}^{\rho}\binom{n}{w}\binom{n-w}{\rho-w} = \binom{n}{\rho} - 2^{-z}\binom{n}{\rho}\sum_{w=d}^{\rho}\binom{\rho}{w}.$$

Отсюда, см. [18, лемма 10.8], получаем оценку доли исправляемых стираний большого веса

$$\delta_\rho \ge \frac{S_\rho}{\binom{n}{\rho}} \approx 1 - 2^{-z}\sum_{w=d}^{\rho}\binom{\rho}{w} \approx 1 - 2^{-z}\cdot 2^{\rho H(d/\rho)} \ge 1 - 2^{\rho-z},\ d \le \rho < z,$$

где $H(d/\rho)$- двоичная энтропия. Контрольная точка $S_d \times \binom{n}{d}^{-1} \approx 1$.

Из предложенной оценки видно, что доля исправляемых стираний большого веса убывает экспоненциально с ростом веса при фиксированном числе проверок. По этой причине можно считать достаточным (мягкое) ограничение интервала весов комбинаций стираний величиной порядка $2d$ (или меньше).

3. РЕКУРРЕНТНАЯ ОЦЕНКА ДОЛИ ИСПРАВЛЯЕМЫХ СТИРАНИЙ

Введем обозначение

$$\lambda(d,\rho) = \begin{cases} 0 & \text{для } d = 3 \\ \sum\limits_{i=2}^{d-2}\binom{\rho-1}{i} & \text{для } d \ge 4 \end{cases}.$$

Лемма 3.1. *Количество S_ρ различных наборов из ρ линейно независимых столбцов проверочной матрицы $[n, n-r, d]$ кода реккурентно оценивается следующим образом:*

$$S_\rho \geq \frac{1}{\rho} S_{\rho-1} \cdot \left(n + 1 - 2^{\rho-1} + \lambda(d,\rho)\right), \quad d \leq \rho \leq r. \tag{3.1}$$

В частности, для $[2^r - 1, 2^r - 1 - r, 3]$ кода Хэмминга имеет место равенство

$$S^H_{\rho,r} = \frac{1}{\rho} S^H_{\rho-1,r} \cdot \left(2^r - 2^{\rho-1}\right), \quad 3 \leq \rho \leq r. \tag{3.2}$$

Доказательство. Набор Γ_ρ из ρ линейно независимых столбцов проверочной матрицы можно получить, добавляя некоторый (правильно выбранный) столбец к набору $\Gamma^{(b)}_{\rho-1}$ из $\rho-1$ линейно независимых столбцов. Здесь b номер набора, $b = 1, 2, \ldots, S_{\rho-1}$. Добавляемый столбец выбирается из $n-(\rho-1)$ столбцов матрицы, не входящих в набор $\Gamma^{(b)}_{\rho-1}$. Это объясняет член $n-\rho+1$ в формуле (3.3) ниже.

Пусть $\rho - 1 \geq d - 1$ и $2 \leq j \leq \rho - 1$. Обозначим через $\Gamma^{(b,u)}_{\rho-1,j}$ подмножество из j столбцов набора $\Gamma^{(b)}_{\rho-1}$, где u - номер подмножества, $u = 1, 2, \ldots, \binom{\rho-1}{j}$. Любое подмножество $\Gamma^{(b,u)}_{\rho-1,j}$ является линейно независимым, и сумма $\Sigma^{(b,u)}_j$ всех столбцов подмножества не равна нулю. Поэтому добавляемый столбец не может быть равен $\Sigma^{(b,u)}_j$ для всех подмножеств $\Gamma^{(b,u)}_{\rho-1,j}$, иначе мы получим линейно зависимый набор из ρ столбцов. Если $2 \leq j \leq d-2$, то в проверочной матрице не может присутствовать столбец, равный $\Sigma^{(b,u)}_j$: это привело бы к существованию в матрице $j+1$ столбцов с нулевой суммой, где $j+1 \leq d-1$. Поэтому далее мы рассматриваем ситуации $d-1 \leq j \leq \rho-1$. В формуле (3.3) ниже член $\sum_{j=d-1}^{\rho-1} \binom{\rho-1}{j}$ оценивает *сверху* число столбцов, которые нельзя добавить к набору $\Gamma^{(b)}_{\rho-1}$. Можно показать, что для фиксированного b и произвольных u, j все суммы $\Sigma^{(b,u)}_j$ различны, иначе набор $\Gamma^{(b)}_{\rho-1}$ не был бы линейно независимым. С другой стороны, столбец, равный $\Sigma^{(b,u)}_j$, может отсутствовать в проверочной матрице. Поэтому член $\sum_{j=d-1}^{\rho-1} \binom{\rho-1}{j}$ является оценкой именно *сверху*, что объясняет знак "$\geq$" в (3.3).

Каждый набор Γ_ρ будет повторен при указанном построении ρ раз, поэтому в (3.3) появляется делитель ρ. Таким образом, количество S_ρ различных наборов Γ_ρ можно оценить формулой

$$S_\rho \geq \frac{1}{\rho} S_{\rho-1} \cdot \left(n - \rho + 1 - \sum_{j=d-1}^{\rho-1} \binom{\rho-1}{j}\right). \tag{3.3}$$

Легко видеть, что

$$-\rho + 1 - \sum_{j=d-1}^{\rho-1} \binom{\rho-1}{j} = -(2^{\rho-1} - 1 - \lambda(d,\rho)),$$

откуда следует (3.1).

В проверочной матрице $[2^r - 1, 2^r - 1 - r, 3]$ кода Хэмминга присутствуют все ненулевые столбцы размера r. Поэтому в (3.3) и, соответственно, в (3.1) неравенство заменяется равенством, откуда следует (3.2). Лемма доказана.

Далее для $[n, n-r, d]$ кода используется функция

$$\Phi(n,d,\rho) = \frac{1}{d(d+1)\ldots\rho} \binom{n}{d-1} \prod_{j=d}^{\rho} \left(n + 1 - 2^{j-1} + \lambda(d,j)\right), \; d \leq \rho \leq r, \tag{3.4}$$

значение которой является нижней оценкой количества конфигураций стираний веса ρ, исправляемых рассматриваемым кодом. (Для кода Хэмминга с $d = 3$ эта оценка точная.)

Теорема 3.1. *Количество S_ρ различных наборов из ρ линейно независимых столбцов проверочной матрицы $[n, n-r, d]$ кода оценивается следующим образом:*

$$S_\rho \geq \Phi(n, d, \rho), \quad d \leq \rho \leq r. \tag{3.5}$$

В частности, для $[2^r - 1, 2^r - 1 - r, 3]$ кода Хэмминга имеет место равенство [2, 3]

$$S^H_{\rho,r} = \frac{1}{\rho!} \prod_{j=1}^{\rho} (2^r - 2^{j-1}), \quad 3 \leq \rho \leq r. \tag{3.6}$$

Доказательство. Полагая $\rho = d-1$ в (1.2) и итеративно применяя (3.1), получаем (3.5). Для кода Хэмминга итеративно применяем (3.2).

Замечание 3. Пусть q - степень простого числа. В [3, лемма, с. 64] доказано, что в $r \times (q^r - 1)$-матрице, содержащей все возможные ненулевые q-ичные r-разрядные столбцы, число линейно независимых наборов из ρ столбцов составляет

$$\frac{1}{\rho!}(q^r - 1)(q^r - q)(q^r - q^2) \dots (q^r - q^{\rho-1}). \tag{3.7}$$

В [4, теорема 2.7, доказательство] показано, что в проверочной матрице q-ичного $[\frac{q^r-1}{q-1}, \frac{q^r-1}{q-1} - r, 3]$ кода Хэмминга число линейно независимых наборов из ρ столбцов равно $\frac{1}{\rho!} \prod_{j=1}^{\rho} \frac{q^r - q^{j-1}}{q-1}$. Соотношение (3.6) является частным случаем приведенных выражений из [3] и [4] для $q = 2$. В [2, лемма 2] выражение (3.6) получено непосредственно для двоичного случая.

Рассмотрим двоичные *коды с четными весами.*

Введем обозначение

$$\lambda^\bullet(d, \rho) = \begin{cases} 0 & \text{для } d = 4 \\ \sum\limits_{i=2}^{d/2-1} \binom{\rho-1}{2i-1} & \text{для } d \geq 6 \end{cases}.$$

Лемма 3.2. *Количество S_ρ различных наборов из ρ линейно независимых столбцов проверочной матрицы $[n, n-r, d]$ кода реккурентно оценивается следующим образом:*

$$S_\rho \geq \frac{1}{\rho} S_{\rho-1} \cdot \left(n - 2^{\rho-2} + \lambda^\bullet(d, \rho)\right), \quad d \leq \rho \leq r, \text{ если все веса кода четные.} \tag{3.8}$$

В частности, для $\left[2^{r-1}, 2^{r-1} - r, 4\right]$ расширенного кода Хэмминга имеет место равенство

$$S^{H\bullet}_{\rho,r} = \frac{1}{\rho} S^{H\bullet}_{\rho-1,r} \cdot \left(2^{r-1} - 2^{\rho-2}\right), \quad 4 \leq \rho \leq r. \tag{3.9}$$

Доказательство. Доказательство аналогично доказательству леммы 3.1. При этом учитываем, что в проверочной матрице кода с четными весами сумма четного числа столбцов не может быть равна никакому столбцу проверочной матрицы. Оценка (3.3) принимает вид

$$S_\rho \geq \frac{1}{\rho} S_{\rho-1} \cdot \left(n - \rho + 1 - \sum_{j=d/2}^{\lceil(\rho-1)/2\rceil} \binom{\rho-1}{2j-1} \right).$$

Легко увидеть, что

$$-\rho+1-\sum_{j=d/2}^{\lceil(\rho-1)/2\rceil}\binom{\rho-1}{2j-1}=-(2^{\rho-2}-\lambda^{\bullet}(d,\rho)),$$

откуда непосредственно следует (3.8).

Для расширенного кода Хэмминга учитываем, что его проверочная матрица содержит все возможные столбцы размера r с единицей в верхней позиции. Лемма доказана.

Далее для $[n, n-r, d]$ кода с четными весами используется функция

$$\Phi^{\bullet}(n,d,\rho)=\frac{1}{d(d+1)\dots\rho}\binom{n}{d-1}\prod_{j=d}^{\rho}\left(n-2^{j-2}+\lambda^{\bullet}(d,\rho)\right), \tag{3.10}$$

значение которой является нижней оценкой количества конфигураций стираний веса ρ, исправляемых рассматриваемым кодом. (Для кода Хэмминга с $d=4$ эта оценка точная.)

Теорема 3.2. *Количество S_ρ различных наборов из ρ линейно независимых столбцов проверочной матрицы $[n, n-r, d]$ кода оценивается следующим образом:*

$$S_\rho\geq\Phi^{\bullet}(n,d,\rho),\quad d\leq\rho\leq r,\ \text{если все веса кода четные.} \tag{3.11}$$

В частности, для $\left[2^{r-1}, 2^{r-1}-r, 4\right]$ расширенного кода Хэмминга имеет место равенство

$$S^{H\bullet}_{\rho,r}=\frac{2^{r-1}}{\rho!}\prod_{j=2}^{\rho}(2^{r-1}-2^{j-2}),\quad 4\leq\rho\leq r. \tag{3.12}$$

Доказательство. Полагая $\rho=d-1$ в (1.2) и итеративно применяя (3.8), получаем (3.11). Для кода Хэмминга итеративно применяем (3.9).

Замечание 4. Соотношение (3.12) впервые получено в [4, теорема 2.8, доказательство].

Из теорем 2.1, 3.1, 3.2 вытекают следствия 3.1, 3.2.

Следствие 3.1. *Доля δ_ρ стираний веса ρ, исправляемых $[n, n-r, d]$ кодом, для $d\leq\rho\leq r$ оценивается следующим образом:*

$$\delta_\rho\geq\prod_{j=d}^{\rho}\frac{n+1-2^{j-1}+\lambda(d,j)}{n+1-j}\quad\text{для произвольного кода;} \tag{3.13}$$

$$\delta_\rho\geq\prod_{j=d}^{\rho}\frac{n-2^{j-2}+\lambda^{\bullet}(d,j)}{n+1-j},\quad\text{если все веса кода четные.} \tag{3.14}$$

В частности, для $[2^r-1, 2^r-1-r, 3]$ и $\left[2^{r-1}, 2^{r-1}-r, 4\right]$ кодов Хэмминга имеют место равенства, соответственно,

$$\delta^{H}_{\rho,r}=\prod_{j=3}^{\rho}\frac{2^r-2^{j-1}}{2^r-j}\ , \tag{3.15}$$

$$\delta^{H\bullet}_{\rho,r}=\prod_{j=4}^{\rho}\frac{2^{r-1}-2^{j-2}}{2^{r-1}+1-j}=\delta^{H}_{\rho-1,r-1}. \tag{3.16}$$

Из (3.13), (3.14) видно, что при фиксированном n оценка доли δ_ρ убывает с ростом ρ. Также из (3.15), (3.16) следует, что при фиксированном r доли $\delta^H_{\rho,r}$ и $\delta^{H^\bullet}_{\rho,r}$ убывают с ростом ρ.

Следствие 3.2. *Количество S_ρ различных наборов из ρ линейно независимых столбцов проверочной матрицы $[n, n-r, d]$ кода, не являющегося неукороченным кодом Хэмминга, для $\rho \le r$ и $\rho - d > \frac{d-1}{2}$ оценивается следующим образом:*

$$S_\rho \ge \begin{cases} \max\{\Psi(n,d,\rho), \Phi(n,d,\rho)\} & \text{для произвольного кода} \\ \max\{\Psi(n,d,\rho), \Phi^\bullet(n,d,\rho)\}, & \text{если все веса кода четные} \end{cases}. \tag{3.17}$$

Из теоремы 2.1 и доказательства теорем 3.1, 3.2 следует, что, как правило, максимум в формуле (3.17) равен $\Psi(n,d,\rho)$, поскольку в проверочной матрице кода присутствуют не все возможные столбцы. Кроме того, в случае, когда имеет место неравенство

$$n \le \begin{cases} 2^{\rho-1} - 1 - \lambda(d,\rho) & \text{для произвольного кода} \\ 2^{\rho-2} - \lambda^\bullet(d,\rho), & \text{если все веса кода четные} \end{cases},$$

справедливо $\Phi(n,d,\rho) \le 0$ и $\Phi^\bullet(n,d,\rho) \le 0$.

С другой стороны, спектр весов кода не всегда известен. Часто имеются сведения только об относительно небольших весах. В таких случаях целесообразно вычислять функцию $\Psi(n,d,\rho)$, пока есть возможность, а затем использовать последнее вычисленное значение $\Psi(n,d,\rho)$ как старт для рекуррентного процесса на основе лемм 3.1 и 3.2. Такой подход использован в следствии 3.3, утверждении 2 и примерах 2, 5, 6.

Следствие 3.3. *Количество S_ρ различных наборов из ρ линейно независимых столбцов проверочной матрицы $[n, n-r, d]$ кода, не являющегося неукороченным кодом Хэмминга, для $d \le \rho_0 < \rho \le r$ оценивается следующим образом.*

1. Для произвольного $[n, n-r, d]$ кода справедливо

$$S_\rho \ge \frac{1}{(\rho_0+1)(\rho_0+2)\dots\cdot\rho}\Psi(n,d,\rho_0)\prod_{j=\rho_0+1}^{\rho}\left(n+1-2^{j-1}+\lambda(d,j)\right). \tag{3.18}$$

2. Если все веса $[n, n-r, d]$ кода четные, то справедливо

$$S_\rho \ge \frac{1}{(\rho_0+1)(\rho_0+2)\dots\cdot\rho}\Psi(n,d,\rho_0)\prod_{j=\rho_0+1}^{\rho}\left(n-2^{j-2}+\lambda^\bullet(d,j)\right). \tag{3.19}$$

Замечание 5. В работе [3] рассмотрено исправление стираний q-ичным циклическим $[n, n-r, d]_q$ кодом. Приведена нижняя оценка доли исправляемых стираний, основанная на соотношении (3.7). Для двоичных кодов с расстоянием $d > 3$ эта оценка хуже, чем оценки, полученные в настоящей статье.

4. ДОЛЯ СТИРАНИЙ, ИСПРАВЛЯЕМЫХ УКОРОЧЕННЫМИ, РАСШИРЕННЫМИ И ВЫКОЛОТЫМИ КОДАМИ

В данном разделе мы показываем, что при укорочении кода доля исправляемых конфигураций стираний не уменьшается и, в принципе, может возрастать. Показано также, что при определенных (часто выполняемых) условиях доли исправляемых конфигураций не меняются при расширении кода. Это относится, в частности, к неукороченным кодам Хэмминга с $d = 3$ и БЧХ с $d = 5$.

4.1. Доля стираний, исправляемых укороченными кодами

Теорема 4.1. *Пусть $\rho \le r$. Пусть проверочная матрица двоичного линейного $[n_0, n_0 - r, d]$ кода C_{n_0} длины n_0 содержит $S_\rho(n_0)$ наборов из ρ линейно независимых столбцов. Тогда существует укороченный $[n, n-r, d]$ код C_n длины $n < n_0$ с проверочной матрицей, содержащей $S_\rho(n)$ наборов из ρ линейно независимых столбцов, где*

$$S_\rho(n) \ge S_\rho(n_0)\frac{\binom{n_0-\rho}{n-\rho}}{\binom{n_0}{n}} = S_\rho(n_0)\frac{\binom{n}{\rho}}{\binom{n_0}{\rho}}. \tag{4.1}$$

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. Каждый набор из ρ линейно независимых столбцов неукороченной проверочной матрицы H_{n_0} остается неизменным в $\binom{n_0-\rho}{n-\rho}$ укороченных матрицах H_n. Следовательно, сумма количества наборов из ρ линейно независимых столбцов проверочной матрицы во всех укороченных кодах C_n равна $S_\rho(n_0)\binom{n_0-\rho}{n-\rho}$. Всего имеется $\binom{n_0}{n}$ укороченных кодов. Проведя усреднение по всем укороченным кодам, получаем $S_\rho(n) \ge S_\rho(n_0)\frac{\binom{n_0-\rho}{n-\rho}}{\binom{n_0}{n}}$. Окончательный вид соотношения (4.1) получаем после несложных преобразований. Теорема доказана.

Следствие 4.1. *Пусть $\rho \le r$. Пусть для проверочной матрицы двоичного $[n_0, n_0 - r, d]$ кода C_{n_0} длины n_0 доля исправляемых стираний веса ρ равна $\delta_\rho(n_0)$. Тогда существует укороченный $[n, n-r, d]$ код C_n длины $n < n_0$ с проверочной матрицей, обеспечивающей долю $\delta_\rho(n)$ исправляемых стираний веса ρ такую, что*

$$\delta_\rho(n) \ge \delta_\rho(n_0). \tag{4.2}$$

Доказательство. Из (4.1) следует, что

$$\delta_\rho(n) = \frac{S_\rho(n)}{\binom{n}{\rho}} \ge \frac{S_\rho(n_0)}{\binom{n_0}{\rho}} = \delta_\rho(n_0).$$

Пример 3, иллюстрирующий теорему 4.1 и следствие 4.1, приведен в разделе 5.2.

Далее для $t-(v,k,\lambda)$ схем обозначения и определения соответствуют [18, Глава 2].

Теорема 4.2. *Пусть $d \le \rho \le r$. Пусть в $[n_0, n_0 - r, d]$ коде C_{n_0} длины n_0 слова любого веса w образуют $1-(n_0, w, \lambda)$ схему. Предположим, что проверочная матрица $[n, n-r, d]$ кода C_n длины $n = n_0 - 1$ получена путем вычеркивания одного столбца из проверочной матрицы кода C_{n_0}. Тогда для всех ρ справедливо*

$$\frac{\Psi(n_0, d, \rho, C_{n_0})}{\binom{n_0}{\rho}} = \frac{\Psi(n, d, \rho, C_n)}{\binom{n}{\rho}}, \tag{4.3}$$

где левая и правая части равенства получены для кодов C_{n_0} и C_n, соответственно.

В частности, если $\rho - d \le \frac{d-1}{2}$, доля исправляемых стираний веса ρ одинакова для кодов C_{n_0} и C_n.

Доказательство. Число блоков $1-(n_0, w, \lambda)$ схемы равно количеству $A_w(C_{n_0})$ слов веса w в коде C_{n_0}. Параметр λ равен числу слов веса w, связанных с каждым столбцом проверочной матрицы кода C_{n_0}. При удалении любого столбца эти слова "разрушаются", и в коде C_n сохранится только $A_w(C_n) = A_w(C_{n_0}) - \lambda$ слов веса w. Из [18, Глава 2, Следствие 10] получаем $\lambda = wA_w(C_{n_0})/n_0$. Следовательно, $A_w(C_n) = A_w(C_{n_0})(n_0 - w)/n_0$. Теперь соотношение (4.3) может быть получено из (2.1) несложными преобразованиями. Заключительное утверждение теоремы следует из (2.3) и (4.3).

Заметим, что в рассмотренных ниже кодах Хэмминга, Панченко и БЧХ слова любого веса w образуют $t-(n_0,w,\lambda)$ схемы с $t\geq 1$.

4.2. Доля стираний, исправляемых расширенными и выколотыми кодами

Утверждение 1. *Пусть проверочная матрица H_0 двоичного $[n,n-r,2t+1]$ кода C_0 с нечетным кодовым расстоянием содержит $S_\rho(H_0)$ наборов из ρ линейно независимых столбцов, $1\leq\rho\leq r$. Пусть $[n+1,n-r,2t+2]$ код C получен из кода C_0 добавлением проверки на четность. Тогда проверочная матрица H кода C содержит $S_\rho(H)$ наборов из ρ линейно независимых столбцов, где*

$$S_\rho(H)\geq S_{\rho-1}(H_0)+S_\rho(H_0),\quad 2\leq\rho\leq r. \tag{4.4}$$

Доказательство. Проверочная матрица H кода C может быть получена добавлением к проверочной матрице H_0 кода C_0 верхней строки из единиц и столбца $(10\ldots0)^T$. Все $S_\rho(H_0)$ наборов из ρ линейно независимых столбцов матрицы H_0 сохраняют линейную независимость и в матрице H. Добавление столбца $(10\ldots0)^T$ к каждому из $S_{\rho-1}(H_0)$ наборов из $\rho-1$ линейно независимых столбцов матрицы H_0 даёт набор из ρ линейно независимых столбцов матрицы H. Знак "$\geq$" в (4.4) объясняется тем, что в матрице H_0 могут существовать $r\times\rho$-подматрицы ранга $\rho-1$, добавление верхней строки из единиц к которым увеличивает ранг подматрицы до ρ. Утверждение доказано.

Заметим, что $r\times\rho$-подматрицы ранга $\rho-1$, упомянутые в доказательстве утверждения 1, существуют, что приводит к знаку "$>$" в (4.4).

Обозначим через $A_w^{(0)}$ и A_w количество слов веса w в кодах утверждения 1 C_0 и C, соответственно. Как известно,

$$A_{2j}=A_{2j-1}^{(0)}+A_{2j}^{(0)}. \tag{4.5}$$

Равенство в (4.5) и неравенство в (4.4) подчеркивают различия в подходах и оценках, связанных со спектром весов и количеством наборов линейно независимых столбцов.

Далее заметим, что выкалывание кода есть операция, обратная расширению.

Определение. [18, раздел 8.5] Код C обладает *свойством P*, если при удалении фиксированной координаты из каждого кодового слова кода C мы получаем выколотый код C^*, который имеет один и тот же весовой весовой спектр, не зависящий от выкалываемой координаты.

Лемма 4.1. [18, раздел 8.5, Теорема 8.14] *Пусть $[n,n-r,2t+2]$ код C, все кодовые слова которого имеют четный вес, обладает свойством P. Тогда код C^*, полученный выкалыванием некоторой координаты кода C, является $[n-1,n-r,2t+1]$ кодом, и при этом справедливо*

$$A_{2j-1}^*=\frac{2j}{n}A_{2j},\quad A_{2j}^*=\frac{n-2j}{n}A_{2j},\quad j=t+1,t+2,\ldots, \tag{4.6}$$

где A_w и A_w^* количество слов веса w в кодах C и C^*, соответственно.

Заметим, что из (4.6) следует равенство $A_{2j}=A_{2j-1}^*+A_{2j}^*$, напоминающее соотношение (4.5). Тем не менее в [18] отмечено, что не всегда расширенный с помощью проверки на четность код обладает свойством P, и дано следующее достаточное условие [18, раздел 8.5, Следствие 15]: *код, инвариантный относительно транзитивной группы подстановок, обладает свойством P.* Многие расширенные коды обладают транзитивными группами подстановок [18]. В частности, см. например [17], неукороченный расширенный код БЧХ является дважды транзитивным.

Теорема 4.3. *Пусть $[n, n-r, 2t+2]$ код C, все кодовые слова которого имеют четный вес, обладает свойством P. Пусть $[n-1, n-r, 2t+1]$ код C^* получен выкалыванием некоторой координаты кода C. Тогда для $\rho = 2t+2, 2t+3, 2t+4, 2t+5$ справедливо*

$$\frac{\Psi(n, 2t+2, \rho, C)}{\binom{n}{\rho}} = \frac{\Psi(n-1, 2t+1, \rho.C^*)}{\binom{n-1}{\rho-1}}, \tag{4.7}$$

где левая и правая части равенства получены для кодов C и C^*, соответственно. В частности, если $\rho-(2t+2) \le \frac{2t+1}{2}$, тогда для $\rho \in \{2t+2, 2t+3, 2t+4, 2t+5\}$ имеем $\delta_\rho(C) = \delta_{\rho-1}(C^*)$, где $\delta_\rho(C)$ и $\delta_{\rho-1}(C^*)$ есть доля стираний веса ρ и $\rho-1$, исправляемых кодом C и C^*, соответственно.

Доказательство. Мы используем соотношение (4.6), подставляем соответствующие веса в (2.1), учитывая $A_{2t+3} = A_{2t+5} = 0$ для кода C, и выполняем несложные преобразования.

Можно предположить, что соотношение (4.7) и вытекающее из него равенство $\delta_\rho(C) = \delta_{\rho-1}(C^*)$ в теореме 4.3 справедливы для всех допустимых значений ρ.

5. ДОЛЯ СТИРАНИЙ, ИСПРАВЛЯЕМЫХ НЕУКОРОЧЕННЫМИ КОДАМИ ХЭММИНГА, ПАНЧЕНКО И БЧХ

5.1. Неукороченные $[2^r-1, 2^r-1-r, 3]$ и $\left[2^{r-1}, 2^{r-1}-r, 4\right]$ коды Хэмминга

Пример 1. Для неукороченного $\left[2^{r-1}, 2^{r-1}-r, 4\right]$ расширенного кода Хэмминга на Рис. 1 показаны графики доли $\delta^{H\bullet}_{\rho,r}$ исправляемых стираний веса ρ как функции от r (см. (3.17)) при $4 \le \rho \le 8$, $\rho \le r$, $7 \le r \le 18$. Напомним, что $\delta^{H\bullet}_{\rho,r} = \delta^{H}_{\rho-1,r-1}$. Следовательно, указанные кривые являются также графиками доли $\delta^{H}_{\rho-1,r-1}$ исправляемых стираний веса $\rho-1$ как функции от $r-1$ в неукороченном $\left[2^{r-1}-1, 2^{r-1}-r, 3\right]$ коде Хэмминга.

Численные значения $\delta^{H\bullet}_{\rho,r}$ представлены в таблице 1.

Таблица 1. Доля $\delta^{H\bullet}_{\rho,r}$ исправляемых стираний веса ρ как функция от r для неукороченного $\left[2^{r-1}, 2^{r-1}-r, 4\right]$ кода Хэмминга (эквивалентно, доля $\delta^{H}_{\rho-1,r-1}$ исправляемых стираний веса $\rho-1$ как функция от $r-1$ для неукороченного $\left[2^{r-1}-1, 2^{r-1}-r, 3\right]$ кода Хэмминга), $4 \le \rho \le 12$, $\rho \le r$, $7 \le r \le 20$

r	$\rho = d = 4$	$\rho = 5$	$\rho = 6$	$\rho = 7$	$\rho = 8$	$\rho = 9$	$\rho = 10$	$\rho = 11$	$\rho = 12$
7	0.9836	0.9180	0.7469	0.4121					
8	0.9920	0.9600	0.8741	0.6879	0.3638				
9	0.9960	0.9802	0.9373	0.8398	0.6476	0.3342			
10	0.9980	0.9902	0.9687	0.9189	0.8152	0.6211	0.3161		
11	0.9990	0.9951	0.9844	0.9592	0.9055	0.7985	0.6042	0.3051	
12	0.9995	0.9976	0.9922	0.9796	0.9522	0.8962	0.7876	0.5936	0.2984
13	0.9998	0.9988	0.9961	0.9898	0.9760	0.9473	0.8901	0.7807	0.5871
14	0.9999	0.9994	0.9980	0.9949	0.9879	0.9735	0.9441	0.8862	0.7764
15	0.9999	0.9997	0.9990	0.9974	0.9940	0.9867	0.9718	0.9420	0.8837
16	1.0000	0.9998	0.9995	0.9987	0.9970	0.9933	0.9858	0.9707	0.9407
17	1.0000	0.9999	0.9998	0.9994	0.9985	0.9967	0.9929	0.9853	0.9701
18	1.0000	1.0000	0.9999	0.9997	0.9992	0.9983	0.9964	0.9926	0.9850
19	1.0000	1.0000	0.9999	0.9998	0.9996	0.9992	0.9982	0.9963	0.9925
20	1.0000	1.0000	1.0000	0.9999	0.9998	0.9996	0.9991	0.9982	0.9962

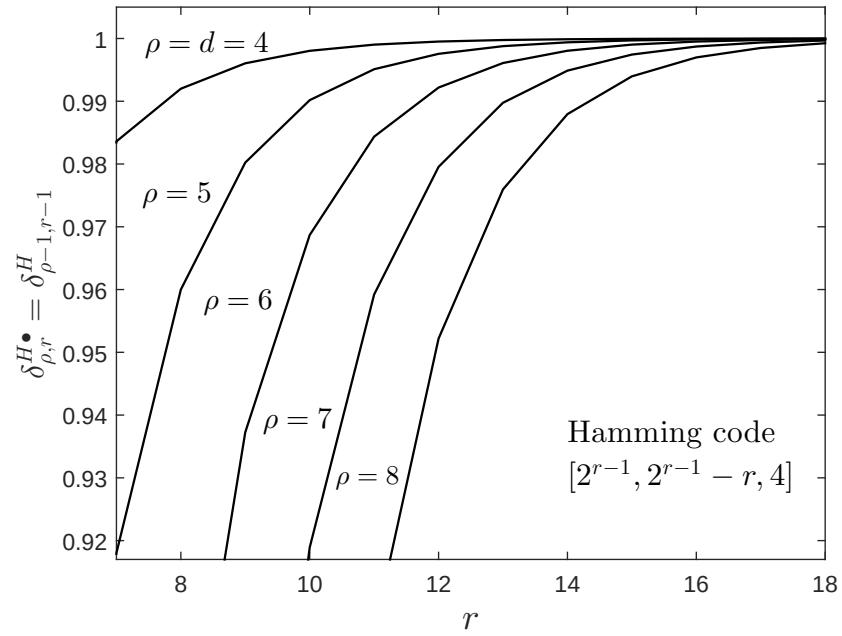

Рис. 1. Доля $\delta^{H\bullet}_{\rho,r}$ исправляемых стираний веса ρ как функция от r для неукороченного $\left[2^{r-1}, 2^{r-1} - r, 4\right]$ кода Хэмминга (эквивалентно, доля $\delta^{H}_{\rho-1,r-1}$ исправляемых стираний веса $\rho - 1$ как функция от $r - 1$ для неукороченного $\left[2^{r-1} - 1, 2^{r-1} - r, 3\right]$ кода Хэмминга), $4 \le \rho \le 8$, $\rho \le r$, $7 \le r \le 18$

5.2. Неукороченный $\left[5 \cdot 2^{r-4}, 5 \cdot 2^{r-4} - r, 4\right]$ код Панченко с расстоянием $d = 4$

В этом разделе рассматривается двоичный $\left[5 \cdot 2^{r-4}, 5 \cdot 2^{r-4} - r, 4\right]$ код Панченко, предложенный В.И. Панченко в работе [13]. В статьях [7, 12] проведен анализ этого кода. Для кода Панченко обозначим: $A^{\Pi}_{w,r}$ количество слов веса w, $S^{\Pi}_{\rho,r}$ – число исправляемых конфигураций стираний веса ρ, $\delta^{\Pi}_{\rho,r}$ – доля исправляемых стираний веса ρ. В соответствии с (1.1),

$$\delta^{\Pi}_{\rho,r} = \frac{S^{\Pi}_{\rho,r}}{\binom{5\cdot 2^{r-4}}{\rho}} \le 1. \tag{5.1}$$

Как известно [7, 12],

$$A^{\Pi}_{4,r} = \frac{5 \cdot 2^{r-6}(2^{r-4} - 1)(2^{r-2} + 5 \cdot 2^{r-5} - 1)}{3}, \tag{5.2}$$

$$A^{\Pi}_{5,r} = 2^{4r-16}. \tag{5.3}$$

Утверждение 2. *Число $S^{\Pi}_{\rho,r}$ исправляемых конфигураций стираний веса ρ для $[5 \cdot 2^{r-4}, 5 \cdot 2^{r-4} - r, 4]$ кода Панченко оценивается следующим образом:*

$$S^{\Pi}_{4,r} = \binom{5 \cdot 2^{r-4}}{4} - \frac{5 \cdot 2^{r-6}(2^{r-4} - 1)(2^{r-2} + 5 \cdot 2^{r-5} - 1)}{3}\ ; \tag{5.4}$$

$$S^{\Pi}_{5,r} = \binom{5 \cdot 2^{r-4}}{5} - \frac{3 \cdot 2^{4r-16} + 5 \cdot 2^{r-6}(2^{r-4} - 1)(2^{r-2} + 5 \cdot 2^{r-5} - 1)(5 \cdot 2^{r-4} - 4)}{3}\ ; \tag{5.5}$$

$$S^{\Pi}_{\rho,r} \geq \frac{1}{6\cdot 7\cdot \ldots \cdot \rho} S^{\Pi}_{5,r} \prod_{j=6}^{\rho} \left(5\cdot 2^{r-4} + 1 - 2^{j-1} + \lambda(4,j)\right), \quad 6 \leq \rho \leq r. \tag{5.6}$$

Доказательство. Для $\rho = 4$ и $\rho = 5$ условие (2.4) выполняется. По формулам (2.1), (2.3) с использованием (5.2), (5.3) получаем (5.4), (5.5). Соотношение (5.6) использует (3.18) с $\rho_0 = 5$, $\Psi(n,d,\rho_0) = S^{\Pi}_{5,r}$.

Пример 2. Для неукороченного $\left[5\cdot 2^{r-4}, 5\cdot 2^{r-4} - r, 4\right]$ кода Панченко на Рис. 2 представлены графики доли $\delta^{\Pi}_{\rho,r}$ исправляемых стираний веса ρ как функции от r при $\rho = 4,5,6$ и $7 \leq r \leq 18$. Точные значения $\delta^{\Pi}_{4,r}$ и $\delta^{\Pi}_{5,r}$ получены по формулам (5.1), (5.4), (5.5). Нижняя оценка величины $\delta^{\Pi}_{6,r}$ вытекает из (5.1), (5.6).

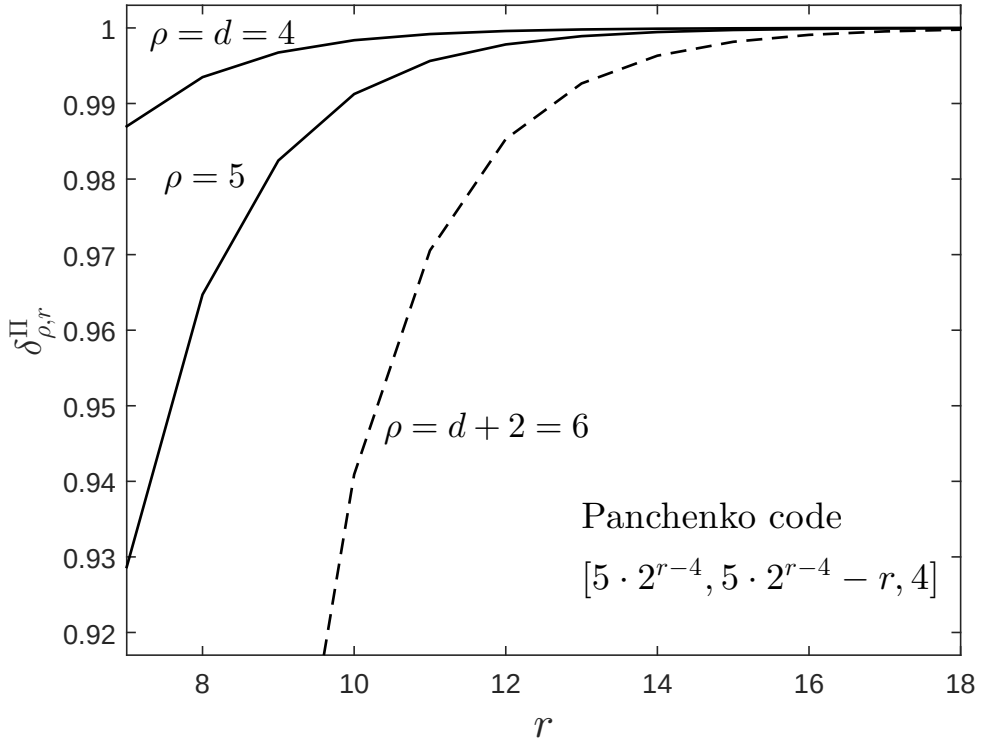

Рис. 2. Доля $\delta^{\Pi}_{\rho,r}$ исправляемых стираний веса ρ как функция от r для неукороченного $\left[5\cdot 2^{r-4}, 5\cdot 2^{r-4} - r, 4\right]$ кода Панченко, $7 \leq r \leq 18$, $\rho = 4,5,6$. Сплошные линии - точные значения $\delta^{\Pi}_{\rho,r}$, пунктирная кривая - нижняя оценка $\delta^{\Pi}_{6,r}$

Численные значения $\delta^{\Pi}_{\rho,r}$ представлены в таблице 2, где для $\rho = 4,5$ даны точные значения $\delta^{\Pi}_{\rho,r}$, а для $\rho = 6$ – нижняя оценка.

Пример 3. Для неукороченного $[80,72,4]$ кода Панченко из (5.1), (5.4), (5.5) получаем $\delta^{\Pi}_{4,8} = 0,993488$, $\delta^{\Pi}_{5,8} = 0,964712$. Для $[72,64,8]$ кода Панченко, укороченного на 8 символов по Алгоритму 1 из [12] с учетом модификации алгоритма в [7], справедливо $A_4 = 6654$, $A_5 = 38586$ [3, таблица 2]. Отсюда по формулам (2.1), (5.1) имеем $\delta^{\Pi(8)}_{4,8} = 0,993532 > \delta^{\Pi}_{4,8}$, $\delta^{\Pi(8)}_{5,8} = 0,964903 > \delta^{\Pi}_{5,8}$, где $\delta^{\Pi(v)}_{\rho,r}$ обозначает долю стираний веса ρ, исправляемых $\left[5\cdot 2^{r-4} - v, 5\cdot 2^{r-4} - v - r, 4\right]$ кодом Панченко, укороченным на v символов. Сказанное иллюстрирует теорему 4.1 и следствие 4.1.

Таблица 2. Доля $\delta^{\Pi}_{\rho,r}$ исправляемых стираний веса ρ как функция от r для неукороченного $\left[5\cdot 2^{r-4}, 5\cdot 2^{r-4}-r, 4\right]$ кода Панченко, $7\le r\le 18$, $\rho=4,5,6$

r	7	8	9	10	11	12
n	40	80	160	320	640	1280
$\rho=d=4$	0.9870	0.9935	0.9967	0.9984	0.9992	0.9996
$\rho=d+1=5$	0.9287	0.9647	0.9825	0.9913	0.9956	0.9978
$\rho=d+2=6\ge$	0.5041	0.7589	0.8810	0.9409	0.9705	0.9853
r	13	14	15	16	17	18
n	2560	5120	10240	20480	40960	81920
$\rho=d=4$	0.9998	0.9999	0.9999	1.0000	1.0000	1.0000
$\rho=d+1=5$	0.9989	0.9995	0.9997	0.9999	0.9999	1.0000
$\rho=d+2=6\ge$	0.9927	0.9963	0.9982	0.9991	0.9995	0.9998

5.3. Неукороченные $[2^{(r-1)/2}-1, 2^{(r-1)/2}-r, 5]$ *и* $[2^{(r-1)/2}, 2^{(r-1)/2}-r, 6]$ *коды БЧХ*

Обозначим через $B^\bullet$ двоичный расширенный $[2^{(r-1)/2}, 2^{(r-1)/2}-r, 6]$ код БЧХ с четными весами. Введем обозначения для этого кода: $A^{B^\bullet}_{w,r}$ – количество слов веса w; $S^{B^\bullet}_{\rho,r}$ – число исправляемых конфигураций стираний веса ρ; $\delta^{B^\bullet}_{\rho,r}$ – доля исправляемых стираний веса ρ. В соответствии с (1.1),

$$\delta^{B^\bullet}_{\rho,r}=\frac{S^{B^\bullet}_{\rho,r}}{\binom{2^{(r-1)/2}}{\rho}}\le 1. \tag{5.7}$$

Как известно [16, с. 434],

$$A^{B^\bullet}_{6,r}=\begin{cases}\frac{2^{(r-1)/2}(2^{(r-1)/2}-1)(2^{(r-1)/2}-2)(2^{(r-1)/2}-8)}{720}, & \text{если } (r-1)/2 \text{ нечетное}\\ \frac{2^{(r-1)/2}(2^{(r-1)/2}-1)(2^{(r-1)/2}-4)^2}{720}, & \text{если } (r-1)/2 \text{ четное}\end{cases}. \tag{5.8}$$

Обозначим через B двоичный $[2^{(r-1)/2}-1, 2^{(r-1)/2}-r, 5]$ код БЧХ, полученный выкалыванием некоторой позиции кода $B^\bullet$. Пусть $\delta^{B}_{\rho,r-1}$ – доля стираний веса ρ, исправляемых кодом B. Поскольку код $B^\bullet$ дважды транзитивный, см. например [17], он обладает свойством P из определения в разделе 4.2. Поэтому в соответствии с теоремой 4.3 для $\rho=6,7,8,9$ справедливо

$$\frac{\Psi(2^{(r-1)/2},6,\rho,B^\bullet)}{\binom{2^{(r-1)/2}}{\rho}}=\frac{\Psi(2^{(r-1)/2}-1,5,\rho-1,B)}{\binom{2^{(r-1)/2}-1}{\rho-1}}, \tag{5.9}$$

где левая и правая части равенства получены для кодов $B^\bullet$ и B, соответственно. Более того, с учетом условия (2.4)

$$\delta^{B^\bullet}_{\rho,r}=\delta^{B}_{\rho-1,r-1},\quad \rho=6,7,8. \tag{5.10}$$

Из (2.1), (2.3), (2.4), (5.7), (5.8), (5.10), с учетом факта, что в коде $B^\bullet$ все веса четные, получаем

Утверждение 3. *Доля* $\delta^{B^\bullet}_{\rho,r}=\delta^{B}_{\rho-1,r-1}$ *стираний веса* ρ *и* $\rho-1$, *исправляемых* $[2^{(r-1)/2}, 2^{(r-1)/2}-r, 6]$ *и* $[2^{(r-1)/2}-1, 2^{(r-1)/2}-r, 5]$ *кодами БЧХ равна*

$$\delta^{B^\bullet}_{6,r}=\delta^{B}_{5,r-1}=1-\begin{cases}\frac{(2^{(r-1)/2}-8)}{(2^{(r-1)/2}-3)(2^{(r-1)/2}-4)(2^{(r-1)/2}-5)}, & \textit{если } (r-1)/2 \textit{ нечетное}\\ \frac{(2^{(r-1)/2}-4)}{(2^{(r-1)/2}-2)(2^{(r-1)/2}-3)(2^{(r-1)/2}-5)}, & \textit{если } (r-1)/2 \textit{ четное}\end{cases}; \tag{5.11}$$

$$\delta^{B^\bullet}_{7,r}=\delta^{B}_{6,r-1}=\delta^{B^\bullet}_{6,r}-6(1-\delta^{B^\bullet}_{6,r}). \tag{5.12}$$

Заметим, что код $B^\bullet$ можно рассматривать как расширение кода B.

Пример 4. Для неукороченного расширенного $[2^{(r-1)/2}, 2^{(r-1)/2}-r, 6]$ кода БЧХ $B^\bullet$ на Рис. 3 представлены графики доли $\delta^{B^\bullet}_{\rho,r}$ исправляемых стираний веса ρ как функции от r (см. (2.1), (2.3), (2.4), (5.7), (5.11), (5.12)) при $\rho = 6, 7, 8, 9$ и $r = 13, 15, 17$. Условие (2.4) в случаях $\rho = 6, 7, 8$ выполняется. При $\rho = 9$ это условие не выполняется, и соответствующий график является нижней оценкой доли $\delta^{B^\bullet}_{9,r}$. При вычислениях для $\rho = 8, 9$ величины $A^{B^\bullet}_{8,r}$ взяты из [19, Приложение A] и [21]. Учитывая (5.9), (5.10), указанные кривые являются также графиками доли $\delta^{B}_{\rho-1,r-1}$ исправляемых стираний веса $\rho-1$ как функции от $r-1$ для $[2^{(r-1)/2}-1, 2^{(r-1)/2}-r, 5]$ кода B.

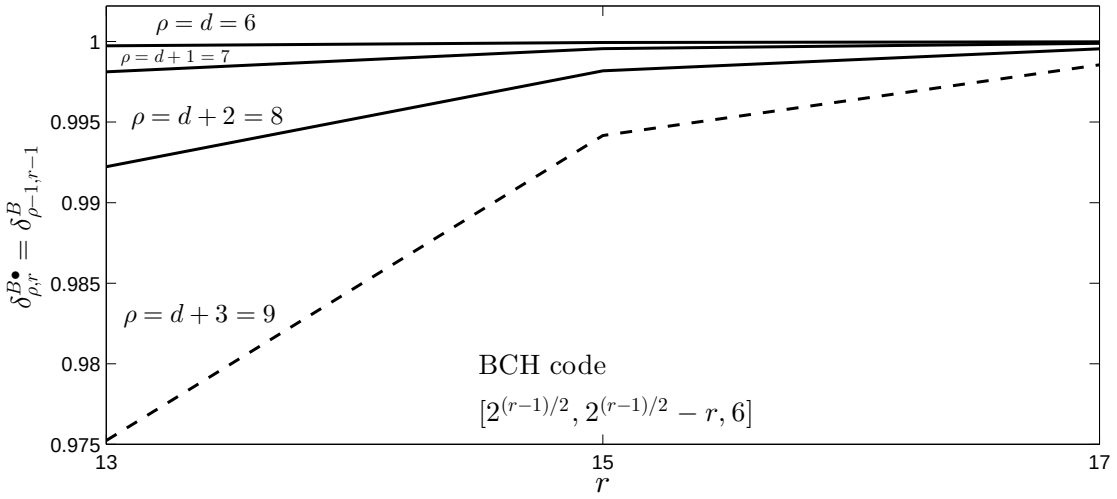

Рис. 3. Доля $\delta^{B^\bullet}_{\rho,r}$ исправляемых стираний веса ρ как функция от r для неукороченного расширенного $[2^{(r-1)/2}, 2^{(r-1)/2}-r, 6]$ кода БЧХ (эквивалентно, доля $\delta^{B}_{\rho-1,r-1}$ исправляемых стираний веса $\rho-1$ как функция от $r-1$ для неукороченного $[2^{(r-1)/2}-1, 2^{(r-1)/2}-r, 5]$ кода БЧХ), $\rho = 6, 7, 8, 9$, $r = 13, 15, 17$. Сплошные линии - точные значения $\delta^{B^\bullet}_{\rho,r} = \delta^{B}_{\rho-1,r-1}$, пунктирная кривая - нижняя оценка $\delta^{B^\bullet}_{9,r} = \delta^{B}_{8,r-1}$

Численные значения $\delta^{B^\bullet}_{\rho,r}$ представлены в таблице 3, где для $\rho = 6, 7, 8$ даны точные значения $\delta^{B^\bullet}_{\rho,r}$, а для $\rho = 9$ - нижняя оценка. Для $r = 19$ вычислены только значения $\delta^{B^\bullet}_{6,19}$, $\delta^{B^\bullet}_{7,19}$.

Таблица 3. Доля $\delta^{B^\bullet}_{\rho,r}$ исправляемых стираний веса ρ как функция от r для неукороченного расширенного $[2^{(r-1)/2}, 2^{(r-1)/2}-r, 6]$ кода БЧХ (эквивалентно, доля $\delta^{B}_{\rho-1,r-1}$ исправляемых стираний веса $\rho-1$ как функция от $r-1$ для неукороченного $[2^{(r-1)/2}-1, 2^{(r-1)/2}-r, 5]$ кода БЧХ), $\rho = 6, 7, 8, 9$, $r = 13, 15, 17, 19$.

r	13	15	17	19
n	64	128	256	512
$\rho = d = 6$	0.9997	0.9999	1.0000	1.0000
$\rho = d+1 = 7$	0.9981	0.9996	0.9999	1.0000
$\rho = d+2 = 8$	0.9922	0.9982	0.9995	
$\rho = d+3 = 9 \geq$	0.9752	0.9942	0.9986	

6. ИСПРАВЛЕНИЕ СТИРАНИЙ С ОБНАРУЖЕНИЕМ ОШИБОК

В данном разделе для $[n, r, d]$ кода рассматривается ситуация, когда произошло ρ стираний и ν ошибок, $d \leq \rho < r$, $\nu > 0$. Введем обозначения:

$\mathbf{A}_\rho^{(\nu)}$ – $r\times(\rho+\nu)$-подматрица проверочной матрицы, соответствующая стираниям и ошибкам;

$\mathbf{A}_\rho$ – $r\times\rho$-подматрица проверочной матрицы, соответствующая только стираниям;

$\mathcal{L}(\mathbf{A}_\rho)$ – переопределенная система r линейных уравнений с ρ неизвестными, матрицей системы является $\mathbf{A}_\rho$, столбец свободных членов есть столбец синдрома;

$\Delta_{\nu,\rho}$ – доля ошибок кратности ν, обнаруживаемых при попытке исправления ρ стираний, которым соответствует $r\times\rho$-матрица $\mathbf{A}_\rho$ ранга ρ.

Заметим, что матрица $\mathbf{A}_\rho$ известна декодеру и является подматрицей матрицы $\mathbf{A}_\rho^{(\nu)}$. Синдром есть сумма столбцов матрицы $\mathbf{A}_\rho^{(\nu)}$. При декодировании решается система $\mathcal{L}(\mathbf{A}_\rho)$. Отказ от декодирования происходит, когда систему $\mathcal{L}(\mathbf{A}_\rho)$ решить невозможно, т.е. в двух случаях:

a) ранг матрицы $\mathbf{A}_\rho$ меньше ρ (система $\mathcal{L}(\mathbf{A}_\rho)$ вырождена);

b) ранг матрицы $\mathbf{A}_\rho$ равен ρ (эквивалентно, стираниям соответствуют ρ линейно независимых столбцов проверочной матрицы), но система $\mathcal{L}(\mathbf{A}_\rho)$ несовместна.

Случай b) трактуется как обнаружение ошибок при попытке исправления ρ стираний, которым соответствует ρ линейно независимых столбцов проверочной матрицы.

Лемма 6.1. *Если имеют место ρ стираний и ν ошибок, $d\le\rho<r$, $\nu>0$, и стираниям соответствуют ρ линейно независимых столбцов проверочной матрицы $[n,r,d]$ кода, то обнаружение ошибок происходит тогда и только тогда, когда ранг $r\times(\rho+\nu)$-матрицы $\mathbf{A}_\rho^{(\nu)}$, соответствующей стираниям и ошибкам, больше или равен $\rho+1$.*

Доказательство. Если ранг матрицы $\mathbf{A}_\rho^{(\nu)}$ не меньше $\rho+1$, то в этой матрице существует столбец h, не принадлежащий подматрице $\mathbf{A}_\rho$ и линейно независимый от столбцов этой подматрицы. Столбец h является одним из слагаемых синдрома, т.е. столбца свободных членов системы $\mathcal{L}(\mathbf{A}_\rho)$. Поэтому ранг расширенной матрицы системы $\mathcal{L}(\mathbf{A}_\rho)$ больше или равен $\rho+1$ и не равен рангу основной матрицы системы, что означает ее несовместность. Если ранг матрицы $\mathbf{A}_\rho^{(\nu)}$ равен ρ, то такого столбца h не существует, и система окажется совместной.

Пусть $\lambda(d,\rho)$ и $\lambda^\bullet(d,\rho)$ определены, как в разделе 3.

Теорема 6.1. *Если имеют место ρ стираний и ν ошибок, $d\le\rho<r$, $\nu>0$, и стираниям соответствуют ρ линейно независимых столбцов проверочной матрицы $[n,r,d]$ кода, то доля $\Delta_{\nu,\rho}$ обнаруживаемых ошибок оценивается следующим образом:*

$$\Delta_{\nu,\rho}\ge 1-\frac{\binom{2^\rho-\rho-1-\lambda(d,\rho+1)}{\nu}}{\binom{n-\rho}{\nu}}\quad \textit{для произвольного } [n,r,d] \textit{ кода;} \tag{6.1}$$

$$\Delta_{\nu,\rho}=1-\frac{\binom{2^\rho-\rho-1}{\nu}}{\binom{2^r-\rho-1}{\nu}}\quad \textit{для } [2^r-1,2^r-1-r,3] \textit{ кода Хэмминга;} \tag{6.2}$$

$$\Delta_{\nu,\rho}\ge 1-\frac{\binom{2^{\rho-1}-\rho-\lambda^\bullet(d,\rho+1)}{\nu}}{\binom{n-\rho}{\nu}},\quad \textit{если все веса } [n,r,d] \textit{ кода четные;} \tag{6.3}$$

$$\Delta_{\nu,\rho}=1-\frac{\binom{2^{\rho-1}-\rho}{\nu}}{\binom{2^{r-1}-\rho}{\nu}}\quad \textit{для } \left[2^{r-1},2^{r-1}-r,4\right] \textit{ кода Хэмминга.} \tag{6.4}$$

Доказательство. Аналогично доказательству леммы 3.1 можно показать, что для матрицы $\mathbf{A}_\rho$ ранга ρ в оставшейся части проверочной матрицы существует совокупность из не менее $m = n + 1 - 2^\rho + \lambda(d, \rho + 1)$ столбцов, добавление любого из которых к $\mathbf{A}_\rho$ дает матрицу ранга $\rho + 1$. Обозначим указанную совокупность через T. Чтобы получить матрицу $\mathbf{A}_\rho^{(\nu)}$, к матрице $\mathbf{A}_\rho$ нужно добавить некоторую $r \times \nu$-матрицу $\mathbf{D}$. Матрица $\mathbf{A}_\rho^{(\nu)}$ имеет ранг ρ (т.е. ошибки не обнаруживаются), если и только если матрица $\mathbf{D}$ не содержит ни одного столбца из T. Число таких матриц $\mathbf{D}$ равно $\binom{n-\rho-m}{\nu}$. Общее количество матриц $\mathbf{D}$ равно $\binom{n-\rho}{\nu}$. Следовательно, существует не менее $\binom{n-\rho}{\nu} - \binom{n-\rho-m}{\nu}$ матриц $\mathbf{A}_\rho^{(\nu)}$ ранга $\geq \rho + 1$. С другой стороны, вне ρ стираний существует $\binom{n-\rho}{\nu}$ ошибок кратности ν. Разделив число "хороших" матриц $\mathbf{A}_\rho^{(\nu)}$ на $\binom{n-\rho}{\nu}$, получаем (6.1). Соотношения (6.2)–(6.4) могут быть доказаны аналогично с использованием подходов, принятых при доказательстве лемм 3.1 и 3.2.

7. АЛГОРИТМЫ РАСШИРЕННОГО ДЕКОДИРОВАНИЯ ДВОИЧНОГО КОДА-ПРОИЗВЕДЕНИЯ

Рассмотрим декодирование кода-произведения с одинаковыми компонентными $[n, n-r, d]$ кодами по строкам и столбцам. Кодовое слово является $n \times n$-матрицей. Пусть $d = 4$ или $d = 6$. Введем обозначения:

H – проверочная $r \times n$-матрица двоичного компонентного кода,

U – $n \times n$-матрица принятого слова с ошибками,

S_{row} – $n \times r$-матрица синдромов строк и S_{col} – $r \times n$-матрица синдромов столбцов.

Алгоритм 1.

1. Вычисление $S_{row} = UH^T$ и $S_{col} = HU$.
2. Составление списка L_{row} номеров строк и списка L_{col} столбцов с обнаруженными ошибками.
3. Проверка подматриц $H(L_{row})$ и $H(L_{col})$ на невырожденность, если хотя бы одна из них невырождена, то исправляем стирания (с помощью подматрицы минимального размера на пересечении двух списков) и выдаем исправленное кодовое слово, иначе <отказ>.

Алгоритм 2.

1. Выполняется Алгоритм 1. Если <отказ>, то п. 2.
2. Просмотр списка L_{row} с исправлением одной ошибки (или до двух для кода БЧХ) и составление обновленного списка L_{row} с сохранением исправлений в матрице U_{res}.
3. Вычисление $S_{col} = HU_{res}$ и составление обновленного списка L_{col}.
4. Проверка подматрицы $H(L_{col})$ на невырожденность (для обновленного L_{col}). Если подматрица невырождена, то исправляются стирания на пересечении обновленных списков и выдается исправленное кодовое слово, иначе <отказ> или п.5.
5. Просмотр списка L_{col} с исправлением одной ошибки (или до двух для кода БЧХ) и составление обновленного списка L_{col} с сохранением исправлений в матрице U_{res}.
6. Вычисление $S_{row} = HU_{res}$ и составление обновленного списка L_{row}.
7. Проверка подматрицы $H(L_{row})$ на невырожденность (для обновленного L_{row}). Если подматрица невырождена, то исправляются стирания на пересечении обновленных списков и выдается исправленное кодовое слово, иначе <отказ> (или п.3 пока не выполнится двойной отказ в п.4 и п.7).

Комментарий.

В предложенных алгоритмах проводится независимое декодирование строк и столбцов до заключительного этапа (Алгоритм 1 этап 3, Алгоритм 2 этап 4 или 7). Такое построение алгоритма позволяет выполнять предварительное декодирование независимо и параллельно по

строкам и столбцам и, тем самым, снижает задержку и сложность декодирования. Однако, при этом несколько снижается и множество декодируемых конфигураций ошибок и вероятность правильного декодирования по сравнению с достижимым наилучшим результатом. Важно отметить, что в погрешность уходят только маловероятные события, и главный член сохраняется.

8. ОЦЕНКА ВЕРОЯТНОСТИ УСПЕШНОГО ДЕКОДИРОВАНИЯ

Для оценки вероятности правильного декодирования предлагается несколько упрощенная общая схема. Упрощение алгоритмов декодирования и схемы расчетов состоит в том, что предварительное декодирование строк и столбцов рассматриваются как независимые события. Независимость в декодировании строк и столбцов позволяет снизить сложность и задержку декодирования двумерного кода, тогда как независимость в расчетах дает оценку главного члена вероятности успешного декодирования.

Обозначим Ω вероятность события – успешного декодирования строк и, независимо, успешного декодирования столбцов для симметричной конструкции двумерного кода-произведения. Тогда вероятность успешного декодирования двумерного кода можно оценить (снизу) как $1-(1-\Omega)^2$, так как вероятность отказа при декодировании столбцов после отказа при декодировании строк может отличаться от величины $1-\Omega$.

Обозначим через p вероятность ошибки в символе на входе декодера. Очевидно,

1. Вероятность строки (столбца) без ошибок равна
$$P_0 = P(0) = (1-p)^n .$$
2. Вероятность хотя бы одной ошибки в строке (столбце) равна
$$P_1 = P(>0) = 1-(1-p)^n .$$
3. Вероятность более одной ошибки в строке (столбце) равна
$$P_2 = P(>1) = 1-(1-p)^n - np(1-p)^{n-1} .$$
4. Вероятность более двух ошибок в строке (столбце) равна
$$P_3 = P(>2) = 1-(1-p)^n - np(1-p)^{n-1} - \binom{n}{2} p^2 (1-p)^{n-2} .$$

Введем обозначения:
d^+ – порог для расширенного исправления стираний, $d^+ \geq d$;
δ_ρ – доля исправляемых компонентным кодом стираний веса ρ.

8.1. Произведение кодов с расстоянием 4

Вероятность того, что ровно ρ строк (столбцов) содержат более одной ошибки:
$$\binom{n}{\rho} (P_2)^\rho (1-P_2)^{n-\rho} .$$

Вероятность успешного декодирования строк (столбцов):
$$\Omega_2 = \sum_{\rho=0}^{d^+} \binom{n}{\rho} (P_2)^\rho (1-P_2)^{n-\rho} \delta_\rho . \tag{8.1}$$

Вероятность отказа для произведения кодов с расстоянием 4:

$$(1-\Omega_2)^2\,. \tag{8.2}$$

Вероятность успешного декодирования произведения кодов с расстоянием 4:

$$P_{prod,4} = 1-(1-\Omega_2)^2\,.$$

Пример 5. В таблицах 4 и 5 для произведения укороченных кодов Панченко $[72,64,4]$ и $[137,128,4]$, соответственно, представлены вероятность отказа $(1-\Omega_2)^2$ в диапазоне входных вероятностей $p = 10^{-1}, 10^{-2}, 5\cdot 10^{-3}, 10^{-3}, 5\cdot 10^{-4}, 10^{-4}$ и значениях $d^+ = 3,4,5,6$. В таблицах запись вида e-m означает 10^{-m}.

Таблица 4. Вероятность отказа для произведения кодов Панченко $[72,64,4]$

p	10^{-1}	10^{-2}	$5\cdot 10^{-3}$	10^{-3}	$5\cdot 10^{-4}$	10^{-4}
$d^+=3$	1	0,996	0,250	1,1e-09	2,3e-14	1,9e-25
$d^+=4$	1	0,988	0,092	1,6e-12	5,1e-18	1,1e-31
$d^+=5$	1	0,967	0,027	7,0e-14	1,045e-18	4,931e-32
$d^+=6$	1	0,926	0,008	5,8e-14	1,029e-18	4,931e-32

Таблица 5. Вероятность отказа для произведения кодов Панченко $[137,128,4]$

p	10^{-1}	10^{-2}	$5\cdot 10^{-3}$	10^{-3}	$5\cdot 10^{-4}$	10^{-4}
$d^+=3$	1	1	0,9999989	9,2e-4	7,4e-8	1,021e-18
$d^+=4$	1	1	0,9999933	4,5e-5	2,8e-10	3,304e-23
$d^+=5$	1	1	0,9999681	2,3e-6	5,0e-12	1,138e-23
$d^+=6$	1	1	0,9998819	4,2e-7	2,5e-12	1,135e-23

В работе [7, Таблица 2] построен $[72,64,4]$ код Панченко с весами $A_4 = 6654$, $A_5 = 38586$, $A_6 = 695799$. Используя эти веса, мы получаем по формулам (2.1)–(2.4) точные значения δ_4, δ_5, и нижнюю оценку для δ_6. Затем таблица 4 заполняется в соответствии с (8.1), (8.2).

В работе [12, с. 899] построен $[137,128,4]$ код Панченко с $A_4 = 45443$. Используя (2.1), (2.3) мы получаем $\Psi(137,4,4)$ и точное значение δ_4, а затем с помощью (3.18), (1.1) находим нижние оценки для δ_5, δ_6. Вероятности $(1-\Omega_2)^2$ в таблице 5 вычисляются в соответствии с (8.1), (8.2).

8.2. Произведение кодов с расстоянием 6

Вероятность того, что ровно ρ строк (столбцов) содержат более двух ошибок:

$$\binom{n}{\rho}(P_3)^\rho\,(1-P_3)^{n-\rho}\,.$$

Вероятность успешного декодирования строк или столбцов

$$\Omega_3 = \sum_{\rho=0}^{d^+}\binom{n}{\rho}(P_3)^\rho\,(1-P_3)^{n-\rho}\,\delta_\rho. \tag{8.3}$$

Вероятность отказа для произведения кодов с расстоянием 6:

$$(1-\Omega_3)^2\,. \tag{8.4}$$

Вероятность успешного декодирования произведения кодов с расстоянием 6:

$$P_{prod,6} = 1-(1-\Omega_3)^2\,.$$

Пример 6. В таблицах 6 и 7 для произведения расширенных четно-весовых кодов БЧХ $[79, 64, 6]$ и $[145, 128, 6]$, соответственно, представлены вероятность отказа $(1 - \Omega_3)^2$ в диапазоне входных вероятностей $p = 10^{-1}, 10^{-2}, 5 \cdot 10^{-3}, 10^{-3}, 5 \cdot 10^{-4}, 10^{-4}$ и значениях $d^+ = 5, 6, 7, 8, 9$.

Таблица 6. Вероятность отказа для произведения кодов БЧХ $[79, 64, 6]$

p	10^{-1}	10^{-2}	$5 \cdot 10^{-3}$	10^{-3}	$5 \cdot 10^{-4}$	10^{-4}
$d^+ = 5$	1	0,02149	8,9e-10	0	0	0
$d^+ = 6$	1	0,00435	5,4e-12	0	0	0
$d^+ = 7$	1	0,00069	2,5e-14	0	0	0
$d^+ = 8$	1	0,00021	3,2e-15	0	0	0
$d^+ = 9$	1	0,00019	3,1e-15	0	0	0

Таблица 7. Вероятность отказа для произведения кодов БЧХ $[145, 128, 6]$

p	10^{-1}	10^{-2}	$5 \cdot 10^{-3}$	10^{-3}	$5 \cdot 10^{-4}$	10^{-4}
$d^+ = 5$	1	0,9999998	0,1981	7,9e-21	1,43e-29	0
$d^+ = 6$	1	0,9999987	0,0827	6,3e-25	1,11e-29	0
$d^+ = 7$	1	0,9999940	0,0282	1,7e-28	1,11e-29	0
$d^+ = 8$	1	0,9999794	0,0103	5,9e-29	1,11e-29	0
$d^+ = 9$	1	0,9999537	0,0066	5,9e-29	1,11e-29	0

В работе [7, Таблица 5] построен $[79, 64, 6]$ код БЧХ с $A_6 = 17375$. Мы получаем по формулам (2.1), (2.3), (2.4) точные значения δ_6, δ_7 и по формуле (3.19) – нижнюю оценку для δ_8, δ_9. Затем таблица 6 заполняется в соответствии с (8.3), (8.4).

Используя [7, Теорема 3.1] и соотношение (5.8), можно показать, что существует $[145, 128, 6]$ четно-весовой код БЧХ с $A_6 = 181611$. Снова мы получаем по формулам (2.1), (2.3), (2.4) точные значения δ_6, δ_7 и по формуле (3.19) – нижнюю оценку для δ_8, δ_9. Вероятности $(1 - \Omega_3)^2$ в таблице 7 вычисляются в соответствии с (8.3), (8.4).

Таблицы 4–7 иллюстрируют ожидаемый факт, что с увеличением d^+ вероятность отказа уменьшается.

9. ЗАКЛЮЧЕНИЕ

В работе построены различные методы оценки количества и доли исправляемых стираний произвольного веса двоичными линейными кодами с известным спектром весов кодовых слов, с частично известным или полностью неизвестным спектром весов. Примеры вычислений даны для кодов Хэмминга и Панченко с расстоянием 3, 4 и кодов БЧХ с расстоянием 6, включая их укорочения. Выбор таких примеров обусловлен предполагаемой областью применения - твердотельные накопители и их модификации. Важно отметить, что, согласно рассчетам, произведение кодов Панченко с расстоянием 4 или кодов БЧХ с расстоянием 6 с одинаковой размерностью кодов 64 или 128 бит, обеспечивают высокую надежность: при вероятности ошибки в ячейке памяти порядка 0,0001 вероятность отказа произведения кодов Панченко [72,64,4] снижается на 7 порядков при расширении области декдирования от 3 до 5 стираний. Для произведения кодов БЧХ той же размерности аналогичный эффект наступает при входной вероятности 0,001. Приведенные примеры показывают, что достаточно относительно небольшого расширения области декодирования – от $d - 1$ до $\frac{3}{2}d$, чтобы получить практически максимальный эффект. По существу, этот результат означает, что выбор практическо-

го ограничения области декодирования за указанным выше интервалом определяется только сложностью процесса исправления стираний.

В теоретической части работы следует выделить различные методы получения оценок: спектральные, комбинаторные, рекуррентные. Показаны возможности комбинирования этих методов в зависимости от объема известных данных о конкретном классе кода. В качестве особого случая рассматривается вывод оценок для укороченных и расширенных кодов. Важным результатом является вывод оценок условной вероятности обнаружения ошибок при исправлении стираний в расширенной области декодирования. Из этих оценок (теорема 6.1) следует, что обнаруживаются практически все ошибки в рассматриваемой области расширенного декодирования.

СПИСОК ЛИТЕРАТУРЫ

1. Forney G.D. Exponential Error Bounds for Erasure, List, and Decision Feedback Schemes. *IEEE Transactions on Information Theory*, 1968, vol. IT-14. no. 2, pp. 206–220.
2. Зяблов В.В., Рыбин П.С. Исправление стираний кодами с малой плотностью проверок. *Проблемы передачи информации*, 2009, т. 45, № 3, стр. 15–32.
3. Назаров М.Н., Мишин С.П. Близкие к оптимальным коды, исправляющие стирания. В кн.: *Вестник Волгоградского Государственного Университета. Серия* 1*: Математика. Физика.* 1999, Вып. 4, стр. 59–69.
4. Ashikhmin A., Barg A. Minimal Vectors in Linear Codes. *IEEE Transactions on Information Theory*, 1998, vol. IT-44, no. 5, pp. 2010–2017.
5. Попов О.В. Об оценке способности линейных кодов исправлять стирания и обнаруживать ошибки при наличии стираний. *Электросвязь*, 1967, №10.
6. Попов О.В. Об исправлении стираний циклическими кодами. *Передача цифровой информации по каналам с памятью.* М.: Наука, 1970, стр. 111–124.
7. Afanassiev V.B., Davydov A.A., Zigangirov D.K. Design and analysis of codes with distance 4 and 6 minimizing the probability of decoder error. *Journal of Communications Technology and Electronics*, 2016, vol. 61, no. 12, pp. 1440–1455.
8. Боссерт М., Брайтбах М., Зяблов В.В., Сидоренко В.Р., Коды, исправляющие множество пятен ошибок или стираний. *Проблемы передачи информации*, 1997, т. 33, № 4, стр. 15–25.
9. 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.
10. Давыдов А.А., Каплан Л.П., Смеркис Ю.В., Тауглих Г.Л. К оптимизации укороченных кодов Хэмминга. *Проблемы передачи информации*, 1981, т. 17, № 4, стр. 63–72.
11. Давыдов А.А., Томбак Л.М. О количестве слов минимального веса в блоковых кодах. *Проблемы передачи информации*, 1988, т. 24, № 1, стр. 11–24.
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. IT-37, no. 3, part II, pp. 897–902.
13. 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.
14. 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.

15. Cheung K.M. *The weight distribution and randomness of linear codes.* Jet Propulsion Lab., California Inst. of Tech., Pasadena, CA. TDA Progress Report 42-97. USA. 1989, pp. 208-215. URL: https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/19890018521.pdf (дата обращения 22.11.2016)

16. Берлекэмп Э. *Алгебраическая теория кодирования.* М.: Мир, 1971. (Berlekamp E.R. *Algebraic Coding Theory.* New-York: McGrow-Hill Book Company, 1968).

17. Krasikov I., Litsyn S. On spectra of BCH codes. *IEEE Transactions on Information Theory*, 1995, vol. IT-41. no. 3, pp. 786–788.

18. 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)

19. Морелос-Сарагоса Р. *Искусство помехоустойчивого кодирования. Методы алгоритмы, применение.* М.: Техносфера, 2005. (Morelos-Zaragoza R.H. *The Art of Error Correcting Coding.* Chichester: Jon Wiley & Sons, Ltd Baffins Lane, 2002).

20. Сидельников В.М. О спектре весов двоичных кодов Боуза-Чоудхури-Хоквингема. *Проблемы передачи информации*, 1971, т. 7, № 1, стр. 14–22.

21. Weight Distribution. URL: http://www.ec.okayama-u.ac.jp//~infsys/kusaka/wd/index.html (дата обращения 27.11.2016)

Estimation of the Conditional Probability of Correct Decoding of Erasure Patterns for Linear Codes

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

There is investigated the conditional probability of correct decoding of erasure patterns of high weight (greater than code distance) for linear codes having partially known or unknown code weight spectrum. Estimates obtained for the conditional probabilities and their calculation methods are regarded to arbitrary binary linear codes and the binary Hamming, Panchenko and BCH codes, including their extending and shortening. Estimates of error detection probability during erasures correction are derived. There are proposed algorithms of product code decoding with high weight erasure patterns correction by component codes Hamming, Panchenko, BCH and the upper estimate of decoding failure probability is given.

KEYWORDS: linear code, erasure correction, product code