

Э. Л. БЛОХ, В. В. ЗЯБЛОВ

# ЛИНЕЙНЫЕ КАСКАДНЫЕ КОДЫ



ИЗДАТЕЛЬСТВО «НАУКА»

АКАДЕМИЯ НАУК СССР  
ИНСТИТУТ ПРОБЛЕМ ПЕРЕДАЧИ ИНФОРМАЦИИ

Э. Л. БЛОХ, В. В. ЗЯБЛОВ

# ЛИНЕЙНЫЕ КАСКАДНЫЕ КОДЫ



ИЗДАТЕЛЬСТВО «НАУКА»

Москва 1982

Блох Э. Л., Зяблов В. В. Линейные каскадные коды.  
М.: Наука, 1982. 229 с.

В книге рассматриваются помехоустойчивые линейные каскадные коды произвольного порядка — обобщенные каскадные коды. Разрабатываются оптимальные по избыточности методы построения каскадных кодов с заданными корректирующими свойствами. Исследуется асимптотическое поведение верхних и нижних границ для кодового расстояния каскадного кода, а также потенциальные возможности каскадного кодирования.

Предлагается для специалистов в области теории информации и кодирования, систем связи, передачи и хранения информации.

Ответственный редактор

Доктор технических наук  
профессор С. И. САМОЙЛЕНКО

Помехоустойчивое кодирование стало эффективным методом повышения верности передачи и хранения цифровой информации. Это хотя и молодое, но быстро развивающееся направление. Так, библиография в монографии [108] насчитывает более 1500 наименований. Настоящая монография посвящена одному из наиболее перспективных классов кодов в помехоустойчивом кодировании — обобщенным каскадным кодам. Перспективность обусловлена практическим применением кодов и тем, что многие теоретические задачи решаются пока только каскадными методами [11].

В мировой литературе каскадным методом, не считая большого числа оригинальных статей, посвящено две монографии: Форни [140] и авторов [23]. Отличие настоящей работы в том, что по сравнению с обеими монографиями в ней расширен класс исследуемых кодов и проведено всестороннее его исследование, а не только вероятностное, как в [140], или алгебраическое в [23].

При изложении материала в книге принят следующий порядок. Анализ каскадных методов построения кодов дан в первой и второй главах, асимптотическое исследование верхних и нижних границ кодового расстояния — в третьей главе, каскадное декодирование описывается и анализируется в четвертой главе. В пятой главе выясняются потенциальные возможности каскадных методов. Обрамлением всего исследования служат проблемы сложности реализации помехоустойчивого кодирования, поставленные в первой главе и решаемые в шестой. Методическое отличие настоящей монографии — в вынесении в приложения большинства доказательств. Это позволило сконцентрировать внимание читателя на основных достижениях и результатах помехоустойчивого каскадного кодирования. Если же читатель заинтересуется и методами доказательств, то найдет их в приложениях.

Монография в основном построена на оригинальных результатах авторов с использованием достижений других специалистов в области каскадных методов. Это в первую очередь различные модернизации каскадного декодирования [37, 47, 58, 65, 67] и решение проблем сложности декодирования [3, 6, 9, 11]. При изложении материала авторы полагали, что читатель знаком с основными положениями теории помехоустойчивого кодирования.

Чтение книги можно рекомендовать всем читателям сначала без обращения к приложениям и лишь при повторном изучении познакомиться с доказательствами в приложениях. Формально после первых двух глав можно знакомиться с любой следующей, т. е. с четвертой, пропустив третью, пятой, пропустив третью и четвертую и т. д.

Вопросы, связанные с технической реализацией каскадного кодирования и декодирования, подробно изложены в работе [23], а потому в настоящей монографии не рассматривались.

## ЦЕЛЬ И ПРОБЛЕМЫ КАСКАДНОГО КОДИРОВАНИЯ

---

В главе рассмотрены основные задачи, стоящие перед помехоустойчивым кодированием. Приведены достижения теории кодирования, определяющие потенциальные возможности корректирующих кодов. Вводятся основные понятия сложности реализации помехоустойчивого кодирования и даются оценки сложности реализации потенциальных корректирующих свойств блочных кодов. На эвристическом и функциональном уровнях описан принцип каскадного кодирования. Дается развернутая формулировка основных задач исследования.

### § 1.1. Блочное помехоустойчивое кодирование

#### 1.1.1. Задачи помехоустойчивого кодирования

Пусть передача некоторой дискретной информации осуществляется по схеме, которая в укрупненном виде показана на рис. 1. 1. Согласно этой схеме информационные символы поступают от источника информации 1 на кодер 2, который для каждых  $k$  информационных символов формирует кодовые слова длины  $n$ . Эти кодовые слова посимвольно передаются по каналу 3 и, искаженные шумами, поступают на декодер 4. Декодер, анализируя принятое слово, формирует решение о том, что выдать получателю информации 5. Отношение  $k/n = R$  называется скоростью передачи кода.

Как правило, решение декодера бывает двух типов:

- 1) если декодер считает, что все ошибки удалось исправить, то принимается решение выдать получателю информационные символы. При этом выдаваемые декодером информационные символы могут быть как правильными (совпадать с переданными), так и ошибочными (отличаться от переданных);
- 2) если ошибки обнаружены, но при данном правиле декодирования они не могут быть исправлены, то принимается решение выдать получателю информации стирание (специальный сигнал, означающий отказ от декодирования).

Такое эвристическое описание кодирования и декодирования переведем на функциональный уровень, для чего введем следующие обозначения:  $\{\mu\}$  — множество информационных слов длины  $n$ , т. е. таких слов, у которых  $k$  символов на заданных позициях выбираются произвольно (они определяются передаваемой информацией), а остальные  $r = n - k$  символов нулевые;  $\{\alpha\}$  — множество кодовых слов длины  $n$ ;  $\{\hat{\alpha}\}$  — множество слов, поступивших на декодер (множество принимаемых слов);  $\{\hat{\varepsilon}\}$  — множество исправляемых при декодировании сочетаний ошибок;

$\{\tilde{e}\}$  — множество обнаруживаемых (но неисправляемых) при декодировании сочетаний ошибок.

Отметим, что любое слово  $\hat{a} \in \{\hat{a}\}$  либо представимо в виде  $\hat{a} = \alpha + \tilde{e}$ ,  $\alpha \in \{\alpha\}$  и  $\tilde{e} \in \{\tilde{e}\}$  и тогда такое представление единственно, либо оно представимо в виде  $\hat{a} = \alpha + \tilde{e}$ ,  $\alpha \in \{\alpha\}$  и  $\tilde{e} \in \{\tilde{e}\}$  и тогда такое представление не единственно.

Кодирование задается функцией  $\varphi$ , взаимно-однозначно отображающей множество информационных слов  $\{\mu\}$  на множество кодовых слов  $\{\alpha\}$ , т. е.  $\alpha = \varphi(\mu)$  и  $\mu = \varphi^{-1}(\alpha)$ . Если  $\{\mu\}$  и  $\{\alpha\}$  — множество слов над полем  $GF(q)$  и  $\varphi$  — линейная над этим полем функция, то код называется линейным.

Декодирование задается функцией  $\Psi$ , отображающей множество принимаемых слов  $\{\hat{a}\}$  на множество информационных слов  $\{\mu\}$ , т. е.

$$\Psi(\hat{a}) = \begin{cases} \tilde{\mu} \in \{\mu\}, & \text{если } \hat{a} = \alpha + \tilde{e}; \\ * (\text{стирание}), & \text{если } \hat{a} = \alpha + \tilde{e}. \end{cases}$$

При этом если полученное при декодировании слово  $\tilde{\mu}$  совпадает с переданным словом  $\mu$  (т. е. если  $\tilde{\mu} = \mu$ ), то говорят о правильном декодировании, в противном случае — об ошибочном декодировании. Так как множества  $\{\mu\}$  и  $\{\alpha\}$  связаны взаимно-однозначным отображением, то под декодированием часто понимают функцию

$$\psi(\hat{a}) = \begin{cases} \tilde{\alpha} \in \{\alpha\}, & \text{если } \hat{a} = \alpha + \tilde{e}; \\ * (\text{стирание}), & \text{если } \hat{a} = \alpha + \tilde{e}. \end{cases}$$

Очевидно, что

$$\Psi(\hat{a}) = \begin{cases} \varphi^{-1}(\psi(\hat{a})), & \text{если } \hat{a} = \alpha + \tilde{e}; \\ \psi(\hat{a}), & \text{если } \hat{a} = \alpha + \tilde{e}. \end{cases}$$

Рассмотрим различие между функциями  $\Psi$  и  $\psi$ . Функция  $\psi$  принятому слову  $\hat{a}$  ставит в соответствие кодовое слово  $\alpha$ , т. е.

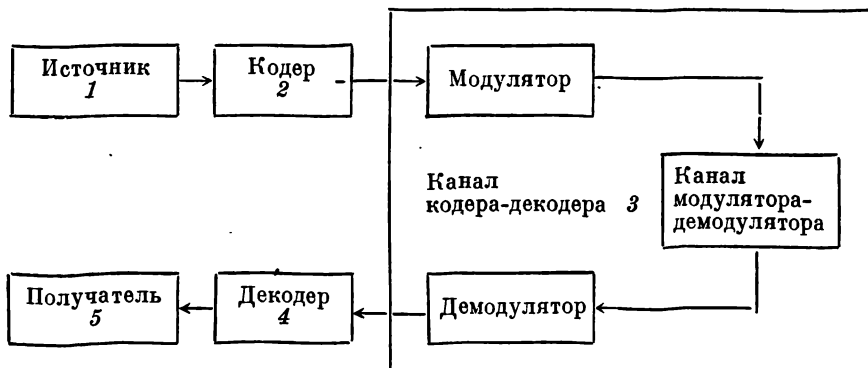


Рис. 1.1. Блок-схема линии связи

как бы осуществляет преобразование, «обратное» по отношению к преобразованию в канале. Конечно, в силу случайности преобразований в канале обратной функции в строгом смысле не существует, но в том и состоит главная проблема теории кодирования, чтобы так выбрать код (функцию  $\varphi$ ) и его декодирование (функцию  $\psi$ ), чтобы в подавляющем большинстве типичных сочетаний ошибок функция  $\psi$  оказывалась бы обратной к преобразованиям в канале. Функция  $\Psi$  представляет собой композицию функций  $\psi$  и  $\varphi^{-1}$ .

Одной из центральных проблем теории помехоустойчивого кодирования является выбор кодов с возможно лучшими корректирующими свойствами. Последние обычно оцениваются следующими характеристиками: 1) минимальным расстоянием между кодовыми словами — кодовым расстоянием  $d$ ; 2) спектром расстояний между кодовыми словами; 3) вероятностью ошибочного декодирования при передаче по заданному каналу; 4) парой вероятностей (ошибочного декодирования и стирания) при передаче по заданному каналу.

Выбор кодов может быть как безусловным (т. е. из множества всех кодов без каких-либо ограничений), так и условным (например, из заданного класса кодов или при наличии ограничений на сложность процесса вычислений при выборе кодов, или при ограничениях на выбор алгоритмов кодирования и декодирования, а также на сложность их реализации).

Оценки лучших корректирующих свойств по всем кодам или по некоторому классу кодов, реализуемых при использовании оптимальных алгоритмов декодирования, будут характеризовать потенциальные возможности кодов вообще или же кодов из данного класса. В то же время аналогичные оценки при ограничении на выбор алгоритмов декодирования будут характеризовать реализуемые корректирующие свойства при заданном алгоритме декодирования.

### 1.1.2. Потенциальные корректирующие свойства блочных кодов

Лучшие из известных авторам оценки потенциальных корректирующих свойств блочных кодов определяются следующими теоремами.

**Теорема 1.1.** Существуют блочные линейные коды над полем  $GF(q)$ , кодовое расстояние  $d = n\delta(R)$  которых при любой скорости передачи  $R$  и  $n \rightarrow \infty$  удовлетворяет неравенству  $\delta(R) \geq \delta_{\text{ВГ}}(R, q)$ , где  $\delta_{\text{ВГ}}(R, q)$  — граница (или оценка) Варшамова—Гилберта для  $q$ -х кодов, определяемая равенством

$$R = 1 + \delta_{\text{ВГ}} \log_q \delta_{\text{ВГ}} + (1 - \delta_{\text{ВГ}}) \log_q (1 - \delta_{\text{ВГ}}) - \delta_{\text{ВГ}} \log_q (q - 1). \quad (1.1)$$

В дальнейшем будут особенно интересны такие два случая:  $q=2$  и  $q \rightarrow \infty$ . При  $q \rightarrow \infty$  формула (1. 1) принимает вид

$$R = 1 - \delta_{\text{ВГ}}, \quad (1. 2)$$

и в этом случае оценка ВГ является асимптотически точной. При  $q=2$  оценка ВГ (1. 1) принимает вид

$$R = 1 + \delta_{\text{ВГ}} \log_2 \delta_{\text{ВГ}} + (1 - \delta_{\text{ВГ}}) \log_2 (1 - \delta_{\text{ВГ}}) = 1 - H(\delta_{\text{ВГ}}) \quad (1. 3)$$

и неизвестно, будет ли она асимптотически точной. Коды, для которых  $\delta(R)$  достигает границы ВГ, будем называть «хорошими», или кодами с «хорошим» кодовым расстоянием.

В дальнейшем для двоичных кодов нам понадобится также оценка сверху для кодового расстояния. Одна из таких оценок определяется следующей теоремой.

**Теорема 1.2.** Не существует двоичных блочных кодов (линейных или нелинейных), для которых  $\delta(R) = d/n$  при  $n \rightarrow \infty$  превосходит величину

$$\delta_{\text{В}}(R) = \begin{cases} \delta_{\text{БЭ}}(R) = 2(1 - \delta_{\text{ВГ}})\delta_{\text{ВГ}} & \text{при } R > 0; \\ \delta_{\Pi}(0) = \frac{1}{2} & \text{при } R \rightarrow 0, \end{cases} \quad (1. 4)$$

где  $\delta_{\text{БЭ}}(R)$  — оценка Бассалыго—Элайеса, а  $\delta_{\Pi}(R)$  — оценка Плотикина, которая справедлива при  $R \rightarrow 0$  и  $n \rightarrow \infty$ , если только  $Rn = k \rightarrow \infty$ .

Таким образом, оценки, определяемые выражениями (1. 3) и (1. 4), являются соответственно нижней и верхней асимптотическими оценками величины  $\delta(R)$  как для линейных, так и нелинейных двоичных блочных кодов. Доказательство теоремы 1.1 и 1.2 дано в работе [115]. Отметим, что оценка, определяемая теоремой 1.2, была улучшена в работах [105, 160].

Рассмотрим теперь спектр расстояний между кодовыми словами. Ограничимся лишь случаем линейных кодов, когда спектр расстояний совпадает со спектром весов кодовых слов. При этом число кодовых слов  $N(w)$  веса  $w$  совпадает с числом слов, находящихся на расстоянии  $w$  от любого кодового слова.

**Теорема 1.3.** Существуют двоичные линейные блочные коды, спектр весов кодовых слов  $\{N(w): w = \overline{0, n}\}$ , которых удовлетворяет соотношениям

$$N(w) = \begin{cases} 1 & \text{при } w = 0; \\ 0 & \text{при } 0 < w < \delta_{\text{ВГ}} n; \\ \leq n C_n^w 2^{-(1-R)n} & \text{при } n \delta_{\text{ВГ}} \leq w \leq n. \end{cases} \quad (1. 5)$$

Коды, спектр весов которых удовлетворяет соотношениям (1. 5), будем называть кодами с «хорошим» спектром весов. Как следует из условия  $N(w) = 0$ , при  $0 < w < n \delta_{\text{ВГ}}$  эти коды автомати-



чески являются «хорошими». Однако неизвестно, совпадает ли множество «хороших» кодов с множеством кодов с «хорошим» спектром весов. Доказательство теоремы 1.3 вытекает из работы [18].

При рассмотрении вероятностей, ошибочного декодирования  $P_e$  и стирания  $P_\tau$  ограничимся только случаем двоичного симметричного канала (ДСК) без памяти с вероятностью ошибки при передаче каждого двоичного символа  $\varepsilon$ .

Оценки искомых вероятностей будем представлять в виде  $P_e \leq \exp \{-nE_e(R)\}$ ,  $P_\tau \leq \exp \{-nE_\tau(R)\}$ , где  $E_e(R)$  — экспонента вероятности ошибочного декодирования, а  $E_\tau(R)$  — экспонента вероятности стирания при декодировании.

Если осуществляется декодирование без стирания, когда каждое принятое слово отождествляется с некоторым кодовым словом, то справедлива следующая теорема.

**Теорема 1.4.** Существуют двоичные линейные блочные коды, для которых экспонента вероятности ошибочного декодирования по максимуму правдоподобия в ДСК без памяти при любой скорости передачи, не превосходящей пропускной способности канала  $C$ , оценивается снизу величиной  $E_0(R)$ , определяемой равенствами

$$\begin{aligned} \text{при } 0 \leq R \leq R_0 \quad (R_0 = 1 - H(2\sqrt{\varepsilon(1-\varepsilon)} / (1 + 2\sqrt{\varepsilon(1-\varepsilon)})); \\ E_0(R) = -\delta_{\text{ВГ}}(R) \ln(2\sqrt{\varepsilon(1-\varepsilon)}); \\ \text{при } R_0 \leq R \leq R_* \quad (R_* = 1 - H(\sqrt{\varepsilon}/(\sqrt{\varepsilon} + \sqrt{1-\varepsilon})), \\ E_0(R) = (1-R) \ln 2 - \ln(1 + 2\sqrt{\varepsilon(1-\varepsilon)}); \\ \text{при } R_* \leq R \leq C \quad (C = 1 - H(\varepsilon)) \\ \left. \begin{aligned} E_0(R) &= \frac{s}{1-s} (1-R) \ln 2 - \\ &- \frac{1}{1-s} \ln(\varepsilon^{1-s} + (1-\varepsilon)^{1-s}) \\ R &= 1 - H(\varepsilon^{1-s} / (\varepsilon^{1-s} + (1-\varepsilon)^{1-s})) \end{aligned} \right\} 0 \leq s \leq 1/2. \end{aligned} \quad (1.6)$$

Теорема 1.4 в наиболее общем виде была доказана Галлагером [52].

### 1.1.3. Обменные соотношения для вероятностей ошибки и стирания

При декодировании по минимуму расстояния, которое для каналов без памяти совпадает с декодированием по максимуму правдоподобия, обязательно выдается некоторое кодовое слово. Однако в результате декодирования наряду с выдачей кодового слова может иметь место и отказ от декодирования. Такое декодирование будем называть декодированием с гарантией, так как принятое слово  $\hat{a}$  отождествляется с некоторым кодовым словом  $a_0$  тогда

и только тогда, когда для всех кодовых слов  $\alpha$ , отличных от  $\alpha_0$ , выполняется условие

$$P(\hat{\alpha} | \alpha_0) \geq e^{\nu} P(\hat{\alpha} | \alpha), \quad \alpha \neq \alpha_0, \quad (1.7)$$

где  $P(\hat{\alpha} | \alpha)$  — условная вероятность принять слово  $\hat{\alpha}$ , если известно, что было передано слово  $\alpha$ , а  $\nu \geq 0$  — коэффициент гарантии.

Декодирование с гарантией ( $\nu > 0$ ) отличается от декодирования по максимуму правдоподобия ( $\nu=0$ ) тем, что при  $\nu > 0$  может оказаться, что среди кодовых слов нет ни одного, для которого выполняется условие (1.7), т. е. будет отказ от декодирования. В дальнейшем вместо условия (1.7) будем пользоваться также следующим условием:

$$P(\hat{\alpha} | \alpha_0) \geq e^{\nu} \sum_{\alpha \neq \alpha_0} P(\hat{\alpha} | \alpha). \quad (1.8)$$

В этом случае возможен отказ от декодирования и при  $\nu=0$ . Потому такое декодирование называют также декодированием со стиранием.

При увеличении коэффициента гарантии  $\nu$  происходит уменьшение зоны приема вокруг каждой кодовой точки, а потому и уменьшение вероятности ошибочного декодирования  $P_e$ . Одновременно увеличивается зона стирания, т. е. вероятность стирания  $P_\tau$ . Это явление будем называть обменом между вероятностями ошибки и стирания. Для нелинейных двоичных кодов соотношения обмена были исследованы Форни [141], а для линейных двоичных кодов соотношения обмена определяются следующей теоремой.

**Теорема 1.5.** Для двоичных линейных блочных кодов оценки экспоненты вероятности ошибки  $E_e(R, \nu)$  и экспоненты вероятности стирания  $E_\tau(R, \nu)$  при декодировании с гарантией ( $\nu > 0$ ) определяются выражениями [32]

$$\begin{aligned} E_e(R, \nu) &= E(R) - \frac{s_0 t_0}{s_0 - r_0} \nu, \\ E_\tau(R, \nu) &= E(R) + \frac{s_0 t_0}{s_0 - r_0} \nu, \end{aligned} \quad (1.9)$$

где  $E(R) = \max_{\substack{s \geq 0 \\ t \leq 0 \\ r \leq 0}} \left\{ \frac{r}{s-r} \ln g(s) - \frac{s}{s-r} \ln g(r) - \right.$

$$\left. - \frac{s}{s-r} \frac{1}{n} \ln \psi \left( \frac{g(r, t)}{g(r)} \right) \right\}, \quad (1.10)$$

$$g(s) = (1 - \epsilon)^{1-s} + \epsilon^{1-s},$$

$$g(r, t) = (1 - \epsilon)^{1-r+t} \epsilon^{-t} + (1 - \epsilon)^{-t} \epsilon^{1-r+t},$$

$\psi(z)$  — производящая функция весов ненулевых кодовых слов,  $s_0, r_0, t_0$  — значения  $s, r, t$ , максимизирующие (1.10).

Доказательство теоремы 1.5 приведено в приложении П.1.1. Согласно теореме 1.5 при увеличении коэффициента гарантии  $\nu$  оценка экспоненты вероятности ошибки  $E_e(R, \nu)$  увеличивается ( $s_0 t_0 / (s_0 - r_0) < 0$ ) ровно настолько, насколько уменьшается оценка экспоненты вероятности стирания  $E_\tau(R, \nu)$ . Такое соответствие между  $E_e(R, \nu)$  и  $E_\tau(R, \nu)$  будем называть эквивалентным обменом. Отметим, что

$$E(R) = E_e(R, 0) = E_\tau(R, 0) \quad (1.11)$$

представляет собой оценку экспоненты вероятности ошибки при декодировании по максимуму правдоподобия. Точное решение (1.10) при произвольном спектре весов ненулевых кодовых слов представляет значительные трудности. Поэтому полезна оценка  $E(R)$ , задаваемая следующим утверждением, доказанным в приложении П.1.2.

**Утверждение 1.1.** Пусть для двоичного линейного кода длины  $n$  со скоростью передачи  $R$  ( $0 \leq R \leq 1$ ) задана производящая функция весов ненулевых кодовых слов  $\psi_R(z)$ . Пусть

$$F(R, s) = \frac{2s-1}{1-s} \ln(\varepsilon^{1-s} + (1-\varepsilon)^{1-s}) - \frac{s}{1-s} \ln(\varepsilon^{2(1-s)} + (1-\varepsilon)^{2(1-s)}) - \frac{s}{1-s} \frac{1}{n} \psi_R\left(\frac{2(\varepsilon(1-\varepsilon))^{1-s}}{\varepsilon^{2(1-s)} + (1-\varepsilon)^{2(1-s)}}\right).$$

Обозначим через  $R_*$  решение уравнения

$$\left. \frac{\partial F(R, s)}{\partial s} \right|_{s=1/2} = 0.$$

Тогда оценка экспоненты вероятности ошибочного декодирования по максимуму правдоподобия ( $\nu=0$ ) в ДСК без памяти определяется при  $0 \leq R \leq R_*$  равенством

$$E(R) = F\left(R, \frac{1}{2}\right) = \frac{1}{n} \ln \psi_R(2\sqrt{\varepsilon(1-\varepsilon)}), \quad (1.12)$$

а при  $R_* \leq R \leq C_1$  параметрическим уравнением  $E(R) = F(R, s)$ ,  $\partial F(R, s)/\partial s = 0$ , где  $C_1$  соответствует скорости передачи, при которой  $E(C_1) = 0$  и  $s = 0$ .

Обменные соотношения (1.9) в условиях утверждения 1.1 принимают вид

$$\begin{aligned} \text{при } 0 \leq R \leq R_* \quad E_e(R, \nu) &= E(R) + \nu/2, \quad E_\tau(R, \nu) = E(R) - \nu/2; \\ \text{при } R_* \leq R \leq C_1 \quad E_e(R, \nu) &= E(R) + s\nu, \quad E_\tau(R, \nu) = E(R) - s\nu. \end{aligned}$$

Для получения на основе утверждения 1.1 конкретной зависимости экспоненты  $E(R)$  от скорости передачи  $R$  необходимо располагать производящей функцией спектра весов ненулевых кодовых слов  $\psi_R(z)$  или оценкой для нее. Эта зависимость в случае двоичных линейных кодов с «хорошим» спектром весов задается доказанным в приложении П.1.3 следующим утверждением.

**Утверждение 1.2.** Для двоичных линейных кодов со спектром весов кодовых слов, удовлетворяющих теореме 1.3, экспонента

$E(R) = E_0(R)$ , где  $E_0(R)$  определяется в соответствии с теоремой 1.4.

В заключение отметим, что асимптотически существуют, к сожалению, только переборные методы построения кодов с описанными в настоящем параграфе потенциальными корректирующими свойствами. О сложности таких алгоритмов будет сказано в следующем параграфе.

## § 1.2. Реализация помехоустойчивого кодирования

### 1.2.1. Проблемы реализации помехоустойчивого кодирования

Значительный теоретический и практический интерес представляет вопрос, насколько сложно реализовать потенциальные корректирующие свойства, описанные в предыдущем параграфе. Чтобы ответить на него, нужно договориться о том, что мы будем понимать под сложностью. При этом будем учитывать, что построение системы с помехоустойчивым кодированием связано с решением следующих задач.

А. Нужно выбрать код  $A(n, k)$  с кодированием  $\varphi_n$  и декодированием  $\psi_n$ .

Б. Передача каждого информационного слова  $\mu$  осуществляется кодированием, т. е. до передачи вычисляется слово  $\alpha = \varphi_n(\mu)$ , и декодированием, т. е. после приема слова  $\hat{\alpha}$  вычисляется слово  $\hat{\mu} = \psi_n(\hat{\alpha})$ .

Подчеркнем разницу задач А и Б с точки зрения построения системы с помехоустойчивым кодированием. Задача А решается единожды при проектировании системы. Решение задачи Б проводится многократно, периодически при передаче каждого слова  $\mu$ . Поэтому для решения задачи А целесообразно использовать некоторый универсальный вычислитель, который занимается задачей А лишь однажды в течение какого-то времени, а до и после этого решает другие задачи. Решение задачи Б в силу ее многократности более целесообразно проводить на специализированном вычислителе.

Остановимся кратко на вопросе выбора универсального и специализированного вычислителя. При этом нужно учитывать, что мы говорим не о выборе реального устройства, а о выборе моделей реальных устройств, посредством которых могут быть получены оценки сложности реализации этих задач.

В качестве универсального вычислителя выберем многоленточную машину Тьюринга (ММТ), описание которой дадим неформально, так как строгое изложение потребует слишком много места и затруднит понимание простых принципов, на которых основана рассматриваемая конструкция.

ММТ состоит из управляющего устройства — конечного автомата и фиксированного числа лент, подчиненных управляющему устройству. Каждая из лент не ограничена в обе стороны и раз-

делена на бесконечную последовательность ячеек. Управляющее устройство имеет на каждой ленте одну считывающую головку, которая обзрывает одну из ячеек данной ленты. Имеется конечное число различных символов, которые могут быть записаны в ячейках лент. Каждая комбинация считываемых головками символов вместе с состоянием управляющего устройства однозначно определяют машинную операцию. Машинная операция заключается в том, что на каждой ячейке ленты, обозреваемой головкой, либо символ остается без изменения, либо стирается старый и печатается новый, ленты же независимо друг от друга сдвигаются на одну ячейку влево или вправо или же остаются на месте, а также изменяется или нет состояние управляющего устройства. Машина после этого готова к выполнению следующей операции. Если же данная операция не требует изменения символов, записанных на лентах, сдвига ни одной из лент и изменения состояния управляющего устройства, то говорят, что машина остановилась.

Выбор ММТ в качестве универсального вычислителя обусловлен следующими соображениями:

в математике ММТ стали классическим объектом, посредством которого решаются вопросы сложности алгоритмов и вычислений по алгоритмам [97, 98, 123];

широкое использование ММТ как математического объекта для описания сложности решения проблем делает общезначимыми полученные характеристики теории кодирования и позволяет проводить аналогии и сравнения;

при необходимости ММТ может быть замоделирована на любой другой универсальной вычислительной машине, что делает полученные результаты пригодными для любого универсального вычислителя.

Обычно сложность решения той или иной проблемы на ММТ оценивается сложностью алгоритма (длиной программы) и временем вычислений (число шагов равно числу машинных операций от начала вычислений до остановки). Поскольку сложность алгоритма конечна и не зависит от длины кода, а время вычислений растет с длиной кода  $n$ , то сложность будем оценивать временем вычислений  $T(n)$ , которое, очевидно, есть некоторая функция от длины кода.

В качестве специализированного вычислителя выберем схему на функциональных элементах [107], которая неформально может быть описана следующим образом. Схема строится из некоторого набора функциональных элементов, например конъюнкции и дизъюнкции двух переменных, отрицания переменной и сложения двух переменных по модулю два. Конструкции из этих элементов представим в виде направленных графов, которые будем называть схемами. В каждой такой схеме-графе  $S$  выделено  $N$  входных вершин (из них начинаются все пути на графе),  $M$  выходных вершин (в них заканчиваются все пути на графе), а в остальных вершинах, называемых функциональными, стоят функциональные элементы. Число ребер, входящих в функцио-

нальную вершину, равно числу входов стоящего в ней элемента. Для каждой схемы  $S$  определим ее сложность  $L(S)$  как сумму сложностей элементов во всех ее функциональных вершинах.

Данная схема  $S'$  реализует функцию  $y=f(x)$ , если при подаче на входы схемы любого слова  $x$ , для которого функция  $f$  определена, на выходе получается слово  $y=f(x)$ . Обозначим через  $G(f)$  множество схем, которые реализуют функцию  $f$ . Сложностью реализации функции  $\kappa(f)$  назовем величину

$$\kappa(f) = \min_{S \in G(f)} L(S).$$

Таким образом, сложность кодирования (декодирования) определяется сложностью самой простой схемы, реализующей это кодирование (декодирование).

На основе введенных понятий будем характеризовать некоторый класс кодов с заданными корректирующими свойствами такими параметрами сложности:  $T(n)$  — характеристика сложности решения на ММТ проблемы А;  $\{\kappa(\varphi_n), \kappa(\psi_n)\}$  — характеристика сложности решения проблемы Б посредством схемы на функциональных элементах.

Отметим, что в большинстве случаев вычисление точных значений  $T(n)$ ,  $\kappa(\varphi_n)$ ,  $\kappa(\psi_n)$  не представляется возможным, и потому ограничимся лишь оценками.

Более подробно эти вопросы рассматриваются в работах [11, 164].

### 1.2.2. Сложность реализации помехоустойчивого кодирования

Для реализации помехоустойчивого кодирования для того или иного класса корректирующих кодов требуется алгоритм, который позволит для заданных длины кода и скорости передачи получить описание схем кодирования и декодирования. Потребитель же на основе корректирующих свойств и схем кодирования и декодирования (точнее, сложности кодирования и декодирования) решает вопрос, устраивает его данная помехоустойчивая система кодирования или нет. Возможности тех или иных классов кодов в смысле сложности приведем в виде утверждений. Коды, удовлетворяющие границе ВГ, могут быть построены по алгоритмам Гилберта [115] и Варшамова [42].

**Утверждение 1.3.** Алгоритм Гилберта позволяет строить для любой скорости передачи  $R$  и длины  $n$  коды с кодовым расстоянием, соответствующим границе ВГ, и со следующими характеристиками сложности [11]:  $T(n) \leq c \cdot 2^{(1+R)n}$ ,  $\kappa(\varphi) \leq c \cdot 2^{Rn}$ ,  $\kappa(\psi) \leq c \cdot 2^{Rn}$ , где  $c$  — некоторая постоянная при декодировании  $\varphi$  по минимуму расстояния.

**Утверждение 1.4.** Алгоритм Варшамова позволяет строить для любой скорости передачи  $R$  и длины кода  $n$  линейные коды

с соответствующим границе ВГ кодовым расстоянием со следующими характеристиками сложности [11]:

$T(n) \leq cn^3 2^{(1-R)n}$ ,  $\kappa(\varphi) \leq cn^2 / \log n$ ,  $\kappa(\psi) \leq cn \min \{2^{(1-R)n}, 2^{Rn}\}$ , где  $c$  — некоторая постоянная, при декодировании  $\psi$  по минимуму расстояния.

Из этих двух утверждений видно, что переход к линейным кодам не ухудшает корректирующих свойств кодов и фактически снимает проблему реализации кодирования. Однако по существу остаются нерешенными проблемы построения кодов и их декодирования.

Следующее утверждение показывает, что можно решить все три проблемы (в смысле уменьшения сложности), но, к сожалению, лишь при асимптотически очень сильном ухудшении корректирующих свойств.

**Утверждение 1.5.** Алгоритм построения двоичных БЧХ кодов позволяет строить для любой скорости передачи  $R$  и длины  $n$  линейные двоичные коды с кодовым расстоянием порядка  $d = cn / \log n$  со следующими характеристиками сложности [11]:

$T(n) = cn^2 (\log n)^3$ ,  $\kappa(\varphi) = cn^2$ ,  $\kappa(\psi) = cn^2 (\log n)^2$ , где  $c$  — некоторая постоянная, и при декодировании  $\psi$  (по алгоритму Берлекэмпа) осуществляется лишь исправление ошибок до кратности  $t < d/2$ .

Для  $q$ -х кодов ограниченной длины  $n \leq q+1$  можно решить все три проблемы при степенном росте сложности без ухудшения их корректирующих свойств.

**Утверждение 1.6.** Алгоритм построения кодов РС над полем позволяет строить для любой скорости передачи  $R$  и длины кода  $n \leq q+1$  линейные коды с кодовым расстоянием  $d = n - k + 1$  со следующими характеристиками сложности [11]:  $T(n) \leq cq^2 (\log q)^3$ ,  $\kappa(\varphi) \leq cq^2 \log q$ ,  $\kappa(\psi) \leq cq^2 (\log q)^2$ , где  $c$  — некоторая постоянная, и при декодировании  $\psi$  (по алгоритму Берлекэмпа) осуществляется лишь исправление ошибок до кратности  $t$  и стираний до кратности  $\tau$ , удовлетворяющих условию  $2t + \tau < d$ .

Таким образом, получить одновременно асимптотически хорошие корректирующие свойства и приемлемые (все неэкспоненциальные) характеристики сложности для кодов с фиксированным основанием не удастся. Как следует из работы [11], в современных условиях это возможно лишь каскадными методами, всестороннему исследованию которых посвящено дальнейшее содержание работы.

## § 1.3. Блочное каскадное кодирование

### 1.3.1. Эвристическое описание каскадного кодирования

Рассмотрим описание схемы каскадного кодирования (рис. 1.2) сначала на эвристическом уровне. Информационные символы поступают от источника информации 1 на кодер 2, с которого преобразованные им символы поступают на другой кодер 3,

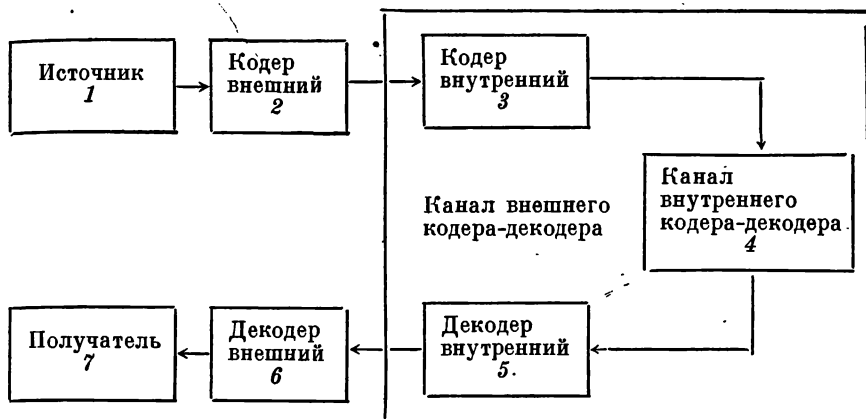


Рис. 1.2. Блок-схема линии связи с каскадным кодированием

откуда они передаются в канал 4. Декодирование символов, поступивших из канала, осуществляется декодером 5, который при декодировании опирается на результаты кодирования кодером 3. Затем декодированные декодером 5 символы поступают на следующий декодер 6, который осуществляет окончательное декодирование, опираясь на результаты кодирования кодером 2, и свое решение выдает получателю 7.

В соответствии с этой схемой кодер 3 и декодер 5, непосредственно примыкающие к каналу связи, можно условно объединить с этим каналом 4 и в совокупности рассматривать как новый расширенный канал, ошибки в котором определяются как помехами в исходном канале 4, так и реализуемыми корректирующими свойствами кода, используемого кодером 3 и декодером 5. Такая точка зрения, принадлежащая Форни [140], позволяет назвать кодер 3 и декодер 5 внутренними, а кодер 2 и декодер 6 — внешними. Коды, используемые внутренними и внешними кодерами и декодерами, назовем соответственно внутренними и внешними кодами. Кроме того, ограничимся случаем, когда все внутренние коды имеют длину  $n_a$ , а все внешние коды — длину  $n_b$ . Число различных внешних кодов назовем порядком каскадного кода. Наиболее существенное отличие схемы кодирования и декодирования каскадных кодов от схемы кодирования и декодирования обычных блочных кодов состоит в том, что каждый из этих процессов осуществляется не сразу, а последовательно (кодирование — сначала внешним, а затем внутренним кодерами, ее кодирование наоборот — внешним, а затем внутренним кодерами, декодирование наоборот — сначала внутренним, а затем внешним декодерами). При этом внутренние коды как бы заменяют исходный (внутренний) канал некоторым вспомогательным (внешним) каналом с меньшим количеством ошибок, окончательная борьба с которыми возлагается на внешние коды. Используя для внутрен-



них кодов различные алгоритмы декодирования (с различным соотношением между числом исправляемых и обнаруживаемых ошибок), мы формируем для внешних кодов различные вспомогательные каналы (с различным соотношением ошибок и стираний) и можем в качестве окончательного результата декодирования выбрать такой, который соответствует наилучшему (с точки зрения некоторого критерия) согласованию внешнего канала с внешними кодами. Возможность такого достаточно гибкого согласования канала с кодами приводит (как будет видно в дальнейшем) к исключительной универсальности каскадных кодов при исправлении ошибок весьма различной (и сложной) конфигурации.

Приведенное описание схемы каскадного кодирования хотя и содержит принципиальные отличия этого метода, однако оставляет в стороне многие существенные детали, определяющие отличительные признаки различных методов каскадного кодирования (особенно это касается каскадных кодов порядка  $m > 1$ ). Поэтому более подробно остановимся на функциональном описании каскадного кодирования и декодирования. Базируясь на этом описании, сформулируем также основные проблемы, подлежащие исследованию в данной монографии.

### 1.3.2. Функциональное описание каскадного кодирования

Очевидно, что кодирование  $\varphi(\mu)$  и декодирование  $\psi(\hat{\alpha})$ , соответствующие описанной выше каскадной схеме, можно представить как композицию функций

$$\varphi(\mu) = \varphi_a(\varphi_b(\mu)), \quad \psi(\hat{\alpha}) = \psi_b(\psi_a(\mu)). \quad (1.13)$$

Однако в сущности каскадное кодирование предполагает значительно большее «измельчение» функций  $\varphi$  и  $\psi$ , нежели (1.13), что и является основной особенностью каскадного кодирования. Зачем вообще нужно «измельчать» функции  $\varphi$  и  $\psi$ , можно понять, если вспомнить, что сложность реализации функции, как правило, тем меньше, чем меньше число переменных, от которых она зависит. В то же время из основополагающих теорем теории кодирования следует, что чем длиннее коды (т. е. чем больше число переменных), тем лучше может быть их корректирующая способность. Удовлетворительное разрешение этого противоречия и является основной целью каскадного кодирования.

Учитывая, что слова  $\mu$ ,  $\alpha$  и  $\hat{\alpha}$  имеют одинаковую длину  $n$ , т. е. состоят из одного и того же числа символов, рассмотрим множество номеров позиций, на которых расположены эти символы. Это множество обозначим через  $N$ . Множество  $N$  тем или иным способом разобьем на  $m+1$  непересекающихся подмножеств  $M_i$ ,  $i=0, \overline{m}$ . Массив переменных (символов), номера которых принадлежат  $M_i$ , обозначим через  $\mu_i$ ,  $\alpha_i$ ,  $\hat{\alpha}_i$ .

Рассмотрим соответствующую кодированию внешними кодами функцию

$$\varphi_b(\mu) = \gamma, \quad (1.14)$$

где  $\gamma$  — вспомогательное двоичное слово длины  $n$ . Это слово будем представлять в виде

$$\gamma = (\gamma_0, \gamma_1, \dots, \gamma_m) = \varphi_b(\mu_0, \mu_1, \dots, \mu_m), \quad (1.15)$$

причем

$$\gamma_i = \varphi_{bi}(\mu_i) \quad (1.16)$$

и номера переменных образующих  $\mu_i$  и  $\gamma_i$  принадлежат  $M_i$ .

Соотношения (1.15) и (1.16) задают разбиение функции  $\varphi_b$  на  $m+1$  функций  $\varphi_{bi}$ , каждая из которых соответствует кодированию некоторым внешним кодам.

Полагая  $n = n_a n_b$ , разобьем вторично множество номеров  $N$  на  $n_b$  непересекающихся подмножеств  $N^{(j)}$  ( $j = \overline{1, n_b}$ ) по  $n_a$  номеров в каждом. Пусть  $N^{(j)} = \{n_a(j-1)+1, n_a(j-1)+2, \dots, n_a j\}$ . Массивы переменных, номера которых принадлежат  $N^{(j)}$ , обозначим через  $\mu^{(j)}$ ,  $\gamma^{(j)}$ ,  $\alpha^{(j)}$  и  $\beta^{(j)}$ .

Рассмотрим теперь соответствующую кодированию внутренними кодами функцию

$$\varphi_a(\gamma) = \alpha. \quad (1.17)$$

Соотношение (1.17) представим в виде

$$\alpha = (\alpha^{(1)}, \alpha^{(2)}, \dots, \alpha^{(n_b)}) = \varphi_a(\gamma^{(1)}, \gamma^{(2)}, \dots, \gamma^{(n_b)}), \quad (1.18)$$

причем

$$\alpha^{(j)} = \varphi_a^{(j)}(\gamma^{(j)}). \quad (1.19)$$

Соотношения (1.18) и (1.19) задают разбиение функции  $\varphi_a$  на  $n_b$  функций  $\varphi_a^{(j)}$ , каждая из которых соответствует кодированию внутренним кодом.

Таким образом, соотношения (1.14) и (1.15)–(1.19) определяют кодирование каскадного кода длины  $n = n_a n_b$ , причем функция кодирования  $\varphi$  расчленяется на  $m+1+n_b$  функций, каждая из которых зависит от значительно меньшего числа переменных. Естественно, что при такой постановке задачи основной проблемой является вопрос о выборе функций  $\varphi_{bi}$ ,  $i = \overline{0, m}$ , и  $\varphi_a^{(j)}$ ,  $j = \overline{1, n_b}$ , при которых результирующая функция  $\varphi$  определяет хороший код. При этом желательно, чтобы  $\varphi_{bi}$  и  $\varphi_a^{(j)}$  выбирались из числа функций, определяющих коды, для которых известны эффективные (не перебором) методы построения, кодирования и декодирования. Этот вопрос исследуется в гл. 2.

Другой проблемой, непосредственно связанной с первой, является оценка основных параметров каскадного кода (в частности, его кодового расстояния), которые могут быть получены при весьма большой длине кода  $n$  (асимптотика) и различных способах каскадного кодирования (т. е. различных  $m$ ,  $n_b$ ,  $\varphi_{bi}$ ,  $\varphi_a^{(j)}$ ). Эта задача рассматривается в гл. 3.

Весьма важным является также вопрос о том, может ли быть каскадное кодирование асимптотически оптимальным, т. е. суще-

ствуют ли среди каскадных кодов такие же «хорошие» коды, как и лучшие известные коды в классе всех линейных кодов. Изучение этого вопроса на базе исследования случайных каскадных кодов проводится в гл. 5.

Таким образом, в гл. 2, 3, 5 изучаются вопросы, связанные с существованием и построением каскадных кодов с хорошими корректирующими свойствами. Однако не менее важен вопрос о декодировании каскадного кода. Конечно, реализация корректирующих свойств каскадных кодов всегда может быть обеспечена при помощи декодирования по минимуму расстояния (по максимуму правдоподобия). Но при таком способе декодирования, техническая реализация которого весьма сложна, не может даже стоять вопрос о практическом применении сколько-нибудь длинных кодов. Поэтому при использовании каскадных кодов естественно применять и каскадное декодирование, суть которого на функциональном уровне может быть описана следующим образом.

Функцию  $\mu = \psi(\hat{\alpha}) = \psi_b(\psi_a(\hat{\alpha}))$ , реализующую декодирование, будем определять, последовательно вычисляя  $\mu_0, \mu_1, \dots, \mu_m$ . Для этого сначала находим  $\gamma_0 = \psi_a^{(0)}(\hat{\alpha})$ , где  $\hat{\gamma}_0 = (\hat{\gamma}_{01}, \hat{\gamma}_{02}, \dots, \hat{\gamma}_{0n_b})$ ,  $\hat{\gamma}_{0j} = \psi_a^{(0,j)}(\hat{\alpha}^{(j)})$ . После этого определяем  $\mu_0 = \psi_b(\hat{\gamma}_0)$  (здесь и в дальнейшем используются обозначения, согласно которым совокупность переменных с номером, принадлежащим множеству  $M_i \cap N^{(j)}$ ,  $i = \overline{0, m}$ ,  $j = \overline{1, n_b}$ , записывается в виде  $\mu_{i,j}, \gamma_{i,j}, \alpha_{i,j}$ ).

Далее вычисляем  $\hat{\gamma}_1 = \psi_a^{(1)}(\hat{\alpha}, \mu_0)$  и  $\mu_1 = \psi_{b1}(\hat{\gamma}_1)$ , где  $\hat{\gamma}_1 = (\hat{\gamma}_{11}, \hat{\gamma}_{12}, \dots, \hat{\gamma}_{1n_b})$ ,  $(\hat{\gamma}_{1j} = \psi_a^{(1,j)}(\hat{\alpha}^{(j)}, \mu_0))$ . Соответственно после вычисления  $\mu_0, \mu_1, \dots, \mu_{s-1}$  находим  $\hat{\gamma}_s = \psi_a^{(s)}(\hat{\alpha}, \mu_0, \mu_1, \dots, \mu_{s-1})$  и  $\mu_s = \psi_{bs}(\hat{\gamma}_s)$ , где  $\hat{\gamma}_s = (\hat{\gamma}_{s1}, \hat{\gamma}_{s2}, \dots, \hat{\gamma}_{sn_b})$ ,  $\hat{\gamma}_{sj} = \psi_a^{(s,j)}(\hat{\alpha}^{(j)}, \mu_0, \dots, \mu_{s-1})$ .

Таким образом, алгоритм каскадного декодирования сводится к последовательному вычислению функций  $\psi_a^{(i,j)}, i = \overline{0, m}, j = \overline{1, n_b}, \psi_{bi}, i = \overline{0, m}$ , т. е. последовательному (многократному) декодированию более коротких кодов, которые использовались при каскадном кодировании.

Основной проблемой исследования каскадного декодирования (кроме построения конкретных функций  $\psi_a^{(i,j)}$  и  $\psi_{bi}$ ) является вопрос о его эффективности, т. е. вопрос о реализуемых при таком декодировании корректирующих свойствах каскадных кодов. Изучению этой проблемы посвящена гл. 4.

Отметим, что на протяжении всей книги предполагается, что информационные слова  $\mu$  и разбиение множества  $N$  на подмножества  $M_i$  и  $N^{(j)}$  формируются так, что массив  $\mu_0$  всегда является нулевым, так что число нетривиальных внешних кодов равно  $m$ .

### 1.3.3. Геометрическая интерпретация линейных каскадных кодов

В дальнейшем ограничимся рассмотрением только линейных двоичных каскадных кодов. При исследовании этих кодов удобно информационные  $\{\mu\}$ , вспомогательные  $\{\gamma\}$  и кодовые слова

$\{a\}$  длины  $n=n_a n_b$  представлять в виде двоичных (т. е. над полем  $GF(2)$ ) матриц размеров  $n_a \times n_b$ . При этом будем считать, что позиции в матрицах пронумерованы номерами из  $N=\{1, 2, \dots, n\}$  последовательно сверху вниз и столбец за столбцом. В этом случае множество номеров  $N^{(j)}=\{n_a(j-1)+1, n_a(j-1)+2, \dots, n_a j\}$  соответствует просто  $j$ -му столбцу, т. е.  $\gamma^{(j)}$  и  $\alpha^{(j)}$  являются  $j$ -ми столбцами слов  $\gamma$  и  $\alpha$  соответственно.

Посредством  $m$  горизонтальных линий разобьем матрицу размеров  $n_a \times n_b$  на  $m+1$  горизонтальных блоков (подматриц). Пусть при этом первая снизу подматрица содержит  $a_0$  строк, вторая —

$a_1$  строк и т. д. Очевидно, что при этом  $\sum_{i=0}^m a_i = n_a$ . Будем считать,

что все позиции первой, т. е. нижней, подматрицы образуют множество  $M_0$ , второй — множество  $M_1$  и т. д., а  $(m+1)$ -й — множество  $M_m$ .

Таким образом, задаются два разбиения множества  $N$  на непесекающиеся подмножества  $N^{(j)}$ ,  $j=\overline{1, n_b}$ , и  $M_i$ ,  $i=\overline{0, m}$ , т. е. расчленение матриц  $\mu$ ,  $\gamma$ ,  $\alpha$  на столбцы  $\mu^{(j)}$ ,  $\gamma^{(j)}$ ,  $\alpha^{(j)}$  и горизонтальные блоки  $\mu_i$ ,  $\gamma_i$ ,  $\alpha_i$ .

В последующем изложении всегда будем предполагать, что в каждом блоке  $\mu_i$  матрицы  $\mu$  информационные символы располагаются в левых  $b_i$  столбцах. Остальные  $n_b - b_i$  столбцов блока  $\mu_i$  заполняются нулями. Условие, сформулированное в конце разд. 1.3.2 о том, что массив  $\mu_0$  является нулевым, эквивалентно условию  $b_0=0$ . Следовательно, общее число подлежащих кодированию

информационных символов  $k = \sum_{i=1}^m a_i b_i$ . Кодирование информационного слова  $\mu$  осуществляется последовательно внешними, а затем внутренними кодами.

При кодировании внешними кодами каждая подматрица  $\mu_i$ ,  $i=\overline{1, m}$ , кодируется соответствующим внешним кодом  $B_i$  с основанием  $q_i=2^{a_i}$  длины  $n_b$  со скоростью передачи  $R_{bi}=b_i/n_b$ . В результате подматрица  $\mu_i$  переходит в подматрицу  $\gamma_i$  тех же размеров  $a_i \times n_b$ , представляющую собой кодовое слово  $i$ -го внешнего кода  $B_i$ . Кодирование внешними кодами превращает матрицу  $\mu$  в матрицу  $\gamma$ , представляющую собой вспомогательное слово.

При кодировании внутренними кодами каждый столбец  $\gamma^{(j)}$ ,  $j=\overline{1, n_b}$ , матрицы  $\gamma$  кодируется соответствующим двоичным внутренним кодом  $A^{(j)}$  длины  $n_a$ , в результате чего он превращается в столбец  $\alpha^{(j)}$ , являющийся кодовым словом кода  $A^{(j)}$ .

Столбцы  $\alpha^{(j)}$  образуют матрицу  $\alpha$ , которая и является кодовым словом каскадного кода порядка  $m$ . Столбцы горизонтальных блоков  $\mu_i$ ,  $\gamma_i$ ,  $\alpha_i$  будем обозначать соответственно через  $\mu_{ij}$ ,  $\gamma_{ij}$ ,  $\alpha_{ij}$  и часто трактовать их как элементы поля  $GF(2^{a_i})$ . Схематично слова  $\mu$ ,  $\gamma$ ,  $\alpha$  показаны на рис. 1.3.

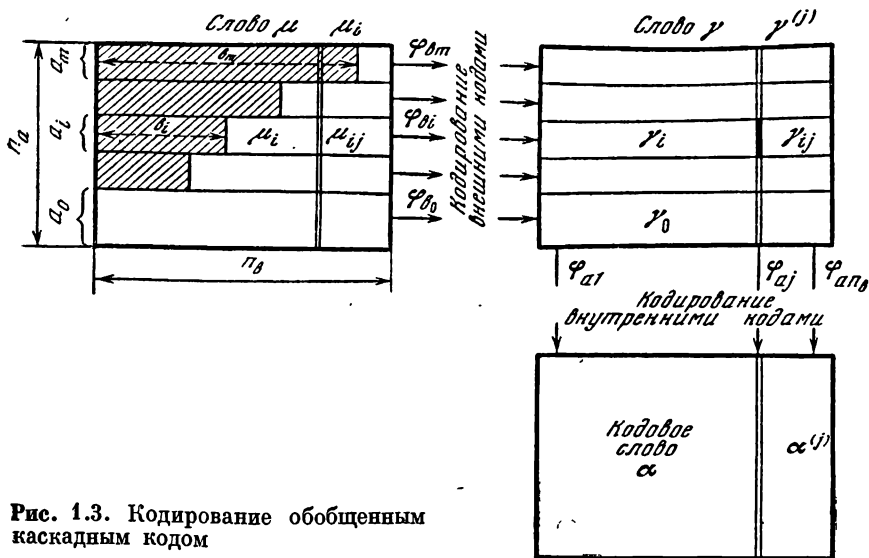


Рис. 1.3. Кодирование обобщенным каскадным кодом

Для того чтобы каскадный код был линейным двоичным кодом, необходимо и достаточно, чтобы все коды  $B_i$  и  $A^{(j)}$  были линейными кодами над  $GF(2)$ , что соответствует требованию линейности над  $GF(2)$  функций  $\varphi_{bi}$  и  $\varphi_a^{(j)}$ ,  $i = \overline{0, m}$ ,  $j = \overline{1, n_b}$ . Но каждому линейному коду  $A^{(j)}$  соответствует некоторая невырожденная матрица  $G_0^{(j)}$  порядка  $n_a$ , такая, что

$$\alpha^{(j)} = G_0^{(j)} \gamma^{(j)}. \quad (1.20)$$

Кодирование внутренними кодами, т. е. отображение  $\varphi_a$ , записывается особенно просто, если  $G_0^{(j)} = G_0$  для всех  $j$ ,  $j = \overline{1, n_b}$ . В этом случае

$$\alpha = G_0 \gamma, \quad (1.21)$$

где  $\alpha$  и  $\gamma$  — матрицы размеров  $n_a \times n_b$ .

Матрицы  $G_0^{(j)}$  (или  $G_0$ ) будем называть кодирующими матрицами. Отметим, что выбор одной и той же кодирующей матрицы  $G_0$  для всех  $j$ ,  $j = \overline{1, n_b}$ , упрощает не только запись, но и построение каскадного кода, так как нужно построить всего одну матрицу  $G_0$ , а не  $n_b$  таких матриц. Кроме того, упрощается реализация кодирования и декодирования в силу того, что для всех столбцов используется одна и та же матрица, а следовательно, могут использоваться одни и те же кодеры и декодеры. Поэтому в дальнейшем, за исключением случая, когда будут исследоваться потенциальные корректирующие свойства, ограничимся одной и той же кодирующей матрицей  $G_0$  для всех столбцов. Дальнейшие условия, налагаемые на выбор матрицы  $G_0$  и внешних кодов  $B_i$  (т. е. на функции  $\varphi_{bi}$ ), сформулируем, исходя из получения воз-

можно лучших оценок для кодового расстояния и других метрических характеристик каскадного кода и по возможности наиболее простых при этом методов построения  $G_0$  и  $B_i$ .

Отметим также, что без уменьшения общности получаемых результатов почти всегда можно считать, что, кроме  $a_0$ , все остальные величины  $a_i = a$ ,  $i = \overline{1, m}$ . Это весьма естественное условие существенно упрощает анализ ряда вопросов, рассматриваемых в настоящей работе.

## § 1.4. Заключение

### 1.4.1. Замечания о проблемах помехоустойчивого кодирования

Основополагающая работа Шеннона [143] уже в 1948 г. открыла неожиданные и заманчивые возможности неограниченного увеличения верности передачи сообщений по шумящим каналам.

Однако, как стало ясным из последующих работ Шеннона [143] и других исследователей [52, 140], для практического осуществления открывающихся перспектив необходимо использовать весьма длинные корректирующие коды. В то же время сложность поиска хороших кодов, их кодирования и декодирования, в общем случае растущая экспоненциально с длиной кода, не оставляла никаких надежд на практическое применение кодов, реализующих теоретические возможности.

Дальнейшие исследования выявили некоторые перспективные направления теории корректирующих кодов [115] и сняли благодаря введению линейных кодов проблему сложности для операции кодирования.

В то же время для кодов большой длины, удовлетворяющих границе Варшамова—Гилберта или обеспечивающих наилучшую из возможных экспоненту вероятности ошибочного декодирования в ДСК без памяти, до сегодняшнего дня остаются открытыми как проблема построения самого кода, так и проблема его декодирования с неэкспоненциальной сложностью реализации.

Использование мощных методов современной алгебры над конечными полями [13, 108] позволило решить ряд задач помехоустойчивого кодирования указанного выше типа, относящихся к кодам длиной в несколько десятков, иногда даже сотен символов, но эти методы быстро теряли свою эффективность с ростом длины кода и асимптотически (при  $n \rightarrow \infty$ ) приводили к плохим результатам.

Вопросы сложности реализации теоретически эффективных корректирующих кодов вначале неявно, а начиная с конца 60-х—начала 70-х годов все более отчетливо ставились в большинстве исследований по помехоустойчивому кодированию.

В последнее время сложность реализации становится одним из основных критериев при оценке перспективности или, наоборот, бесперспективности того или иного направления теории помехоустойчивого кодирования.

Чтобы открыть помехоустойчивому кодированию дорогу к практическому применению, с самого начала развития теории кодирования большое внимание уделялось поиску методов построения кода и его декодирования хотя и не оптимальных, но достаточно эффективных и, главное, обладающих приемлемой сложностью реализации при большой длине кода. Сюда безусловно относятся произведения кодов [144], коды с мажоритарным (пороговым) декодированием [82, 84], коды, построенные по схемам итерации Зива [174], каскадные коды [140] и, наконец, обобщенные каскадные коды (или каскадные коды произвольного порядка) [23, 26]. Характерным отличием большинства подобных систем кодирования (кроме кодов с мажоритарным декодированием) является то, что длинный код получается в результате некой композиции более коротких кодов, что позволяет упростить как построение самих кодов, так и их декодирование.

#### 1.4.2. Основные направления исследования каскадных методов кодирования

Остановимся подробнее на проблемах, рассматриваемых в монографии и тех, которые хотя и относятся к каскадному кодированию, но в силу ограниченности объема книги или отсутствия достаточно развитых методов исследования и принципиально новых результатов не рассматриваются в настоящей работе.

Прежде всего отметим, что в дальнейшем изучаются только блочные двоичные линейные каскадные и обобщенные каскадные коды <sup>1</sup>.

Диапазон исследований указанных кодов охватывает такие проблемы, как выбор внутренних и внешних кодов; анализ весовой структуры каскадных кодов произвольного порядка; комбинаторное исследование верхних и нижних оценок кодового расстояния; разработка алгоритмов каскадного декодирования; анализ реализуемых корректирующих свойств при каскадном декодировании; осуществление равной и неравной защиты информационных символов; эффективное исправление ошибок в каналах со сложным характером ошибок; потенциальные возможности каскадного кодирования и влияние структуры каскадного кода произвольного порядка на его потенциальные характеристики.

Хотя все эти проблемы рассматриваются лишь в рамках оговоренных выше ограничений, распространение полученных результатов на случай недвоичных каскадных кодов достаточно тривиально и не связано ни с какими дополнительными принципиальными трудностями. Недвоичные каскадные коды не рассматриваются лишь в силу необходимости сокращения объема книги и более лаконичного и простого изложения.

---

<sup>1</sup> Так как каскадные коды являются обобщенными каскадными кодами первого порядка, то мы не будем использовать термин «обобщенные каскадные коды», а называть и те и другие каскадными кодами с указанием порядка.

Авторы совсем не касаются теории сверточных каскадных кодов, так как к моменту написания монографии эта теория находилась еще в зачаточном состоянии.

Аналогичное замечание относится и к теории нелинейных каскадных кодов произвольного порядка. Построение этой теории требует дополнительных исследований, которые, как можно ожидать, откроют новые принципиальные возможности и теоретического, и прикладного плана. В качестве одной из таких возможностей отметим совместное рассмотрение модуляции и кодирования как каскадной схемы кодирования, в которой выбор внутренних кодов представляет собой выбор модуляции, а внешних — действительно кодов, наилучшим образом соответствующих модуляции и демодуляции.

Несмотря на очевидную перспективность применения каскадных методов кодирования в каналах с различным числом входов и выходов, например, таких, как широковещательные каналы или каналы Блекуэла, эти вопросы из-за отсутствия к моменту окончания книги сколько-нибудь существенных результатов в ней не рассматриваются.

Перечисленные выше вопросы каскадного кодирования, не затрагиваемые в настоящей монографии, являются объектом пристального изучения многими исследователями, о чем свидетельствуют появившиеся в последнее время многочисленные публикации, посвященные этим вопросам.



## КОДИРОВАНИЕ И ВЕСОВАЯ СТРУКТУРА КАСКАДНЫХ КОДОВ

---

В этой главе рассматривается класс двоичных линейных каскадных кодов произвольного порядка. Вводится система вложенных внутренних кодов и описываются методы несистематического и систематического кодирования. Изучается весовая структура каскадных кодов и исследуется связь основных параметров каскадного кода с соответствующими параметрами внешних и внутренних кодов. Обсуждаются требования, предъявляемые к внутренним и внешним кодам, и исследуются системы вложенных внутренних кодов, когда кодирование определяется умножением на произвольную невырожденную матрицу, нижнюю треугольную матрицу и, ненулевой элемент поля. Показано, что во втором случае всегда может быть выполнено систематическое кодирование.

Обсуждается и аргументируется целесообразность выбора кодов РС над полем  $GF(2^{a_i})$  и их модификаций в качестве внешних кодов.

### § 2.1. Кодирование каскадных кодов

#### 2.1.1. Линейные каскадные коды

Ограничиваясь в дальнейшем рассмотрением только двоичных линейных каскадных кодов с каскадным алгоритмом кодирования, будем в соответствии с результатами разд. 1.3.3 кодировать блоки  $\mu_i$  информационного слова групповыми над полем  $GF(2^{a_i})$  внешними кодами  $B_i$  длины  $n_i$  со скоростью передачи  $R_{b_i} = b_i/n_i$ , а кодирование столбцов  $\gamma^{(j)}$  вспомогательного слова  $\gamma$  осуществлять умножением его слева на невырожденную матрицу  $G_0$  порядка  $n_a$ .

Прежде всего покажем, что требование о невырожденности матрицы  $G_0$  не является слишком обременительным и во всяком случае не уменьшает возможностей выбора внутреннего двоичного

кода  $A_1$  со скоростью передачи  $R_{a1} = \frac{1}{n_a} \sum_{i=1}^m a_i$ , определяемого этой матрицей.

Действительно, так как последние  $a_0$  строк вспомогательного слова  $\gamma$  нулевые ( $\gamma_0 = 0$ ), то выражение

$$\alpha^{(j)} = G_0 \gamma^{(j)} \quad \text{или} \quad \alpha = G_0 \gamma, \quad (2.1)$$

определяющее результат кодирования внутреннего кода  $A_1$ , не зависит от последних  $a_0$  столбцов матрицы  $G_0$ , которые поэтому

могут выбираться совершенно произвольно. В то же время линейный код  $A_1$  полностью определяется своей кодирующей матрицей  $G_1$  размеров  $n_a \times (n_a - a_0)$ , которая, что совершенно очевидно, получается из матрицы  $G_0$  отбрасыванием ее последних  $a_0$  столб-

цов. Так как при скорости передачи  $R_{a1} = \frac{1}{n_a} \sum_{i=1}^m a_i$ , ранг матрицы  $G_1$

должен быть равен  $\sum_{i=1}^m a_i = n_a - a_0$ , то при выполнении этого условия всегда можно так выбрать последние  $a_0$  столбцов матрицы  $G_0$ , чтобы она оказалась невырожденной.

Учитывая, что в силу линейности внешних кодов  $B_i$  блоки  $\mu_i$  и  $\gamma_i$  одновременно являются либо нулевыми, либо ненулевыми, введем множество  $J_i$  таких двоичных столбцов  $\gamma^{(j)}$  длины  $n_a$ , у которых нижние  $r_{ai} = \sum_{s=0}^{i-1} a_s$  символов нулевые, а остальные  $k_{ai} = n_a - r_{ai}$  символов могут быть любыми. Тогда имеют место очевидные включения

$$J_1 \supset J_2 \supset \dots \supset J_m. \quad (2.2)$$

Пусть  $x \in J_i$ , тогда полученное посредством отображения  $y = G_0 x$  множество

$$A_i = \{y : y = G_0 x \text{ и } x \in J_i\} \quad (2.3)$$

назовем  $i$ -м внутренним кодом (или  $i$ -м кодом первой ступени). Обозначим через  $d_{ai}$  и  $R_{ai} = k_{ai}/n_a$  соответственно кодовое расстояние и скорость передачи этого кода. В силу (2.2) и (2.3) справедливы включения

$$A_0 \supset A_1 \supset \dots \supset A_m, \quad (2.4)$$

где  $A_0$  — код без избыточности, т. е. множество всех двоичных слов длины  $n_a$ .

Так как код  $A_{i+1}$  является подкодом кода  $A_i$ , то множество кодов (2.4) назовем системой вложенных (внутренних) кодов. Для системы вложенных кодов выполняются очевидные неравенства

$$\begin{aligned} 1 = d_{a0} &\leq d_{a1} \leq d_{a2} \leq \dots \leq d_{am}, \\ 1 = R_{a0} &> R_{a1} > R_{a2} > \dots > R_{am} > R_{a, m+1} = 0, \end{aligned} \quad (2.5)$$

а их производящие матрицы  $G_i$ ,  $i = \overline{0, m}$ , получаются из матрицы  $G_0$  отбрасыванием ее последних  $\sum_{s=0}^{i-1} a_s$  столбцов.

Матрицу  $G_0$  запишем в клеточной форме

$$G_0 = \left\| \begin{array}{cccc} Q_{mm} & Q_{m, m-1} & \dots & Q_{m0} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ Q_{0m} & Q_{0, m-1} & \dots & Q_{00} \end{array} \right\|, \quad (2.6)$$

где клетки  $Q_{is}$  представляют собой матрицы размеров  $a_i \times a_s$ , так что диагональные клетки  $Q_{ii}$  являются квадратными матрицами порядка  $a_i$ . Тогда матрица

$$G_i = \| G_m^* G_{m-1}^* \dots G_i^* \|, \quad (2.7)$$

где

$$G_i^* = \left\| \begin{array}{c} Q_{ms} \\ \cdot \\ \cdot \\ \cdot \\ Q_{0s} \end{array} \right\|$$

является кодирующей матрицей внутреннего кода  $A_i$ . Таким образом, кодирующая матрица  $G_i$  кода  $A_i$  получается из кодирующей матрицы  $G_{i-1}$  кода  $A_{i-1}$  отбрасыванием ее последних  $a_{i-1}$  столбцов.

Как следует из определения системы вложенных кодов, внутренние коды не являются независимыми друг от друга (как это имеет место для внешних кодов). Все внутренние коды  $A_i$ ,  $i=1, m$ , полностью определяются одним (основным) кодом  $A_1$  (т. е. набором составляющих его кодовых слов) и выбранным для него правилом кодирования. Поэтому способ построения этого кода определяет не только его характеристики, но и характеристики каждого из кодов  $A_i$ ,  $i > 1$ , образующих вложенную систему. Поэтому выбор матрицы  $G_0$ , однозначно определяющий не только набор кодовых слов кода  $A_1$ , но и правило кодирования, играет определяющую роль для всех характеристик (в том числе кодового расстояния и спектра весов кодовых слов) внутренних кодов  $A_i$ ,  $i=1, m$ .

Покажем на примере, что при различном выборе матриц  $G_0$ , определяющих один и тот же основной код  $A_1$  с кодовым расстоянием  $d_{a1}$ , можно получить разные системы вложенных кодов с различными кодовыми расстояниями  $d_{ai}$  каждого из внутренних кодов. В качестве примера рассмотрим две системы вложенных кодов, порождаемых одним и тем же основным кодом (7, 6), максимально возможное кодовое расстояние которого равно  $d_{a1}=2$  и достигается тогда, когда  $A_1$  представляет собой множество всех двоичных векторов длины 7, содержащих четное число единиц. Однако кодирование может осуществляться различным способом, один из которых состоит в том, что подлежащее кодирова-

нию слово  $\gamma^{(j)}$  (последний символ которого нулевой) умножается слева на кодирующую матрицу

$$G'_0 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Легко проверить, что при таком способе кодирования кодовое слово  $\alpha^{(j)}$  отличается от  $\gamma^{(j)}$  лишь в последнем символе, который выбирается равным 0 или 1 так, чтобы число единиц в слове  $\alpha^{(j)}$  было четным, следовательно,  $d'_{a1}=2$ .

В качестве другого способа рассмотрим кодирование, при котором слово  $\gamma^{(j)}$  умножается слева на матрицу

$$G''_0 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

Так как первые шесть столбцов матрицы  $G''_0$  (так же, как и матрицы  $G'_0$ ) имеют четный вес, а подлежащие кодированию слова  $\gamma^{(j)}$  в последней позиции содержат 0, то вес слов  $\alpha^{(j)} = G''_0 \gamma^{(j)}$  также является четным, откуда следует, что  $d''_{a1}$  по-прежнему равно 2. В то же время, если в качестве второго кода  $A_2$  выберем код (7, 3), то множество кодовых слов этого кода при первом и втором способах кодирования приведем в табл. 2.1, из которой видно,

Таблица 2.1

Слова кода $A'_2$	Слова кода $A''_2$	Слова кода $A'_2$	Слова кода $A''_2$
0 0 0 0 0 0 0	0 0 0 0 0 0 0	1 1 0 0 0 0 0	1 1 0 0 0 1 1
1 0 0 0 0 0 1	1 0 0 1 1 1 0	1 0 1 0 0 0 0	1 0 1 1 1 0 0
0 1 0 0 0 0 1	0 1 0 1 1 0 1	0 1 1 0 0 0 0	0 1 1 1 0 1 0
0 0 1 0 0 0 1	0 0 1 0 1 1 1	1 1 1 0 0 0 1	1 1 1 0 1 0 0

что при первом способе кодирования кодовое расстояние кода  $A_2 - d'_{a2} = 2$ , в то время как при втором способе кодирования кодовое расстояние этого кода  $d''_{a2} = 4$ .

Так как максимально возможное кодовое расстояние  $d_{a2}$  кода (7, 3) равно 4, то никаким другим способом кодирования кодовое расстояние кода  $A_2$  не может быть сделано большим, чем при втором способе кодирования.

Приведенный пример указывает на необходимость изучения оценок достижимых характеристик систем вложенных кодов и методов построения матриц  $G_0$ , обеспечивающих получение системы вложенных кодов с достаточно хорошими характеристиками.

Для исследования этих вопросов необходимо располагать связью между кодирующей матрицей  $G_0$  и проверочными матрицами каждого из кодов  $A_i$ , образующих вложенную систему.

Так как подлежащие кодированию внутренним кодом слова

$$\gamma^{(j)} = \begin{pmatrix} \gamma_{mj} \\ \gamma_{m-1,j} \\ \vdots \\ \gamma_{1j} \\ \gamma_{0j} \end{pmatrix}, \quad j = \overline{1, n_b}, \text{ где } \gamma_{0j} = 0,$$

связаны с получаемыми в результате кодирования словами, которые являются кодовыми словами одного из внутренних кодов  $A_i$ ,  $i = \overline{1, m}$ ,

$$\alpha^{(j)} = \begin{pmatrix} \alpha_{mj} \\ \alpha_{m-1,j} \\ \vdots \\ \alpha_{1j} \\ \alpha_{0j} \end{pmatrix}, \quad j = \overline{1, n_b},$$

соотношением

$$\alpha^{(j)} = G_0 \gamma^{(j)}, \quad (2.8)$$

умножая (слева) это равенство на матрицу  $H_0$ , обратную матрице  $G_0$  ( $H_0 = G_0^{-1}$ ), получаем

$$H_0 \alpha^{(j)} = \gamma^{(j)}. \quad (2.9)$$

Запишем матрицу  $H_0$  в клеточной форме:

$$H_0 = \left\| \begin{array}{cccc} P_{mm} & P_{m,m-1} & \dots & P_{m0} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ P_{0m} & P_{0m-1} & \dots & P_{00} \end{array} \right\| = \left\| \begin{array}{c} H_m^* \\ \cdot \\ \cdot \\ \cdot \\ H_0^* \end{array} \right\|, \quad (2.10)$$

где клетки  $P_{is}$  представляют собой матрицы размеров  $a_i \cdot a_s$ , так что диагональные клетки  $P_{ii}$  являются квадратными матрицами порядка  $a_i$ . Если для слов  $\gamma^{(j)}$ , подлежащих кодированию кодом  $A_i$ , элементы  $\gamma_{0j} = \gamma_{1j} = \dots = \gamma_{i-1j} = 0$ , то

$$H_i \alpha^{(j)} = 0, \quad (2.11)$$

где

$$H_i = \left\| \begin{array}{c} H_{i-1}^* \\ \cdot \\ \cdot \\ \cdot \\ H_0^* \end{array} \right\|,$$

а  $H_s^* = \|P_{sm} P_{s,m-1} \dots P_{s0}\|$ ,  $s = \overline{0, i-1}$ . Соотношение (2.11) означает, что матрица  $H_i$  размеров  $(a_0 + a_1 + \dots + a_{i-1}) \times n_a$  представляет собой проверочную матрицу кода  $A_i$ . Таким образом, проверочная матрица кода  $A_i$  получается из проверочной матрицы кода  $A_{i+1}$  отбрасыванием ее верхних  $a_i$  строк.

Матрицу  $H_0$ , определяющую все проверочные матрицы  $H_i$ ,  $i = \overline{1, m}$ , будем называть проверочной матрицей системы вложенных кодов. Если известна проверочная матрица  $H_0$ , то, как следует из ее определения, кодирующая матрица  $G_0$  в свою очередь определяется равенством  $G_0 = H_0^{-1}$ , так что кодирование внутренними кодами можно с одинаковым успехом задавать как матрицей  $G_0$ , так и матрицей  $H_0$ , выбирая ту из них, построение которой (с учетом возможных дополнительных условий) осуществляется проще.

Отметим также используемые в дальнейшем соотношения, вытекающие из определения матриц  $G_0$  и  $H_0$ . Так как

$$H_0 G_0 = \left\| \begin{array}{c} H_m^* \\ H_{m-1}^* \\ \cdot \\ \cdot \\ \cdot \\ H_0^* \end{array} \right\| \cdot \|G_m^* G_{m-1}^* \dots G_0^*\| = E_{n_a}^x,$$

то

$$H_i^* G_j^* = \begin{cases} E_{a_i} & \text{при } i = j; \\ 0 & \text{при } i \neq j, \end{cases} \quad (2.12)$$

где  $E_{\sigma_i}$  — единичная матрица порядка  $a_i$ . Кроме того,

$$H_0 G_i^* \gamma_{ij} = \begin{pmatrix} 0 \\ \vdots \\ \gamma_{ij} \\ \vdots \\ 0 \end{pmatrix}. \quad (2.13)$$

## 2.1.2. Несистематическое кодирование

Предполагая, что в качестве внешних кодов  $B_i$  всегда используются систематические коды, рассмотрим два способа преобразования информационного слова  $\mu$  во вспомогательное слово  $\gamma$ .

Первый способ состоит в непосредственном кодировании каждого слова  $\mu_i$  кодом  $B_i$ ,  $i = \overline{1, m}$ , в результате чего слова  $\mu$  преобразуются в слово  $\gamma$ , такое, что  $\gamma_{ij} = \mu_{ij}$  для  $j = \overline{1, b_i}$ ,  $i = \overline{1, m}$ . Тогда после умножения каждого столбца  $\gamma^{(j)}$  слова  $\gamma$  слева на матрицу  $G_0^{(j)}$  (или всего слова  $\gamma$  на матрицу  $G_0$ , если  $G_0^{(j)} = G_0$  для всех  $j$ ) получаем кодовое слово  $\alpha$  каскадного кода, такое, что в нем,

вообще говоря,  $\alpha_{ij} \neq \mu_{ij}$  для  $j = \overline{b_i + 1, n_b}$ ,  $i = \overline{1, m}$ . Это значит, что полученный при этом (в результате кодирования внешними и внутренними кодами) каскадный код будет несистематическим.

Второй способ, приводящий к систематическому коду, состоит в том, что перед кодированием слова  $\mu$  к нему предварительно добавляется специально выбираемое слово  $\beta$ , в котором так же, как и в слове  $\mu$ , элементы  $\beta_{ij} = 0$  при  $j = \overline{b_i + 1, n_b}$ ,  $i = \overline{1, m}$ . Что касается элементов  $\beta_{ij}$  при  $j = \overline{1, b_i}$ ,  $i = \overline{1, m}$ , то они подчиняются дополнительным условиям, которые будут сформулированы ниже.

Таким образом, слово  $\beta$  можно трактовать как некоторое специально выбираемое информационное слово, соответствующее подлежащему передаче информационному слову  $\mu$ .

Полученное таким образом слово  $v = \mu + \beta$ , которое назовем вспомогательным информационным словом, кодируется кодами  $B_i$ ,  $i = \overline{1, m}$ , в результате чего оно преобразуется во вспомогательное слово  $\gamma$ , такое, что  $\gamma_{ij} = v_{ij}$  при  $j = \overline{1, b_i}$ ,  $i = \overline{1, m}$ , причем  $v_{ij}$ , вообще говоря, отличается от  $\mu_{ij}$ . Слово  $\beta$ , если это возможно, выберем так, чтобы после умножения каждого столбца  $\gamma^{(j)}$  вспомогательного слова  $\gamma$  слева на матрицу  $G_0^{(j)}$  получаемое кодовое слово каскадного кода  $\alpha$  удовлетворяло условию

$$\alpha_{ij} = \mu_{ij} \text{ при } j = \overline{1, b_i}, i = \overline{1, m}. \quad (2.14)$$

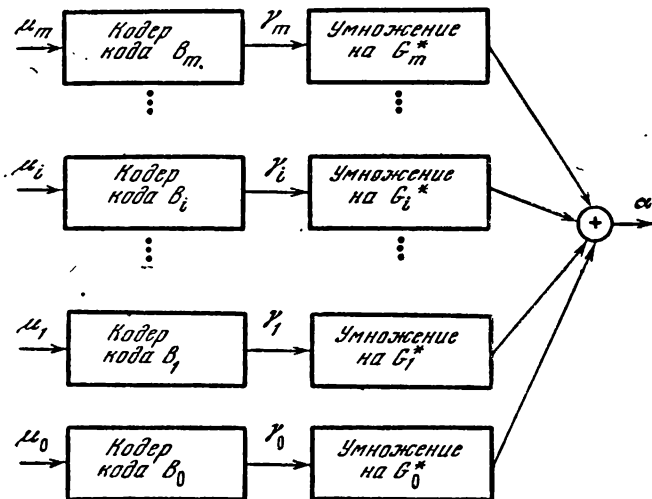


Рис. 2.1. Блок-схема несистематического кодирования обобщенным каскадным кодом

Таким образом, мы выделяем два способа кодирования, при которых приходим к несистематическим и систематическим каскадным кодам.

Для несистематических каскадных кодов кодирование кодового слова схематично можно представить в виде  $\mu \rightarrow \gamma \rightarrow \alpha$ , причем  $\mu_{i,j} = \gamma_{i,j} \neq \alpha_{i,j}$  при  $j = \overline{1, b_i}$ ,  $i = \overline{1, m}$ . Для систематических каскадных кодов аналогичная схема имеет вид  $\mu \rightarrow \nu \rightarrow \gamma \rightarrow \alpha$ , причем  $\mu_{i,j} = \alpha_{i,j} \neq \nu_{i,j} = \gamma_{i,j}$  при  $j = \overline{1, b_i}$ ,  $i = \overline{1, m}$ .

Однако для систематических кодов остаются открытыми вопросы о существовании и способах построения слов  $\beta$ , удовлетворяющих указанным выше условиям. Эти вопросы будут рассмотрены в разд. 2.1.3.

В соответствии с определением несистематического кодирования каскадного кода реализация такого кодирования может быть осуществлена следующим образом.

Сначала по слову  $\mu$  находим слово  $\gamma$ , т. е. определяем  $\gamma_i$ , которые являются кодовыми словами, полученными в результате кодирования информационных слов  $\mu_i$  кодами  $B_i$ . Затем слово  $\gamma$  кодируем внутренними кодами, т. е. находим кодовое слово  $\alpha$  каскадного кода как матричное произведение

$$\alpha = G_0 \gamma, \quad (2.15)$$

что и завершает кодирование.

Реализация (2.15) может быть выполнена поэтапно последовательным вычислением каждого столбца  $\alpha^{(j)} = G_0 \gamma^{(j)}$ . Схематически кодирование представлено на рис. 2.1.



Иногда на практике в целях увеличения быстродействия проводится распараллеливание вычислений. Убедимся, что кодирование каскадного кода порядка  $m$  естественным образом распараллеливается. Для этого матрицу  $G_0$  представим в виде  $G_0 = \|G_m^* G_{m-1}^* \dots G_1^*\|$ , где  $G_i^*$  — матрица размера  $n_a \times a_i$ . Нетрудно убедиться, учитывая представление вспомогательного слова  $\gamma$  через подматрицы  $\gamma_i$ , что

$$\alpha = \sum_{i=0}^m G_i^* \gamma_i. \quad (2.16)$$

Кодирование посредством (2.15) или (2.16) при использовании систематических кодов  $B_i$  приводит к несистематическому каскадному коду.

### 2.1.3. Систематическое кодирование

Переходя к вопросу о существовании и определении слов  $\beta$ , необходимых для построения систематического каскадного кода, начнем с рассмотрения наиболее общего случая, когда кодирующая матрица  $G_0$  (или матрицы  $G_0^{(j)}$ ,  $j = \overline{1, n_b}$ ) является произвольной невырожденной матрицей порядка  $n_a$ .

Для формулировки условий, обеспечивающих возможность систематического кодирования, введем для каждой матрицы  $G_0$  (см. (2.6)) квадратные подматрицы

$$\begin{aligned} G_{11} &= \left\| \begin{array}{ccc} Q_{m1} & \dots & Q_{m1} \\ \vdots & & \vdots \\ Q_{1m} & \dots & Q_{11} \end{array} \right\| \\ \dots & \dots \\ G_{ii} &= \left\| \begin{array}{ccc} Q_{mi} & \dots & Q_{mi} \\ \vdots & & \vdots \\ Q_{im} & \dots & Q_{ii} \end{array} \right\| \\ \dots & \dots \\ G_{mm} &= Q_{mm} \end{aligned}$$

Тогда имеет место следующее утверждение, справедливость которого доказывается в приложении 2.1.

**Утверждение 2.1.** Для реализации систематического кодирования необходимо и достаточно, чтобы все квадратные подматрицы  $G_{ii}$ ,  $i = \overline{1, m}$ , кодирующей матрицы  $G_0$  были невырожденными.

Легко видеть, что условия утверждения 2.1 выполняются автоматически, если в качестве кодирующей матрицы  $G_0$  выбирается

невыврожденная нижняя треугольная матрица, которая в клеточной форме имеет вид

$$G_0 = \begin{vmatrix} T_{mm} & & & \\ Q_{m-1, m} & T_{m-1, m-1} & & 0 \\ \cdot & \cdot & \cdot & \\ \cdot & \cdot & \cdot & \\ Q_{0m} & Q_{0m-1} & \dots & T_{00} \end{vmatrix}, \quad (2.17)$$

где  $T_{ii}$  — невырожденные нижние треугольные матрицы порядка  $a_i$ . Тогда все матрицы  $G_{ii}$  являются невырожденными нижними треугольными матрицами.

Соотношения, определяющие в этом случае элементы  $\beta_{ij}$  слова  $\beta$ , приведены в приложении 2.2. Из этих соотношений непосредственно следует, что систематическое кодирование каскадного кода с треугольной кодирующей матрицей  $G_0$  может быть осуществлено при помощи следующего алгоритма.

1. Полагаем  $i=m$ .
2. Формируем информационные элементы  $\mu_{ij} = \alpha_{ij}$ ,  $j = \overline{1, b_i}$ .
3. Для каждого  $j = \overline{1, b_i}$  определяем элементы  $\mu_{ij} + \beta_{ij}$  по формуле

$$\begin{aligned} \mu_{ij} + \beta_{ij} = & T_{ii}^{-1} \mu_{ij} + T_{ii}^{-1} Q_{i+1, i} (\mu_{i+1, j} + \beta_{i+1, j}) + \dots \\ & \dots + T_{ii}^{-1} Q_{im} (\mu_{mj} + \beta_{mj}). \end{aligned} \quad (2.18)$$

4. Элементы  $\mu_{ij} + \beta_{ij}$ ,  $j = \overline{1, b_i}$ , принимаем в качестве информационных символов внешнего кода  $B_i$  и в результате соответствующего кодирования формируем кодовое слово  $\gamma_i$  этого кода.

5. Для каждого  $j = \overline{b_i + 1, n_b}$  находим элемент  $\alpha_{ij}$  каскадного кода по формуле

$$\alpha_{ij} = \sum_{v=i}^m Q_{iv} \gamma_{vj}.$$

6. Если  $i > 0$ , то  $i: i-1$  и переходим к п. 2. Если  $i=0$ , то кодирование завершено, так как найдены все элементы  $\alpha_{ij}$ , определяющие кодовое слово каскадного кода. Последовательность вычислений для каждого  $i$ ,  $i = \overline{0, m}$ , назовем шагом алгоритма кодирования. Таким образом, систематическое кодирование каскадного кода осуществляется за  $m+1$  шагов. При выполнении последнего шага, соответствующего  $i=0$ , следует иметь в виду, что  $b_0=0$ , так что  $\gamma_{0j}=0$  для всех  $j = \overline{1, n_b}$ .

Заметим, что в том случае, когда  $G_0$  является нижней треугольной матрицей, обратная ей матрица  $G_0^{-1} = H_0$ , т. е. проверочная

матрица также будет нижней треугольной с обратными по отношению  $T_{ii}$  диагональными клетками

$$H_0 = \begin{vmatrix} T_{mm}^{-1} & & & \\ P_{m-1, m} & T_{m-1, m-1}^{-1} & & \\ \cdot & \cdot & \cdot & \\ \cdot & \cdot & \cdot & \\ P_{0m} & P_{0m-1} & \dots & T_{00}^{-1} \end{vmatrix}. \quad (2.19)$$

Тогда систематическое кодирование может быть легко осуществлено не только с помощью кодирующей матрицы  $G_0$ , но и с помощью проверочной матрицы  $H_0$ . Соответствующий алгоритм кодирования имеет следующий вид.

1. Полагаем  $i = m$ .

2. Формируем информационные элементы

$$\mu_{ij} = \alpha_{ij}, \quad j = \overline{1, b_i}.$$

3. Для каждого  $j = \overline{1, n_b}$  определяем элемент  $\beta_{ij}$  по формуле

$$\beta_{ij} = \| P_{im} P_{im-1} \dots P_{i, i+1} \| \cdot \begin{vmatrix} \alpha_{mj} \\ \alpha_{m-1, j} \\ \cdot \\ \cdot \\ \alpha_{i+1, j} \end{vmatrix},$$

причем  $\beta_{mj} = 0$ .

4. Для каждого  $j = \overline{1, b_i}$  находим элементы  $\gamma_{ij}$  по формуле  $\gamma_{ij} = \beta_{ij} + T_{ii} \alpha_{ij}$ . При этом из  $\beta_{mj} = 0$  следует, что  $\gamma_{mj} = T_{mm} \alpha_{mj}$ .

5. Элементы  $\gamma_{ij}$ ,  $j = \overline{1, b_i}$ , принимаем в качестве информационных символов внешнего кода  $B_i$ , в результате кодирования которым находим проверочные символы  $\gamma_{ij}$ ,  $j = \overline{b_i + 1, n_b}$ , т. е. формируем кодовое слово  $\gamma_i$  этого кода.

6. Для каждого  $j = \overline{b_i + 1, n_b}$  находим элемент  $\alpha_{ij}$  по формуле  $\alpha_{ij} = T_{ii}^{-1} (\beta_{ij} + \gamma_{ij})$ .

7. Если  $i > 0$ , то заменяем  $i$  на  $i-1$  и переходим к п. 2. В противном случае ( $i=0$ ) кодирование завершено, так как найдены все элементы  $\alpha_{ij}$ , т. е. все кодовое слово  $\alpha$ .

Убедимся теперь в том, что полученное в результате таких вычислений слово  $\alpha$  является кодовым словом каскадного кода  $m$ -го порядка. Прежде всего заметим, что из структуры матрицы  $H_0$  (см. (2.19)) и алгоритма кодирования следует, что

$$\gamma_{ij} = H_i^* \alpha^{(j)}, \quad j = \overline{1, n_b}, \quad (2.20)$$

где  $\alpha^{(j)}$  — столбец слова  $\alpha$ , а  $H_i^* = \|P_{im}P_{i,m-1} \dots P_{i,i+1}T_{ii}^{-1}0_i\|$ , причем  $0_i$  — матрица из нулей размеров

$$a_i \times \sum_{s=0}^{i-1} a_s.$$

Из (2. 20) вытекает, что  $\gamma_i = H_i^* \alpha$ , где  $\gamma_i$  — слово кода  $B_i$ . Отсюда с учетом (2. 19) имеем  $\gamma = H_0 \alpha$  или  $\alpha = G_0 \gamma$ , это и завершает доказательство того факта, что в результате вычислений по приведенному алгоритму получается слово каскадного кода.

Отметим, что мы получим тот же самый каскадный код в не-систематическом виде, если применим алгоритм кодирования, описанный в разд. 2.1.2. При этом тому же набору информационных символов будет соответствовать другое кодовое слово. Подчеркнем еще одно различие этих методов кодирования. При не-систематическом кодировании выбор слова  $\gamma_i$  из кода  $B_i$  определяется только значениями информационных символов подматрицы  $\mu_i$ . При систематическом кодировании выбор слова  $\gamma_i$  из кода  $B_i$  определяется не только значениями информационных символов в подматрице  $\mu_i$ , но и значениями информационных символов в подматрицах  $\mu_s$ ,  $s = i + 1, m$ .

В дальнейшем условимся, что если кодирующая матрица  $G_0$  (или проверочная  $H_0$ ) задана в виде нижней треугольной матрицы, то будем говорить о каскадном коде как о систематическом независимо от того, каким кодированием для него пользуемся.

## § 2.2. Весовая структура каскадных кодов

### 2.2.1. Анализ весовой структуры каскадных кодов

Перейдем теперь к анализу весовой структуры каскадного кода, одна из основных характеристик которой определяется следующей теоремой.

**Теорема 2. 1.** Если два кодовых слова  $\alpha^*$  и  $\alpha^{**}$  линейного каскадного кода таковы, что соответствующие им вспомогательные слова  $\gamma^*$  и  $\gamma^{**}$  удовлетворяют условиям  $\gamma_s^* = \gamma_s^{**}$ ,  $s = 1, i - 1$ ;  $\gamma_i^* \neq \gamma_i^{**}$ ;  $\gamma_s^*$  и  $\gamma_s^{**}$  произвольны при  $s > i$ , то расстояние  $d(\alpha^*, \alpha^{**})$  между этими словами удовлетворяет соотношению

$$d(\alpha^*, \alpha^{**}) \geq d_i^{(n)} = d_{a_i} d_{b_i}. \quad (2. 21)$$

**Доказательство.** Так как каскадный код линейен над полем характеристики два, то  $d(\alpha^*, \alpha^{**})$  равно весу слова  $\alpha = \alpha^* + \alpha^{**}$ , которое также является словом этого кода. Но в слове  $\gamma$ , соответствующем слову  $\alpha$ , согласно условиям теоремы  $\gamma_s = 0$ ,  $s = 1, i - 1$ ;  $\gamma_i \neq 0$ , так что  $\gamma_i$  содержит не менее чем  $d_{b_i}$  ненулевых элементов  $\gamma_{ij}$ . Каждому из этих элементов соответствует ненулевой столбец  $\gamma^{(j)}$ , который порождает ненулевое слово кода  $A_i$ ,

весом не менее чем  $d_{a_i}$ . Таким образом, вес  $|\alpha|$  слова  $\alpha$  удовлетворяет неравенству  $|\alpha| = d(\alpha^*, \alpha^{**}) \geq d_{a_i} d_{b_i}$ .

**С л е д с т в и е 2.1.** Кодовое расстояние  $d$  линейного каскадного кода порядка  $m$  удовлетворяет неравенству

$$d \geq d^{(n)} = \min_{1 \leq i \leq m} \{d_i^n\}. \quad (2.22)$$

Величину  $d^{(n)}$  будем называть нижней оценкой кодового расстояния каскадного кода.

Учитывая, что в подматрице  $\mu_i$  информационные символы располагаются в левых  $b_i$  столбцах, получаем для скорости передачи  $i$ -го внешнего кода  $B_i$ ,  $i = \overline{1, m}$ , выражение  $R_{b_i} = b_i/n_{b_i}$ .

Так как в каждой из подматриц  $\mu_i$  информационные символы выбираются независимо друг от друга и  $b_0 = 0$ , то общее число информационных символов каскадного кода равно

$$k = \sum_{i=1}^m k_i = \sum_{i=1}^m a_i b_i, \quad (2.23)$$

где  $k_i = a_i b_i$  — число двоичных информационных символов  $i$ -го внешнего кода.

В соответствии с теоремой 2.1 весовой структуре каскадного кода можно дать следующую интерпретацию: каскадный код представляет собой множество из  $M = 2^k$  различных слов. Это множество слов естественным образом разбивается на  $2^{k_1}$  подмножеств  $M(l_1)$ ,  $l_1 = \overline{1, 2^{k_1}}$ , содержащих каждое по  $2^{k-k_1}$  слов. (В каждое из множеств  $M(l_1)$  входят все слова каскадного кода с одними и теми же информационными символами в подматрице  $\mu_1$ .)

Из теоремы 2.1 следует, что расстояние между любыми двумя множествами  $^1 M(l'_1)$  и  $M(l''_1)$  не менее чем  $d_1^{(n)} = d_{a_1} d_{b_1}$ . Выберем теперь одно из множеств  $M(l_1)$  и разобьем его на  $2^{k_2}$  подмножеств  $M(l_1, l_2)$  по  $2^{k-k_1-k_2}$  слов в каждом так, чтобы в  $M(l_1, l_2)$ ,  $l_2 = \overline{1, 2^{k_2}}$ , входили все слова множества  $M(l_1)$  с одними и теми же информационными символами в подматрице  $\mu_2$ . Таким образом, каждое из множеств  $M(l_1, l_2)$  содержит кодовые слова с совпадающими информационными символами в подматрицах  $\mu_1$  и  $\mu_2$ .

Из теоремы 2.1 следует, что расстояние между двумя множествами  $M(l'_1, l'_2)$  и  $M(l''_1, l''_2)$  удовлетворяет неравенству

$$d(M(l'_1, l'_2), M(l''_1, l''_2)) \geq \begin{cases} d_2^{(n)} = d_{a_2} d_{b_2}, & \text{если } l'_1 = l''_1 \text{ и } l'_2 \neq l''_2; \\ \min \{d_1^{(n)}, d_2^{(n)}\}, & \text{если } l'_1 \neq l''_1. \end{cases}$$

Соответственно множество  $M(l_1, l_2, \dots, l_{i-1})$  разбивается на  $l_i = \overline{1, 2^{k_i}}$  подмножеств  $M(l_1, l_2, \dots, l_{i-1}, l_i)$  по  $2^{k-k_1-\dots-k_i}$  слов каскадного кода в каждом, где в  $M(l_1, l_2, \dots, l_{i-1}, l_i)$  входят

<sup>1</sup> Под расстоянием  $d(A, B)$  между двумя множествами  $A$  и  $B$  понимается  $\min_{(a, b)} \{d(a, b)\}$ , где  $a \in A$ ,  $b \in B$ .

все слова множества  $M(l_1, l_2, \dots, l_{i-1})$  с одними и теми же информационными символами в подматрице  $\mu_i$ . Таким образом, каждое из множеств  $M(l_1, l_2, \dots, l_{i-1}, l_i)$  содержит кодовые слова с совпадающими информационными символами в подматрицах  $\mu_1, \mu_2, \dots, \mu_i$ .

Из теоремы 2.1 следует, что расстояние между двумя множествами  $M(l'_1, l'_2, \dots, l'_i)$  и  $M(l''_1, l''_2, \dots, l''_i)$  удовлетворяет неравенству

$$\begin{aligned} d(M(l'_1, \dots, l'_i), M(l''_1, \dots, l''_i)) &\geq \\ &\geq \begin{cases} d_i^{(n)} = d_{a_i} d_{b_i}, & \text{если } l'_s = l''_s, s = \overline{1, i-1} \text{ и } l'_i = l''_i; \\ \min_{s_0 \leq s \leq i} \{d_s^{(n)}\}, & \text{если } l'_s = l''_s, s = \overline{1, s_0-1} \text{ и } l'_{s_0} \neq l''_{s_0}. \end{cases} \quad (2.24) \end{aligned}$$

Из проведенного анализа весовой структуры каскадного кода непосредственно следует, что выбором величин  $d_i^{(n)} = d_{a_i} d_{b_i}$  можно обеспечить неравную защиту информационных символов. Возможность неравной защиты информационных символов определяется следующей теоремой.

**Теорема 2.2.** Пусть при передаче слова каскадного кода возникли ошибки, число которых  $t$ , такое, что  $2t \geq d_{i+1}^{(n)}$  и  $2t < d_i^{(n)}$ ,  $s = \overline{1, i}$ , тогда при декодировании каскадного кода по минимуму расстояния информационные символы первых  $i$  подматриц  $\mu_s$ ,  $s = \overline{1, i}$ , будут декодированы правильно, хотя информационные символы других подматриц  $\mu_s$ ,  $s > i$ , могут быть декодированы неверно.

**Доказательство.** Рассмотрим множество  $M' = M(l'_1, \dots, l'_i)$ , к которому принадлежит переданное кодовое слово  $\alpha$ . Так как любое другое множество  $M'' = M(l''_1, \dots, l''_i)$  отстоит от множества  $M'$  на расстояние, не меньшее, чем  $\min_{1 \leq s \leq i} \{d_s^{(n)}\} > 2t$ , то никакие  $t$  ошибок не могут превратить слово  $\alpha$

в слово  $\hat{\alpha}$ , расположенное к  $M''$  ближе, чем к  $M'$ , и, следовательно, при декодировании по минимуму расстояния слово  $\hat{\alpha}$  будет отождествлено с некоторым кодовым словом  $\tilde{\alpha} \in M'$ , не обязательно совпадающим со словом  $\alpha$ . Но в силу условия  $\tilde{\alpha} \in M'$  слова  $\tilde{\alpha}$  и  $\alpha$  имеют одинаковые информационные символы в подматрицах  $\mu_1, \mu_2, \dots, \mu_i$ , что и доказывает теорему 2.2.

### 2.2.2. Требования к внешним и внутренним кодам

Как следует из результатов предыдущего раздела, скорость передачи каскадного кода  $R$  и основные характеристики его весовой структуры, включая кодовое расстояние  $d$ , определяются параметрами внешних и внутренних кодов. В связи с этим остановимся на основных требованиях к выбору этих кодов.

Так как длина каскадного кода (в двоичных символах)  $n = n_a n_b$ , то на основании (2.23) для скорости передачи каскадного кода имеем

$$R = \frac{k}{n} = \sum_{i=1}^m \frac{a_i b_i}{n_a n_b} = \sum_{i=1}^m (R_{a_i} - R_{a_{i+1}}) R_{b_i}, \quad (2.25)$$

где  $R_{a_{m+1}} = 0$ , а  $R_{a_i}$  и  $R_{b_i}$  — скорости передачи соответственно  $i$ -х внутренних и внешних кодов.

Как следует из (2.24), расстояние между двумя подмножествами  $M(l'_1, l'_2, \dots, l'_{i-1}, l'_i)$  и  $M(l''_1, l''_2, \dots, l''_{i-1}, l''_i)$  множества  $M(l_1, l_2, \dots, l_{i-1})$  оценивается снизу величиной  $d_i^{(a)} = d_{a_i} d_{b_i}$ , а кодовое расстояние  $d$  в соответствии с выражением (2.22) удовлетворяет неравенству

$$d \geq d^{(a)} = \min_{1 \leq i \leq m} \{d_{a_i} d_{b_i}\}. \quad (2.26)$$

Выбор каскадного кода, как правило, сводится к решению одной из следующих задач.

**Задача 1.** При заданной скорости передачи  $R$  максимизировать нижнюю оценку  $\delta^{(a)} = d^{(a)}/n$  кодового расстояния или при заданном  $\delta^{(a)}$  максимизировать  $R$ .

**Задача 2.** При заданном наборе величин  $R_i = k_i/n$ ,  $i = \overline{1, m}$ , где  $\sum_{i=1}^m R_i = R$ , максимизировать все или некоторые из величин  $\delta_i^{(a)} = d_i^{(a)}/n$  или при заданном наборе  $\delta_i^{(a)}$  максимизировать  $R$  при некоторых дополнительных ограничениях, налагаемых на  $R_i$ .

Первая задача типична при равной защите всех информационных символов РЗ; вторая задача типична для случаев, когда различные информационные символы имеют различную ценность и поэтому должны быть защищены по-разному (НЗ).

Указанные основные задачи и некоторые их модификации индуцируют требования, предъявляемые к внутренним и внешним кодам и выбору структуры каскадного кода. Под структурой каскадного кода будем понимать связь между скоростями передачи внутренних и внешних кодов, т. е. множество пар  $\{(R_{a_i}, R_{b_i}): i = \overline{1, m}\}$ .

Основное требование, предъявляемое к внутренним кодам, состоит в необходимости разработать такие методы выбора системы вложенных кодов, которые при заданном наборе скоростей передачи  $R_{a_i}$  максимизируют кодовые расстояния  $d_{a_i}$ ,  $i = \overline{1, m}$ .

Основное требование, предъявляемое к внешним кодам, состоит в выборе таких кодов (т. е. функций  $\varphi_{b_i}$ ,  $i = \overline{1, m}$ ), которые при заданном наборе скоростей передачи  $R_{b_i}$  максимизируют величины  $d_{b_i}$ . Пусть задача выбора внутренних и внешних кодов

решена. Однако при этом остается еще не решенной задача построения каскадного кода, т. е. выбора его структуры. Последняя задача существенно связана с назначением каскадного кода, например с необходимостью обеспечить равную или неравную защиту информационных символов.

В первом случае при построении каскадных кодов РЗ, как правило, задаются порядок кода и нижняя оценка кодового расстояния, а его структура выбирается так, чтобы максимизировать скорость передачи.

Во втором случае, т. е. при построении каскадных кодов НЗ, разнообразие задач существенно возрастает. В частности, при построении каскадных кодов НЗ с двумя степенями защиты, определяемыми  $\delta^{(u, 1)}$  и  $\delta^{(u, 2)} < \delta^{(u, 1)}$ , обычно задают порядок кода, степени защиты  $\delta^{(u, 1)}$  и  $\delta^{(u, 2)}$ , а также число информационных символов  $nR^{(2)}$  с наименьшей защитой, а его структуру выбирают так, чтобы максимизировать число информационных символов  $nR^{(1)}$  с наибольшей защитой (или, что то же самое, максимизировать скорость передачи  $R = R^{(1)} + R^{(2)}$ ).

## § 2.3. Внутренние коды

### 2.3.1. Система вложенных кодов БЧХ

В качестве важного, имеющего самостоятельное значение примера рассмотрим способ построения матрицы  $H_0$  при условии, что все коды  $A_i$  (при надлежащем выборе параметров  $a_i$ ) являются кодами БЧХ, которые представляют собой достаточно хорошие известные коды с удобной для практической реализации процедурой кодирования и декодирования.

Проверочный многочлен  $h_i(x)$  кода БЧХ —  $A_i$  представляет собой произведение минимальных неприводимых над полем GF(2) многочленов  $m_i(x)$  [25]. Тогда, выбирая проверочный многочлен  $h_m(x)$ , определяющий внутренний код  $A_m$ , и добавляя к нему один или несколько множителей  $m_i(x)$ , получим последовательность многочленов  $h_{m-1}(x)$ ,  $h_{m-2}(x)$ , ...,  $h_1(x)$ , которые примем в качестве проверочных многочленов внутренних кодов  $A_{m-1}$ ,  $A_{m-2}$ , ...,  $A_1$ .

Учитывая сказанное, будем представлять проверочный многочлен  $i$ -го внутреннего кода  $A_i$  в виде

$$h_i(x) = h_m^*(x) h_{m-1}(x) \dots h_1(x), \quad (2.27)$$

где каждый из многочленов  $h_i(x)$  представляет собой один или произведение нескольких минимальных многочленов  $m_i(x)$  и имеет степень, равную  $a_i$ .

Тогда справедливо следующее утверждение, доказательство которого приводится в приложении 2.3.





скоростью передачи  $R_{a,v} = (n_a - v)/n_a$ ,  $v = \overline{1, n_a - 1}$ , порождаемого матрицей  $G_0$ , достигают границы ВГ, т. е.

$$d_{a,v} \geq n_a \delta_{\text{ВГ}}(R_{a,v}). \quad (2.29)$$

**Теорема 2.4.** Для любого  $n_a$  существует невырожденная матрица  $G_0$ , такая, что спектр весов  $N_v(w)$  любого кода  $A_v$  со скоростью передачи  $R_{a,v} = (n_a - v)/n_a$ ,  $\log_2 3n_a \leq v \leq n_a - 1$ , порождаемого матрицей  $G_0$ , будет удовлетворять неравенству

$$N_v(w) = \begin{cases} 1 & \text{при } w = 0; \\ 0 & \text{при } 0 < w < n_a \delta_{\text{ВГ}}(R_{a,v}); \\ \leq n_a C_{n_a}^w 2^{-n_a(1-R_{a,v})} & \text{при } n_a \delta_{\text{ВГ}}(R_{a,v}) \leq w \leq n_a - 1, \end{cases} \quad (2.30)$$

где  $N_v(w)$  — число кодовых слов веса  $w$  в коде  $A_v$ .

### 2.3.3. Система вложенных кодов на базе треугольной невырожденной матрицы

Выбирая в качестве  $G_0$  ту или иную матрицу порядка  $n_a$ , прежде всего необходимо убедиться в том, что она является невырожденной. Однако этот вопрос автоматически снимается, если в качестве матрицы  $G_0$  выбирается треугольная нижняя (или верхняя) матрица  $n_a$ -го порядка, все диагональные элементы которой равны единице.

В этом случае матрица  $H_0$  также является треугольной. В клеточной форме матрицы  $G_0$  и  $H_0$  имеет соответственно вид (2.17) и (2.19).

Частным случаем треугольной матрицы  $G_0$  является матрица, которую будем называть специальной треугольной матрицей. Она отличается от рассмотренной выше треугольной матрицы только тем, что ее диагональные клетки порядка  $a_i$  являются единичными матрицами  $E_{a_i}$ , т. е.  $T_{ii} = T_{ii}^{-1} = E_{a_i}$ . В этом случае матрица, обратная матрице  $G_0$ , т. е. матрица  $H_0$ , также является специальной треугольной матрицей.

Систему вложенных кодов, определяемую невырожденной треугольной матрицей, будем называть системой вложенных кодов на базе треугольной матрицы. Каскадные коды, построенные с использованием такой системы, назовем систематическими каскадными кодами.

Однако вопрос о существовании треугольных и специальных треугольных матриц, удовлетворяющих теоремам 2.3 и 2.4, остается открытым. Поэтому для таких матриц аналогичные теоремы доказываются отдельно в приложении 2.5.

**Теорема 2.5.** Для любого  $n_a$  существует невырожденная нижняя треугольная матрица  $G_0$ , такая, что кодовые расстояния  $d_{a,v}$  любого кода  $A_v$  со скоростью передачи  $R_{a,v} = (n_a - v)/n_a$ ,  $v = \overline{1, n_a - 1}$ ,

порождаемого матрицей  $G_0$ , достигают границы ВГ., т. е.  $d_{a_v} \geq n_a \delta_{ВГ}(R_{a_v})$ .

**Теорема 2.6.** Для любого  $n_a$  существует невырожденная нижняя треугольная матрица  $G_0$ , такая, что спектр весов  $N_v(w)$  любого кода  $A$ , со скоростью передачи  $R_{a_v} = (n_a - v)/n_a$ ,  $\log_2 3n_a \leq v \leq n_a - 1$ , порождаемого матрицей  $G_0$ , будет удовлетворять неравенству (2.30).

### 2.3.4. Система вложенных кодов на базе ненулевого элемента поля $GF(2^{n_a})$

Рассмотрим еще один частный случай кодирующей матрицы  $G_0$ , который определяется условием, что матричное произведение  $G_0 \gamma^{(j)}$  эквивалентно произведению некоторого ненулевого элемента  $g_0 \in GF(2^{n_a})$  на вектор-столбец  $\gamma^{(j)}$ , также трактуемого как элемент того же поля. Элемент  $g_0$  будем называть кодирующим. Тогда равенство (2.8), определяющее способ кодирования внутренним кодером, принимает вид

$$\alpha^{(j)} = g_0 \gamma^{(j)}, \quad (2.31)$$

где  $g_0, \gamma^{(j)}, \alpha^{(j)} \in GF(2^{n_a})$ .

Из (2.31) получаем соотношение

$$g_0^{-1} \alpha^{(j)} = \gamma^{(j)}, \quad (2.32)$$

элемент  $h_0 = g_0^{-1}$  назовем проверочным элементом.

Существование и невырожденность матрицы  $G_0$ , удовлетворяющие указанному условию (для любого  $g_0 \neq 0$ ), очевидны. Один из способов ее построения состоит в следующем.

Элементы  $g_0, \gamma^{(j)}, \alpha^{(j)}$ , двоичная запись которых имеет вид  $g_0 = (a_{n_a-1}, a_{n_a-2}, \dots, a_0)$ ,  $\gamma^{(j)} = (b_{n_a-1}, b_{n_a-2}, \dots, b_0)$ ,  $\alpha^{(j)} = (c_{n_a-1}, c_{n_a-2}, \dots, c_0)$ , где  $a_s, b_s, c_s \in GF(2)$ , представим как многочлены над  $GF(2)$   $g_0(x) = a_{n_a-1}x^{n_a-1} + \dots + a_s x^s + \dots + a_0$ ,  $\gamma^{(j)}(x) = b_{n_a-1}x^{n_a-1} + \dots + b_s x^s + \dots + b_0$ ,  $\alpha^{(j)}(x) = c_{n_a-1}x^{n_a-1} + \dots + c_s x^s + \dots + c_0$ .

Тогда  $\alpha^{(j)}(x)$  представляет собой произведение первых двух многочленов по модулю примитивного многочлена  $F(x)$ , определяющего запись всех элементов  $GF(2^{n_a})$  в виде соответствующих многочленов.

Записывая теперь матрицу  $G_0$  в виде

$$G_0 = \begin{vmatrix} g_{n_a-1, n_a-1} & g_{n_a-1, n_a-2} & \dots & g_{n_a-1, 0} \\ \vdots & \vdots & & \vdots \\ \vdots & \vdots & & \vdots \\ g_{0, n_a-1} & g_{0, n_a-2} & \dots & g_{0, 0} \end{vmatrix},$$

имеем (в матричной форме)

$$\alpha^{(j)} = \begin{bmatrix} c_{n_a-1} \\ c_{n_a-2} \\ \vdots \\ c_0 \end{bmatrix} = G_0 \gamma^{(j)} = G_0 \cdot \begin{bmatrix} b_{n_a-1} \\ b_{n_a-2} \\ \vdots \\ b_0 \end{bmatrix} = \begin{bmatrix} \sum_{s=0}^{n_a-1} g_{n_a-1,s} b_s \\ \sum_{s=0}^{n_a-1} g_{n_a-2,s} b_s \\ \vdots \\ \sum_{s=0}^{n_a-1} g_{0,s} b_s \end{bmatrix},$$

откуда следует, что

$$c_v = \sum_{s=0}^{n_a-1} g_{v,s} b_s, \quad v = \overline{0, n_a-1}. \quad (2.33)$$

Но в силу условия (2.31)  $c_v$  представляют собой линейные комбинации элементов  $b_s$ , коэффициенты которых зависят от заданных элементов  $a_0, a_1, \dots, a_{n_a-1}$ . Тогда, сравнивая коэффициенты при  $b_s$  в правой и левой частях равенств (2.33), находим все элементы  $g_{v,s}$  матрицы  $G$ . К сожалению, в настоящее время для кодов, кодирование которых определяется условием (2.31), отсутствует сколько-нибудь развитая алгебраическая теория, на основе которой можно было бы дать какие-либо рекомендации по выбору кодирующего элемента  $g_0$  или указать оценку кодового расстояния, соответствующего выбранному элементу  $g_0$ .

Поэтому начнем с рассмотрения одного примера построения системы вложенных кодов для  $GF(2^7)$ .

Необходимый для этого список всех ненулевых элементов поля  $GF(2^7)$  приведен в табл. П.2.1 приложения 2.6. Эта таблица составлена на основе примитивного многочлена  $F(x) = x^7 + x^3 + 1$ .

Так как любой элемент поля может быть представлен как степень примитивного элемента  $\beta$ , то в табл. П.2.1 наряду с элементами поля указаны соответствующие этим элементам степени примитивного элемента.

Множество  $J_1$ , информационных слов кода  $A_1$  состоит из нулевого элемента и элементов, являющихся следующими степенями примитивного элемента  $\beta$ :

1	2	3	4	5	6	8	9	10	12	13	16	17	18	20	24	26
29	32	33	34	35	36	39	40	43	45	47	48	49	52	53	58	60
63	64	65	66	67	70	72	78	80	81	83	85	86	87	90	94	95
96	104	105	106	107	111	116	117	119	122	123	125	126				

Множество  $J_2$  информационных слов кода  $A_2$  состоит из элементов

$$\begin{aligned}(0\ 0\ 0\ 0\ 0\ 0\ 0) &= 0, & (1\ 1\ 0\ 0\ 0\ 0\ 0) &= \beta^{36}, \\(1\ 0\ 0\ 0\ 0\ 0\ 0) &= \beta^6, & (0\ 1\ 1\ 0\ 0\ 0\ 0) &= \beta^{35}, \\(0\ 1\ 0\ 0\ 0\ 0\ 0) &= \beta^5, & (1\ 0\ 1\ 0\ 0\ 0\ 0) &= \beta^{66}, \\(0\ 0\ 1\ 0\ 0\ 0\ 0) &= \beta^4, & (1\ 1\ 1\ 0\ 0\ 0\ 0) &= \beta^{107}.\end{aligned}$$

Выбирая в качестве кодирующего элемента  $g_0 = \beta^{42} = (0101011)$ , получим ненулевые кодовые слова кода

$$\begin{aligned}\beta^6\beta^{42} &= \beta^{48} = (1\ 1\ 1\ 0\ 1\ 0\ 0), & \beta^{36}\beta^{42} &= \beta^{78} = (1\ 0\ 0\ 1\ 1\ 1\ 0), \\ \beta^5\beta^{42} &= \beta^{47} = (0\ 1\ 1\ 1\ 0\ 1\ 0), & \beta^{35}\beta^{42} &= \beta^{77} = (1\ 0\ 1\ 0\ 0\ 1\ 1), \\ \beta^4\beta^{42} &= \beta^{46} = (0\ 0\ 1\ 1\ 1\ 0\ 1), & \beta^{66}\beta^{42} &= \beta^{108} = (1\ 1\ 0\ 1\ 0\ 0\ 1), \\ & & \beta^{107}\beta^{42} &= \beta^{22} = (1\ 0\ 1\ 0\ 0\ 1\ 1).\end{aligned}$$

Отсюда видно, что кодовое расстояние  $d_{A_2}$  кода  $A_2$  равно 4.

Что касается кодового расстояния  $d_{A_1}$  кода  $A_1$ , то для того, чтобы проверить, будет ли оно равно 2 (большей величины этот код иметь не может) или 1, надо составить аналогичный список кодовых слов кода  $A_1$ .

Убедимся, что в данном случае  $d_{A_1} = 1$ , проверку этого предоставим выполнить читателю.

Более того, можно показать, что при  $n_a = 7$ ,  $m = 2$ ,  $a_1 = a_2 = 3$  не существует кодирующего элемента  $g_0 \in \text{GF}(2^7)$ , при котором  $d_{A_2} = 4$ , а  $d_{A_1} = 2$ , как это имело место в примере, рассмотренном в разд. 2.2.1, где кодирование осуществлялось умножением на треугольную матрицу.

Что касается матрицы  $G_0$  для этого случая, то для любого  $g_0$ , выполняя описанные выше операции после простых, но достаточно громоздких преобразований, получаем

$$G_0 = \begin{vmatrix} a_0 + a_4 & a_1 + a_5 & a_1 + a_6 & a_3 & a_4 & a_5 & a_6 \\ a_3 + a_6 & a_0 + a_4 & a_1 + a_5 & a_2 + a_6 & a_3 & a_4 & a_5 \\ a_2 + a_5 + a_6 & a_3 + a_6 & a_0 + a_4 & a_1 + a_5 & a_2 + a_6 & a_3 & a_4 \\ a_1 + a_4 + a_5 & a_2 + a_5 + a_6 & a_3 + a_6 & a_0 + a_4 & a_1 + a_5 & a_2 + a_6 & a_3 \\ a_3 & a_4 & a_5 & a_6 & a_0 & a_1 & a_2 \\ a_2 + a_6 & a_3 & a_4 & a_5 & a_6 & a_0 & a_1 \\ a_1 + a_5 & a_2 + a_6 & a_3 & a_4 & a_5 & a_6 & a_0 \end{vmatrix}.$$

Если в качестве кодирующего элемента  $g_0$ , так же как и в рассмотренном выше примере, выбрать элемент  $g_0 = \beta^{42}$ , т. е. положить

$a_0=1, a_1=1, a_2=0, a_3=1, a_4=0, a_5=1, a_6=0$ , то порождающая матрица  $G_0$  принимает вид

$$G_0 = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

Систему вложенных кодов, определяемую соотношением (2.31), будем называть системой вложенных кодов на базе ненулевого элемента поля. Каскадные коды, построенные с использованием такой системы, назовем несистематическими каскадными кодами на базе элемента поля. Несмотря на то что множество всех различных ненулевых элементов поля  $GF(2^{n_a})$  значительно меньше, нежели множество всех различных треугольных, а тем более всех произвольных невырожденных матриц порядка  $n_a$ , для системы вложенных кодов на базе элемента поля справедливы следующие теоремы, аналогичные теоремам 2.3—2.6. Доказательства этих теорем приводятся в приложении 2.8.

**Теорема 2.7.** Для любого  $n_a$  существует ненулевой элемент  $g_0$  поля  $GF(2^{n_a})$ , такой, что кодовое расстояние  $d_{a,}$  любого кода  $A$ , со скоростью передачи  $R_a = (n_a - \nu)/n_a$ ,  $\nu = 1, n_a - 1$ , порождаемого элементом  $g_0$ , достигает границы ВГ.

**Теорема 2.8.** Для любого  $n_a$  существует ненулевой элемент  $g_0$  поля  $GF(2^{n_a})$ , такой, что спектр весов  $N_i(w)$  любого кода  $A$ , со скоростью передачи  $R_a = (n_a - \nu)/n_a$ ,  $\nu = 1, n_a - 1$ , порождаемого элементом  $g_0$ , будет удовлетворять неравенству

$$N_i(w) = \begin{cases} 1 & \text{при } w = 0; \\ 0 & \text{при } 0 < w < n_a \delta_{\text{ВГ}}(R_a); \\ \leq n_a^2 C_{n_a}^w 2^{-n_a(1-R_a)} & \text{при } n_a \delta_{\text{ВГ}}(R_a) \leq w \leq n_a - 1. \end{cases} \quad (2.34)$$

## § 2.4. Внешние коды

### 2.4.1. Выбор основания внешних кодов

Так как внешние коды  $B$ , никак не связаны друг с другом, то при их выборе имеется гораздо больше свободы, нежели при выборе внутренних кодов  $A_i$ , образующих систему вложенных кодов. В частности, не уменьшая общности получаемых результатов, в качестве внешних кодов можно всегда выбирать систематические коды. Кроме того, в разд. 2.1.1 указывалось, что все коды  $B$ , групповые над полем  $GF(2^{n_b})$  и имеют одну и ту же длину  $n_b$ ,

совпадающую с числом столбцов кодового слова  $\alpha$ . Покажем, что последнее ограничение естественным образом вытекает из требований, предъявляемых к внешним кодам.

Действительно, каждый внешний код  $B_i$  (линейный над полем  $GF(2)$  по условию линейности каскадного кода) должен обеспечить кодирование  $a_i b_i$  двоичных информационных символов в кодовое слово  $\gamma_i$ , содержащее  $a_i n_b$  двоичных символов, т. е. иметь скорость передачи  $R_{bi} = b_i / n_b$ . При этом в общем случае основание кода  $q_i = 2^{s_i}$  и его длина  $n_{bi}$  должны удовлетворять лишь двум условиям:  $a_i b_i$  должно быть кратно  $s_i$  и  $s_i n_{bi} = a_i n_b$ , где  $1 \leq s_i \leq \leq a_i b_i$ .

Однако при любом из возможных выборов величин  $s_i$  и  $n_{bi}$  блок  $\gamma_i$ , полученный в результате кодирования кодом  $B_i$ , можно интерпретировать как групповой (не обязательно линейный) код над полем  $GF(2^{s_i})$  длины  $n_b$  с той же самой скоростью передачи. Таким образом, во всех случаях минимальное число ненулевых столбцов в  $\gamma_i$  есть кодовое расстояние  $d_{bi}$  группового кода над полем  $GF(2^{s_i})$ .

#### 2.4.2. Коды РС в качестве внешних кодов

В предыдущем разделе было показано, что в качестве внешних кодов  $B_i$  целесообразно выбирать групповые над полем  $GF(2^{s_i})$  коды с максимальным значением величины  $\delta(R_{bi}) = d_{bi} / n_b$ . При  $n_b \leq 2^{s_i} + 1$  этому условию полностью удовлетворяют линейные над полем  $GF(2^{s_i})$  коды РС и их модификации: укороченные и удлиненные коды РС. Для всех этих кодов величина  $\delta(R_{bi})$  достигает теоретически возможного предела  $\delta(R_{bi}) = 1 - R_{bi} + 1/n_b \approx 1 - R_{bi}$ . При этом если  $n_b < 2^{s_i} - 1$ , то следует использовать укороченные коды РС, если  $n_b = 2^{s_i} - 1$ , то собственно коды РС и если  $2^{s_i} - 1 < n_b \leq 2^{s_i} + 1$ , то удлиненные коды РС.

Весьма важным является также и то, что для кодов РС и указанных их модификаций известны алгебраические методы декодирования, сравнительно просто реализуемые (со степенным законом сложности) при всех значениях  $n_b$ .

## КОМБИНАТОРНЫЕ ОЦЕНКИ МИНИМАЛЬНЫХ РАССТОЯНИЙ

В этой главе выводятся нижние и верхние оценки для кодового расстояния каскадных кодов произвольного порядка. Исследуется зависимость этих оценок от порядка и структуры каскадных кодов. Вводятся каскадные коды бесконечного порядка и указываются такие из них, для которых асимптотически точно известно кодовое расстояние, причем отношение  $d/n = \delta(R)$  не стремится к нулю при  $n \rightarrow \infty$ . Рассматриваются также нижние и верхние оценки степеней защиты для каскадных кодов с неравной защитой информационных символов.

### § 3.1. Нижние оценки минимальных расстояний

#### 3.1.1. Равная защита символов

Пусть  $d$  — кодовое расстояние каскадного кода длины  $n = n_a n_b$ . Обозначим через  $\delta^{(n)}(R, m)$  нижнюю оценку отношения  $d/n$  при заданных скорости передачи  $R$  каскадного кода и его порядка  $m$ . Для краткости величину  $\delta^{(n)}(R, m)$  будем называть нижней оценкой кодового расстояния.

Условимся, если не оговорено противное, в качестве внутренних  $A_i$  и внешних  $B_i$  кодов выбирать лучшие из известных, т. е. двоичные коды  $A_i$ , удовлетворяющие оценке ВГ,  $d_{ai}/n_{ai} \geq \delta_{\text{ВГ}}(R_{ai})$ ,  $i = \overline{1, m}$ , и коды  $B_i$  над полем  $\text{GF}(2^{q_i})$ , для которых  $d_{bi}/n_{bi} \geq 1 - R_{bi}$ ,  $i = \overline{1, m}$ . Обозначая через  $\delta_i^{(n)} = \delta_{\text{ВГ}}(R_{ai})(1 - R_{bi})$ , исключим из выражения (2.25) для скорости передачи  $R$  величины  $R_{bi}$ . Тогда после очевидных преобразований получаем

$$R = R_{a1} - \sum_{i=1}^m (R_{ai} - R_{a, i+1}) \delta_i^{(n)} / \delta_{\text{ВГ}}(R_{ai}), \quad (3.1)$$

где  $\delta_i^{(n)}$  — нижняя оценка,  $d_i/n = (d_{ai}/n_{ai})(d_{bi}/n_{bi}) = \delta_i^{(n)}$ .

Для кодов равной защиты (кодов РЗ) естественным требованием (см. разд. 2.2.2) является

$$d_1 = d_2 = \dots = d_m. \quad (3.2)$$

Переноса условия (3.2) на нижние оценки минимальных расстояний, получаем

$$\delta_1^{(n)} = \delta_2^{(n)} = \dots = \delta_m^{(n)}. \quad (3.3)$$

Всякое ограничение, налагаемое на величины  $\delta_i^{(n)}$ , связывающие между собой величины  $R_{ai}$  и  $R_{bi}$ , представляет собой ограничение



на структуру каскадного кода, которая определяется распределением скоростей передачи внутренних и внешних кодов.

В дальнейшем структуры каскадного кода, удовлетворяющие условию (3. 3), будем называть структурами типа  $A$  или (короче) структурой  $A$  и соответствующие им величины  $\delta_A^{(n)}(R, m)$  обозначать  $\delta_A^{(n)}(R, m)$ .

Как следует из (3. 1) и (2. 26), при заданном наборе величин  $R_{a_i}$ ,  $i = \overline{1, m}$ , структура  $A$  приводит к максимизации скорости передачи  $R$  при заданном значении  $\delta_A^{(n)}(R, m)$  или, что то же самое, к максимизации  $\delta_A^{(n)}(R, m)$  (при заданной скорости передачи  $R$ ). Это обстоятельство свидетельствует о том, что каскадные коды структуры  $A$  представляют особенно большой интерес, тем более что (как будет показано в гл. 4) при каскадном декодировании реализуется кодовое расстояние, равное  $n\delta_A^{(n)}(R, m)$ . При выполнении условия (3. 3) выражение (3. 1) принимает вид

$$R = R_{a_1} - \delta_A^{(n)}(R, m) \sum_{i=1}^m (R_{a_i} - R_{a_{i+1}}) / \delta_{\text{ВГ}}(R_{a_i}), \quad (3.4)$$

из которого следует, что

$$\delta_A^{(n)}(R, m) = (R_{a_1} - R) / \sum_{i=1}^m (R_{a_i} - R_{a_{i+1}}) / \delta_{\text{ВГ}}(R_{a_i}). \quad (3.5)$$

Однако равенства (3. 3) еще не определяют однозначно выбор величин  $R_{a_i}$ ,  $i = \overline{1, m}$ . Поэтому на скорости передачи внутренних кодов могут быть наложены дополнительные условия, определяющие различные варианты структуры  $A$ .

В дальнейшем мы ограничимся рассмотрением двух видов структуры  $A$  — структуры  $A_0$ , при которой для каждого значения  $\delta_A^{(n)}(R, m)$  величины  $R_{a_i}$  выбираются из условия максимизации скорости передачи  $R$ , и структуры  $A_1$ , при которой все  $a_i = a$ ,  $i = \overline{1, m}$ , так что скорости передачи внутренних кодов  $R_{a_i} = \frac{m-i+1}{m} R_{a_1}$ , а скорость  $R_{a_1}$  выбирается из условия максимизации  $R$ . Структура  $A_1$  интересна тем, что для нее все внешние коды имеют одно и то же основание  $g = 2^a$ , что приводит к существенному упрощению аппаратуры кодирования и декодирования. Таким образом, мы приходим к следующему утверждению.

**Утверждение 3.1.** Максимальная скорость передачи  $R$  каскадного кода структуры  $A$  при заданной величине  $\delta_A^{(n)}(R, m)$  определяется равенством

$$R = \max_{\{R_{a_i}\}} \left\{ R_{a_1} - \delta_A^{(n)}(R, m) \sum_{i=1}^m (R_{a_i} - R_{a_{i+1}}) / \delta_{\text{ВГ}}(R_{a_i}) \right\}. \quad (3.6)$$

Это равенство, справедливое для кодов структуры А0, при структуре А1 принимает вид

$$R = \max_{R_{a1}} \left\{ R_{a1} \left[ 1 - \delta_A^{(n)}(R, m) m^{-1} \sum_{i=1}^m \left( \delta_{\text{ВГ}} \left( \frac{m-i+1}{m} R_{a1} \right) \right)^{-1} \right] \right\}. \quad (3.7)$$

Величины  $\delta_A^{(n)}(R, m)$  для этих вариантов структуры А будем обозначать соответственно  $\delta_{A0}^{(n)}(R, m)$  и  $\delta_{A1}^{(n)}(R, m)$ . Так как максимизация по параметрам  $R_{a1}$  при заданном значении  $\delta_A^{(n)}(R, m)$  эквивалентна максимизации  $\delta_A^{(n)}(R, m)$  при заданном значении  $R$ , то зависимость между  $R$  и  $\delta_A^{(n)}(R, m)$ , определяемая для каскадных кодов структуры А0 и А1 соответственно выражениями (3.6) и (3.7), может быть найдена из эквивалентных выражений, являющихся следствием равенства (3.5). Именно для структуры А0

$$\delta_{A0}^{(n)}(R, m) = \max_{\{R_{a1}\}} \left\{ (R_{a1} - R) / \sum_{i=1}^m (R_{a1} - R_{a, i+1}) / \delta_{\text{ВГ}}(R_{a1}) \right\}, \quad (3.8)$$

а для структуры А1

$$\delta_{A1}^{(n)}(R, m) = \max_{R_{a1}} \left\{ (R_{a1} - R) m / \left[ R_{a1} \sum_{i=1}^m \left( \delta_{\text{ВГ}} \left( \frac{m-i+1}{m} R_{a1} \right) \right)^{-1} \right] \right\}. \quad (3.9)$$

### 3.1.2. Неравная защита символов

При рассмотрении каскадных кодов с неравной защитой информационных символов (кодов НЗ) ограничимся для простоты изложения случаем двух уровней защиты. Это значит, что  $R^{(1)}$  информационных символов, расположенных в первых  $m_1$  блоках  $\mu_i$ ,  $i=1, m_1$ , имеют защиту  $d^{(1)} = n\delta^{(1)}$ , а  $R^{(2)}$  информационных символов, расположенных в оставшихся  $m_2 = m - m_1$  блоках  $\mu_i$ ,  $i=m_1+1, m$ , имеют защиту  $d^{(2)} = n\delta^{(2)}$ . При этом  $R^{(1)} + R^{(2)} = R$ .

Как следует из теоремы 2.2, для реализации неравной защиты информационных символов необходимо, чтобы  $\delta^{(1)} > \delta^{(2)}$ . В противном случае, если  $\delta^{(1)} \leq \delta^{(2)}$ , будет осуществляться равная защита всех информационных символов, определяемая величиной  $\delta^{(1)}$ . Величины  $\delta^{(1)}$  и  $\delta^{(2)}$  будем называть уровнями защиты.

В соответствии с традицией, сложившейся при исследовании кодов НЗ, будем, как правило, считать заданными нижние оценки величин  $\delta^{(1)}$  и  $\delta^{(2)}$ , обозначая их  $\delta^{(1n)}$  и  $\delta^{(2n)}$ , а также параметр  $R^{(2)}$  и решать задачу максимизации скорости передачи  $R$  или, что то же самое, параметра  $R^{(1)}$ .

Представляет интерес и другая постановка задачи при неравной защите, когда заданными являются величина  $\delta^{(2n)}$  и параметры  $R^{(1)}$  и  $R^{(2)}$  (а значит, и скорость передачи  $R$ ) и требуется максимизировать величину  $\delta^{(1n)} \geq \delta^{(2n)}$ . По самой постановке ясно, что

эта задача является простым обращением первой и может считаться решенной, если первая задача решена для достаточно большого числа пар  $(\delta^{(1n)}, \delta^{(2n)})$ . Однако на практике удобно иметь ее самостоятельное решение, техническое выполнение которого по существу не отличается от решения первой задачи.

Из определения величин  $R^{(1)}$  и  $R^{(2)}$  следует, что

$$R^{(1)} = \sum_{i=1}^{m_1} (R_{ai} - R_{a, i+1}) R_{ai},$$

$$R^{(2)} = \sum_{i=m_1+1}^m (R_{ai} - R_{a, i+1}) R_{ai}.$$
(3.10)

Для кодов НЗ с двумя уровнями защиты естественными требованиями являются

$$d_1 = d_2 = \dots = d_{m_1} = d^{(1)}, \quad d_{m_1+1} = d_{m_1+2} = \dots = d_m = d^{(2)}.$$
(3.11)

Переносим условия (3.11) на нижние оценки минимальных расстояний, получаем

$$\delta_1^{(n)} = \delta_2^{(n)} = \dots = \delta_{m_1}^{(n)} = \delta^{(1n)}, \quad \delta_{m_1+1}^{(n)} = \delta_{m_1+2}^{(n)} = \dots = \delta_m^{(n)} = \delta^{(2n)}.$$
(3.12)

В дальнейшем структуру каскадных кодов НЗ, выбираемых в соответствии с (3.12), будем называть структурой 2А.

Однако, как и в случае равной защиты, соотношения (3.12) еще не определяют однозначный выбор величин  $R_{ai}$ ,  $i = \overline{1, m}$ , и поэтому на них можно налагать дополнительные ограничения, аналогичные условиям, принимаемым для кодов РЗ структуры А.

При выполнении условий (3.12) выражение (3.1) принимает вид

$$R = R_{a1} - \delta^{(1n)} \sum_{i=1}^{m_1} (R_{ai} - R_{a, i+1}) / \delta_{\text{ВГ}}(R_{ai}) -$$

$$- \delta^{(2n)} \sum_{i=m_1+1}^m (R_{ai} - R_{a, i+1}) / \delta_{\text{ВГ}}(R_{ai}),$$
(3.13)

из которого вытекает следующее утверждение.

**Утверждение 3.2.** Максимальная скорость передачи  $R$  каскадного кода структуры 2А при заданных значениях нижних оценок уровней защиты  $\delta^{(1n)}$  и  $\delta^{(2n)}$  определяется равенством

$$R = \max_{\{R_{ai}\}} \left\{ R_{a1} - \delta^{(1n)} \sum_{i=1}^{m_1} (R_{ai} - R_{a, i+1}) / \delta_{\text{ВГ}}(R_{ai}) - \right.$$

$$\left. - \delta^{(2n)} \sum_{i=m_1+1}^m (R_{ai} - R_{a, i+1}) / \delta_{\text{ВГ}}(R_{ai}) \right\}.$$
(3.14)

Отметим, что распространение полученных результатов на случай  $z > 2$  уровней защиты достаточно очевидно и приводит лишь к более громоздким выражениям. Коды НЗ с  $z$  уровнями защиты естественно назвать кодами структуры  $zA$ , причем порядок  $m$  таких кодов должен удовлетворять очевидному условию  $m \geq z$ ,  $z \geq 2$ .

### 3.1.3. Влияние порядка каскадного кода на нижнюю оценку кодового расстояния

Рассмотрим каскадный код порядка  $m$ , такой, для которого среди величин  $a_i$ ,  $i = \overline{1, m}$ , есть хотя бы одна, например  $a_s$ , для которой выполняется условие

$$2^{a_s/2} \geq n_b - 1, \quad (3.15)$$

и выясним, можно ли за счет увеличения его порядка увеличить скорость передачи без ухудшения нижней оценки кодового расстояния. Ответ на этот вопрос дает следующее утверждение, доказанное в приложении 3.1.

**Утверждение 3.3.** Если существует каскадный код порядка  $m$  с нижней оценкой кодового расстояния  $\delta^{(n)}(R, m)$  и скоростью передачи  $R$ , удовлетворяющий условию (3.15), то существует каскадный код (таких же размеров  $n_a \times n_b$ ) порядка  $m' > m$  с той же нижней оценкой кодового расстояния  $\delta^{(n)}(R', m') = \delta^{(n)}(R, m)$  и скоростью передачи  $R' > R$ .

Из утверждения 3.3 непосредственно следует, что при фиксированной скорости передачи можно посредством увеличения порядка  $m$  каскадного кода увеличить нижнюю оценку его кодового расстояния.

## § 3.2. Верхние оценки минимальных расстояний

### 3.2.1. Верхние оценки для произвольных каскадных кодов

Переходя к рассмотрению верхних оценок минимальных расстояний в линейных каскадных кодах, отметим, что для них, очевидно, справедливы все известные верхние оценки для произвольных блочных линейных кодов. Поэтому можно ставить задачи лишь о нахождении более сильных оценок, но уже справедливых только для каскадных кодов того или иного порядка, той или иной структуры.

Пусть для каскадного кода порядка  $m$  заданы скорость передачи  $R$  и скорости передачи внутренних и внешних кодов, т. е.  $R_{a_i}$  и  $R_{b_i}$ ,  $i = \overline{1, m}$ . Пусть  $\delta(R) = d/n$ , где  $d$  — кодовое расстояние каскадного кода. Тогда верхняя оценка  $\delta^{(n)}(R, m)$  величины  $\delta(R)$  определяется следующим утверждением, доказанным в приложении 3.2.

**Утверждение 3.4.** Для каскадного кода порядка  $m$  со структурой  $R_{ai}, R_{bi}, i = \overline{1, m}$ , верхняя оценка кодового расстояния  $\delta^{(a)}(R, m)$  определяется соотношением

$$\delta^{(a)}(R, m) = \min_i \{ (1 - R_{bi}) \min_{r_i} \{ \delta_B(r_i) \times \\ \times (R_{ai} - R_{a, i+1}) / (R_{ai} - R_{a, i+1} - r_i) \} \}, \quad (3.16)$$

где  $\delta_B(r_i)$  — любая верхняя оценка кодового расстояния блочного линейного кода со скоростью передачи  $r_i$ , а минимум для каждого  $i$  берется по всем значениям  $r_i$ , для которых

$$\frac{1}{n_b}(R_{ai} - R_{a, i+1}) \leq r_i \leq R_{bi}(R_{ai} - R_{a, i+1}). \quad (3.17)$$

Остановимся теперь на минимизации правой части (3.16) по  $r_i$ . Если в качестве верхней оценки  $\delta_B(r_i)$  выбрать оценку Бассалыго—Элайеса (см. теорему 1.2), согласно которой

$$\delta_B(r_i) = \delta_{БЭ}(r_i) = 2(1 - \delta_{ВГ}(r_i))\delta_{ВГ}(r_i), \quad (3.18)$$

то после элементарного исследования на экстремум получаем:

1. Если  $R_{ai} - R_{a, i+1} \leq 1/(2 \ln 2) \approx 0,648$ , то оптимальное значение  $r_i = \frac{1}{n_b}(R_{ai} - R_{a, i+1}) \rightarrow 0$  при  $n_b \rightarrow \infty$ .

2. Если  $R_{ai} - R_{a, i+1} > 1/(2 \ln 2)$  и  $(R_{ai} - R_{a, i+1})R_{bi} < r_i^*$ , где  $r_i^*$  — решение уравнения  $x - \delta_{ВГ}(x)/\delta_{ВГ}'(x) = R_{ai} - R_{a, i+1}$ , то оптимальное значение  $r_i = (R_{ai} - R_{a, i+1})R_{bi}$ .

3. Если  $R_{ai} - R_{a, i+1} > 1/(2 \ln 2)$  и  $(R_{ai} - R_{a, i+1})R_{bi} \geq r_i^*$ , то оптимальное значение  $r_i = r_i^*$ .

Отметим, что функция  $\varphi(x) = x - \delta_{ВГ}(x)/\delta_{ВГ}'(x)$  почти линейно возрастает от 0,721 до 1 на отрезке  $[0, 1]$ .

В тех случаях, когда для всех  $i = \overline{1, m}$  разность  $R_{ai} - R_{a, i+1} \leq 1/2 \ln 2$ , что для всех  $m$  имеет место в диапазоне малых скоростей передачи, который с увеличением  $m$  быстро расширяется, целесообразно пользоваться для нахождения верхних оценок не утверждением 3.4, а следствием из него.

**С л е д с т в и е 3.1.** В качестве верхней оценки кодового расстояния каскадного кода порядка  $m$  можно использовать выражение

$$\delta^{(a)}(R, m) = \frac{1}{2} \min_i (1 - R_{bi}). \quad (3.19)$$

Соотношение (3.19) получается из (3.16) подстановкой  $r_i = 0$ , при котором любая верхняя оценка  $\delta_B(0) = 1/2$ . Несмотря на грубость оценки (3.19), она во многих случаях совпадает с оценкой (3.16). Однако при малых значениях  $m$  и больших скоростях передачи она может оказаться хуже не только оценки (3.16), но и тривиальной оценки  $\delta_B(R)$ .

Рассмотрим теперь случай неравной защиты информационных символов. Пусть для каскадного кода порядка  $m$  имеется два

уровня защиты (см. разд. 3.1.2). При этом защита информационных символов в блоках  $\mu_i, i = \overline{1, m_1}$ , определяется величиной  $\delta^{(1)}$ , а защита информационных символов в блоках  $\mu_i, i = \overline{m_1 + 1, m}$ , — величиной  $\delta^{(2)}$ . Тогда следующее утверждение позволяет получить верхние оценки  $\delta^{(1, \text{в})}$  и  $\delta^{(2, \text{в})}$  величин  $\delta^{(1)}$  и  $\delta^{(2)}$  соответственно.

**Утверждение 3.5.** Для каскадного кода НЗ порядка  $m$  с двумя уровнями защиты верхние оценки  $\delta^{(1, \text{в})}$  и  $\delta^{(2, \text{в})}$  определяются соотношениями

$$\begin{aligned} \delta^{(1, \text{в})} &= \min_{1 \leq i \leq m_1} \{ (1 - R_{bi}) \min_{r_i} \{ \delta_{\text{в}}(r_i) (R_{ai} - R_{a, i+1}) / (R_{ai} - R_{a, i+1} - r_i) \} \}, \\ \delta^{(2, \text{в})} &= \min_{m_1 < i \leq m} \{ (1 - R_{bi}) \min_{r_i} \{ \delta_{\text{в}}(r_i) (R_{ai} - R_{a, i+1}) / (R_{ai} - R_{a, i+1} - r_i) \} \}, \end{aligned} \quad (3.20)$$

где  $\delta_{\text{в}}(r_i)$  — любая верхняя оценка кодового расстояния блочного линейного кода со скоростью передачи  $r_i$ , а минимум для каждого берется по всем значениям  $r_i$ , удовлетворяющим условию (3.17).

Доказательство утверждения 3.5 аналогично доказательству утверждения 3.4 (см. приложение 3.2).

Отметим, что, как и в случае равной защиты, когда для всех  $i = \overline{1, m}$  разность  $R_{ai} - R_{a, i+1} \leq 1/2 \ln 2$ , целесообразно пользоваться не утверждением 3.5, а следствием из него.

**С л е д с т в и е 3.2.** В качестве верхних оценок уровней защиты информационных символов для каскадного кода НЗ порядка  $m$  с двумя уровнями защиты можно использовать выражения

$$\delta^{(1, \text{в})} = \frac{1}{2} \min_{1 \leq i \leq m_1} (1 - R_{bi}), \quad \delta^{(2, \text{в})} = \frac{1}{2} \min_{m_1 < i \leq m} (1 - R_{bi}). \quad (3.21)$$

Соотношения (3.21) получаются из (3.20) подстановкой  $r_i = 0$ .

Так же, как и для кодов РЗ, во многих интересных случаях (3.21) совпадают с (3.20). Возможное отличие между ними будет тем меньше, чем больше  $m_1$  и  $m - m_1$ .

### 3.2.2. Верхние оценки для каскадных кодов структуры А

В предыдущем разделе при выводе верхних оценок не налагалось каких-либо ограничений на структуру каскадных кодов, поэтому эти оценки справедливы для любой структуры, в том числе и структуры А. Однако в последнем случае удастся проследить связь верхних и нижних оценок, которая определяется утверждениями 3.6 и 3.7, доказанными в приложении 3.3.

**Утверждение 3.6.** Для каскадных кодов структуры А верхние оценки кодового расстояния  $\delta_A^{(\text{в})}(R, m)$ , определяемые в соответствии со следствием 3.4, и нижние оценки  $\delta_A^{(\text{н})}(R, m)$ , определяемые в соответствии с утверждением 3.1, связаны соотношением

$$\delta_A^{(\text{в})}(R, m) = \delta_A^{(\text{н})}(R, m) / 2\delta_{\text{вг}}(R_{\text{ам}}). \quad (3.22)$$

**Утверждение 3.7.** Для каскадных кодов НЗ структуры 2А верхние оценки уровней защиты  $\delta_{2A}^{(1, \text{в})}$  и  $\delta_{2A}^{(2, \text{в})}$ , определяемые в соответствии со следствием 3.2, и нижние оценки  $\delta_{2A}^{(1, \text{н})}$  и  $\delta_{2A}^{(2, \text{н})}$ , определяемые в соответствии с утверждением 3.2, связаны соотношениями

$$\delta_{2A}^{(1, \text{в})} = \delta_{2A}^{(1, \text{н})} / 2\delta_{\text{ВГ}}(R_{am}), \quad \delta_{2A}^{(2, \text{в})} = \delta_{2A}^{(2, \text{н})} / 2\delta_{\text{ВГ}}(R_{am}). \quad (3.23), (3.24)$$

### 3.2.3. Верхние оценки для систематических каскадных кодов

В гл. 2 мы условились называть систематическими каскадными кодами такие, для которых в качестве кодирующей матрицы  $G_0$  используется нижняя треугольная матрица. В этом случае можно несколько усилить верхние оценки по сравнению с оценками, полученными в разд. 3.2.1 и 3.2.2. Верхнюю оценку кодового расстояния для систематических каскадных кодов (т. е. каскадных кодов на базе нижней треугольной матрицы  $G_0$ ) будем обозначать  $\delta^{(\text{в})}(R, m)$ . Для таких кодов имеет место следующее утверждение.

**Утверждение 3.8.** Для систематического каскадного кода порядка  $m$  со структурой  $R_{ai}, R_{bi}, i = \overline{1, m}$ , верхняя оценка кодового расстояния  $\delta^{(\text{в})}(R, m)$  определяется соотношением

$$\delta^{(\text{в})}(R, m) = \min_i \{ (1 - R_{bi})(1 - R_{a, i+1}) \min_{r_i} [\delta_{\text{В}}(r_i) \times \\ \times (R_{ai} - R_{a, i+1}) / (R_{ai} - R_{a, i+1} - r_i(1 - R_{a, i+1}))] \}, \quad (3.25)$$

где  $\delta_{\text{В}}(r_i)$  — любая верхняя оценка кодового расстояния блочного линейного кода со скоростью передачи  $r_i$ , а минимум для каждого берется по всем значениям  $r_i$ , удовлетворяющим условиям

$$(R_{ai} - R_{a, i+1}) / [n_b(1 - R_{a, i+1})] \leq r_i \leq \\ \leq R_{bi}(R_{ai} - R_{a, i+1}) / (1 - R_{a, i+1}). \quad (3.26)$$

Доказательство утверждения 3.8 повторяет доказательство утверждения 3.4 (см. приложение 3.2) с той лишь разницей, что в силу треугольности матрицы  $G_0$  фактическая длина слов кода  $V_i$  будет определяться не соотношением (П.3.4), а равенством

$$n^* = n - n_a x_i - (n_b - x_i) \sum_{s=i+1}^m a_s. \quad (3.27)$$

Остановимся теперь на минимизации правой части (3.25) по  $r_i$ . Как и для систематических кодов, если  $\delta_{\text{В}}(r_i)$  определяется равенством (3.18), то после элементарного исследования на экстремум получаем:

1. Если  $(R_{ai} - R_{a, i+1}) / (1 - R_{a, i+1}) \leq 1 / (2 \ln 2)$ , то оптимальное значение  $r_i \rightarrow 0$  при  $n_b \rightarrow \infty$ .

2. Если  $(R_{ai} - R_{a,i+1})/(1 - R_{a,i+1}) > 1/(2 \ln 2)$  и  $R_{bi}(R_{ai} - R_{a,i+1})/(1 - R_{a,i+1}) \leq r_i^*$ , где  $r_i^*$  — решение уравнения  $x - \delta_{\text{ВГ}}(x)/\delta'_{\text{ВГ}}(x) = (R_{ai} - R_{a,i+1})/(1 - R_{a,i+1})$ , (3.28)

то оптимальное значение  $r_i = (R_{ai} - R_{a,i+1})R_{bi}/(1 - R_{a,i+1})$ .

3. Если  $(R_{ai} - R_{a,i+1})/(1 - R_{a,i+1}) > 1/(2 \ln 2)$  и  $r_i^* \geq (R_{ai} - R_{a,i+1})R_{bi}/(1 - R_{a,i+1})$ , где  $r_i^*$  — решение (3.28), то оптимальное значение  $r_i = r_i^*$ .

Пусть для всех  $i$ ,  $i = \overline{1, m}$ , имеет место

$$(R_{ai} - R_{a,i+1})/(1 - R_{a,i+1}) \leq 1/(2 \ln 2), \quad (3.29)$$

тогда для нахождения верхних оценок удобно пользоваться следующим следствием из утверждения 3.8.

**С л е д с т в и е 3.3.** В качестве верхней оценки кодового расстояния систематического каскадного кода порядка  $m$  можно использовать выражение

$$\delta^{(n)}(R, m) = \frac{1}{2} \min_i \{(1 - R_{a,i+1})(1 - R_{bi})\}. \quad (3.30)$$

Соотношение (3.30) получается из (3.25) подстановкой  $r_i = 0$ . Поэтому оно всегда будет верхней оценкой, но может быть более грубой, чем (3.25), если (3.29) выполняется не для всех  $i$ .

Для систематических, как и для несистематических каскадных кодов структуры  $A$ , нетрудно установить связь верхних и нижних оценок кодового расстояния.

**Утверждение 3.9.** Для систематических каскадных кодов структуры  $A$  верхние оценки кодового расстояния  $\delta_A(R, m)$ , определяемые в соответствии со следствием 3.3, и нижние оценки  $\delta_A^{(n)}(R, m)$ , определяемые в соответствии с утверждением 3.1, связаны соотношением

$$\delta_A^{(n)}(R, m) = \delta_A^{(n)}(R, m) \min_i \{(1 - R_{a,i+1})/2\delta_{\text{ВГ}}(R_{ai})\}. \quad (3.31)$$

Доказательство этого утверждения аналогично доказательству утверждения 3.6 (см. приложение 3.3).

Для систематических каскадных кодов НЗ верхние оценки уровней защиты получаются рассуждениями, аналогичными приведенным в разд. 3.2.1.

**Утверждение 3.10.** Для систематического каскадного кода НЗ порядка  $m$  с двумя уровнями защиты верхние оценки  $\delta^{(1,n)}$  и  $\delta^{(2,n)}$  определяются соотношениями

$$\begin{aligned} \delta^{(1,n)} &= \min_{1 \leq i \leq m_1} \{(1 - R_{a,i+1})(1 - R_{bi}) \min_{r_i} [\delta_{\text{В}}(r_i) \times \\ &\quad \times (R_{ai} - R_{a,i+1})/(R_{ai} - R_{a,i+1} - r_i(1 - R_{a,i+1}))]\}, \quad (3.32) \\ \delta^{(2,n)} &= \min_{m_1 < i \leq m} \{(1 - R_{a,i+1})(1 - R_{bi}) \min_{r_i} [\delta_{\text{В}}(r_i) \times \\ &\quad \times (R_{ai} - R_{a,i+1})/(R_{ai} - R_{a,i+1} - r_i(1 - R_{a,i+1}))]\}, \end{aligned}$$



где  $\delta_B(r)$  — любая верхняя оценка кодового расстояния блочного линейного кода со скоростью передачи  $r$ , а минимум для каждого  $i$  берется по всем значениям  $r_i$ , удовлетворяющим условиям (3. 26).

Доказательство этого утверждения аналогично доказательству утверждений 3.5 и 3.8 (см. приложение 3.2).

Как и в случае равной защиты, когда для всех  $i$  выполняется (3. 29), удобно пользоваться следующим следствием.

**С л е д с т в и е 3.4.** В качестве верхних оценок уровней защиты информационных символов для систематического каскадного кода порядка  $m$  с двумя уровнями защиты можно использовать выражения

$$\begin{aligned}\delta^{(1, \text{в})} &= \frac{1}{2} \min_{1 \leq i \leq m} \{(1 - R_{a, i+1})(1 - R_{bi})\}, \\ \delta^{(2, \text{в})} &= \frac{1}{2} \min_{m_1 < i \leq m} \{(1 - R_{a, i+1})(1 - R_{bi})\}.\end{aligned}\tag{3. 33}$$

### § 3.3. Анализ оценок кодового расстояния каскадных кодов структуры А

#### 3.3.1. Коды первого порядка

Анализ оценок кодового расстояния каскадных кодов естественно начать с кодов первого порядка, которые обычно называют каскадными кодами, и они впервые рассматривались Форни [140].

Отметим, что каскадные коды первого порядка всегда являются кодами с равной защитой информационных символов, т. е. кодами РЗ. Кроме того, каскадный код первого порядка с произвольной кодирующей матрицей  $G_0$  всегда эквивалентен в смысле кодового расстояния и спектра весов каскадному коду с нижней треугольной кодирующей матрицей, т. е. систематическому каскадному коду.

Структура каскадных кодов первого порядка полностью определяется зависимостью между  $R_{a1}$  и  $R_{b1}$ , произведение которых равно скорости передачи, т. е.

$$R = R_{a1}R_{b1},\tag{3. 34}$$

так что структуры А0 и А1 для каскадного кода первого порядка совпадают.

В силу утверждения 3.1 скорость передачи связана с нижней оценкой кодового расстояния следующими соотношениями

$$R = \max_{R_{a1}} \{R_{a1}(1 - \delta^{(\text{в})}(R, 1)/\delta_{\text{вГ}}(R_{a1}))\}\tag{3. 35}$$

$$\text{или } \delta^{(\text{в})}(R, 1) = \max_{R_{a1}} \{(1 - R/R_{a1})\delta_{\text{вГ}}(R_{a1})\}.\tag{3. 36}$$

Из утверждений 3.4 и 3.6 имеем следующие верхние оценки кодового расстояния каскадного кода первого порядка:

$$\delta^{(n)}(R, 1) = (1 - R/R_{a1}) \min_r \{ \delta_B(r) / (1 - r/R_{a1}) \} \quad (3.37)$$

$$\text{и } \delta^{(n)}(R, 1) = \frac{1}{2} (1 - R/R_{a1}) = \delta^{(n)}(R, 1) / 2\delta_{\text{вг}}(R_{a1}). \quad (3.38)$$

Результаты расчетов по формулам (3.36)–(3.38) вместе с оптимальными значениями  $R_{a1}$ , определяющими структуру  $A$  и  $r$ , приведены в табл. 3.1 и на рис. 3.1, на котором кроме нижней оценки  $\delta_A^{(n)}(R, 1)$  и верхних оценок  $\delta^{(n)}(R, 1)$ , вычисленных по формулам (3.37) и (3.38), представлен график  $\delta_{\text{вг}}(R)$ .

Таблица 3.1

$R$	$R_{a1}$ (структура $A$ )	$r(R_{a1})$	$\delta_A^{(n)}(R, 1)$	$\delta^{(n)}(R, 1)$	
				(3.37)	(3.38)
0,99720	0,99853	0,988	$1,33 \cdot 10^{-7}$	0,000265	0,000400
0,99480	0,99725	0,980	$4,92 \cdot 10^{-7}$	0,000539	0,000800
0,98835	0,99380	0,959	$2,74 \cdot 10^{-7}$	0,001387	0,00200
0,97873	0,98859	0,931	$9,98 \cdot 10^{-8}$	0,002804	0,00402
0,96990	0,98377	0,907	$2,12 \cdot 10^{-8}$	0,004249	0,00600
0,94604	0,97054	0,851	$7,57 \cdot 10^{-8}$	0,006801	0,01240
0,91695	0,95459	0,782	0,000196	0,014659	0,01972
0,85737	0,91921	0,644	0,000673	0,02821	0,03364
0,75925	0,85856	0,434	0,00231	0,05401	0,05784
0,67883	0,80561	0,261	0,00468	0,07684	0,07869
0,61005	0,75771	0,113	0,00780	0,09707	0,09744
0,49667	0,67256	0,000	0,01570	0,13076	0,13076
0,40626	0,59782	0,000	0,02487	0,16022	0,16022
0,33251	0,53100	0,000	0,03738	0,18690	0,18690
0,27159	0,47064	0,000	0,05075	0,21147	0,21147
0,19885	0,39016	0,000	0,07355	0,24517	0,24517
0,13190	0,27807	0,000	0,1051	0,29494	0,29494
0,06092	0,18872	0,000	0,1693	0,33868	0,33868
0,02903	0,11871	0,000	0,2266	0,37773	0,37773
0,00000	0,00000	0,000	0,5000	0,50000	0,50000

Отметим, что при  $R > 0,946$  значения  $\delta^{(n)}(R, 1)$ , вычисляемые по (3.38), больше  $\delta_{\text{вг}}(R)$ , в качестве которой в данном случае была выбрана граница Бассалыго—Элайеса.

На рис. 3.1 видно, что для каскадных кодов первого порядка структуры  $A$  при скоростях передачи  $R < 0,175$  кодовое расстояние принципиально не может достигнуть границы ВГ, так как в этом случае  $\delta^{(n)}(R, 1) < \delta_{\text{вг}}(R)$ .

Для сравнительно небольших значений  $n_a$ , что не исключает достаточно большую общую длину  $n = n_a n_b$  каскадного кода, естественно использовать в качестве внутренних кодов коды БЧХ, которые являются одними из лучших известных в настоящее время

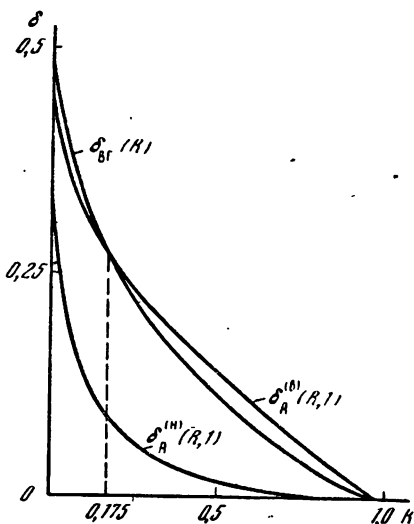


Рис. 3.1. Нижние и верхние оценки кодового расстояния каскадных кодов первого порядка

поэтому ничего нового по сравнению с результатами, полученными в разд. 3.3.1, дать не может.

В качестве примера рассмотрим каскадный код длины  $n=1023$  с параметрами  $n_a=31$ ;  $n_b=33$ ;  $a_1=5\mu$ ;  $\mu=1,6$ . Для каждого  $\mu$  в качестве внутреннего кода выберем код БЧХ  $(31, 5\mu)$  с кодовым расстоянием  $d_{a1}$ , причем для

$$\begin{array}{lll} \mu=1, & d_{a1}=16, & \mu=4, & d_{a1}=6, \\ \mu=2, & d_{a1}=12, & \mu=5, & d_{a1}=4, \\ \mu=3, & d_{a1}=8, & \mu=6, & d_{a1}=2. \end{array}$$

В качестве внешних кодов будем использовать коды РС (33,  $b_1$ ),  $b_1=\overline{1,33}$ , причем для  $\mu=1$  воспользуемся удлинненным кодом РС над полем GF ( $2^5$ ), а при  $\mu > 1$  — укороченным кодом РС над полем GF ( $2^{5\mu}$ ) с кодовым расстоянием, равным во всех случаях  $d_{b1}=n_b-b_1+1=34-b_1$ . Тогда нижняя оценка кодового расстояния таких каскадных кодов первого порядка определяется равенством  $d^{(H)}=d_{a1}(34-k/5\mu)$ , где  $k=5\mu b_1$  — число информационных символов каскадного кода. Результаты расчетов для всех возможных значений  $\mu$  и  $k$  (приведенные в приложении 3.4) показывают, что среди каскадных кодов первого порядка длины  $1023=31 \times 33$  с кодами БЧХ в качестве внутренних и кодами РС в качестве внешних кодов при  $\mu=1$  и  $\mu=2$  существуют такие, кодовое расстояние которых совпадает или незначительно уступает кодовому расстоянию кодов БЧХ ( $d=d_{\text{БЧХ}}$ ) при близком числе информационных сим-

алгебраических двоичных кодов. Предполагая, как и всегда, что  $2^{a_1} \geq n_b-1$ , в качестве внешних кодов будем использовать коды РС.

Тогда, выбирая надлежащим образом длину  $n=n_a n_b$ , можно получить достаточно обширное множество каскадных кодов первого порядка с различными скоростями передачи и оценить снизу кодовое расстояние этих кодов. Нижняя оценка  $\delta(R, 1)$  определяется очевидным равенством

$$\delta^{(H)}(R, 1) = (1 - R/R_{a1}) \delta_{\text{БЧХ}}(R_{a1}), \quad (3.39)$$

где  $\delta_{\text{БЧХ}}(R_{a1})$  — отношение  $d/n_a$  для кода БЧХ.

Верхняя оценка не зависит от характера внутреннего кода и

волов ( $k \simeq k_{\text{БЧХ}}$ ). Параметры этих кодов и значения  $d_{\text{БЧХ}}$  и  $k_{\text{БЧХ}}$  соответствующих кодов БЧХ приведены в табл. 3.2.

Таблица 3.2

$\mu$	$a_1$	$b_1$	$d_{a1}$	$d_{b1}$	$d^{(n)}$	$k$	$d_{\text{БЧХ}}$	$k_{\text{БЧХ}}$
1	5	11	16	23	368	55	384	55
1	5	9	16	25	400	45	400	45
1	5	7	16	27	432	35	448	35
1	5	5	16	29	464	25	480	25
1	5	2	16	32	512	10	512	10
2	10	14	12	20	240	140	254	142
2	10	13	12	21	252	130	256	132

При  $\mu > 2$  кодовое расстояние каскадных кодов первого порядка при всех  $k$  значительно уступает кодовому расстоянию кодов БЧХ при  $k \simeq k_{\text{БЧХ}}$ .

В заключение рассмотрим также представляющий известный интерес вопрос об асимптотическом ( $n \rightarrow \infty$ ) поведении нижней оценки величины  $\delta(R)$  для каскадного кода первого порядка с кодами БЧХ в качестве внутренних кодов.

Для этого воспользуемся хорошо известной [115] (правда, достаточно грубой) нижней оценкой кодового расстояния кодов БЧХ, порождаемых примитивным элементом.

В этом случае после простых преобразований получаем (при весьма больших  $n$ ) для кодов БЧХ

$$\delta_{\text{БЧХ}}^{(n)}(R, n) = 2(1 - R)/\log_2 n, \quad (3.40)$$

а для каскадного кода первого порядка с кодом БЧХ в качестве внутреннего кода  $\delta^{(n)}(R, 1, n) = 2(1 - R_{a1})(1 - R/R_{a1})/(\log_2 \log_2 n - \log_2 R_{a1})$ . Если  $\log_2 n \gg R_{a1}^{-1}$ , то последнее выражение можно заменить равенством  $\delta^{(n)}(R, 1, n) = 2(1 - R_{a1})(1 - R/R_{a1})/\log_2 \log_2 n$ . При заданных значениях  $R$  и  $n$  максимизация правой части этого выражения достигается при  $R_{a1} = \sqrt{R}$ , так что наибольшее значение  $\delta^{(n)}(R, 1, n)$  (при весьма больших  $n$ ) имеет вид

$$\delta^{(n)}(R, 1, n) = 2(1 - \sqrt{R})^2/\log_2 \log_2 n. \quad (3.41)$$

Характерной особенностью полученных оценок является то, что хотя обе они стремятся к нулю при  $n \rightarrow \infty$ , уменьшение  $\delta^{(n)}(R, 1, n)$  для каскадного кода оказывается более медленным, нежели для кодов БЧХ. Таким образом, каскадные коды первого порядка с кодами БЧХ в качестве внутренних и кодами РС в качестве внешних кодов имеют асимптотически лучшие характеристики, нежели сами коды БЧХ.

Как видно из (3.40) и (3.41), если  $n$  удовлетворяет равенству  $(\log_2 \log_2 n)/\log_2 n = (1 - \sqrt{R})/(1 + \sqrt{R})$ , то  $\delta_{\text{БЧХ}}^{(n)}(R, n) = \delta^{(n)}(R, 1, n)$

и при дальнейшем увеличении  $n$  нижняя оценка кодового расстояния каскадного кода первого порядка оказывается выше аналогичной оценки для кодов БЧХ.

Например, при  $R=0,360$  и  $n > 2^{16}=65\,536$  каскадный код будет иметь преимущество (по кодовому расстоянию) перед кодом БЧХ той же длины.

Зависимость между  $n$  и  $R$ , определяющая такие значения, начиная с которых каскадный код 1-го порядка имеет преимущество по кодовому расстоянию перед кодом БЧХ той же длины, следующая:  $R=[(1-\log_2 \log_2 n / \log_2 n) / (1+\log_2 \log_2 n / \log_2 n)]^2$ . Соответствующие этой зависимости значения  $n$  и  $R$  приведены в табл. 3.3.

Таблица 3.3

$n$	$R$	$n$	$R$
1 024	0,251	65 536	0,360
4 096	0,292	262 144	0,389
16 384	0,328	1 048 576	0,404

### 3.3.2. Каскадные коды второго порядка

Каскадные коды второго порядка в отличие от кодов первого порядка могут быть как с равной (РЗ), так и с неравной (НЗ) защитой информационных символов.

Соотношение (3. 5), связывающее скорость передачи  $R$  с нижней оценкой  $\delta_A^{(n)}(R, m)$  кодового расстояния каскадных кодов (РЗ) структуры  $A$  для кодов второго порядка, имеет вид

$$\delta_A^{(n)}(R, 2) = (R_{a1} - R) / \{ (R_{a1} - R_{a2}) / \delta_{\text{ВГ}}(R_{a1}) + R_{a2} / \delta_{\text{ВГ}}(R_{a2}) \}. \quad (3.42)$$

При этом для кодов структуры  $A0$  величины  $R_{a1}$  и  $R_{a2}$  определяются из системы уравнений

$$\partial \delta_A^{(n)}(R, 2) / \partial R_{a1} = 0, \quad \partial \delta_A^{(n)}(R, 2) / \partial R_{a2} = 0. \quad (3.43)$$

Для кодов структуры  $A1$  соотношение (3. 42) принимает вид

$$\delta_{A1}^{(n)}(R, 2) = 2(R_{a1} - R) / \left\{ R_{a1} / \delta_{\text{ВГ}}(R_{a1}) + R_{a1} / \delta_{\text{ВГ}}\left(\frac{1}{2} R_{a1}\right) \right\}. \quad (3.44)$$

При этом максимизирующее  $\delta_{A1}^{(n)}(R, 2)$  значение величины  $R_{a1}$  определяется из уравнения

$$\partial \delta_{A1}^{(n)}(R, 2) / \partial R_{a1} = 0. \quad (3.45)$$

Значения величин  $R_{a1}$  и  $R_{a2}$ , являющихся решением (3. 43), приведены в табл. 3.4, а значения величины  $R_{a1}$ , являющейся решением (3. 45), — в табл. 3.5.

Таблица 3.4

$R$	$R_{a2}$	$R_{a1}$	$R_{a2}/R_{a1}$	$R$	$R_{a2}$	$R_{a1}$	$R_{a2}/R_{a1}$
0,9911	0,945	0,996	0,949	0,4495	0,430	0,673	0,639
0,9822	0,932	0,994	0,938	0,3439	0,340	0,564	0,603
0,9590	0,890	0,984	0,904	0,2378	0,271	0,471	0,575
0,9379	0,853	0,971	0,878	0,1020	0,144	0,278	0,518
0,9061	0,807	0,955	0,845	0,0236	0,058	0,119	0,487
0,8214	0,720	0,919	0,783	0,0027	0,014	0,029	0,482
0,7340	0,643	0,859	0,749	0,0000	0,000	0,000	—
0,5622	0,510	0,758	0,673				

Таблица 3.5

$R$	$R_{a1}$	$R$	$R_{a1}$	$R$	$R_{a1}$
0,9926	0,9961	0,8532	0,9192	0,2456	0,4706
0,9883	0,9938	0,7486	0,8586	0,0998	0,2781
0,9697	0,9878	0,5889	0,7577	0,0249	0,1187
0,9454	0,9705	0,4998	0,6726	0,0027	0,0290
0,9165	0,9546	0,3390	0,5635		

При рассмотрении верхних оценок  $\delta^{(n)}(R, 2)$  ограничимся случаем, когда они определяются утверждением 3.6 для несистематических и утверждением 3.9 для систематических каскадных кодов. Таким образом, для несистематических кодов имеем

$$\delta_{A0}^{(n)}(R, 2) = \delta_{A0}^{(n)}(R, 2)/2\delta_{\text{ВГ}}(R_{a2}) \quad (3.46)$$

и

$$\delta_{A1}^{(n)}(R, 2) = \delta_{A1}^{(n)}(R, 2)/2\delta_{\text{ВГ}}\left(\frac{1}{2}R_{a1}\right), \quad (3.47)$$

а для систематических кодов получаем

$$\delta_{A0}^{(n)}(R, 2) = \delta_{A0}^{(n)}(R, 2) \min \left\{ \frac{1}{2\delta_{\text{ВГ}}(R_{a2})}; \frac{1 - R_{a2}}{2\delta_{\text{ВГ}}(R_{a1})} \right\} \quad (3.48)$$

и

$$\delta_{A1}^{(n)}(R, 2) = \delta_{A1}^{(n)}(R, 2) \min \left\{ \frac{1}{2\delta_{\text{ВГ}}\left(\frac{1}{2}R_{a1}\right)}; \frac{1 - R_{a1}/2}{2\delta_{\text{ВГ}}(R_{a1})} \right\}. \quad (3.49)$$

Обозначим через  $z_0 = R_{a2}/R_{a1}$  такое отношение  $R_{a2}$  к  $R_{a1}$ , при котором имеет место равенство

$$(1 - R_{a2})/\delta_{\text{ВГ}}(R_{a1}) = 1/\delta_{\text{ВГ}}(R_{a2}). \quad (3.50)$$

Значения  $z_0$  в зависимости от  $R_{a1}$  приведены в табл. 3.6 и на рис. 3.2, из которых видно, что при всех значениях  $R_{a1}$  величина  $z_0 \geq 0,685$ .

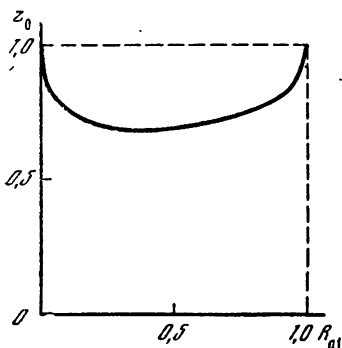


Рис. 3.2. График функции  $z_0 = z(R_{a1})$

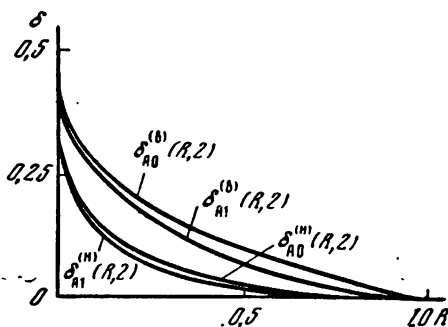


Рис. 3.3. Верхние и нижние оценки кодового расстояния каскадного кода второго порядка структуры  $A$

Для кодов структуры  $A0$  при  $R_{a2}/R_{a1} \leq z_0$  выражение (3.48) совпадает с (3.46), а при  $R_{a2}/R_{a1} > z_0$  выражение (3.48) имеет вид

$$\delta_{A0}^{(n)}(R, 2) = \delta_{A0}^{(n)}(R, 2)(1 - R_{a2})/2\delta_{\text{ВГ}}(R_{a1}). \quad (3.51)$$

Однако, как видно из табл. 3.4, для структуры  $A0$  отношение  $R_{a2}/R_{a1} \leq z_0$ , так что при всех скоростях передачи выражение (3.48) совпадает с (3.46). Точно так же для структуры  $A1$  отношение  $R_{a2}/R_{a1} = 0,5 < z_0$ , следовательно, выражение (3.49) при всех  $R$  совпадает (3.47). Нижние и верхние оценки кодового расстояния каскадных кодов второго порядка, вычисленные по формулам, полученным в настоящем разделе, приведены в табл. 3.7, 3.8 и на рис. 3.3. Как видно из приведенных результатов, для структур  $A0$  и  $A1$  соответствующие оценки весьма незначительно отличаются друг от друга почти во всем диапазоне изменения скорости передачи  $R$ .

Таблица 3.6

$R_{a1}$	$z_0$	$R_{a1}$	$z_0$	$R_{a1}$	$z_0$
0,9987	0,9718	0,8605	0,7815	0,2746	0,6873
0,9969	0,9576	0,8282	0,7656	0,1667	0,7123
0,9905	0,9280	0,7947	0,7523	0,0883	0,7471
0,9720	0,8833	0,7269	0,7305	0,0363	0,8014
0,9483	0,8491	0,6588	0,7144	0,0082	0,8823
0,9213	0,8225	0,5585	0,6985	0,0000	1,0000
0,8918	0,8002	0,4047	0,6871		

Таблица 3.7

$R$	$\delta_{A0}^{(n)}(R, 2)$	$\delta_{A0}^{(n)}(R, 2) = \delta_{A0}^{(n)}(R, 2)$	$R$	$\delta_{A0}^{(n)}(R, 2)$	$\delta_{A0}^{(n)}(R, 2) = \delta_{A0}^{(n)}(R, 2)$
0,9911	0,000015	0,00119	0,4495	0,03083	0,114
0,9822	0,000049	0,00302	0,3439	0,04917	0,140
0,9590	0,00020	0,00684	0,2378	0,07775	0,190
0,9379	0,00041	0,00976	0,1020	0,1487	0,266
0,9061	0,00086	0,0144	0,0236	0,2614	0,362
0,8214	0,00282	0,0290	0,0027	0,3753	0,4350
0,7340	0,00614	0,045	0,0000	0,5000	0,5000
0,5622	0,01783	0,083			

Таблица 3.8

$R$	$\delta_{A1}^{(n)}(R, 2)$	$\delta_{A1}^{(n)}(R, 2) = \delta_{A1}^{(n)}(R, 2)$	$R$	$\delta_{A1}^{(n)}(R, 2)$	$\delta_{A1}^{(n)}(R, 2) = \delta_{A1}^{(n)}(R, 2)$
0,9926	0,000002	0,000010	0,4698	0,02683	0,07777
0,9883	0,000006	0,000025	0,3390	0,04930	0,12431
0,9697	0,000042	0,000186	0,2456	0,07452	0,16784
0,9454	0,000151	0,000657	0,0996	0,15046	0,26159
0,9165	0,000383	0,001628	0,0249	0,25769	0,36004
0,8532	0,00133	0,00563	0,0027	0,37485	0,43689
0,7486	0,00446	0,01652	0,0000	0,50000	0,50000
0,5889	0,01416	0,04577			

### 3.3.3. Коды произвольного порядка

При рассмотрении каскадных кодов порядка  $m > 2$  ограничимся лишь каскадными кодами структуры  $A1$ . В этом случае нижняя оценка  $\delta_{A1}^{(n)}(R, m)$  в соответствии с утверждением 3.1 принимает вид

$$\delta_{A1}^{(n)}(R, m) = \max_{R_{a1}} \left\{ m(R_{a1} - R) \left[ R_{a1} \sum_{i=1}^m \left( \delta_{\text{ВГ}} \left( \frac{m-i+1}{m} R_{a1} \right) \right)^{-1} \right] \right\}. \quad (3.52)$$

Верхняя оценка  $\delta_{A1}^{(n)}(R, m)$  в соответствии с утверждением 3.6 для несистематических кодов

$$\delta_{A1}^{(n)}(R, m) = \delta_{A1}^{(n)}(R, m) / 2\delta_{\text{ВГ}}(R_{a1}/m), \quad (3.53)$$

а в соответствии с утверждением 3.9 для систематических кодов

$$\delta_{A1}^{(n)}(R, m) = \delta_{A1}^{(n)}(R, m) \min_i \left\{ (1 - R_{a, i+1}) / 2\delta_{\text{ВГ}} \left( \frac{m-i+1}{m} R_{a1} \right) \right\}. \quad (3.54)$$



Таблица 3.9

$R$	$\delta_{A1}^{(1)}(R, 3)$	$\delta_{A1}^{(1)}(R, 3) = \delta_{A1}^{(2)}(R, 3)$	$R$	$\delta_{A1}^{(1)}(R, 5)$	$\delta_{A1}^{(1)}(R, 5) = \delta_{A1}^{(2)}(R, 5)$	$R$	$\delta_{A1}^{(1)}(R, 10)$	$\delta_{A1}^{(2)}(R, 10) = \delta_{A1}^{(3)}(R, 10)$
0,9925	$0,32 \cdot 10^{-6}$	$0,92 \cdot 10^{-6}$	0,9925	$0,53 \cdot 10^{-6}$	$1,09 \cdot 10^{-6}$	0,9924	$1,05 \cdot 10^{-6}$	$1,66 \cdot 10^{-6}$
0,9983	$0,82 \cdot 10^{-6}$	$2,34 \cdot 10^{-6}$	0,9882	$1,37 \cdot 10^{-6}$	$2,81 \cdot 10^{-6}$	0,9789	$2,73 \cdot 10^{-6}$	$4,31 \cdot 10^{-6}$
0,9995	$6,33 \cdot 10^{-6}$	$17,9 \cdot 10^{-6}$	0,9689	$10,5 \cdot 10^{-6}$	$21,4 \cdot 10^{-6}$	0,9671	$20,7 \cdot 10^{-6}$	$32,6 \cdot 10^{-6}$
0,9446	0,00023	0,00065	0,9428	0,00037	0,00075	0,9378	0,00071	0,00112
0,9147	0,00057	0,00153	0,9107	0,00093	0,00187	0,9012	0,00169	0,00264
0,8484	0,00200	0,00537	0,8389	0,00305	0,00602	0,8213	0,00500	0,00773
0,7382	0,00630	0,01607	0,7214	0,00918	0,01759	0,6982	0,0131	0,0199
0,5726	0,01880	0,04409	0,5522	0,0247	0,04491	0,5308	0,0312	0,0460
0,4526	0,0340	0,07440	0,4338	0,0421	0,07322	0,4163	0,0500	0,0718
0,3239	0,0593	0,1183	0,3090	0,0695	0,1139	0,2962	0,0789	0,1092
0,2334	0,0864	0,1591	0,2221	0,0980	0,1526	0,2127	0,1082	0,1450
0,0950	0,1645	0,2549	0,0891	0,1772	0,2447	0,0850	0,1880	0,2238
0,0233	0,2701	0,3522	0,0220	0,2810	0,3429	0,0210	0,2900	0,3325
0,00255	0,3822	0,4321	0,00239	0,3887	0,4271	0,00227	0,3939	0,4206
0,0000	0,5000	0,5000	0,0000	0,5000	0,5000	0,0000	0,5000	0,5000

Нетрудно убедиться, что в (3. 54) минимум достигается при  $i=t$ , следовательно, (3. 54) совпадает с (3. 53), т. е. верхняя оценка кодового расстояния систематических и несистематических каскадных кодов структуры А1 одна и та же.

Результаты расчетов по формулам (3. 52) и (3. 53) для  $m=3, 5$  и 10 приведены в табл. 3.9 и на рис. 3.4, на котором для сравнения приведена также оценка  $\delta_{\text{ВГ}}(R)$ . Как видно из графиков, верхние оценки  $\delta_{A1}^{(t)}(R, m)$  почти во всем диапазоне скоростей передачи  $0 < R < 1$  располагаются ниже оценки  $\delta_{\text{ВГ}}(R)$ . Таким образом, при этих скоростях передачи и  $m \geq 3$  не существует каскадных кодов структуры А1, кодовое расстояние которых удовлетворяло бы границе ВГ.

Отметим, что по мере увеличения  $m$  различие между нижней  $\delta_{A1}^{(1)}(R, m)$  и верхней  $\delta_{A1}^{(t)}(R, m)$  оценками для каскадных кодов структуры А1 быстро уменьшается.

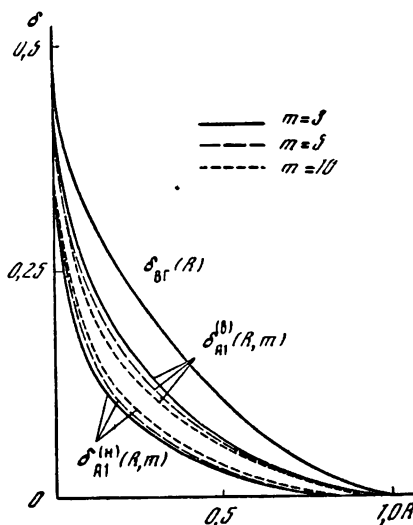


Рис. 3.4. Верхние и нижние оценки кодового расстояния каскадного кода порядка  $m=3, 5, 10$  структуры А1

## § 3.4. Каскадные коды бесконечного порядка

### 3.4.1. Основные ограничения и структура каскадных кодов бесконечного порядка

Перейдем теперь к рассмотрению предельного случая, когда порядок каскадного кода  $m \rightarrow \infty$ . Такие коды назовем каскадными кодами бесконечного порядка.

В соответствии с определением каскадных кодов произвольного (конечного) порядка  $m$  введем величины  $a_{\min}$  и  $a_{\max}$ , представляющие собой наименьшее и наибольшее из чисел  $a_i$ ,  $i=1, m$ .

Предполагаем, как и раньше, что в качестве внешних кодов с основанием  $q=2^{a_i}$  всегда используются либо коды РС, либо их модификации, так что для любого  $i$ ,  $i=1, m$ ,

$$2^{a_i} \geq n_i - 1.$$

Таким образом,

$$2^{a_{\min}} \geq n_i - 1.$$

(3. 55)

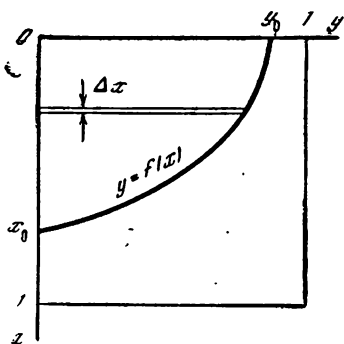


Рис. 3.5. Схематическое представление слова каскадного кода бесконечного порядка

При  $m \rightarrow \infty$  длина  $n_a$  внутренних кодов  $n_a = \sum_{i=0}^m a_i > m a_{\min} \gg m \log_2(n_b - 1) \rightarrow \infty$ . В то же время длина  $n_b$  внешних кодов при  $m \rightarrow \infty$  может оставаться как ограниченной, так и неограниченно расти.

Первый случай не представляет большого интереса, так как наиболее удобными для реализации (при заданном  $n = n_a n_b$ ) являются такие каскадные коды, для которых при всех значениях  $m$  выполняется условие  $n_b > n_a$ .

Поэтому ограничимся рассмотрением лишь таких каскадных кодов, для которых при  $m \rightarrow \infty$  величины  $n_a \rightarrow \infty$  и  $n_b \rightarrow \infty$ , а следовательно, и  $a_{\min} \rightarrow \infty$ . Так как во всех случаях  $m < n_a$ , то при  $m \rightarrow \infty$   $m/n < n_a/n = 1/n_b \rightarrow 0$ , значит  $\frac{a_i}{n_a} \leq \frac{a_i}{n_a - a_0} \leq \frac{a_i}{m a_{\min}} \leq \frac{a_{\max}}{a_{\min}} \frac{1}{m}$ .

В дальнейшем будем рассматривать только такие каскадные коды, для которых при  $m \rightarrow \infty$  отношение  $a_{\max}/a_{\min}$  остается ограниченным, так что

$$\lim_{m \rightarrow \infty} \frac{a_i}{n_a} = 0, \quad i = \overline{1, m}. \quad (3.56)$$

Если при выполнении перечисленных выше условий построить слово  $\alpha$  каскадного кода (порядок которого  $m$  достаточно велик), относя его горизонтальный и вертикальный размеры соответственно к  $n_b$  и  $n_a$ , то получим единичный квадрат, в котором каждый из кодов второй ступени изображается горизонтальной полоской шириной  $\Delta x_i$  ( $\Delta x_i \rightarrow 0$  при  $m \rightarrow \infty$ ).

Предельный случай такого квадрата (при  $m \rightarrow \infty$ ), изображающего кодовое слово  $\alpha$  каскадного кода бесконечного порядка, показан на рис. 3.5. Кривая  $y = f(x)$  полностью определяет структуру каскадного кода бесконечного порядка, т. е. связь между скоростями передачи внутренних  $R_{a_i} = x$  и внешних кодов  $R_{b_i} = y$ . При этом для выполнения условия  $b_i \leq b_{i+1}$  следует в качестве  $f(x)$  выбирать невозрастающую функцию. Возможность характеризовать структуру каскадного кода бесконечного порядка одной лишь функцией  $y = f(x)$  значительно упрощает и делает более обзримым исследование оценок кодового расстояния в зависимости от структуры кода в случае, когда  $m \rightarrow \infty$ , по сравнению со случаями конечных значений  $m$ .

Что касается скорости передачи  $R$  каскадного кода бесконечного порядка, то она определяется очевидным равенством

$$R = \int_0^{x_0} y dx, \quad (3.57)$$

где  $x_0 = R_{a1}$  — скорость передачи основного (первого) внутреннего кода при  $m \rightarrow \infty$ .

Величина  $y_0 = f(0)$ , соответствующая  $x = 0$ , представляет собой скорость передачи последнего внешнего кода при  $m \rightarrow \infty$ , так что  $y_0 = R_{b\infty}$ . В заключение отметим частный случай, когда  $a_{\min}/a_{\max} = 1$ , т. е. такой, для которого  $a_i = a$ ,  $i = 1, m$ , следовательно,  $n_a = a_0 + ma$ . Полагая  $n_b = 2^a$  и выбирая  $a = \log_2 Am'$ , где  $A$  и  $v$  — произвольные положительные числа, приходим к каскадным кодам, для которых  $n_b = Am'$ ,  $n_a = a_0 + m \log_2 A + vm \log_2 m$ , так что при  $v \rightarrow 1$  и  $m \rightarrow \infty$

$$\lim_{m \rightarrow \infty} \frac{n_a - a_0}{n_b} = 0.$$

### 3.4.2. Нижние и верхние оценки кодового расстояния каскадных кодов бесконечного порядка

Рассмотрим сначала нижнюю оценку кодового расстояния, основанную на результате, полученном в разд. 2.2.2, согласно которому кодовое расстояние любого каскадного кода удовлетворяет неравенству  $d \geq \min \{d_{ai}, d_{bi}\}$ . Так как при  $n_a \rightarrow \infty$  и  $n_b \rightarrow \infty$  кодовое расстояние всех внутренних кодов может достигать границ ВГ, т. е. при  $m \rightarrow \infty$   $d_{ai} \geq n_a \delta_{ВГ}(R_{ai}) = n_a \delta_{ВГ}(x)$ , а кодовое расстояние внешних кодов

$$d_{bi} = n_b (1 - R_{bi} + 1/n_b) \simeq n_b (1 - y),$$

получаем, что существуют каскадные коды бесконечного порядка, для которых  $\delta(R) = d/n \geq \min_x \{(1 - y) \delta_{ВГ}(x)\}$ , где  $y = f(x)$  определяет структуру кода.

Величина

$$\delta^{(n)}(R) = \min_x \{(1 - y) \delta_{ВГ}(x)\} \quad (3.58)$$

представляет собой нижнюю оценку величины  $\delta(R)$  для каскадных кодов бесконечного порядка.

Эта оценка, справедливая как для систематических, так и не-систематических каскадных кодов, определяется структурой кода  $y = f(x)$ .

Если функция  $\delta_x^{(n)} = (1 - y) \delta_{ВГ}(x)$  монотонно убывает при увеличении  $x$ , то минимум достигается при  $x = x_0 = R_{a1}$  (когда  $y = 0$ ), так что  $\delta^{(n)}(R) = \delta_{ВГ}(R_{a1}) = \delta_{ВГ}(x_0)$ . При этом возможна

только равная защита информационных символов. Если же  $\delta_x^{(n)}$  возрастает при увеличении  $x$ , то минимум достигается при  $x=0$ , так что  $\delta^{(n)}(R) = 1/2(1 - y_0)$ ; при этом возможна неравная защита информационных символов.

Для построения верхних оценок каскадного кода бесконечного порядка воспользуемся простейшими оценками (3.19) и (3.30), полученными в разд. 3.2.1 и 3.2.3, которые соответствуют условию  $r_i = 0$ . Использование этого условия вполне допустимо, так как в рассматриваемом случае все  $R_{a_i} - R_{a_{i+1}} \rightarrow 0$ .

Тогда, заменяя в выражениях (3.19) и (3.30) скорости передачи внутренних и внешних кодов соответственно на  $x$  и  $y$ , получаем верхние оценки величины  $\delta(R)$  соответственно для несистематических каскадных кодов бесконечного порядка

$$\delta^{(n)}(R) = \frac{1}{2} \min_x \{1 - y\}, \quad (3.59)$$

$$\xi^{(n)}(R) = \frac{1}{2} \min_x \{(1 - y)(1 - x)\}. \quad (3.60)$$

Так как мы рассматриваем каскадные коды, у которых величина  $f(x)$  не возрастает с увеличением  $x$ , то при любой структуре (удовлетворяющей этому условию) для несистематических кодов верхняя оценка  $\delta^{(n)}(R) = 1/2(1 - y_0)$ . Что касается систематических кодов, то для них  $\delta^{(n)}(R) = 1/2(1 - y_0) = \delta^{(n)}(R)$ , если функция  $\delta^{(n)}(R) = (1 - y)(1 - x)$  возрастает, и  $\delta^{(n)}(R) = 1/2(1 - x_0)$ , если  $\delta_x^{(n)} = (1 - y)(1 - x)$  убывает.

### 3.4.3. Коды структуры А

Для каскадных кодов бесконечного порядка структура А определяется равенством  $\delta_x^{(n)} = (1 - y)\delta_{\text{ВГ}}(x) = \text{const.}$  Так как в этом случае  $\delta_A^{(n)}(R, \infty) = \delta_x^{(n)}$  при всех  $x$ , то, полагая  $x=0$ , получаем  $\delta_A^{(n)}(R, \infty) = 1/2(1 - y_0)$ . Учитывая, что при этом верхние оценки

$$\delta_A^{(n)}(R, \infty) = \frac{1}{2} \min_x (1 - y) = \frac{1}{2} (1 - y_0) = \delta_A^{(n)}(R, \infty)$$

и

$$\xi_A^{(n)}(R, \infty) = \frac{1}{2} \min_x \{(1 - y)(1 - x)\} = \frac{1}{2} (1 - y_0) = \delta_A^{(n)}(R, \infty),$$

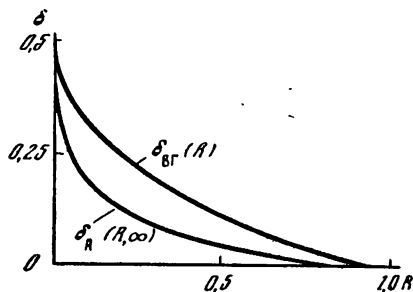
видим, что для каскадных кодов бесконечного порядка структуры А (как систематических, так и несистематических) нижняя и верхние оценки совпадают:  $\delta_A^{(n)}(R, \infty) = \xi_A^{(n)}(R, \infty) = \delta_A^{(n)}(R, \infty) = \delta_A(R, \infty)$ . Таким образом, для таких кодов получаем асимптотически точное значение  $\delta(R) = d/n$ , причем структура А определяется выражением  $y = 1 - \delta_A(R, \infty)/\delta_{\text{ВГ}}(x)$ , а скорость пере-

дачи  $R$  каскадного кода бесконечного порядка структуры  $A$  в соответствии с (3.57) равна

$$R = x_0 - \delta_A(R, \infty) \int_0^{x_0} \frac{dx}{\delta_{BG}(x)},$$

где величина  $x_0$  находится из уравнения  $\delta_{BG}(x_0) = \delta_A(R, \infty)$  или  $x_0 = 1 - H(\delta_A(R, \infty))$ . Значения интеграла  $I(x) = \int_0^x \frac{du}{\delta_{BG}(u)}$  приведены в приложении 3.5. Полученные соотношения позволяют

Рис. 3.6. Асимптотически точная оценка кодового расстояния каскадного кода бесконечного порядка структуры  $A$



вычислить  $\delta_A(R, \infty)$  и построить для каждого  $R$  функцию  $y = f(x)$ , определяющую структуру  $A$  каскадного кода бесконечного порядка.

Результаты соответствующих расчетов приведены в табл. 3.10 и на рис. 3.6, на котором для сравнения показан график функции  $\delta_{BG}(R)$ .

Таблица 3.10

$R$	$\delta_A(R, \infty)$	$\delta_A(R, \infty) / \delta_{BG}(R)$	$R$	$\delta_A(R, \infty)$	$\delta_A(R, \infty) / \delta_{BG}(R)$
0,99977	0,0000016	0,125	0,66097	0,01999	0,318
0,99966	0,0000025	0,125	0,61461	0,02500	0,332
0,99897	0,000009	0,136	0,57376	0,02999	0,345
0,99815	0,000018	0,143	0,50383	0,03999	0,368
0,99701	0,000033	0,148	0,44550	0,04999	0,388
0,99453	0,000068	0,156	0,35283	0,06997	0,423
0,99241	0,000102	0,162	0,25231	0,09997	0,469
0,98724	0,000196	0,172	0,14486	0,14993	0,536
0,95538	0,00100	0,204	0,08067	0,19991	0,598
0,90095	0,00300	0,234	0,04207	0,24990	0,658
0,85927	0,00500	0,251	0,00723	0,349814	0,780
0,80770	0,00799	0,270	0,000015	0,44926	0,915
0,77792	0,01000	0,280	0,00000	0,50000	1,000

Как видно из рис. 3.6, значения  $\delta_A(R, \infty)$  для каскадных кодов бесконечного порядка структуры  $A$  во всем диапазоне изменения скорости передачи  $0 < R < 1$  не достигают границы ВГ.

Следует отметить, что каскадные коды бесконечного порядка структуры  $A$  представляют собой уникальный пример блочных двоичных кодов, у которых  $d/n$  не стремится к нулю при  $n \rightarrow \infty$  и асимптотически точно известно кодовое расстояние  $d = n\delta_A(R, \infty)$ .

### 3.4.4. Коды структуры $B$

Для каскадных кодов бесконечного порядка введем, кроме структуры  $A$ , другие характерные структуры, которые будут в дальнейшем (см. гл. 5) играть существенную роль при исследовании потенциальных корректирующих свойств каскадных кодов.

Одну из этих структур, которую определим из условия максимизации скорости передачи  $R$  систематического каскадного кода при заданной верхней оценке  $\delta^{(n)}(R, \infty)$ , назовем структурой  $B$ . Для каскадных кодов структуры  $B$  оценки  $\delta^{(n)}(R, \infty)$ ,  $\delta_B^{(n)}(R, \infty)$ ,  $\delta_B^{(n)}(R, \infty)$  будем обозначать соответственно  $\delta_B^{(n)}(R, \infty)$ ,  $\delta_B^{(n)}(R, \infty)$ ,  $\delta_B^{(n)}(R, \infty)$ . Структура  $B$  определяется следующим утверждением, доказанным в приложении 3.6.

**Утверждение 3.11.** В систематическом каскадном коде бесконечного порядка (с нижней треугольной кодирующей матрицей  $G_0$ ) структура

$$y = f_B(x) = 1 - 2\delta_B^{(n)}(R, \infty)/(1 - x) \quad (3.61)$$

при заданной верхней оценке  $\delta_B^{(n)}(R, \infty)$  максимизирует скорость передачи  $R$ .

Подставляя (3.61) в выражение для скорости передачи, получаем

$$R = x_0 - 2\delta_B^{(n)}(R, \infty) \int_0^{x_0} \frac{dx}{1-x} = x_0 + 2\delta_B^{(n)}(R, \infty) \ln(1 - x_0), \quad (3.62)$$

где значение  $x_0 < 1$  находится из условия  $f_B(x_0) = 0$ , которое приводит к равенству

$$x_0 = 1 - 2\delta_B^{(n)}(R, \infty). \quad (3.63)$$

Так как в данном случае функция  $(1 - f(x)) \delta_{BG}(x)$  убывает с ростом  $x$ , то нижняя оценка  $\delta_B^{(n)}(R, \infty)$  в соответствии с выражением (3.58) принимает вид

$$\delta_B^{(n)}(R, \infty) = \delta_{BG}(x_0). \quad (3.64)$$

Так как для несистематических каскадных кодов бесконечного порядка верхняя оценка определяется выражением (3.59), то для таких кодов структуры  $B$  имеем  $\delta_B^{(n)}(R, \infty) = \frac{1}{2}(1 - f_B(0))$ , что согласно выражению (3.61) приводит к равенству  $\delta_B^{(n)}(R, \infty) = \delta_B^{(n)}(R, \infty)$ .

Используя соотношения (3.62)–(3.64), можно для каждого  $R$  вычислить оценки  $\delta_B^{(u)}(R, \infty)$  и  $\delta_B^{(n)}(R, \infty)$ . Результаты соответствующих расчетов приведены в табл. 3.11 и на рис. 3.7. Там же представлено отношение  $\delta_B^{(u)}(R, \infty)/\delta_{\text{ВГ}}(R)$ .

Так как это отношение для всех скоростей передачи меньше единицы, то, учитывая, что структура  $B$  определяет для каждого значения  $R$  максимально возможную величину верхней оценки кодового расстояния систематического каскадного кода бесконечного порядка, следовательно, получаем, что среди этих кодов нет таких, кодовое расстояние которых достигает границы ВГ.

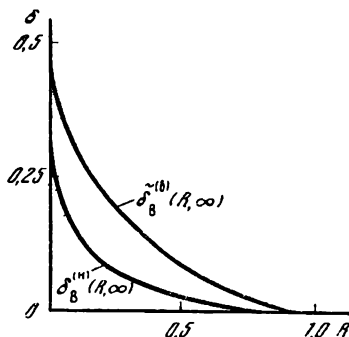


Рис. 3.7. Верхние и нижние оценки кодового расстояния каскадного кода бесконечного порядка структуры  $B$

Таблица 3.11

$R$	$\delta_B^{(u)}(R, \infty)$	$\delta_B^{(n)}(R, \infty)$	$\delta_B^{(u)}(R, \infty)/\delta_{\text{ВГ}}(R)$	$R$	$\delta_B^{(u)}(R, \infty)$	$\delta_B^{(n)}(R, \infty)$	$\delta_B^{(u)}(R, \infty)/\delta_{\text{ВГ}}(R)$
0,9020	0,0019	0,010	0,787	0,2342	0,0795	0,200	0,896
0,7711	0,0070	0,0300	0,806	0,1533	0,1100	0,250	0,912
0,6703	0,0130	0,0500	0,822	0,0940	0,1461	0,300	0,933
0,6262	0,0163	0,0600	0,830	0,0501	0,1894	0,350	0,949
0,5000	0,0284	0,0933	0,848	0,0215	0,2432	0,400	0,966
0,4782	0,0312	0,100	0,851	0,0052	0,3163	0,450	0,983
0,3391	0,0532	0,150	0,875	0,0000	0,500	0,500	1,000

### 3.4.5. Коды структуры $C$

Рассмотрим несистематические каскадные коды бесконечного порядка и для них найдем структуру  $y=f(x)$ , такую, которая при заданной верхней оценке  $\delta^{(u)}(R, \infty)$ , максимизирует скорость передачи  $R$ . Эта структура определяется следующим утверждением.

Утверждение 3.12. В несистематическом каскадном коде бесконечного порядка структура  $y=f(x)=1-2\delta^{(u)}(R, \infty)$  при заданной верхней оценке  $\delta^{(u)}(R, \infty)$  и  $x_0=1$  максимизирует скорость передачи  $R$ . Отсюда следует, что

$$\delta^{(u)}(R, \infty) = (1 - R)/2 > \delta_{\text{ВГ}}(R), \quad 0 < R < 1. \quad (3.65)$$

Доказательство утверждения 3.12 аналогично доказательству утверждения 3.11 (см. приложение 3.6). Утверждение 3.12 в отличие от утверждения 3.11 не приводит к новым результатам,



относящимся к верхним оценкам кодового расстояния, так как в результате получена известная верхняя граница Плоткина, справедливая для любых блочных двоичных кодов. Однако, учитывая (3.65), можно поставить задачу об отыскании таких структур несистематического каскадного кода бесконечного порядка, для которых верхняя оценка  $\delta^{(n)}(R, \infty)$  совпадает с границей ВГ. Одну из таких структур, которая, так же как и структура  $B$ , будет играть важную роль при изучении потенциальных корректирующих свойств каскадных кодов, назовем структурой  $C$ . Соответствующие ей нижнюю и верхние оценки будем обозначать  $\delta_{\text{ВГ}}^{(n)}(R, \infty)$ ,  $\delta_{\text{ВГ}}^{(n)}(R, \infty)$  и  $\delta_{\text{ВГ}}^{(n)}(R, \infty) = \delta_{\text{ВГ}}(R)$ . Структура  $C$  определяется следующим утверждением, доказанным в приложении 3.7.

**Утверждение 3.13.** Структура

$$y = f_c(x) = 1 - \delta_{\text{ВГ}}^{(n)}(R, \infty) 2^{1-x} / (2^{1-x} - 1) \quad (3.66)$$

определяет несистематический каскадный код бесконечного порядка, для которого верхняя оценка  $\delta_{\text{ВГ}}^{(n)}(R, \infty)$  при всех  $R: 0 \leq R \leq 1$  совпадает с границей ВГ, т. е.

$$\delta_{\text{ВГ}}^{(n)}(R, \infty) = \delta_{\text{ВГ}}(R). \quad (3.67)$$

Таким образом, структура  $C$  определяется равенством

$$y = f_c(x) = 1 - \delta_{\text{ВГ}}(R) 2^{1-x} / (2^{1-x} - 1). \quad (3.68)$$

Нижняя оценка  $\delta_{\text{ВГ}}^{(n)}(R, \infty)$  для каскадного кода бесконечного порядка структуры  $C$  находится из выражения  $\delta_{\text{ВГ}}^{(n)}(R, \infty) = \min_{0 \leq x \leq x_0} \{(1-y) \delta_{\text{ВГ}}(x)\}$ . Так как функция  $(1-y) \delta_{\text{ВГ}}(x) = \delta_{\text{ВГ}}(R) 2^{1-x} \delta_{\text{ВГ}}(x) / (2^{1-x} - 1)$  убывает с ростом  $x$ , то минимум достигается при  $x = x_0$ , когда  $y = 0$ .

Таким образом,

$$\delta_{\text{ВГ}}^{(n)}(R, \infty) = \delta_{\text{ВГ}}(x_0), \quad (3.69)$$

где  $x_0 = 1 + \log_2(1 - \delta_{\text{ВГ}}(R)) = \log_2\{2(1 - \delta_{\text{ВГ}}(R))\}$ .

Верхняя оценка  $\delta_{\text{ВГ}}^{(n)}(R, \infty)$  для систематического каскадного кода бесконечного порядка структуры  $C$  находится из выражения

$$\delta_{\text{ВГ}}^{(n)}(R, \infty) = \frac{1}{2} \min_{0 \leq x \leq x_0} \{(1-y)(1-x)\}.$$

Так как функция  $(1-y)(1-x) = \delta_{\text{ВГ}}(R) 2^{1-x}(1-x) / (2^{1-x} - 1)$  убывает с ростом  $x$ , то минимум достигается при  $x = x_0$ , когда  $y = 0$ , так что

$$\delta_{\text{ВГ}}^{(n)}(R, \infty) = \frac{1}{2}(1 - x_0) = -\frac{1}{2} \log_2(1 - \delta_{\text{ВГ}}(R)). \quad (3.70)$$

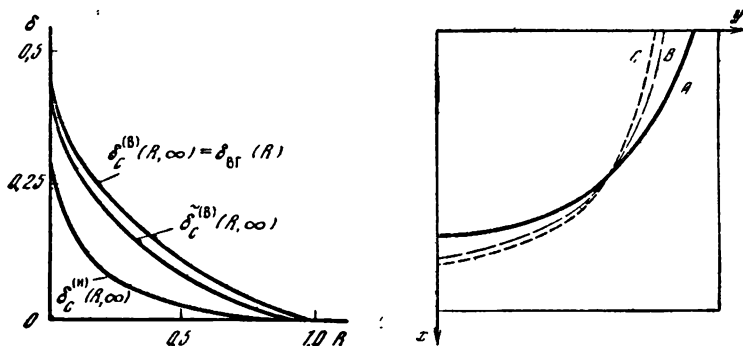


Рис. 3.8. Верхние и нижние оценки кодового расстояния каскадного кода бесконечного порядка структуры  $C$

Рис. 3.9. Структуры  $A$ ,  $B$ ,  $C$  каскадных кодов бесконечного порядка со скоростью передачи  $R=0,5$

Используя выражения (3. 69), (3. 67) и (3. 70), можно для каждого значения  $R$  вычислить  $\delta_C^{(H)}(R, \infty)$ ,  $\delta_C^{(B)}(R, \infty)$ ,  $\delta_C^{(B)}(R, \infty)$ . Результаты соответствующих расчетов приведены в табл. 3.12 и на рис. 3.8.

Таблица 3.12

$R$	$\delta_C^{(H)}(R, \infty)$	$\delta_C^{(B)}(R, \infty)$	$\delta_C^{(B)}(R, \infty) = \delta_{BF}(R)$	$R$	$\delta_C^{(H)}(R, \infty)$	$\delta_C^{(B)}(R, \infty)$	$\delta_C^{(B)}(R, \infty) = \delta_{BF}(R)$
0,919	0,0013	0,007	0,010	0,390	0,0382	0,1170	0,150
0,805	0,0048	0,022	0,030	0,278	0,0587	0,1610	0,200
0,673	0,0113	0,0445	0,060	0,189	0,0877	0,2075	0,250
				0,119	0,1150	0,2575	0,300
0,598	0,0163	0,0600	0,080	0,029	0,2080	0,3685	0,400
0,531	0,0220	0,0760	0,100	0,007	0,2850	0,4313	0,450
0,471	0,0280	0,0920	0,120	0,000	0,5000	0,5000	0,500

Как видно из табл. 3.12 и рис. 3.8, при всех скоростях передачи  $R : 0 < R < 1$  для каскадных кодов бесконечного порядка структуры  $C$   $\delta_C^{(H)}(R, \infty) < \delta_C^{(B)}(R, \infty) < \delta_C^{(B)}(R, \infty) = \delta_{BF}(R)$ .

Для иллюстрации различия между структурами  $A$ ,  $B$  и  $C$  на рис. 3.9 приведены графики функций  $y=f(x)$ , определяющие каждую из этих структур при одной и той же скорости передачи  $R=0,5$ .

## § 3.5. Анализ уровней защиты каскадных кодов НЗ

### 3.5.1. Каскадные коды НЗ второго порядка

Переходя к рассмотрению каскадных кодов НЗ, заметим, что коды второго порядка представляют собой простейший тип каскадных кодов, для которых возможна неравная защита информационных

символов. Так как в данном случае возможны лишь две градации уровней защиты  $\delta^{(1)}$  и  $\delta^{(2)}$ , то выражение (3.13), определяющее нижние оценки уровней защиты, принимает вид

$$R = R_{a1} - \delta^{(1,n)} (R_{a1} - R_{a2}) / \delta_{\text{ВГ}}(R_{a1}) - \delta^{(2,n)} R_{a2} / \delta_{\text{ВГ}}(R_{a2}), \quad (3.71)$$

при этом

$$R_{b1} = 1 - \delta^{(1,n)} / \delta_{\text{ВГ}}(R_{a1}), \quad R_{b2} = 1 - \delta^{(2,n)} / \delta_{\text{ВГ}}(R_{a2}), \quad (3.72)$$

$$\text{а } R^{(1)} = (R_{a1} - R_{a2}) R_{b1}, \quad R^{(2)} = R_{a2} R_{b2}. \quad (3.73)$$

Исключая при помощи равенств (3.72) величины  $R_{b1}$ ,  $R_{b2}$  из (3.73), получаем выражения

$$R^{(1)} = (R_{a1} - R_{a2}) (1 - \delta^{(1,n)} / \delta_{\text{ВГ}}(R_{a1})), \quad (3.74)$$

$$R^{(2)} = R_{a2} (1 - \delta^{(2,n)} / \delta_{\text{ВГ}}(R_{a2})), \quad (3.75)$$

удобные для решения первой из сформулированных в разд. 3.12 задач для кодов с неравной защитой, которая состоит в максимизации  $R^{(1)}$  при заданных значениях  $\delta^{(1,n)}, \delta^{(2,n)} \leq \delta^{(1,n)}, R^{(2)}$ .

Для решения этой задачи будем задавать различные значения  $R_{a2}$  и для каждого из них по (3.75) находить  $R^{(2)}$ . Затем для каждого из выбранных  $R_{a2}$  находим  $R_{a1} = R_{a1}^*$ , максимизирующее величину  $R_1$ , определяемую выражением (3.74).

Учитывая, что  $R^{(2)}$  достигает максимума при некотором  $R_{a2} = R_{a2}^*$ , отметим три возможных варианта, определяемых различными (фиксированными) значениями  $\delta^{(1,n)}, \delta^{(2,n)}$ :

- 1) при  $R_{a2} = R_{a2}^*$   $R^{(1)} > 0$ ;
- 2) при  $R_{a2} = R_{a2}^*$   $R^{(1)} = 0$ ;
- 3) при  $R_{a2} < R_{a2}^*$   $R^{(1)} = 0$ .

Соответствующая этим трем случаям зависимость между  $R^{(1)}$  и  $R^{(2)}$  схематически показана на рис. 3.10, где различные кривые отвечают одному и тому же значению  $\delta^{(1,n)}$ , но различным  $\delta^{(2,n)} \leq \delta^{(1,n)}$ .

Следует отметить, что каскадные коды с параметрами  $R_{a1} = R_{a1}^*$  и  $R_{a2} > R_{a2}^*$  не представляют практического интереса, так как при  $R_{a2} < R_{a2}^*$  существует каскадный код с тем же значением  $R^{(2)}$ , но большим значением  $R^{(1)}$ . Поэтому участки кривых, соответствующих значениям  $R_{a2} > R_{a2}^*$ , показанные на рис. 3.10 пунктиром, могут быть отброшены. Точка  $M$  на кривой  $\delta^{(1,n)} = \delta^{(2,n)}$ , касательная в которой отсекает на осях координат равные отрезки  $R_M = R^{(1)} + R^{(2)}$ , определяет каскадный код второго порядка, для которого при равной защите информационных символов достигается наибольшая скорость передачи  $R = R_M$ . Для такого кода все информационные символы можно произвольно разбить на две части по  $nR^{(1)}$  и  $nR^{(2)}$  символов в каждой при условии, что  $R^{(1)} + R^{(2)} = R_M$ . Но это значит, что неравную защиту целесообразно осуществлять только в том случае, если для выбранных значений  $\delta^{(1,n)}$  и  $\delta^{(2,n)} < \delta^{(1,n)}$  точка с координатами  $R^{(1)}$  и  $R^{(2)}$  лежит выше

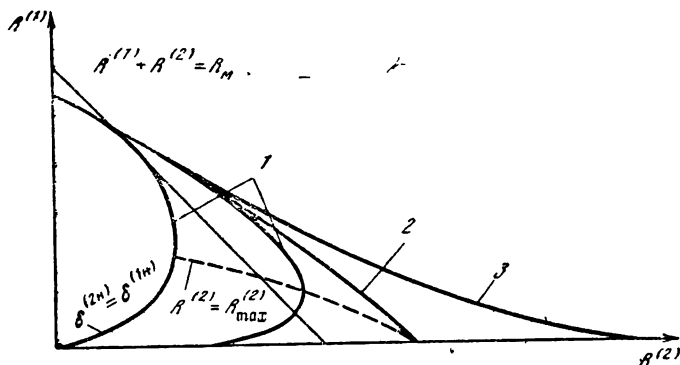


Рис. 3.10. Зависимость между  $R^{(1)}$  и  $R^{(2)}$  при различных уровнях неравной защиты для каскадных кодов второго порядка

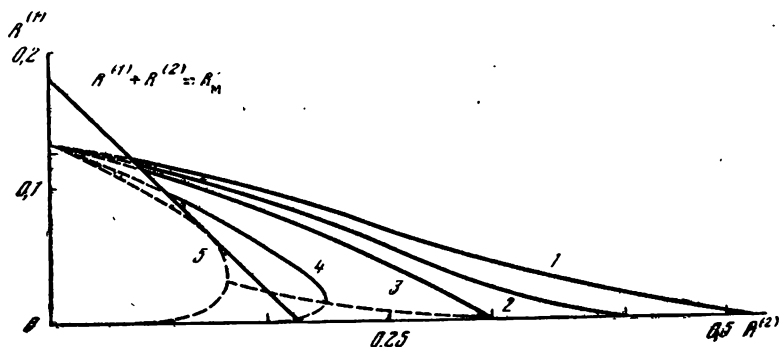


Рис. 3.11. Зависимость между  $R^{(1)}$  и  $R^{(2)}$

1 —  $\delta^{(1n)} = 0,1$  и  $\delta^{(2n)} = 0,000$ ; 2 —  $0,020$ ; 3 —  $0,0374$ ; 4 —  $0,070$ ; 5 —  $0,1$  для каскадных кодов второго порядка

прямой  $R^{(1)} + R^{(2)} = R_M$ . Поэтому можно исключить из рассмотрения также и те части кривых, показанных на рис. 3.10, которые расположены ниже прямой  $R_M = R^{(1)} + R^{(2)}$ .

Результаты соответствующих расчетов для  $\delta^{(1, n)} = 0,1$  и  $\delta^{(2, n)} = 0,000; 0,020; 0,0374; 0,070$  и  $0,1$  приведены в табл. 3.13 и на рис. 3.11, на котором удалены те участки кривых, где  $R_{a2} > R_{a2}^*$ , и те, которые располагаются ниже прямой  $R^{(1)} + R^{(2)} = R_M$ .

Значение  $\delta^{(2, n)} = 0,0374$  определяет при  $\delta^{(1, n)} = 0,1$  ту кривую, для которой  $R^{(1)} = 0$  при  $R_{a2} = R_{a2}^*$ .

Как видно из рис. 3.11, при весьма малых значениях  $R^{(2)}$  нецелесообразно применять коды НЗ. Вместо этого надо использовать оптимальный каскадный код второго порядка, т. е. код структуры А0 с  $\delta^{(n)} = \delta^{(1n)}$ . Это замечание справедливо при  $\delta^{(1n)} = 0,1$  для  $R^{(2)} < 0,067$ .

Таблица 3.13

$R_{a1}$	$R_{a2}$	$R^{(1)}$	$R^{(2)}$				
			$\delta^{(2, \pi)} = 0,10$	0,07	0,0374	0,020	0,000
0,5310	0,5310	0,0000	0,0000	0,1593	0,3324	0,4248	0,531
0,5001	0,4669	0,0030	0,0820	0,1975	0,3230	0,03899	0,4669
0,4706	0,4017	0,0115	0,1255	0,2084	0,2984	0,3464	0,4017
0,4426	0,3356	0,0247	0,1416	0,1998	0,2630	0,2968	0,3356
0,4158	0,2691	0,0419	0,1375	0,1770	0,2199	0,2428	0,2691
0,3902	0,2095	0,0627	0,1186	0,1439	0,1711	0,1857	0,2025
0,3657	0,1360	0,0861	0,0885	0,1028	0,1183	0,1265	0,1360
0,3423	0,0701	0,1121	0,0070	0,0559	0,0625	0,0660	0,0701
0,3199	0,0049	0,1400	0,0038	0,0042	0,0045	0,0047	0,0049

Переходя к рассмотрению верхних оценок уровней защиты  $\delta^{(1, \pi)}$  и  $\delta^{(2, \pi)}$  для несистематических и  $\delta^{(1, \pi)}$  и  $\delta^{(2, \pi)}$  для систематических каскадных кодов НЗ, воспользуемся наиболее простой связью между ними и нижними оценками  $\delta^{(1\pi)}$  и  $\delta^{(2\pi)}$ . Эта связь определяется выражениями (3.24) и (3.33), которые для каскадных кодов второго порядка принимают вид

$$\delta^{(1, \pi)} = \delta^{(1, \pi)} / 2\delta_{\text{ВГ}}(R_{a1}); \quad \delta^{(2, \pi)} = \delta^{(2, \pi)} / 2\delta_{\text{ВГ}}(R_{a2}), \quad (3.76)$$

$$\delta^{(1, \pi)} = \delta^{(1, \pi)} (1 - R_{a1}) / 2\delta_{\text{ВГ}}(R_{a1}); \quad \delta^{(2, \pi)} = \delta^{(2, \pi)} / 2\delta_{\text{ВГ}}(R_{a2}) = \delta^{(2, \pi)}. \quad (3.77)$$

Располагая величинами  $R_{a1}$  и  $R_{a2}$  (см. табл. 3.13), которые определяют  $R^{(1)}$  и  $R^{(2)}$  при фиксированных значениях  $\delta^{(1, \pi)}$  и  $\delta^{(2, \pi)}$ , и используя равенства (3.76) и (3.77), легко найти верхние оценки уровней защиты.

Для решения второй задачи неравной защиты информационных символов, которая состоит в максимизации величины  $\delta^{(1, \pi)}$  при заданных значениях  $R^{(1)}$ ,  $R^{(2)}$ ,  $\delta^{(2, \pi)} < \delta^{(1, \pi)}$ , перепишем выражения (3.74) и (3.75) в виде

$$\delta^{(1, \pi)} = (1 - R^{(1)}) / (R_{a1} - R_{a2}) \delta_{\text{ВГ}}(R_{a1}), \quad (3.78)$$

$$\delta^{(2, \pi)} = (1 - R^{(2)} / R_{a2}) \delta_{\text{ВГ}}(R_{a2}). \quad (3.79)$$

Тогда, задавая различные назначения  $R_{a2}$  для каждого из них по (3.79), находим  $R^{(2)}$ , затем для выбранного  $R_{a2}$  находим  $R_{a1} = R_{a1}^*$ , максимизирующее величину  $\delta^{(1\pi)}$ , определяемую выражением (3.78).

Верхние оценки  $\delta^{(1, \pi)}$ ,  $\delta^{(2, \pi)}$  и  $\delta^{(1\pi)}$ ,  $\delta^{(2\pi)}$ , так же как и для первой задачи, определяются выражениями (3.76), (3.77), только теперь следует их рассматривать как функции одной из величин  $\delta^{(1\pi)}$  или  $\delta^{(2\pi)}$  при фиксированных значениях  $R^{(1)}$  и  $R^{(2)}$ .

### 3.5.2. Каскадные коды НЗ произвольного порядка

Для каскадных кодов произвольного порядка  $m > 2$  с двумя уровнями защиты, т. е. для кодов НЗ структуры 2А (см. разд. 3.1.2), справедливо равенство (3.13). При этом имеют место очевидные соотношения

$$R^{(1)} = (R_{a1} - R_{a, m+1}) - \delta^{(1, n)} \sum_{i=1}^{m_1} (R_{ai} - R_{a, i+1}) / \delta_{\text{вг}}(R_{ai}), \quad (3.80)$$

$$R^{(2)} = R_{a, m+1} - \delta^{(2, n)} \sum_{i=m_1+1}^m (R_{ai} - R_{a, i+1}) / \delta_{\text{вг}}(R_{ai}). \quad (3.81)$$

Как видно из сопоставления с (3.4), выражение (3.81) определяет нижнюю оценку кодового расстояния каскадного кода структуры А порядка  $m - m_1$  с равной защитой информационных символов  $\delta_A^{(n)} = \delta^{(2n)}$  и скоростью передачи  $R = R^{(2)}$ .

В рассматриваемом случае (когда  $m - m_1 > 1$ ) решение в наиболее общем виде как первой, так и второй задачи неравной защиты наталкивается на трудности, которые проиллюстрируем на простейшем (после  $m=2$ ) примере  $m=3$ .

При  $m=3$  и  $m_1=1$  выражения (3.80) и (3.81) принимают вид

$$R^{(1)} = (R_{a1} - R_{a2})(1 - \delta^{(1, n)} / \delta_{\text{вг}}(R_{a1})), \quad (3.82)$$

$$R^{(2)} = R_{a2} - ((R_{a2} - R_{a3}) / \delta_{\text{вг}}(R_{a2}) + R_{a3} / \delta_{\text{вг}}(R_{a3})) \delta^{(2, n)}. \quad (3.83)$$

Тогда для решения без каких-либо дополнительных ограничений, например, первой задачи неравной защиты надо выбрать такие  $R_{a2}$  и  $R_{a3}$ , которые при фиксированном  $\delta^{(2n)}$  приведут к заданному значению  $R^{(2)}$ . Учитывая, что таких пар  $R_{a2}$ ,  $R_{a3}$  имеется бесчисленное множество, надо определить такую пару, чтобы при последующей максимизации (3.82) по  $R_{a1}$  (при выбранном уже  $R_{a2}$ ) мы получили наибольшее из возможных значение  $R^{(1)}$ . Трудности выбора  $R_{ai}$ ,  $i = m_1 + 1, m$ , удовлетворяющих этому требованию, существенно возрастают с увеличением разности  $m - m_1$ . Однако при больших значениях  $m_1$  и  $m - m_1$  можно решать рассматриваемую задачу при дополнительных ограничениях, налагаемых на  $R_{ai}$ ,  $i = 1, m$ , полагая, что все  $R_{ai} - R_{a, i+1} = (R_{a1} - R_{a, m_1+1}) / m_1$  при  $i = 1, m_1$ , а все  $R_{ai} - R_{a, i+1} = R_{1, m_1+1} / (m - m_1)$  при  $i = m_1 + 1, m$ , т. е. вместо исследования структуры 2А0 ограничиться рассмотрением структуры 2А1. При таком ограничении решения обеих задач НЗ по трудоемкости почти не отличаются от их решения для случая  $m=2$ . Так, в примере  $m=3$ ,  $m_1=1$  приходим к соотношениям

$$R^{(1)} = (R_{a1} - R_{a2})(1 - \delta^{(1n)} / \delta_{\text{вг}}(R_{a1})),$$

$$R^{(2)} = R_{a2} \{1 - ((\delta_{\text{вг}}(R_{a2}))^{-1} - (\delta_{\text{вг}}(R_{a2}/2))^{-1}) \delta^{(2, n)} / 2\},$$

при помощи которых решения указанных задач НЗ не вызывают ни принципиальных, ни технических затруднений.

Точно так же не вызывает затруднений изучение верхних оценок уровней защиты, если использовать связь между ними и ниж-

ними оценками, определяемую простейшими соотношениями (3. 24) и (3. 33). Однако задача значительно упрощается, если рассматривать каскадные коды НЗ бесконечного порядка.

### 3.5.3. Каскадные коды НЗ бесконечного порядка структуры 2А

При рассмотрении каскадных кодов бесконечного порядка с двумя уровнями защиты информационных символов разобьем отрезок  $[0, x_0]$  на две части  $[0, x_1]$  и  $[x_1, x_0]$ ,  $0 < x_1 < x_0$ , тогда для  $R^{(1)}$  и  $R^{(2)}$  получаем

$$R^{(1)} = \int_{x_1}^{x_0} f_1(x) dx; \quad R^{(2)} = \int_0^{x_1} f_2(x) dx, \quad (3.84)$$

где функции  $f_1(x)$  и  $f_2(x)$  определяют структуру кода соответственно на участках  $[x_1, x_0]$  и  $[0, x_1]$ .

Используя выражения для нижних и верхних оценок уровней защиты, приведенных в разд. 3.1.2, и переходя от кодов конечного к кодам бесконечного порядка (подобно тому, как это было сделано в § 3.4), приходим к соотношениям

$$\delta^{(1,*)} = \min_{x_1 \leq x \leq x_0} \{(1 - f_1(x)) \delta_{\text{ВГ}}(x)\}; \quad \delta^{(2,*)} = \min_{0 \leq x \leq x_1} \{(1 - f_2(x)) \delta_{\text{ВГ}}(x)\}, \quad (3.85)$$

$$\delta^{(1,*)} = \frac{1}{2} \min_{x_1 \leq x \leq x_0} \{1 - f_1(x)\}; \quad \delta^{(2,*)} = \frac{1}{2} \min_{0 \leq x \leq x_1} \{1 - f_2(x)\}, \quad (3.86)$$

$$\xi^{(1,*)} = \frac{1}{2} \min_{x_1 \leq x \leq x_0} \{(1 - f_1(x)) (1 - x)\}, \quad (3.87)$$

$$\xi^{(2,*)} = \frac{1}{2} \min_{0 \leq x \leq x_1} \{(1 - f_2(x)) (1 - x)\}.$$

Под кодами бесконечного порядка структуры 2А будем понимать коды (по аналогии с кодами РЗ), для которых при всех  $x$ :  $x_1 \leq x \leq x_0$  выражение  $(1 - f_1(x)) \delta_{\text{ВГ}}(x)$  сохраняет постоянное значение, очевидно равное  $\delta^{(1,*)}$ , а для всех  $x$ :  $0 \leq x \leq x_1$  выражение  $(1 - f_2(x)) \delta_{\text{ВГ}}(x)$  сохраняет значение, равное  $\delta^{(2,*)}$ . Отсюда получаем, что

$$f_1(x) = 1 - \delta^{(1,*)} / \delta_{\text{ВГ}}(x), \quad x_1 < x \leq x_0, \quad (3.88)$$

$$f_2(x) = 1 - \delta^{(2,*)} / \delta_{\text{ВГ}}(x), \quad 0 \leq x \leq x_1.$$

Подставляя выражения (3.88) в равенства (3.86), приходим к соотношениям

$$R^{(1)} = x_0 - x_1 - \delta^{(1,*)} (I(x_0) - I(x_1)), \quad (3.89)$$

$$R^{(2)} = x_1 - \delta^{(2,*)} I(x_1), \quad (3.90)$$

где  $I(x) = \int_0^x \frac{du}{\delta_{\text{ВГ}}(u)}.$

Так как в точке  $x = x_0$ ,  $f_1(x_0) = 0$ , то первое из равенств (3.88) приводит к соотношению

$$\delta^{(1, n)} = \delta_{\text{вг}}(x_0), \text{ или } x_0 = 1 - H(\delta^{(1, n)}). \quad (3.91)$$

Соотношения (3.89), (3.90) и (3.21) показывают, что при заданных значениях  $\delta^{(1, n)}$ ,  $\delta^{(2, n)}$ ,  $R^2$  не возникает задачи максимизации величины  $R^{(1)}$ , так как в этом случае однозначно определяются значения  $x_1$  и  $x_0$ , а значит, и величина  $R^{(1)}$ .

Таким образом, для решения основных задач НЗ для каскадных кодов бесконечного порядка структуры 2А следует при фиксированном значении  $\delta^{(2, n)}$  задать произвольные значения  $x_1 < x$  и для каждого из них определить соответствующее ему значение  $R^{(2)}$ . Затем по заданному значению  $\delta^{(1, n)}$  для первой задачи (или по заданному значению  $R^{(1)}$  для второй задачи) вычислить  $R^{(1)}$  (или  $\delta^{(1, n)}$ ).

Результаты соответствующих расчетов для первой задачи при  $\delta^{(1, n)} = 0,1$  и  $\delta^{(2, n)} = 0,00; 0,020; 0,0374; 0,070; 0,1$  приведены на рис. 3.12.

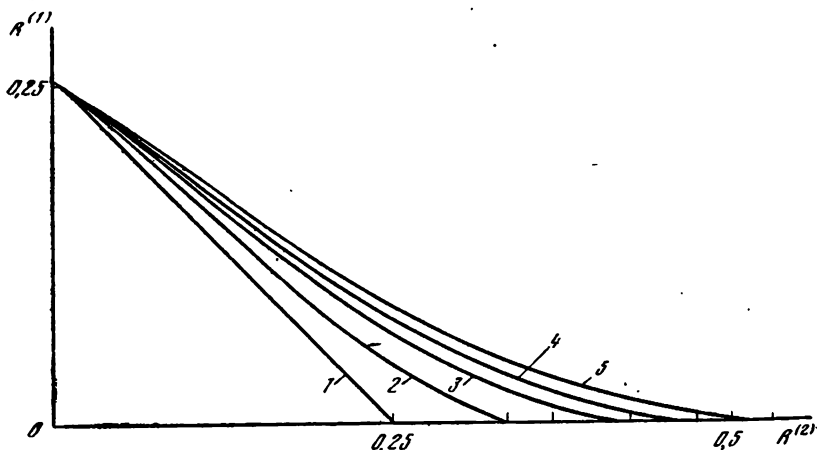


Рис. 3.12. Зависимость между  $R^{(1)}$  и  $R^{(2)}$

1 — при  $\delta^{(1, n)} = 0,1$  и  $\delta^{(2, n)} = 0,000$ ; 2 — 0,020; 3 — 0,0374; 4 — 0,070; 5 — 0,1

Что касается верхних оценок уровней защиты, то в соответствии с (3.86)–(3.88) получаем

$$\delta^{(1, n)} = \frac{1}{2} \delta^{(1, n)} \min_{x_1 \leq x \leq x_0} \{(\delta_{\text{вг}}(x))^{-1}\} = \delta^{(1, n)} / 2\delta_{\text{вг}}(x_1); \quad \delta^{(2, n)} = \delta^{(2, n)},$$

$$\delta^{(1, n)} = \frac{1}{2} \delta^{(1, n)} \min_{x_1 \leq x \leq x_0} \{(1-x)/\delta_{\text{вг}}(x)\} = \delta^{(1, n)} (1-x_1) / 2\delta_{\text{вг}}(x_1);$$

$$\delta^{(2, n)} = \delta^{(2, n)}.$$

Из приведенных выражений видно, что как для несистематических, так и для систематических каскадных кодов структуры 2А оценка меньшего из уровней защиты  $\delta^{(2)}$  является асимптотически точной, т. е.  $\delta^{(2, n)} = \delta^{(2, n)} = \delta^{(2, n)} = \delta^{(2)}$ .



КАСКАДНОЕ ДЕКОДИРОВАНИЕ

---

Декодирование — исправление ошибок представляет собой наиболее трудно реализуемую часть при практическом использовании помехоустойчивого кодирования. Поэтому естественно поставить перед каскадными кодами задачу упрощения реализации именно этой части. И нужно сделать это не за счет ухудшения реализуемых корректирующих свойств, а разработкой специальных, просто реализуемых алгоритмов декодирования. Подобная задача решается в настоящей главе посредством каскадного декодирования, суть которого в том, что вместо декодирования длинного каскадного кода выполняется последовательность декодирований значительно более коротких внутренних и внешних кодов. При этом реализуемые корректирующие свойства оцениваются исходя из возможностей каскадного кода в целом. В связи с этим основная решаемая в главе задача состоит не только в том, чтобы разработать простые алгоритмы декодирования, но и в том, чтобы дать подробный анализ реализуемых при этих алгоритмах корректирующих свойств.

### § 4.1. Описание каскадного декодирования

#### 4.1.1. Общий принцип каскадного декодирования

Описание каскадного декодирования на функциональном уровне было дано в гл. 1. Теперь сузим и детализируем это описание для случая линейных каскадных кодов.

Рассмотрим линейный каскадный код  $m$ -го порядка, определяемый внутренними  $A_i$  и внешними  $B_i$ ,  $i=\overline{1, m}$ , кодами с заданными для них алгоритмами декодирования.

Целью каскадного декодирования является получение декодированного слова каскадного кода при помощи комбинирования декодирований внутренних и внешних кодов.

Каскадное декодирование обозначим через  $\psi$  и подчиним его условию, определяющему общий принцип каскадного декодирования.

Согласно этому условию при декодировании каскадного кода порядка  $m$  алгоритм  $\psi$  распадается на  $m$  шагов  $\psi_i$ ,  $i=\overline{1, m}$ , на каждом из которых как результат декодирования кодами  $A_i$ ,

и  $B_i$  получаем информационные символы  $i$ -го блока (или, что то же самое, находим кодовое слово  $i$ -го внешнего кода  $B_i$ , т. е.  $\tilde{\gamma}_i$ ). Таким образом, при каскадном декодировании шаг за шагом определяем  $\tilde{\gamma}_1, \dots, \tilde{\gamma}_m$  и, следовательно, все вспомогательное слово  $\tilde{\gamma}$  (знак  $\sim$  означает, что соответствующее слово получено в результате декодирования, в то время как знак  $\wedge$  будет обозначать, что слово подлежит декодированию, например, подлежащее декодированию слово  $\hat{\gamma}_i$  декодируется кодом  $B_i$  в слово  $\tilde{\gamma}_i$ ).

На первом шаге  $\phi_1$  декодированию подлежит принятое слово  $\hat{\alpha}$ , представляющее собой переданное кодовое слово  $\alpha$ , искаженное ошибкой  $\xi$ . Обозначая принятое слово  $\hat{\alpha}$  через  $\hat{\alpha}(0)$ , а соответствующее ему кодовое слово  $\alpha$  и вспомогательное слово  $\gamma$  через  $\alpha(0)$  и  $\gamma(0)$ , имеем  $\hat{\alpha}(0) = \alpha(0) + \xi$ ,

$$\gamma(0) = \begin{pmatrix} \gamma_m \\ \vdots \\ \gamma_1 \\ 0 \end{pmatrix},$$

где  $\xi$  — слово-ошибка.

Каждый столбец  $\hat{\alpha}^{(j)}(0)$  слова  $\hat{\alpha}(0)$  представляет собой искаженное ошибкой  $\xi^{(j)}$  кодовое слово  $\alpha^{(j)}(0)$  первого внутреннего кода  $A_1$ . Это значит, что столбцы  $\hat{\alpha}^{(j)}(0)$  можно декодировать при помощи кода  $A_1$  и получить столбцы  $\tilde{\alpha}^{(j)}(0)$ . По каждому нестертому столбцу  $\tilde{\alpha}^{(j)}(0)$ , используя матрицу  $H_0 = G_0^{-1}$ , можно вычислить элементы  $\hat{\gamma}_{1j}$  (стертым столбцам  $\tilde{\alpha}^{(j)}(0)$  соответствуют стертые элементы  $\hat{\gamma}_{1j}(0)$ ) и полученное в результате этой операции слово  $\hat{\gamma}_1 = (\hat{\gamma}_{11}, \dots, \hat{\gamma}_{1n_b})$  декодировать первым внешним кодом  $B_1$ , получив в результате кодовое слово этого кода  $\tilde{\gamma}_1 = (\tilde{\gamma}_{11}, \tilde{\gamma}_{12}, \dots, \tilde{\gamma}_{1n_b})$ . Для того чтобы на втором шаге  $\phi_2$  каскадного декодирования выполнялись в точности те же самые операции, что и на первом шаге, но только вместо кодов  $A_1$  и  $B_1$  использовались коды  $A_2$  и  $B_2$ , надо, чтобы исходным (входным) словом второго шага (обозначим его  $\hat{\alpha}(1)$ ) было слово, которому соответствует вспомогательное слово  $\gamma(1)$ , имеющее вид

$$\gamma(1) = \begin{pmatrix} \gamma_m \\ \vdots \\ \gamma_2 \\ 0 \\ 0 \end{pmatrix}.$$

При этом слово  $\hat{\alpha}(1)$  должно содержать те же самые ошибки, что и слово  $\hat{\alpha}(0)$ , т. е. оба они должны принадлежать одному и тому же смежному классу.

Для построения слова  $\hat{\alpha}(1)$  рассмотрим вспомогательное слово

$$\tilde{\gamma}(1) = \gamma(0) + \begin{vmatrix} 0 \\ \vdots \\ 0 \\ \tilde{\gamma}_1 \\ 0 \end{vmatrix} = \begin{vmatrix} \gamma_m \\ \vdots \\ \gamma_2 \\ \gamma_1 + \tilde{\gamma}_1 \\ 0 \end{vmatrix}, \quad (4.1)$$

которому соответствует кодовое слово каскадного кода

$$\alpha(1) = G_0 \tilde{\gamma}(1) = \alpha(0) + G_0 \begin{vmatrix} 0 \\ \vdots \\ 0 \\ \tilde{\gamma}_1 \\ 0 \end{vmatrix}.$$

Добавляя к правой и левой части этого выражения слово-ошибку, получаем

$$\alpha(1) + \xi = \hat{\alpha}(0) + G_0 \begin{vmatrix} 0 \\ \vdots \\ 0 \\ \tilde{\gamma}_1 \\ 0 \end{vmatrix}.$$

Если в результате декодирования кодами  $A_1$  и  $B_1$  блок  $\gamma_1$  определен правильно, т. е. если  $\tilde{\gamma}_1 = \gamma_1$ , то слову  $\alpha(1) + \xi$  согласно (4.1) соответствует вспомогательное слово

$$\tilde{\gamma}(1) = \begin{vmatrix} \gamma_m \\ \vdots \\ \gamma_2 \\ 0 \\ 0 \end{vmatrix} = \gamma(1).$$

Но это значит, что каждый столбец слова  $\alpha(1) + \xi$  представляет собой кодовое слово второго внутреннего кода, искаженное той же самой ошибкой  $\xi^{(j)}$ , что и слово  $\alpha^{(j)}(0)$ , т. е.  $\alpha(1) + \xi = \hat{\alpha}(1)$ .

Таким образом, слово  $\hat{\alpha}(1)$ , определяемое вместе с блоком  $\tilde{\gamma}_1$  на первом шаге  $\psi_1$  каскадного декодирования, представляет собой входное (т. е. подлежащее декодированию) слово на втором шаге  $\psi_2$  каскадного декодирования. Приведенные рассуждения повторяются без всяких изменений на каждом следующем шаге до последнего  $\psi_m$  шага каскадного декодирования, что приводит нас к общей схеме каскадного декодирования, показанной на рис. 4.1.

При этом связь между входными словами  $\hat{\alpha}(i-1)$  и  $\hat{\alpha}(i)$  на  $i$ -м и  $(i+1)$ -м шагах каскадного декодирования определяется следующим утверждением, которое непосредственно вытекает из приведенных выше рассуждений.

**Утверждение 4.1.** Если  $\hat{\alpha}(i-1)$  — входное слово на  $i$ -м шаге каскадного декодирования, а  $\tilde{\gamma}_i$  —  $i$ -й блок вспомогательного слова  $\gamma$ , найденный на  $i$ -м шаге, то входное слово  $\hat{\alpha}(i)$  на  $(i+1)$ -м шаге каскадного декодирования определяется равенством

$$\begin{pmatrix} 0 \\ \vdots \\ 0 \\ \tilde{\gamma}_i \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \hat{\alpha}(i-1) + G_i^* \tilde{\gamma}_i. \quad (4.2)$$

При этом каждый из столбцов слов  $\hat{\alpha}(i-1)$  и  $\hat{\alpha}(i)$  с одним и тем же номером представляет собой кодовое слово соответственно кодов  $A_i$  и  $A_{i+1}$ , искаженного одним и тем же сочетанием ошибок. Если для каждого столбца каскадного кода используется своя кодирующая матрица  $G_0^{(j)}$ , то выражение (4.2) следует заменить  $n_b$  равенствами

$$\hat{\alpha}^{(j)}(i) = \hat{\alpha}^{(j)}(i-1) + G_0^{(j)} \tilde{\gamma}_{i,j}, \quad j = \overline{1, n_b}. \quad (4.3)$$

Так как на каждом шаге  $\psi_i$  каскадного декодирования возможен также и отказ от декодирования, то результатом вычислений на  $i$ -м шаге будет либо отказ от дальнейшего декодирования,

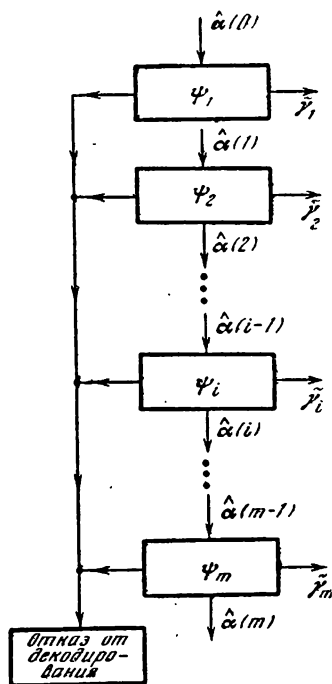


Рис. 4.1. Блок-схема алгоритма каскадного декодирования

либо пара  $\tilde{\gamma}_i$  и  $\hat{\alpha}(i)$ . Последний случай назовем успешным завершением  $i$ -го шага. Очевидно, что  $i$ -й шаг  $\psi_i$  выполняется лишь при успешном завершении  $(i-1)$ -го шага  $\psi_{i-1}$ . Если на каждом шаге  $\psi_i$  блок  $\tilde{\gamma}_i$  декодирован правильно, т. е. если  $\tilde{\gamma}_i = \gamma_i$ ,  $i = \overline{1, m}$ , то слово  $\hat{\alpha}(m)$ , полученное на последнем  $m$ -м шаге, представляет собой сочетание ошибок, искажающих переданное кодовое слово  $\alpha$ , т. е.  $\hat{\alpha}(m) = \xi$ .

#### 4.1.2. Составной алгоритм каскадного декодирования по расстоянию

В предыдущем разделе при описании каскадного декодирования были отмечены лишь его основные принципиальные особенности. Очевидно, что, выбирая различные алгоритмы декодирования внутренних и внешних кодов, можно построить различные конкретные алгоритмы каскадного декодирования. В дальнейшем ограничимся составным алгоритмом каскадного декодирования, когда результат определяется числом исправляемых ошибок или вероятностью ошибочного декодирования. В первом случае будем говорить о составном алгоритме декодирования по расстоянию, а во втором — по вероятности ошибки, обозначая их соответственно через  $\psi^d(z_1, z_2, \dots, z_m)$  и  $\psi^p(z_1, z_2, \dots, z_m)$ .

В настоящем разделе опишем составной алгоритм каскадного декодирования по расстоянию. Этот алгоритм реализуется как последовательность процедур  $\psi_1^d(z_1), \psi_2^d(z_2), \dots, \psi_m^d(z_m)$ .

Рассмотрим процедуру  $\psi_i^d(z_i)$ , выполняемую на  $i$ -м шаге каскадного декодирования по расстоянию.

1. Каждый столбец  $\hat{\alpha}^{(j)}(i-1)$  слова  $\hat{\alpha}(i-1)$  декодируется  $i$ -м внутренним кодом  $A_i$  с исправлением всех ошибок до кратности  $t < d_{A_i}/2$ . В результате от слова  $\hat{\alpha}(i-1)$  переходим к слову  $\tilde{\alpha}(i) = (\tilde{\alpha}^{(1)}(i), \tilde{\alpha}^{(2)}(i), \dots, \tilde{\alpha}^{(n_b)}(i))$ , где  $\tilde{\alpha}^{(j)}(i)$  — слово кода  $A_i$  или стирание, если в коде  $A_i$  не нашлось кодового слова, расположенного от «принятого» слова  $\hat{\alpha}^{(j)}(i-1)$  на расстоянии, меньшем, чем  $d_{A_i}/2$ .

2. По словам  $\hat{\alpha}(i-1)$  и  $\tilde{\alpha}(i)$  строим вектор  $\Delta(i) = (\Delta_1(i), \Delta_2(i), \dots, \Delta_{n_b}(i))$ , где

$$\Delta_j(i) = \begin{cases} d(\hat{\alpha}^{(j)}(i-1), \tilde{\alpha}^{(j)}(i)), & \text{если } \tilde{\alpha}^{(j)}(i) \in A_i; \\ d_{A_i}/2, & \text{если } \tilde{\alpha}^{(j)}(i) \text{ — стирание.} \end{cases}$$

3. Для нестертых столбцов  $\tilde{\alpha}^{(j)}(i)$  вычисляем

$$\hat{\gamma}_{i,j} = H_i^* \tilde{\alpha}^{(j)}(i), \quad (4.4)$$

где  $H_i^*$  — подматрица размеров  $\alpha_i \times n_a$  проверочной матрицы  $H_0 = G_0^{-1}$  (см. (2.10)).

Вычислив все  $\hat{\gamma}_{i,j}$ , находим слово  $\hat{\gamma}_i = (\hat{\gamma}_{i1}, \hat{\gamma}_{i2}, \dots, \hat{\gamma}_{i,n_b})$ , где  $\hat{\gamma}_{i,j}$  либо вычисляется в соответствии с (4.4), либо стирается, если столбец  $\tilde{\alpha}^{(j)}(i)$  стерт.

4. Для каждого критерия  $T_k^{(i)}$  из заданного множества  $\{T_1^{(i)}, T_2^{(i)}, \dots, T_{i-1}^{(i)}\}$ , где  $T_k^{(i)} < d_{a_i}/2$  — неотрицательные целые числа и  $T_k^{(i)} < T_{k+1}^{(i)}$ , слово  $\hat{\gamma}_i$  преобразуется в слово  $\hat{\gamma}_i^k = (\hat{\gamma}_{i,1}(k), \hat{\gamma}_{i,2}(k), \dots, \hat{\gamma}_{i,n_b}(k))$ , где

$$\hat{\gamma}_{i,j}(k) = \begin{cases} \hat{\gamma}_{i,j}, & \text{если } \Delta_j(i) \leq T_k^{(i)}; \\ \text{стирание}, & \text{если } \Delta_j(i) > T_k^{(i)}. \end{cases}$$

Это значит, что символ  $\hat{\gamma}_{i,j}$  остается без изменения, если он стерт или если расстояние Хемминга  $d(\hat{\alpha}^{(j)}(i-1), \hat{\alpha}^{(j)}(i)) \leq T_k^{(i)}$ , в противном случае символ  $\hat{\gamma}_{i,j}$  стирается.

В результате получается множество слов  $\hat{\Gamma}(i) = \{\hat{\gamma}_i^k\}$ . Отметим, что если для различных критериев  $T_k^{(i)}$  получаются одинаковые слова  $\hat{\gamma}_i^k$ , то во множество  $\hat{\Gamma}(i)$  включается только одно из них. Ясно, что по мере увеличения номера  $k$  число стертых символов не увеличивается, оно может либо уменьшиться, либо остаться неизменным (в этом случае  $\hat{\gamma}_i^k = \hat{\gamma}_i^{k+1}$ ).

5. Каждое слово  $\hat{\gamma}_i^k$  из множества  $\hat{\Gamma}(i)$  декодируется внешним кодом  $B_i$ . В результате декодирования  $\hat{\gamma}_i^k$  получаем  $\tilde{\gamma}_i^k$ , которое является либо словом кода  $B_i$ , либо стиранием. Множество всех различных слов  $\hat{\gamma}_i^k$  (включая стирание) обозначим через  $\tilde{\Gamma}(i)$ .

6. Для каждого нестертого  $\tilde{\gamma}_i^k \in \tilde{\Gamma}(i)$  вычисляем числовой параметр

$$t(i, k) = \sum_{j=1}^{n_b} t_j(k),$$

где

$$t_j(k) = \begin{cases} d_{a_i} - \Delta_j(i), & \text{если } \hat{\gamma}_{i,j} \neq \tilde{\gamma}_{i,j}(k) \text{ и } \hat{\gamma}_{i,j} \text{ не стерто;} \\ \Delta_j(i), & \text{если } \hat{\gamma}_{i,j} = \tilde{\gamma}_{i,j}(k) \text{ или } \hat{\gamma}_{i,j} \text{ — стирание.} \end{cases}$$

В качестве результата декодирования по процедуре  $\psi_i^d(z_i)$  выбирается слово  $\tilde{\gamma}_i = \tilde{\gamma}_i^k$ , которому соответствует наименьшее значение параметра  $t(i, k)$ . Если нескольким словам  $\tilde{\gamma}_i^k$  соответствует одно наименьшее значение параметра  $t(i, k)$ , то отказываемся от дальнейшего декодирования. Заметим, что процедура  $\psi_i^d(z_i)$  завершается отказом от декодирования, если при декодировании каждого из слов  $\hat{\gamma}_i^k \in \hat{\Gamma}(i)$  получаем стирание.

7. После выбора слова  $\tilde{\gamma}_i$  вычисляем слово  $\hat{\alpha}(i)$  по формуле  $\hat{\alpha}(i) = \hat{\alpha}(i-1) + G_i^* \tilde{\gamma}_i$ .

Если все  $z_i = 1, i = \overline{1, m}$ , то каждое множество  $\hat{\Gamma}(i), i = \overline{1, m}$ , содержит лишь одно слово. Тогда необходимость определения параметра  $t(i, k)$  по п. 6 процедуры  $\psi_i^d(z_i)$  отпадает. В этом случае алгоритм  $\psi^d(z_1, z_2, \dots, z_m) = \psi^d(1, 1, \dots, 1)$  будем называть простым алгоритмом каскадного декодирования по расстоянию.

Введем теперь множество  $\mathcal{E}(i)$  ошибок, при наличии которых алгоритм  $\psi^d(z_1, z_2, \dots, z_m)$  до  $i$ -го шага включительно будет при-

водить к верным решениям, т. е. когда  $\tilde{\gamma}_s = \gamma_s$ ,  $s = \overline{1, i}$ . В силу определения  $\mathcal{E}(i)$  имеют место очевидные включения

$$\mathcal{E}(1) \supset \mathcal{E}(2) \supset \dots \supset \mathcal{E}(m). \quad (4.5)$$

Таким образом, именно  $\mathcal{E}(m)$  задает те сочетания ошибок, при которых верно декодируется все слово каскадного кода. Кроме того, если  $\mathcal{E}(i) \neq \mathcal{E}(i+1)$ , то в силу (4.5) блок  $\gamma_i$  защищен от ошибок лучше, чем блок  $\gamma_{i+1}$ . В дальнейшем будет показано, что во многих случаях это именно так.

Сформулируем теперь необходимые и достаточные условия, при которых некоторое сочетание ошибок  $\xi$ , принадлежащее  $\mathcal{E}(i-1)$ , будет принадлежать  $\mathcal{E}(i)$ .

**Лемма 4.1.** Для того чтобы при сочетании  $\xi \in \mathcal{E}(i-1)$  на  $i$ -м шаге был правильно декодирован блок  $\gamma_i$ , т. е. чтобы  $\xi \in \mathcal{E}(i)$ , необходимо и достаточно, чтобы при выполнении процедуры  $\psi_i^q(z_i)$ : а) множество  $\tilde{\Gamma}(i)$  содержало слово  $\tilde{\gamma}_i^k = \gamma_i$ ; б) для любого слова  $\tilde{\gamma}_i^k \in \tilde{\Gamma}(i)$ ,  $k \neq k_0$ , имело место неравенство  $t(i, k_0) < t(i, k)$ .

**Д о к а з а т е л ь с т в о.** Необходимость условия а) следует из того, что нельзя выбрать верное слово  $\gamma_i$  из множества, в котором оно не содержится. Необходимость условия б) вытекает из того, что в случае, когда оно не выполнено, верное слово  $\gamma_i$ , даже если оно принадлежит  $\tilde{\Gamma}(i)$ , будет отброшено. Достаточность приведенных условий очевидна.

#### 4.1.3. Составной алгоритм каскадного декодирования по вероятности

В настоящем разделе опишем составной алгоритм каскадного декодирования, отличающийся от рассмотренного в предыдущем разделе в основном тем, что в качестве критерия выбора будут служить не кратности исправляемых ошибок, а логарифмы апостериорных вероятностей ошибочного декодирования. Этот алгоритм также реализуется как последовательность процедур  $\psi_1^q(z_1)$ ,  $\psi_2^q(z_2)$ , ...,  $\psi_m^q(z_m)$ .

Рассмотрим процедуру  $\psi_i^q(z_i)$ , выполняемую на  $i$ -м шаге каскадного декодирования по вероятности.

1. Каждый столбец  $\hat{\alpha}^{(j)}(i-1)$  слова  $\hat{\alpha}(i-1)$  декодируется  $i$ -м внутренним кодом  $A_i$  в ближайшее кодовое слово или стирание, если таких слов несколько. В результате от слова  $\hat{\alpha}(i-1)$  переходим к слову  $\tilde{\alpha}(i) = (\tilde{\alpha}^{(1)}(i), \tilde{\alpha}^{(2)}(i), \dots, \tilde{\alpha}^{(n_i)}(i))$ , где  $\tilde{\alpha}^{(j)}(i)$  — слово кода  $A_i$  или стирание.

2. По словам  $\hat{\alpha}(i-1)$  и  $\tilde{\alpha}(i)$  строим вектор  $\Delta(i) = (\Delta_1(i), \Delta_2(i), \dots, \Delta_{n_i}(i))$ , где

$$\Delta_j(i) = \begin{cases} \tilde{v}_j^i, & \text{если } \hat{\alpha}^{(j)}(i) \in A_i \text{ и } \tilde{v}_j^i \geq 0; \\ 0, & \text{если } \tilde{v}_j^i < 0 \text{ или } \tilde{\alpha}^{(j)}(i) \text{ — стирание, а} \end{cases}$$

$\tilde{\alpha}_i^j$  при  $\tilde{\alpha}^j(i) \in A_i$  определяется как

$$\tilde{\alpha}_i^j = \frac{1}{n_a} \log_2 \left[ P(\hat{\alpha}^{(j)}(i-1) | \tilde{\alpha}^j(i)) \middle/ \sum_{\substack{x \in A_i \\ x \neq \tilde{\alpha}^j(i)}} P(\hat{\alpha}^{(j)}(i-1) | x) \right].$$

3. Для нестертых столбцов  $\tilde{\alpha}^{(j)}(i)$  вычисляем

$$\hat{\gamma}_{i,j} = H_i^* \tilde{\alpha}^{(j)}(i), \quad (4.6)$$

где  $H_i^*$  — подматрица размеров  $a_i \times n_a$  проверочной матрицы  $H_0 = G_0^{-1}$  (см. (2.10)).

Вычислив все  $\hat{\gamma}_{i,j}$ , находим слово  $\hat{\gamma}_i = (\hat{\gamma}_{i1}, \hat{\gamma}_{i2}, \dots, \hat{\gamma}_{in_b})$ , где  $\hat{\gamma}_{i,j}$  либо вычисляется в соответствии с (4.6), либо происходит стирание, если столбец  $\tilde{\alpha}^{(j)}(i)$  стер.

4. Для каждого критерия  $T_k^{(i)}$  из заданного множества  $\{T_1^{(i)}, T_2^{(i)}, \dots, T_{n_b}^{(i)}\}$ , где  $T_k^{(i)} < E_0(R_{a_i})$  — неотрицательные числа и  $T_k^{(i)} < T_{k+1}^{(i)}$ , слово  $\hat{\gamma}_i$  преобразуется в слово  $\gamma_i^k = (\gamma_{i1}(k), \gamma_{i2}(k), \dots, \gamma_{in_b}(k))$ , где

$$\gamma_{i,j}(k) = \begin{cases} \hat{\gamma}_{i,j}, & \text{если } \Delta_j(i) \geq T_k^{(i)}, \\ \text{стирание}, & \text{если } \Delta_j(i) < T_k^{(i)}. \end{cases}$$

Это значит, что символ  $\hat{\gamma}_{i,j}$  остается без изменения, если он стерт или если

$$\frac{1}{n_a} \log_2 \left[ P(\hat{\alpha}^{(j)}(i-1) | \tilde{\alpha}^{(j)}(i)) \middle/ \sum_{\substack{x \in A_i \\ x \neq \tilde{\alpha}^{(j)}(i)}} P(\hat{\alpha}^{(j)}(i-1) | x) \right] \geq T_k^{(i)},$$

в противном случае  $\hat{\gamma}_{i,j}$  стирается. В результате получается множество слов  $\hat{\Gamma}(i) = \{\hat{\gamma}_i^k\}$ . Отметим, что как и при декодировании по расстоянию, для различных критериев  $T_k^{(i)}$  могут получиться одинаковые  $\hat{\gamma}_i^k$ . В этом случае в множество  $\hat{\Gamma}(i)$  включается только одно из них. Ясно, что по мере увеличения номера  $k$  число стертых символов не уменьшается.

5. Каждое слово  $\hat{\gamma}_i^k$  из множества  $\hat{\Gamma}(i)$  декодируется внешним кодом  $B_i$ . В результате декодирования  $\hat{\gamma}_i^k$  получаем  $\tilde{\gamma}_i^k$ , которое является либо словом кода  $B_i$ , либо стиранием. Множество всех различных слов  $\tilde{\gamma}_i^k$  (включая стирание) обозначим через  $\tilde{\Gamma}(i)$ .

6. Для каждого нестертого  $\tilde{\gamma}_i^k \in \tilde{\Gamma}(i)$  вычисляем числовой параметр

$$E(i, k) = \sum_{j=1}^{n_b} E_j(k),$$

где

$$E_j(k) = \begin{cases} (E_0(R_{a_i}) + h_i \Delta_j(i)) n_a, & \text{если } \hat{\gamma}_{i,j} \neq \tilde{\gamma}_{i,j}(k) \text{ и } \hat{\gamma}_{i,j} \text{ не стерто;} \\ (E_0(R_{a_i}) - h_i \Delta_j(i)) n_a, & \text{если } \hat{\gamma}_{i,j} = \tilde{\gamma}_{i,j}(k); \\ E_0(R_{a_i}) n_a, & \text{если } \hat{\gamma}_{i,j} \text{ стерто,} \end{cases}$$



$a \ h_i > 0$  — некоторая постоянная, определяемая скоростью передачи  $R_{ai}$ .

В качестве результата декодирования по процедуре  $\psi_i^p(z_i)$  выбирается слово  $\hat{\gamma}_i^k = \tilde{\gamma}_i$ , которому соответствует наименьшее значение параметра  $E(i, k)$ . Если нескольким словам  $\tilde{\gamma}_i^k$  соответствует одно наименьшее значение параметра  $E(i, k)$ , то отказываемся от дальнейшего декодирования. Заметим, что процедура  $\psi_i^p(z_i)$  также завершается отказом от декодирования, если при декодировании каждого из слов  $\hat{\gamma}_i^k \in \hat{\Gamma}(i)$  получается стирание.

7. После выбора слова  $\tilde{\gamma}_i$  вычисляем слово  $\hat{\alpha}(i)$  по формуле  $\hat{\alpha}(i) = \hat{\alpha}(i-1) + G_{01i}^* \tilde{\gamma}_i$ . Если все  $z_i = 1, i = \overline{1, m}$ , то каждое множество  $\hat{\Gamma}(i), i = \overline{1, m}$ , содержит лишь одно слово. Тогда необходимость определения параметра  $E(i, k)$  по п. 6 процедуры  $\psi_i^p$  отпадает. В этом случае алгоритм  $\psi^p(z_1, z_2, \dots, z_m) = \psi^p(1, 1, \dots, 1)$  будем называть простым алгоритмом каскадного декодирования по вероятности. Как и при декодировании по расстоянию, в данном случае может быть введено множество  $\mathcal{E}(i)$  ошибок, при наличии которых алгоритм  $\psi^p(z_1 \dots z_m)$  до  $i$ -го шага включительно будет приводить к верным решениям, когда  $\tilde{\gamma}_s = \gamma_s, s = \overline{1, i}$ . В этом случае также справедливы включения (4.5) и лемма 4.1 с точностью до замены параметров  $t(i, k)$  на параметры  $E(i, k)$ .

## § 4.2. Возможности каскадного декодирования по расстоянию

### 4.2.1. Ошибки, исправляемые при каскадном декодировании по расстоянию

В разд. 4.1.2 было введено множество ошибок  $\mathcal{E}(i)$ , такое, что при любой ошибке  $\xi \in \mathcal{E}(i)$  алгоритм  $\psi^d(z_1, z_2, \dots, z_m)$  приводит к верным решениям до  $i$ -го шага включительно.

В настоящем разделе введем реализуемое расстояние  $d_i^*$ , определяемое условием, что любое сочетание ошибок кратности  $t_i < d_i^*/2$  принадлежит множеству  $\mathcal{E}(i)$ . Это значит, что  $d_i^*$  представляет собой диаметр шара, все внутренние точки которого принадлежат  $\mathcal{E}(i)$ . Оценку снизу величины  $d_i^*$  дает следующая теорема.

Теорема 4.1. Всегда можно выбрать множества критериев  $\{T_1^{(s)}, T_2^{(s)}, \dots, T_{z_s}^{(s)}\}, s = \overline{1, i}$ , составного алгоритма  $\psi^d(z, z_2, \dots, z_m)$ , чтобы реализуемое этим алгоритмом до  $i$ -го шага включительно кодовое расстояние  $d_i^*$  удовлетворяло неравенству

$$d_i^* \geq d_i^{(n)} = \min_{1 \leq s \leq i} \left\{ \frac{2z_s}{2z_s + 1} d_{as} d_{bs} \right\}. \quad (4.7)$$

Доказательство теоремы 4.1 вытекает из следующих лемм.

Лемма 4.2. Пусть истинное число ошибок, внесенных каналом,  $t < d_{as} d_{bs} z_s / (2z_s + 1)$  и пусть все  $\tilde{\gamma}_s, s = \overline{1, i-1}$ , декодированы правильно, тогда при использовании процедуры  $\psi_i^d(z_i)$  (т. е. при

выполнении  $i$ -го шага) найдется такое множество критериев  $\{T_1^{(i)}, T_2^{(i)}, \dots, T_{z_i}^{(i)}\}$ , что по крайней мере одному из них в множестве  $\bar{\Gamma}(i)$  будет соответствовать верное слово  $\tilde{\gamma}_i^{k_0} = \gamma_i$ . Эти значения критериев  $T_k^{(i)}$  определяются равенством

$$T_k^{(i)} = k \frac{d_{a_i} + 1}{2z_i + 1} - 1. \quad (4.8)$$

**Лемма 4.3.** Пусть истинное число ошибок, внесенных каналом,  $t < d_{a_i} d_{b_i} / 2$  и пусть все  $\gamma_s$ ,  $s = \overline{1, i-1}$ , декодированы правильно, тогда при использовании процедуры  $\psi_i^d(z_i)$  параметр  $t(i, k_0)$ , соответствующий верному слову  $\tilde{\gamma}_i^{k_0} = \gamma_i$ , и параметр  $t(i, k)$ ,  $k \neq k_0$ , соответствующий любому другому слову  $\tilde{\gamma}_i^k \neq \gamma_i$ , удовлетворяют неравенствам  $t(i, k_0) < d_{a_i} d_{b_i} / 2 \leq t(i, k)$ .

Доказательство лемм 4.2 и 4.3 приведено в приложениях П.4.1 и П.4.2.

**Доказательство теоремы 4.1.** Из леммы 4.2 следует, что на каждом шаге от 1 до  $i$  можно так выбрать множества критериев  $\{T_1^{(s)}, T_2^{(s)}, \dots, T_{z_s}^{(s)}\}$ ,  $s = \overline{1, i}$ , что при любом сочетании ошибок кратности  $t < d_{a_s} d_{b_s} z_s / (2z_s + 1)$  выполняется условие а) леммы 4.1. Из леммы 4.3 вытекает, что в этом случае будет выполнено также и условие б) леммы 4.1. Но это значит, что на всех шагах до  $i$ -го шага включительно выполнены необходимые и достаточные условия правильного декодирования, что и доказывает теорему 4.1.

В дальнейшем исследование реализуемых при алгоритме декодирования  $\psi^d(z_1, z_2, \dots, z_m)$  корректирующих свойств каскадных кодов будет проводиться в предположении, что множество критериев  $\{T_1^{(i)}, T_2^{(i)}, \dots, T_{z_i}^{(i)}\}$  выбирается в соответствии с (4.8).

При оценке наибольшей длины исправляемого при каскадном декодировании  $\psi^d(z_1, z_2, \dots, z_m)$  пакета ошибок будем предполагать, что символы каскадного кода передаются по каналу в соответствии с их нумерацией, т. е. сверху вниз и столбец за столбцом.

Оценим снизу наибольшую длину пакета ошибок  $l_i$ , такую, что любой одиночный пакет ошибок длины  $l \leq l_i$  принадлежит множеству  $\mathcal{E}(i)$ .

**Теорема 4.2.** Пусть

$$l_i^{(n)} = \min_{1 \leq s \leq i} l_s^*, \quad \text{где} \quad (4.9)$$

$$l_s^* = \begin{cases} n_a(d_{b_s} - 3)/2 - T_{z_s}^{(s)} - T_1^{(s)}, & \text{если } d_{b_s} \text{ нечетно;} \\ n_a(d_{b_s} - 4)/2 - 2d_{a_s} - 2T_1^{(s)} - 1, & \text{если } d_{b_s} \text{ четно,} \end{cases}$$

а  $T_k^{(s)}$  определяется равенством (4.8). Тогда при алгоритме каскадного декодирования  $\psi^d(z_1, \dots, z_m)$  значение  $l_i \geq l_i^{(n)}$ .

Доказательство теоремы 4.2 опирается на следующие леммы.  
**Лемма 4.4.** Пусть длина пакета ошибок

$$l \leq l_i(v),$$

где

$$l_i(v) = n_a(v-1) + d_{a,i}, \quad (4.11)$$

а  $v \geq 1$  — натуральное число. Тогда этот пакет ошибок при использовании процедуры  $\psi_i^d(z_i)$  вызовет в любом слове  $\hat{\gamma}^k \in \hat{\Gamma}(i)$  такое число ошибок  $e_k$  и стираний  $\tau_k$ , что  $2e_k + \tau_k \leq 2v$ .

**Лемма 4.5.** Пусть длина одиночного пакета  $l \leq l_i^*$  и пусть все  $\tilde{\gamma}_s$ ,  $s = \overline{1, i-1}$ , декодированы правильно, тогда при использовании процедуры  $\psi_i^d(z_i)$  с множеством критериев  $\{T_k^{(i)}\}$ , выбранным в соответствии с (4.8), по крайней мере для одного  $T_{k_0}^{(i)}$  множество  $\hat{\Gamma}(i)$  будет содержать верное слово  $\tilde{\gamma}_{i,k_0}^* = \gamma_i$ .

**Лемма 4.6.** Пусть длина одиночного пакета

$$l \leq \begin{cases} n_a(d_{b,i} - 3)/2 + d_{a,i} + t_{a,i}, & \text{если } d_{b,i} \text{ нечетно;} \\ n_a(d_{b,i} - 4)/2 + 2d_{a,i} - 1, & \text{если } d_{b,i} \text{ четно,} \end{cases} \quad (4.12)$$

где  $t_{a,i} = \left\lfloor \frac{d_{a,i} - 1}{2} \right\rfloor$ , и пусть все  $\tilde{\gamma}_s$ ,  $s = \overline{1, i-1}$ , декодированы правильно, тогда при использовании процедуры  $\psi_i^d(z_i)$  параметр  $t(i, k_0)$ , соответствующий верному слову  $\tilde{\gamma}_{i,k_0}^* = \gamma_i$ , и параметр  $t(i, k)$ ,  $k \neq k_0$ , соответствующий любому неверному слову  $\tilde{\gamma}_i^k \neq \gamma_i$ , удовлетворяют неравенству

$$t(i, k_0) < d_{a,i} d_{b,i} / 2 \leq t(i, k). \quad (4.13)$$

Доказательство лемм 4.4—4.6 приведено в приложениях П.4.3—П.4.5.

**Доказательство теоремы 4.2.** Из лемм 4.4 и 4.5 следует, что если длина пакета ошибок  $l \leq l_i^{(n)}$ , то выполняется условие а) леммы 4.1 на всех шагах от 1 до  $i$ . Из леммы 4.6 вытекает, что на всех шагах до  $i$ -го шага включительно выполняется условие б) леммы 4.1. Но это значит, что при  $l \leq l_i^{(n)}$  выполняются необходимые и достаточные условия правильного декодирования слов  $\tilde{\gamma}_s$ ,  $s = \overline{1, i}$ , что и доказывает теорему 4.2.

Посмотрим теперь случай, когда одновременно с независимыми ошибками имеется  $v$  пакетов ошибок с распределением длин  $l^{(u)}$  и  $u = \overline{1, v}$ .

Ответ на вопрос, в каком случае набор из указанных  $v$  пакетов ошибок и  $t$  независимых ошибок принадлежит  $\mathcal{E}(i)$ , дается следующей теоремой.

**Теорема 4.3.** Пусть имеется  $\nu$  пакетов ошибок длины  $l^{(u)}$ ,  $u = \overline{1, \nu}$ , и пусть для каждой пары  $u$  и  $s$ ,  $s = \overline{1, i}$ , выбрано наименьшее целое число  $v_{us}$ , такое, что

$$l^{(u)} \leq l_s(v_{us}) = (v_{us} - 1)n_a + d_{as}. \quad (4.14)$$

Тогда любое сочетание ошибок из этих  $\nu$  пакетов при любом их расположении и еще из  $t$  независимых ошибок при декодировании по алгоритму  $\psi^d(z_1, \dots, z_m)$  принадлежит  $\mathcal{E}(i)$ , если

$$t \leq \min_{1 \leq s \leq i} \{d_s(\rho_s) z_s / (2z_s + 1)\}, \quad (4.15)$$

$$\text{где } d_s(\rho_s) = (d_{bs} - 2\rho_s) d_{as}, \quad (4.16)$$

$$\rho_s = \sum_{u=1}^{\nu} v_{us} < d_{bs}/2. \quad (4.17)$$

Доказательство теоремы 4.3 опирается на следующие леммы.

**Лемма 4.7.** Пусть имеется  $\nu$  пакетов ошибок и  $t$  независимых ошибок, удовлетворяющих условиям теоремы 4.3, и пусть все  $\tilde{\gamma}_s$ ,  $s = \overline{1, i-1}$ , декодированы правильно. Тогда при использовании процедуры  $\psi_i^d(z_i)$  с множеством критериев  $\{T_k^i\}$ , выбранных в соответствии с (4.8), по крайней мере для одного  $T_{k_0}^i$  множество  $\tilde{\Gamma}(i)$  будет содержать верное слово  $\tilde{\gamma}_{i, k_0}^i = \gamma_i$ .

**Лемма 4.8.** Пусть имеется  $\nu$  пакетов ошибок и  $t$  независимых ошибок, удовлетворяющих условиям теоремы 4.3, и пусть все  $\tilde{\gamma}_s$ ,  $s = \overline{1, i-1}$ , декодированы правильно. Тогда при использовании процедуры  $\psi_i^d(z_i)$  параметр  $t(i, k_0)$ , соответствующий верному слову  $\tilde{\gamma}_{i, k_0}^i = \gamma_i$ , и параметр  $t(i, k)$ ,  $k \neq k_0$ , соответствующий любому другому слову  $\tilde{\gamma}_{i, k}^i \neq \gamma_i$ , удовлетворяют неравенствам

$$t(i, k_0) < d_{as} d_{bi}/2 \leq t(i, k). \quad (4.18)$$

Доказательство лемм 4.7 и 4.8 приведено в приложениях П.4.6 и П.4.7.

**Доказательство теоремы 4.3.** Из леммы 4.7 следует, что выполняется условие а) леммы 4.1 на всех шагах декодирования от 1 до  $i$ . Из леммы 4.8 вытекает, что на всех шагах до  $i$ -го включительно вытекает также и условие б) леммы 4.1. Но это значит, что выполнены необходимые и достаточные условия правильного декодирования  $\tilde{\gamma}_s$ ,  $s = \overline{1, i}$ , при любом сочетании из  $\nu$  пакетов ошибок и  $t$  независимых ошибок, удовлетворяющих условиям (4.15)–(4.17), что завершает доказательство теоремы 4.3.

#### 4.2.2. Простой и полный алгоритмы каскадного декодирования

В предыдущем параграфе были получены оценки реализуемых корректирующих свойств каскадных кодов при декодировании по  $\psi^d(z_1, z_2, \dots, z_m)$  для произвольного набора  $z_i$ ,  $i = \overline{1, m}$ ,  $1 \leq z_i \leq$

$\leq t_{a_i} + 1 = \left\lceil \frac{d_{a_i} - 1}{2} \right\rceil + 1$ . Для выяснения того, каковы пределы изменения корректирующих свойств при изменении наборов, рассмотрим два крайних случая:  $\{z_i = 1, i = \overline{1, m}\}$  и  $\{z_i = t_{a_i} + 1, i = \overline{1, m}\}$ , т. е. алгоритмы  $\psi^d(1, 1, \dots, 1)$  и  $\psi^d(t_{a_1} + 1, t_{a_2} + 1, \dots, t_{a_m} + 1)$ . Первый из этих алгоритмов был назван в разд. 4.1.2 простым. Второй будем называть полным составным алгоритмом.

Рассмотрим сначала простой алгоритм  $\psi^d(1, 1, \dots, 1)$ , для которого все результаты получаются как очевидные следствия из теорем 4.1—4.3.

С л е д с т в и е из т е о р е м ы 4.1.

$$d_i = \frac{2}{3} \min_{1 \leq s \leq i} \{d_{a_s} d_{b_s}\}. \quad (4.19)$$

С л е д с т в и е из т е о р е м ы 4.2.

$$l_i^{(n)} = \min_{1 \leq s \leq i} l_s^*, \quad (4.20)$$

где

$$l_s^* = \begin{cases} n_a(d_{b_s} - 3)/2 + d_{a_s}, & \text{если } d_{b_s} \text{ нечетно;} \\ n_a(d_{b_s} - 4)/2 + (4d_{a_s} - 7)/3, & \text{если } d_{b_s} \text{ четно.} \end{cases} \quad (4.21)$$

С л е д с т в и е из т е о р е м ы 4.3

$$t \leq \frac{1}{3} \min_{1 \leq s \leq i} d_s(p_s). \quad (4.22)$$

Таким образом, из (4.19)—(4.22) вытекает, что при простом алгоритме  $\psi^d(1, 1, \dots, 1)$  не более чем на  $1/3$  снижается доля исправляемых независимых ошибок как при наличии, так и при отсутствии пакетов ошибок. Что же касается длин исправляемых пакетов ошибок, то их оценки незначительно уменьшаются при наличии только одиночного пакета ошибок и не меняются при наличии пакетов ошибок и независимых ошибок одновременно. Учитывая, что декодирование по простому алгоритму  $\psi^d(1, 1, \dots, 1)$  проще, чем по составному, простой алгоритм можно рекомендовать в тех случаях, когда ошибки в основном группируются в пакеты и доля независимых ошибок незначительна.

Рассмотрим теперь полный алгоритм  $\psi^d(t_{a_1} + 1, \dots, t_{a_m} + 1)$ , когда параметры  $z_i$  принимают наибольшее возможное значение  $z_i = t_{a_i} + 1$ . В этом случае критерии  $T_k^{(i)}$  принимают все возможные значения от 0 до  $t_{a_i}$ , так что

$$T_1^{(i)} = 0, T_2^{(i)} = 1, \dots, t_{a_i}^{(i)} = z_i - 1 = t_{a_i}, \quad (4.23)$$

и, следовательно, выражение (П.4.6), определяющее наименьшую кратность ошибки, при которой на  $i$ -ом шаге возможно непра-

вильное декодирование слова  $\hat{t}_i$ , принимает вид  $t = d_{bi}(t_{ai} + 1) + e_{xi}(d_{ai} - 2t_{ai} - 2)$ . Подставляя вместо  $t_{ai}$  его значение, получаем

$$t = \begin{cases} d_{ai}d_{bi}/2, & \text{если } d_{ai} \text{ четно;} \\ d_{ai}d_{bi}/2 + d_{bi}/2 - e_{xi}, & \text{если } d_{ai} \text{ нечетно.} \end{cases}$$

Так как должно выполняться условие  $2e_{xi} < d_{bi}$ , то в качестве нижней оценки  $t$  для всех  $d_{ai}$  (как четных, так и нечетных) получаем  $t = d_{ai}d_{bi}/2$ .

Таким образом, для полного составного алгоритма  $\psi^d(t_{a1} + 1, \dots, t_{am} + 1)$  равенство (4.7) из теоремы 4.1 заменяется равенством

$$d_i^{(n)} = \min_{1 \leq s \leq i} \{d_{ai}d_{bi}\}. \quad (4.24)$$

Для одиночного пакета ошибок в качестве следствия из теоремы 4.2 получаем

$$l_i^{(n)} = \min_{1 \leq s \leq i} l_s^*, \quad (4.25)$$

где

$$l_s^* = \begin{cases} n_a(d_{bs} - 3)/2 + d_{as} + t_{as}, & \text{если } d_{bs} \text{ нечетно;} \\ n_a(d_{bs} - 4)/2 + 2d_{as} - 1, & \text{если } d_{bs} \text{ четно.} \end{cases} \quad (4.26)$$

Наконец, в качестве следствия из теоремы 4.3 с учетом (4.23) имеем

$$t \leq \frac{1}{2} \min_{1 \leq s \leq i} d_s(p_s). \quad (4.27)$$

Из выражений (4.24)–(4.27) следует, что улучшение реализуемых при полном составном алгоритме  $\psi^d(t_{a1} + 1, \dots, t_{am} + 1)$  корректирующих свойств каскадного кода по сравнению с тем, что имеет место при простом алгоритме  $\psi^d(1, 1, \dots, 1)$ , касается в основном исправления независимых ошибок как при наличии, так и при отсутствии пакетов ошибок. Следует также отметить, что при исправлении независимых ошибок при отсутствии пакетов ошибок алгоритм  $\psi^d(t_{a1} + 1, \dots, t_{am} + 1)$  полностью реализует нижнюю оценку кодового расстояния каскадного кода.

#### 4.2.3. Эффективное декодирование при сложном характере ошибок

Многие реальные каналы связи имеют сложный характер ошибок, при котором кодовые слова могут быть поражены как независимыми ошибками, так и пакетами ошибок, а также сочетанием пакетов ошибок с независимыми ошибками.

Обычно в теории помехоустойчивого кодирования (за редким исключением) исследуются корректирующие свойства кодов, предназначенных для исправления либо только одиночного пакета

ошибок, либо только независимых ошибок. Для согласования теории с практикой каналы с группирующимися ошибками пытаются превратить в каналы с независимыми ошибками посредством разнесения по времени символов кодового слова (так называемое чередование позиций или декорреляция ошибок).

Однако более привлекательно иметь код, который эффективно исправлял бы независимые ошибки, пакеты ошибок и те и другие одновременно. Кроме того, так как декодер, как правило, не имеет информации относительно характера имевших место в канале ошибок при передаче данного кодового слова, то естественно требовать, чтобы все эти корректирующие свойства кода реализовались одним и тем же алгоритмом декодирования. Отметим, что в теории кодирования, к сожалению, о таких универсальных кодах и алгоритмах декодирования не было известно. В то же время из теорем 4.1 и 4.2 и особенно 4.3 следует, что реализуемые алгоритмом  $\psi^d(z_1, \dots, z_m)$  корректирующие свойства каскадного кода весьма универсальны.

Действительно, рассмотрение следующих примеров показывает, что богатые возможности в этом направлении открывают именно каскадные коды, которые мы будем сравнивать с лучшими двоичными блочными кодами, предназначенными для исправления некоторого определенного типа ошибок, построенными в соответствии с рекомендациями книги Питерсона, Уэлдона [115].

Рассмотрим передачу информации блоками длины  $n=1024$  по каналу, который может находиться в одном из четырех случайно возникающих состояний. При этом, чтобы обеспечить необходимую верность передачи, надо исправлять в зависимости от состояния следующие типы ошибок: в первом — все независимые ошибки кратности  $t \leq 63$ ; во втором — одиночный пакет ошибок длиной  $l \leq 243$ ; в третьем — два пакета ошибок (один длиной  $l^{(1)} \leq 90$ , другой длиной  $l^{(2)} \leq 50$  и еще независимые ошибки кратности  $t \leq 25$ ; в четвертом — четыре пакета ошибок длины  $l^{(u)} \leq 50$ ,  $u=1, 4$ , и еще независимые ошибки кратности  $t \leq 7$ . Допустим, что кодеру и декодеру до передачи соответствующего блока сообщают, в каком из четырех состояний будет находиться канал. Тогда для каждого состояния можно выбрать лучший из известных кодов с соответствующей процедурой декодирования. При этом ограничимся циклическими кодами БЧХ. Тогда для первого состояния лучшим будет код БЧХ с параметрами  $n=1024$ ,  $k=453$  ( $R=0,442$ ) и  $d=128$ .

Во втором состоянии можно использовать код Файра с параметрами  $n=1024$ ,  $k=296$  ( $R=0,239$ ), но лучше использовать код Рида—Соломона над полем  $GF(2^8)$  длины  $n=128$  с  $d=65$ , т. е. двоичный код с параметрами  $n=1024$ ,  $k=512$  ( $R=0,5$ ).

В третьем состоянии можно использовать коды БЧХ с параметрами  $n=1024$ ;  $k=133$  ( $R=0,130$ ) и  $d \geq 256$ , но лучше использовать код РС над полем  $GF(2^8)$  длины  $n=128$  с  $d=95$ , т. е. двоичный код с параметрами  $n=1024$ ,  $k=275$  ( $R=0,269$ ).

В четвертом состоянии можно использовать код БЧХ с параметрами  $n=1024$ ,  $k=123$  ( $R=0,120$ ) и  $d=342$ , но лучше использовать код РС над полем  $GF(2^8)$  длины  $n=128$  с  $d=79$ , т. е. двоичный код с параметрами  $n=1024$ ,  $k=400$  ( $R=0,391$ ).

Полагая, что состояние канала заранее не известно, будем во всех случаях использовать каскадный код первого порядка с внутренним кодом  $(8,7)$   $d_{a1}=2$  и внешним удлинненным кодом РС над полем  $GF(2^7)$  с  $n_b=128$ ,  $d_{b1}=64$  и  $k_b=65$ , т. е. двоичный код с параметрами  $n=1024$ ,  $k=455$  ( $R=0,444$ ),  $d \geq 128$ . При этом в качестве алгоритма декодирования будем использовать алгоритм  $\psi^d(1)$ , который для  $d_{a1}=2$  является одновременно и простым и полным.

Тогда, как следует из теоремы 4.1, будут исправляться все ошибки кратности  $t \leq 63$ . Из теоремы 4.2 вытекает, что тот же код с тем же алгоритмом декодирования исправит все ошибки во втором состоянии, а из теоремы 4.3 получаем, что ошибки в третьем и четвертом состояниях также будут исправлены.

В силу того что используемый код и алгоритм декодирования не меняются, приходим к выводу, что выбранный каскадный код обладает для данного канала (с четырьмя состояниями) универсальными корректирующими свойствами. При этом такая универсальность достигается не за счет потери скорости передачи, а, наоборот, при выигрыше в скорости передачи в трех из четырех возможных состояниях канала (первом, третьем и четвертом). Причем если во втором состоянии канала использовать код Файра, то каскадный код и в этом случае выигрывает в скорости передачи.

В качестве второго примера рассмотрим каскадный код третьего порядка ( $m=3$ ) с параметрами  $n=1023$ ;  $k=185$ ;  $n_a=31$ ,  $n_b=33$ ,  $a_1=a_2=a_3=5$ ,  $b_1=4$ ,  $b_2=14$ ,  $b_3=19$ . В качестве внутренних выберем коды БЧХ: первый код  $(31,15)$  с  $d_{a1}=8$ ; второй код  $(31,10)$  с  $d_{a2}=12$ ; третий код  $(31,5)$  с  $d_{a3}=16$ . В качестве внешних выберем удлинненные коды РС: первый код  $(33,4)$  с  $d_{b1}=30$ ; второй код  $(33,14)$  с  $d_{b2}=20$ ; третий код  $(33,19)$  с  $d_{b3}=15$ .

Для кодового расстояния каскадного кода получаем оценку  $d \geq \min \{16 \cdot 15; 12 \cdot 20; 8 \cdot 30\} = 240$ .

Используем полный алгоритм каскадного декодирования  $\psi^d(4, 6, 8)$ . Тогда согласно (4.24) для реализуемого кодового расстояния  $d_i$ ,  $i = \overline{1, 3}$ , получаем  $d_1^{(n)} = d_2^{(n)} = d_3^{(n)} = 240$ , так что этот каскадный код при использовании полного алгоритма декодирования может исправить все независимые ошибки, кратность которых  $t \leq 119$ .

Наилучший из кодов БЧХ длины  $n=1023$  с такой же корректирующей способностью имеет несколько меньшее число информационных символов (182 вместо 185).

В соответствии с (4.25) и (4.26) для наибольшей длины исправляемого одиночного пакета ошибок получаем  $l_1^{(n)}=422$ ,  $l_2^{(n)}=271$ ,  $l_3^{(n)}=217$ . Заметим, что код Файра с такой же скоростью передачи исправляет одиночный пакет ошибок длины  $l \leq 280$ .



Если возникают два пакета ошибок длины  $l^{(1)}=75$  и  $l^{(2)}=40$ , то в соответствии с теоремой 4.3 имеем

$$\begin{array}{llll} v_{11}=4, & v_{12}=2, & p_1=6, & d_1(p_1)=18 \cdot 8 = 144, \\ v_{21}=4, & v_{22}=2, & p_2=6, & d_2(p_2)=18 \cdot 12 = 112, \\ v_{31}=3, & v_{32}=2, & p_3=5, & d_3(p_3)=5 \cdot 16 = 80. \end{array}$$

Приведенные результаты означают, что:

а) при независимых ошибках все информационные символы защищены одинаково, причем исправляются любые ошибки кратности  $t \leq 119$ ;

б) двадцать информационных символов, расположенных в блоке  $\gamma_1$ , защищены от одиночного пакета длины от 272 до 242. Девяносто информационных символов, расположенных в блоках  $\gamma_1$  и  $\gamma_2$ , защищены от одиночного пакета длины от 218 до 271, и все информационные символы защищены от одиночного пакета длины не более 217;

в) если имеют место два пакета ошибок длины  $l^{(1)} \leq 75$  и  $l^{(2)} \leq 40$ , то двадцать информационных символов в блоке  $\gamma_1$  защищены от этих пакетов и дополнительных независимых ошибок кратности до 71. Девяносто информационных символов в блоках  $\gamma_1$  и  $\gamma_2$  защищены от этих пакетов и дополнительных независимых ошибок кратности до 55, и все информационные символы защищены от этих пакетов и дополнительных независимых ошибок кратности до 40.

Следует отметить, что неизвестны примеры других некаскадных кодов той же длины и скорости передачи, которые при неизменном алгоритме декодирования могли бы исправлять независимые ошибки кратности  $t \leq 119$ , одиночный пакет ошибок длины  $l \leq 217$  и совокупность из двух пакетов ошибок длины 75 и 40 и независимых ошибок кратности  $t < 40$ . Это обстоятельство еще раз свидетельствует об универсальности каскадных кодов и алгоритма декодирования  $\psi^d(z_1, \dots, z_m)$  применительно к каналам со сложным характером ошибок.

Кроме того, приведенный пример наглядно показывает, что при каскадном декодировании только в каналах с независимыми ошибками можно говорить о равной защите информационных символов, что следует также и из общего анализа теорем 4.1 — 4.3.

В каналах со сложным характером ошибок для каскадных кодов порядка  $m > 1$  мы всегда имеем случай неравной защиты информационных символов.

Особенно наглядно универсальность каскадных кодов в каналах со сложным характером ошибок проявляется при рассмотрении асимптотических ( $n \rightarrow \infty$ ) корректирующих свойства этих кодов. Действительно, если  $n \rightarrow \infty$  ( $n_a \rightarrow \infty$ ,  $n_b \rightarrow \infty$ ), то при использовании полного алгоритма каскадного декодирования по расстоянию (при условии, что  $d_{a,b,i} \geq d_{a,i+1}d_{b,i+1}$ ) из теорем 4.1 — 4.3 получаем

$$\frac{t_i}{n} = \frac{1}{2} \frac{d_{ai} d_{bi}}{n_a n_b} = \frac{1}{2} \delta_{\text{ВГ}}(R_{ai})(1 - R_{bi}), \quad (4.28)$$

$$\frac{l_i}{n} = \frac{1}{2} \frac{d_{bi}}{n_b} = \frac{1}{2} (1 - R_{bi}), \quad (4.29)$$

$$\frac{t_i^*}{n} = \frac{d_{ai}}{n_a} \left( \frac{1}{2} \frac{d_{bi}}{n_b} - \frac{L_i}{n} \right) = \delta_{\text{ВГ}}(R_{ai}) \left( \frac{1}{2} (1 - R_{bi}) - \frac{L_i}{n} \right). \quad (4.30)$$

В этих выражениях  $t_i$ ,  $l_i$ ,  $t_i^*$  соответственно наибольшая кратность независимых ошибок при отсутствии пакетов ошибок, наибольшая длина одиночного пакета ошибок и наибольшая кратность независимых ошибок при наличии любого числа пакетов ошибок суммарной длины  $L_i$ , от которых защищены информационные символы, расположенные в первых  $\gamma_s$ ,  $s=1, i$ , блоках. Равенства (4.28) и (4.29) являются частными случаями (4.30). Так, формула (4.28) получается из (4.30) при  $L_i=0$ , а формула (4.29) — из (4.30) при  $t_i^*=0$ . Отсюда, в частности, следует, что определяемая выражением (4.29) величина  $l_i$  может трактоваться как наибольшая суммарная длина любого числа пакетов ошибок (при отсутствии независимых ошибок), от которых защищены информационные символы, расположенные в блоках  $\gamma_s$ ,  $s=1, i$ .

### § 4.3. Возможности каскадного декодирования по вероятности

#### 4.3.1. Оценка вероятности неправильного декодирования

В дальнейшем при рассмотрении каскадного декодирования будем считать, что все слова каскадного кода передаются с одной и той же вероятностью и что двоичные символы передаются до ДСК без памяти с вероятностью трансформации символа, равной  $\epsilon$ .

Пусть принятое слово каскадного кода декодируется по алгоритму  $\psi^p(z_1, \dots, z_m)$ , описанному в разд. 4.1.3, и пусть на первых  $(i-1)$ -х шагах декодирования закончилось правильно. Оценим при этих условиях экспоненту  $E_i^*$  вероятности неправильного декодирования на  $i$ -м шаге, т. е. при использовании процедуры  $\psi_i^p(z_i)$ .

Обозначим через  $D_i^{(j)}$  событие, состоящее в том, что в  $j$ -м столбце «принятым» на  $i$ -м шаге декодирования окажется слово  $\hat{a}^{(j)}(i-1)$  (см. разд. 4.11) при условии, что на первых  $(i-1)$ -х шагах декодирования закончилось правильно. Событию  $D_i^{(j)}$  поставим в соответствие параметр

$$F_i^{(j)} = (E_0(R_{ai}) - h_i v_i^j) n_a, \quad (4.31)$$

где  $E_0(R_{ai})$  — экспонента вероятности ошибки при декодировании кода  $A_i$  по минимуму расстояния,  $h_i > 0$  — некоторый коэффициент, зависящий от скорости передачи  $R_{ai}$ ,

$$v_i^j = \frac{1}{n_a} \log_2 \left[ P(\hat{a}^{(j)}(i-1) | \alpha^{(j)}(i)) \left| \sum_{\substack{x \in A_i \\ x \neq \hat{a}^{(j)}(i)}} P(\hat{a}^{(j)}(i-1) | x) \right| \right], \quad (4.32)$$

$\alpha^{(j)}(i)$  — «переданное» слово кода  $A_i$ , расположенное в  $j$ -м столбце.

Обозначим через  $D_i$  сложное событие, состоящее в том, что для каждого  $j, j=1, n_b$ , имеет место событие  $D_i^{(j)}$ . Событию  $D_i$  поставим в соответствие параметр

$$F_i = \sum_{j=1}^{n_b} F_i^{(j)}, \quad (4.33)$$

где  $F_i^{(j)}$  определяется в соответствии с (4.31). Тогда справедливо следующее утверждение.

**Утверждение 4.2.** Вероятность того, что имеет место событие  $D_i$ , оценивается как

$$P(D_i) \leq 2^{-F_i}. \quad (4.34)$$

Доказательство утверждения 4.2 опирается на следующие леммы.

**Лемма 4.9.** Пусть в  $j$ -м столбце передано слово  $\alpha^{(j)}(i)$ , а принято слово  $\hat{\alpha}^{(j)}(i-1)$ . Пусть в результате декодирования выдается слово  $\hat{\alpha}^{(j)}(i)$ , если для него выполняется условие

$$\log_2 \left[ P(\hat{\alpha}^{(j)}(i-1) | \hat{\alpha}^{(j)}(i)) \left| \sum_{\substack{x \in A_i \\ x \neq \hat{\alpha}^{(j)}(i)}} P(\hat{\alpha}^{(j)}(i-1) | x) \right] > \nu_i n_a, \quad (4.35)$$

где  $\nu_i > 0$  — числовой параметр, и выдается стирание, если это условие не выполняется ни для одного слова кода  $A_i$ . Тогда вероятность стирания  $P_{\text{ст}}$  и вероятность ошибки  $P_{\text{ом}}$ , т. е.  $\hat{\alpha}^{(j)}(i) \neq \alpha^{(j)}(i)$ , оценивается сверху как

$$P_{\text{ст}} \leq 2^{-n_a(E_0(R_{a,i}) - h_i \nu_i)}, \quad P_{\text{ом}} \leq 2^{-n_a(E_0(R_{a,i}) + h_i \nu_i)}, \quad (4.36)$$

где  $h_i > 0$  — тот же числовой параметр, что и в (4.31).

Лемма 4.9 доказывается в приложении П.4.8 и используется при доказательстве леммы 4.10.

**Лемма 4.10.** Вероятность того, что в  $j$ -м столбце имеет место событие  $D_i^{(j)}$ , оценивается сверху как

$$P(D_i^{(j)}) \leq 2^{-F_i^{(j)}}. \quad (4.37)$$

Доказательство леммы 4.10 приведено в приложении П.4.9.

**Доказательство утверждения 4.2.** Событие  $D_i$  по определению заключается в одновременном осуществлении событий  $D_i^{(j)}, j=1, n_b$ , т. е.  $D_i = \bigcap_{j=1}^{n_b} D_i^{(j)}$ . Так как канал по условию без памяти, а код  $A_i$  — линейный, то  $D_i^{(j)}$  — независимые события, следовательно,

$$P(D_i) = \prod_{j=1}^{n_b} P(D_i^{(j)}). \quad (4.38)$$

Подставляя (4. 37) в (4. 38) и учитывая (4. 33), получаем доказательство утверждения 4.2.

**С л е д с т в и е** из у т в е р ж д е н и я 4.2. Вероятность  $P(D_i)$  того, что будет «принято» слово  $\hat{a}(i-1)$ , которому соответствует параметр  $F_i > n(1-R_{bi})E_0(R_{ai})$ , оценивается сверху как

$$P(D_i) \leq 2^{-F_i} \leq 2^{-n(1-R_{bi})E_0(R_{ai})}. \quad (4.39)$$

Оценку для экспоненты  $E_i^*$  получаем из следующей теоремы.

**Теорема 4.4.** Всегда можно выбрать множество критериев  $\{T_1^{(i)}, T_2^{(i)}, \dots, T_{z_i}^{(i)}\}$  составного алгоритма  $\psi^P(z_1, \dots, z_m)$  так, чтобы реализуемая процедурой  $\psi_i^P(z_i)$  экспонента вероятности неправильного декодирования  $E_i^*$  при условии, что на предшествующих  $i-1$  шагах декодирование закончилось правильно, удовлетворяла неравенству

$$E_i^* \geq E_0(R_{ai})(1-R_{bi})2z_i/(2z_i+1). \quad (4.40)$$

Доказательство теоремы вытекает из следующих лемм, доказанных в приложениях П.4.10 и П.4.11.

**Лемма 4.11.** Пусть для «принятого» слова  $\hat{a}(i-1)$  значение параметра  $F_i$ , определяемого в соответствии с (4.33), удовлетворяет условию

$$F_i < nE_0(R_{ai})(1-R_{bi})2z_i/(2z_i+1), \quad (4.41)$$

и пусть все  $\gamma_s$ ,  $s = \overline{1, i-1}$ , декодированы правильно, тогда при использовании процедуры  $\psi_i^P(z_i)$  найдется такое множество критериев  $\{T_1^{(i)}, T_2^{(i)}, \dots, T_{z_i}^{(i)}\}$ , что по крайней мере одному из них —  $T_{k_0}^{(i)}$  в множестве  $\tilde{\Gamma}(i)$  будет соответствовать верное слово  $\tilde{\gamma}_i^{k_0} = \gamma_i$ . Соответствующие значения  $T_k^{(i)}$  определяются равенством

$$T_k^{(i)} = E_0(R_{ai})(2k-1)/(h_i(2z_i+1)). \quad (4.42)$$

**Лемма 4.12.** Пусть для «принятого» слова  $\hat{a}(i-1)$  значение параметра  $F_i$  удовлетворяет условию  $F_i < nE_0(R_{ai})(1-R_{bi})$ , и пусть все  $\gamma_s$ ,  $s = \overline{1, i-1}$ , декодированы правильно, тогда при использовании процедуры  $\psi_i^P(z_i)$  параметр  $E(i, k_0)$ , соответствующий верному слову, и параметр  $E(i, k)$ ,  $k \neq k_0$ , соответствующий любому другому слову  $\tilde{\gamma}_i^{k_0} \neq \gamma_i$ , удовлетворяют неравенствам

$$E(i, k_0) < nE_0(R_{ai})(1-R_{bi}) \leq E(i, k). \quad (4.43)$$

**Доказательство теоремы 4.4.** Из леммы 4.11 следует, что в условиях теоремы 4.4 на  $i$ -м шаге декодирования множество  $\tilde{\Gamma}(i)$  будет содержать верное слово  $\tilde{\gamma}_i^{k_0} = \gamma_i$ . Из леммы 4.12 следует, что в соответствии с процедурой  $\psi_i^P(z_i)$  (см. п. 6 процедуры  $\psi_i^P(z_i)$ ) именно это слово будет выдано в качестве результата декодирования, что и доказывает справедливость теоремы 4.4.

Непосредственно из утверждения 4.2, следствия из него и теоремы 4.4 вытекает следующее утверждение.

**Утверждение 4.3.** Экспонента вероятности неправильного декодирования  $E_i$  до  $i$ -го шага включительно удовлетворяет неравенству

$$E_i \geq E_i^{(n)} = \min_{1 \leq s \leq i} \{E_0(R_{as})(1 - R_{bs})2z_s/(2z_s + 1)\} (1 + o(1)), \quad (4.44)$$

где  $E_i^{(n)}$  — нижняя оценка экспоненты вероятности неправильного декодирования до  $i$ -го шага включительно.

#### 4.3.2. Анализ реализуемой экспоненты вероятности неправильного декодирования

Из утверждения 4.3 следует, что нижняя оценка  $E^{(n)}(R, m)$  экспоненты вероятности неправильного декодирования для всех информационных символов каскадного кода ( $i = m$  и  $E^{(n)}(R, m) = E_m^{(n)}$ ) определяется выражением  $E^{(n)}(R, m) = \min_i \{E_0(R_{ai}) \times (1 - R_{bi})(2z_i/(2z_i + 1) + o(1))\}$ . Отсюда при  $n \rightarrow \infty$  и  $z_i \rightarrow \infty$  получаем

$$E^{(n)}(R, m) = \min_i \{E_0(R_{ai})(1 - R_{bi})\}. \quad (4.45)$$

Таким образом, нижняя оценка экспоненты вероятности неправильного декодирования структурно совпадает с введенной в гл. 2 (см. (2.26)) и подробно изученной в гл. 3 нижней оценкой кодового расстояния каскадного кода. Поэтому исследование  $E^{(n)}(R, m)$  для каскадных кодов произвольного порядка производится точно так же, как и исследование нижней оценки кодового расстояния. Учитывая это обстоятельство, опустим при рассмотрении  $E^{(n)}(R, m)$  ряд деталей, подробно обсуждавшихся в гл. 3. В случае равной защиты всех информационных символов, что соответствует условию  $E_0(R_{ai})(1 - R_{bi}) = E^{(n)}(R, m)$ ,  $i = 1, m$ , после преобразований, аналогичных проведенным в гл. 3, получаем

$$E^{(n)}(R, m) = (R_{a1} - R) \left/ \sum_{i=1}^m [(R_{ai} - R_{a,i+1})/E_0(R_{ai})], \right. \quad (4.46)$$

где  $R = \sum_{i=1}^m (R_{ai} - R_{a,i+1}) R_{bi}$ ,  $R_{a,m+1} = 0$ . Так же, как и в гл. 3, для каскадного кода порядка  $m$  можно выбирать оптимальные значения  $R_{ai}$ , т. е. определять такую структуру каскадного кода, которая максимизирует  $E^{(n)}(R, m)$ . Учитывая полную аналогию в исследовании величин  $E^{(n)}(R, m)$  и  $\delta^{(n)}(R, m)$ , из множества различных вариантов ограничений, налагаемых на структуру каскадного кода и рассмотренных в гл. 3 при  $m > 1$ , остановимся лишь на одном практически наиболее интересном случае, когда  $R_{ai} = R_{a1}(m - i + 1)/m$ . Подставляя это выражение для  $R_{ai}$  в (4.46), получаем

$$E^{(n)}(R, m) = \max_{R_{a1}} \left\{ m(R_{a1} - R) \left/ \left[ R_{a1} \sum_{i=1}^m (E_0(R_{a1}(m - i + 1)/m))^{-1} \right] \right. \right\}. \quad (4.47)$$

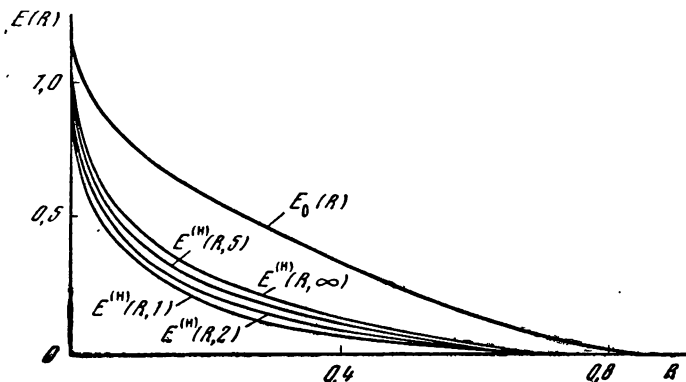


Рис. 4.2. Экспонента вероятности неправильного каскадного декодирования обобщенного каскадного кода в ДСК без памяти с вероятностью ошибки в символе  $\epsilon=0,01$

При  $m \rightarrow \infty$ , повторяя рассуждения, проведенные в гл. 3 для кодов бесконечного порядка структуры  $A$ , получаем для структуры, максимизирующей нижнюю оценку экспоненты вероятности неправильного декодирования:  $y=1-E^{(\infty)}(R, \infty)/E_0(x)$ , где

$$R = \int_0^{x_0} y dx = x_0 - E^{(\infty)}(R, \infty) \int_0^{x_0} \frac{dx}{E_0(x)} \quad E^{(\infty)}(R, \infty) = E_0(x_0).$$

Результаты соответствующих расчетов для  $m=1, 2, 5$  и  $\infty$  при вероятности трансформации каждого из передаваемых двоичных символов, равной  $\epsilon=0,01$ , приведены в табл. 4.1 и на рис. 4.2.

Таблица 4.1

$m=1$		$m=2$		$m=5$		$m=\infty$	
$R$	$E^{(1)}(R, 1)$	$R$	$E^{(2)}(R, 2)$	$R$	$E^{(5)}(R, 5)$	$R$	$E^{(\infty)}(R, \infty)$
0,0000	1,1645	0,0000	1,1645	0,0000	1,1645	0,0000	1,1645
0,0222	0,5724	0,0190	0,6423	0,0175	0,6925	0,0158	0,7358
0,0670	0,3761	0,0580	0,4540	0,0522	0,5150	0,0437	0,5655
0,1293	0,2506	0,1136	0,3250	0,1017	0,3881	0,0927	0,4405
0,2167	0,1549	0,1926	0,2194	0,2172	0,2303	0,1533	0,3382
0,3387	0,0769	0,3094	0,1231	0,3446	0,1298	0,2428	0,2382
0,4725	0,0302	0,4495	0,0538	0,4954	0,0570	0,3696	0,1420
0,6018	0,0096	0,5897	0,0183	0,6455	0,0182	0,5198	0,0682
0,7424	0,0015	0,7394	0,0030	0,7291	0,0069	0,6894	0,0209
0,8146	0,0003	0,8899	0,00001	0,8103	0,0015	0,8740	0,0006
0,9192	0,0000	0,9192	0,0000	0,9192	0,0000	0,9192	0,0000

Отсюда непосредственно следует, что при всех  $m$  нижняя оценка вероятности неправильного декодирования  $E^{(m)}(R, m)$  существенно

уступает оценке Галлагера  $E_0(R)$  и по мере увеличения  $m$  быстро приближается к значению  $E^{(n)}(R, \infty)$ .

Исследование вопросов неравной защиты информационных символов осуществляется точно так же, как и в § 3.5 гл. 3 при анализе уровней защиты каскадных кодов НЗ. Аналогичные результаты проиллюстрируем лишь на одном примере каскадного кода бесконечного порядка, когда символы, соответствующие значениям  $x$ :  $x_1 \leq x \leq x_0$  и  $x$ :  $0 \leq x \leq x_1$ , защищены с экспонентой вероятности неправильного декодирования, нижняя оценка которой соответственно равна  $E^{(1n)}$  и  $E^{(2n)} < E^{(1n)}$ .

В этом случае структура каскадного кода определяется равенствами  $y = 1 - E^{(1n)}/E_0(x)$  при  $x_1 \leq x \leq x_0$ ,  $y = 1 - E^{(2n)}/E_0(x)$  при  $0 \leq x < x_1$ . Связь  $R^{(1)}$  и  $R^{(2)}$  с величинами  $E^{(1n)}$  и  $E^{(2n)}$  задается соотношениями

$$R^{(1)} = x_0 - x_1 - E^{(1n)} \int_{x_1}^{x_0} \frac{du}{E_0(u)}, \quad R^{(2)} = x_1 - E^{(2n)} \int_0^{x_1} \frac{du}{E_0(u)},$$

где  $E^{(1n)} = E_0(x_0)$ . При этом скорость передачи  $R = R^{(1)} + R^{(2)}$ .

## СЛУЧАЙНЫЕ КАСКАДНЫЕ КОДЫ

В предшествующих главах были исследованы конструктивно достижимые корректирующие свойства, т. е. возможность построения каскадных кодов непереборным методом с наилучшими корректирующими свойствами, и реализуемые корректирующие свойства при каскадном декодировании. К сожалению, нет обоснованных надежд, что эти эффективно получаемые оценки корректирующих свойств в большинстве исследованных случаев могут быть улучшены. Поэтому значительный теоретический интерес представляет исследование предельных потенциальных возможностей каскадных кодов, т. е. когда нет ограничений на сложность построения и декодирования.

В теории помехоустойчивого кодирования обычно потенциальные возможности того или иного класса кодов выясняются при исследовании всех кодов из данного класса. Для этого на всем классе кодов задается некоторое распределение вероятностей, т. е. строится ансамбль, выясняются средние по классу корректирующие свойства. Очевидно, что потенциальные корректирующие свойства лучших кодов не хуже средних по ансамблю. Успех такого метода для частных классов кодов определяется удачным выбором ансамбля, т. е. ограничений на класс кодов и распределения вероятностей на нем.

В настоящей главе разработаем методику построения и исследования ансамблей каскадных кодов различного порядка. Эта методика связана с решением следующих задач:

- разработкой различных ансамблей случайных каскадных кодов;

- построением и исследованием систем вложенных кодов, которые будут использоваться в качестве внутренних кодов в ансамблях каскадных кодов;

- исследованием свойств случайных  $q$ -чных кодов и случайных кодов РС, используемых в качестве внешних кодов;

- разработкой методики построения производящих функций средних весов кодовых слов в ансамблях каскадных кодов;

- разработкой способов оценки среднего по ансамблю кодового расстояния каскадного кода;

- исследованием ограничений на скорости передачи внутренних и внешних кодов, при выполнении которых в ансамбле существуют коды, удовлетворяющие границе ВГ;

- определением условий, при которых средний по ансамблю спектр весов слов каскадных кодов позволяет утверждать, что существуют каскадные коды с лучшей из известных экспонентой



вероятности ошибки при декодировании по максимуму правдоподобия;

сравнением потенциальных и реализуемых при каскадном декодировании корректирующих свойств.

Все эти результаты и некоторые другие будут получены в настоящей главе.

## § 5.1. Ансамбли каскадных кодов

### 5.1.1. Случайные линейные блочные коды

Рассмотрим некоторое множество линейных блочных кодов длины  $n$  над полем  $GF(q)$  с одинаковой для всех кодов скоростью передачи  $R$ . Если на множестве этих кодов задано распределение вероятностей, то оно образует ансамбль линейных блочных кодов.

Код, выбираемый из ансамбля с соответствующей этому коду вероятностью, будем называть случайным кодом.

Рассмотрим все  $q$ -чные слова длины  $n$  и веса  $w$ , общее число которых равно  $B(w) = (q-1)^w C_n^w$ , перенумеруем их в некотором порядке и выделим вполне определенное слово с номером  $k = \overline{1, B(w)}$ . После этого выберем из ансамбля случайный код и обозначим через  $P_k(w)$  — вероятность того, что выделенное  $k$ -е слово веса  $w$  является кодовым словом этого случайно выбранного кода. Тогда при равномерном распределении случайных кодов среднее по ансамблю (т. е. приходящееся на каждый случайный код) число кодовых слов  $\bar{N}(w)$  веса  $w$  определяется равенством (см. приложение П.5.1)

$$\bar{N}(w) = \sum_{k=1}^{B(w)} P_k(w). \quad (5.1)$$

Соотношение (5.1) определяет (при известных  $P_k(w)$ ) средний по ансамблю спектр весов случайного кода.

Обозначим через  $\bar{M}(w)$  среднее число ненулевых кодовых слов случайного кода, вес которых не превосходит  $w$ . Тогда

$$\bar{M}(w) = \sum_{v=1}^w \bar{N}(v), \quad (5.2)$$

и если для некоторого  $w = n\delta$  величина  $\bar{M}(n\delta) < 1$ , то это означает, что среди кодов, образующих ансамбль, есть такие, которые не содержат кодовых слов веса, меньшего или равного  $n\delta$ . В силу линейности кодов это в свою очередь означает, что в ансамбле имеются коды, кодовое расстояние которых превосходит величину  $n\delta$ .

Очевидно, что  $\bar{M}(n\delta)$  является верхней оценкой вероятности того, что кодовое расстояние  $d$  случайного кода не превосходит величины  $n\delta$ , т. е.

$$P(d \leq n\delta) \leq \bar{M}(n\delta) = \sum_{w=1}^{n\delta} \bar{N}(w). \quad (5.3)$$

Если правая часть (5.3) больше или равна единице, то оценка оказывается тривиальной, если же она меньше единицы, то это гарантирует существование в ансамбле кодов с кодовым расстоянием  $d > n\delta$ .

### 5.1.2. Оценки кодового расстояния и спектра весов случайных кодов

Для оценки сверху среднего спектра весов  $\bar{N}(w)$  и вероятности  $P(d \leq n\delta)$  используем производящую функцию  $\psi(z)$  среднего числа ненулевых кодовых слов веса  $w$ , содержащихся в случайном коде из данного ансамбля. Так как

$$\psi(z) = \sum_{v=1}^n \bar{N}(v) z^v, \quad (5.4)$$

то при любом  $z$ :  $0 < z < 1$  и  $w \geq 1$  справедливо неравенство  $\bar{N}(w) z^w \leq M(w) z^w \leq \sum_{v=1}^w \bar{N}(v) z^v \leq \sum_{v=1}^n \bar{N}(v) z^v = \psi(z)$  и, следовательно,

$$\bar{N}(w) \leq M(w) \leq \inf_{0 < z < 1} \{\psi(z)/z^w\}. \quad (5.5)$$

Для многих представляющих интерес ансамблей точное определение производящей функции (5.4) является либо слишком сложным, либо практически невозможным. Однако почти во всех случаях удастся сравнительно просто найти верхнюю оценку производящей функции, т. е. указать такую функцию  $\Psi(z)$  с неотрицательными при  $z^v$  коэффициентами, что для всех  $z > 0$   $\psi(z) \leq \Psi(z)$ . Тогда приведенную выше верхнюю оценку для  $\bar{N}(w)$  можно заменить соотношением

$$\bar{N}(w) \leq M(w) \leq \inf_{0 < z < 1} \{\Psi(z)/z^w\}. \quad (5.6)$$

Обозначим через  $\delta^*(R)$  такое наибольшее значение  $\delta$ , что при  $w = n\delta^*$  правая часть (5.6) обращается в единицу, тогда, учитывая (5.3) и что  $P(d \leq n\delta)$  возрастает с увеличением  $\delta$ , приходим к выводу, что для любого  $\varepsilon > 0$   $P\{d \leq n(\delta^*(R) - \varepsilon)\} < 1$ . Но, как уже отмечалось выше, это значит, что среди кодов, образующих данный ансамбль, есть такие, кодовое расстояние которых  $d > n(\delta^*(R) - \varepsilon)$ . Так как  $\varepsilon > 0$  может выбираться сколь угодно малым, то величина  $\delta^*(R)$  представляет собой границу заведомо достижимого для случайных кодов из рассматриваемого ансамбля отношения  $d/n = \delta(R)$ . Эту границу, определяемую равенством

$$\inf_{0 < z < 1} \{\Psi(z)/z^{n\delta^*(R)}\} = 1, \quad (5.7)$$

будем называть нижней границей величины  $\delta(R)$  для случайных линейных кодов. Случайные коды, для которых  $d > n(\delta^*(R) -$

$\varepsilon$ ), будем называть «хорошими», а коды, для которых  $d \leq n(\delta^* - \varepsilon)$ , — «плохими». При этом доля  $\xi$  «плохих» кодов определяется очевидным равенством

$$\xi = P\{d \leq n(\delta^* - \varepsilon)\}. \quad (5.8)$$

Перейдем к рассмотрению спектра весов, характеризуемого числом кодовых слов веса  $w$ , содержащихся в случайном коде. Верхняя оценка  $N(w)$  определяется следующим утверждением, доказательство которого приведено в приложении П.5.2.

**Утверждение 5.1.** Среди случайных линейных кодов над полем  $GF(q)$  при  $n \rightarrow \infty$  существуют коды со спектром весов

$$\begin{aligned} N(w) &= 0 && \text{при } 1 \leq w \leq n(\delta^* - \varepsilon), \\ N(w) &\leq f(n) \bar{N}(w) && \text{при } n(\delta^* - \varepsilon) < w \leq n, \end{aligned} \quad (5.9)$$

где  $\delta^*$  — граница достижимого для данного ансамбля отношения  $d/n$ , а  $f(n)$  — функция, возрастающая не быстрее степенной, с показателем степени  $k > 1$ , т. е.  $f(n) \leq An^k$ .

Спектр весов, удовлетворяющий условию (5.9), будем называть «хорошим».

В заключение отметим, что в ряде случаев (с ними мы столкнемся при исследовании случайных каскадных кодов) производящая функция  $\psi(z)$  (или ее оценка  $\bar{\psi}(z)$ ) представляет собой

сумму функций  $\psi(z) = \sum_{s=1}^k \psi_s(z)$ , каждая из которых имеет вид

$$\psi_s(z) = \sum_{w=1}^n \bar{N}_s(w) z^w, \quad \bar{N}_s(w) \geq 0.$$

Тогда, очевидно, имеем  $\bar{N}(w) = \sum_{s=1}^k \bar{N}_s(w)$ , и если для каждого  $\bar{N}_s(w)$  найдем верхнюю оценку  $\bar{N}_s(w) \leq \inf_{0 < z < 1} \{\psi_s(z)/z^w\}$ , то выражение (5.5) заменится выражением

$$\bar{N}(w) \leq M(w) \leq \sum_{s=1}^k \inf_{0 < z < 1} \{\psi_s(z)/z^w\}. \quad (5.10)$$

Заменяя  $w$  на  $n\delta$ , получаем

$$P(d \leq n\delta) \leq M(n\delta) \leq \sum_{s=1}^k \inf_{0 < z < 1} \{\psi_s(z)/z^{n\delta}\}. \quad (5.11)$$

При этом  $\inf_{0 < z < 1} \{\psi(z)/z^{n\delta}\} = \inf_{0 < z < 1} \left\{ \sum_{s=1}^k \psi_s(z)/z^{n\delta} \right\} \geq \sum_{s=1}^k \inf_{0 < z < 1} \{\psi_s(z)/z^{n\delta}\}$ , так что в этом случае оценка (5.10) оказывается лучше оценки (5.5).

### 5.1.3. Ансамбли каскадных кодов заданной структуры

Напомним, что линейные двоичные каскадные коды заданной структуры, которая характеризуется порядком каскадного кода  $m$  и величинами  $R_{a_i}$ ,  $R_{b_i}$ ,  $i = \overline{1, m}$ , определяются набором из  $n_b$  невыро-

жденных двоичных матриц  $G_0^{(j)}$  (или  $H_0^{(j)}$ ),  $j = \overline{1, n_b}$ , порядка  $n_a$  и  $m$ , линейными над полем  $GF(2^{a_i})$  внешними кодами  $(n_b, b_i)$ ,  $i = \overline{1, m}$ .

Поэтому ансамбли каскадных кодов заданной структуры можно строить, выбирая случайно хотя бы одну из матриц  $G_0^{(j)}$  или хотя бы один из внешних кодов  $(n_b, b_i)$ . При этом очевидна возможность построения весьма разнообразных по своему характеру ансамблей каскадных кодов. Существенно сузим класс таких ансамблей, отметив лишь ансамбли, при построении которых либо все матрицы  $G_0^{(j)}$ ,  $j = \overline{1, n_b}$ , выбираются случайно из некоторого множества невырожденных матриц, либо все внешние коды  $(n_b, b_i)$ ,  $i = \overline{1, m}$ , являются случайными, либо когда выполняются оба эти условия.

Основные ансамбли каскадных кодов, отвечающие этой классификации, приведены в табл. 5.1, в которой под ненулевым эле-

Таблица 5.1

Характер матриц $G_0^{(j)}$	Внешние коды. Класс матриц $G_0^{(j)}$	Случай- ные коды над полем $GF(2^{a_i})$	Случайные коды РС над полем $GF(2^{a_i})$	Неслучай- ные коды РС над полем $GF(2^{a_i})$
$G_0^{(j)}$ — случайные матрицы	Произвольные невыро- жденные матрицы	II	I	I <sup>a</sup>
	Нижние треугольные матрицы	IV	III	III <sup>a</sup>
	Ненулевые элементы поля	II <sup>a</sup>	I <sup>b</sup>	I <sup>a</sup>
$G_0^{(j)}$ — неслучай- ная матрица	Произвольная невыро- жденная матрица	II <sup>b</sup>	I <sup>г</sup>	—
	Нижняя треугольная матрица	V	VI	—
	Ненулевой элемент поля	VII	VIII	—

ментом поля  $GF(2^{n_a})$  подразумевается выбор такой матрицы  $G_0^{(j)}$ , умножение на которую столбца  $\gamma^{(j)}$  эквивалентно умножению на ненулевой элемент поля  $GF(2^{n_a})$  указанного столбца  $\gamma^{(j)}$ , рассматриваемого как элемент этого же поля (см. разд. 2.3.4). Под случайным кодом РС подразумевается случайный линейный код над полем  $GF(2^{a_i})$ , кодовое расстояние и спектр весов которого совпадает с кодовым расстоянием и спектром весов кода РС. (Подробно о построении таких кодов будет сказано в дальнейшем).

Следует отметить, что у ансамблей, для которых  $G_0^{(j)}$  — неслучайные матрицы, можно при всех  $j = \overline{1, n_b}$  выбирать одну и ту же (наилучшую в некотором смысле) матрицу  $G_0$  (как это делалось в предыдущих главах).

Приведенные в табл. 5.1 десять различных ансамблей каскадных кодов отличаются друг от друга объемом, характером декодирования входящих в них кодов, а в ряде случаев и статистическими свойствами.

Случайные каскадные коды, входящие в ансамбли, отмеченные одним и тем же номером, как будет показано, асимптотически обладают одинаковыми средними по ансамблю корректирующими свойствами. В то же время сложность декодирования таких кодов и объемы ансамблей, в которые они входят, могут быть существенно различны.

Перейдем к определению общих соотношений для вероятности того, что слово  $\alpha$  является кодовым словом случайного каскадного кода из некоторого ансамбля случайных кодов. В соответствии с определением каскадного кода произвольная ненулевая (веса  $w$ ) двоичная матрица  $\alpha$  размеров  $n_a \times n_b$  является кодовым словом случайного каскадного кода из данного ансамбля, если вспомогательная матрица  $\gamma$ , каждый столбец которой  $\gamma^{(j)}$ ,  $j = \overline{1, n_b}$ , получается из столбца  $\alpha^{(j)}$  матрицы  $\alpha$  посредством умножения его слева на матрицу  $H_0^{(j)} = (G_0^{(j)})^{-1}$ ,  $\gamma^{(j)} = H_0^{(j)} \alpha^{(j)}$  удовлетворяет условию, что каждый ее горизонтальный блок размеров  $a_i \times n_b$  (вектор длины  $n_b$  над полем  $\text{GF}(2^{a_i})$ )  $\gamma_i = (\gamma_{i1}, \gamma_{i2}, \dots, \gamma_{in_b})$  является кодовым словом соответствующего внешнего кода над полем  $\text{GF}(2^{a_i})$ ,  $i = \overline{1, m}$ . Так как нулевому столбцу  $\alpha^{(j)}$  соответствует нулевой столбец  $\gamma^{(j)}$ , ясно, что указанная вероятность существенно зависит от числа ненулевых столбцов слова  $\alpha$ .

Если в качестве матриц  $H_0^{(j)}$  выбираются невырожденные нижние треугольные матрицы и верхние  $k$  векторов  $\alpha_i$ ,  $i = \overline{m-k+1, m}$ , нулевые (т. е.  $\alpha_{ij} = 0$ ,  $i = \overline{m-k+1, m}$ ,  $j = \overline{1, n_b}$ ), то соответствующие им векторы  $\gamma_i$ ,  $i = \overline{m-k+1, m}$ , также являются нулевыми и автоматически принадлежат любому внешнему коду. Поэтому в данном случае искомая вероятность зависит не только от числа ненулевых столбцов слова, но и от числа верхних  $k$  нулевых векторов  $\alpha_i$ ,  $i = \overline{m-k+1, m}$ , этого слова.

Обозначим через  $C_i$  событие, состоящее в том, что  $\gamma_i = 0$ , а через  $D_i$ , что  $\gamma_i$  является ненулевым кодовым словом  $i$ -го внешнего кода. Ненулевое слово  $\alpha$  веса  $w = \overline{1, n}$  является кодовым словом случайного каскадного кода тогда и только тогда, когда блок  $\gamma_0 = 0$ , все блоки  $\gamma_i$ ,  $i = \overline{1, m}$ , являются кодовыми словами (ненулевыми или нулевыми) соответствующих внешних кодов и по крайней мере одно  $\gamma_i \neq 0$ . Это событие, которое обозначим через  $L$ , можно за-

писать в виде  $L = \sum_{i=1}^m D_i \prod_{s \neq i}^m (C_s + D_s) C_0$ . Тогда

$$P(L) = P(C_0) \sum_{i=1}^m P(D_i) \prod_{s \neq i}^m (P(C_s) + P(D_s)). \quad (5.12)$$

Выражение (5.12) будет использоваться в случаях, когда внутренние коды определяются произвольными невырожденными матрицами  $G_0^{(j)}$  или ненулевыми элементами поля  $GF(2^{n_a})$ .

Если же внутренние коды определяются невырожденными нижними треугольными матрицами, то событие  $L$  следует детализировать, представляя его как  $L = \sum_{k=0}^{m-1} L_k$ , где событие  $L_k$ ,  $k = \overline{0, m-1}$ , соответствует слову  $\alpha$ , верхние блоки  $\alpha_i$  ( $i = \overline{m-k+1, m}$ ) которого нулевые, а блок  $\alpha_{m-k} \neq 0$ .

Так как в этом случае  $L_k = \sum_{i=1}^{m-k} D_i \prod_{s \neq i}^{m-k} (C_s + D_s) C_0$ , то

$$P(L_k) = P(C_0) \sum_{i=1}^{m-k} D_i \prod_{s \neq i} (P(C_s) + P(D_s)). \quad (5.13)$$

Вероятности  $P(L)$  и  $P(L_k)$ , существенно зависящие от числа ненулевых столбцов слова  $\alpha$  и характера внешних кодов, будем в дальнейшем обозначать соответственно через  $P_l(w) = P(L)$  и  $P_l^{(k)}(w) = P(L_k)$ , где  $w \neq 0$  — вес слова  $\alpha$ , а  $l$  — число его ненулевых столбцов. Условие  $w \neq 0$  является существенным, так как при  $w = 0$  во всех случаях  $P_l(w) = P_l^{(k)}(w) = 1$ .

## § 5.2. Ансамбли внутренних кодов

### 5.2.1. Ансамбль невырожденных матриц

Рассмотрим случай, когда матрицы  $G_0^{(j)}$ , определяющие внутренние коды каскадного кода, выбираются из множества всех двоичных невырожденных матриц  $n_a$ -го порядка. Общее число всех таких матриц

$$S = \prod_{s=0}^{n_a-1} (2^{n_a} - 2^s) \simeq c 2^{n_a^2}, \quad (5.14)$$

где  $c \simeq 0,288777$ .

Будем считать множество указанных матриц заданным и каждую из матриц  $H_0^{(j)}$  выбирать случайно (с вероятностью  $1/S$ ) из этого множества. Полученные таким образом матрицы  $H_0^{(j)}$  будем называть невырожденными случайными матрицами. Однако при указанном выборе матриц  $H_0^{(j)}$  нет оснований считать, что все двоичные символы, образующие  $H_0^{(j)}$ , независимы и равновероятны. Поэтому для вычисления вероятностей  $P(D_i)$  и  $P(C_i)$  нам понадобится следующая лемма, доказательство которой приведено в приложении П.5.3.

**Лемма 5.1.** Если  $H_0^{(j)}$  — невырожденная случайная матрица, то вероятность того, что заданные ненулевые слова  $\alpha^{(j)}$  и  $\gamma^{(j)}$  связаны соотношением

$$H_0^{(j)} \alpha^{(j)} = \gamma^{(j)}, \quad (5.15)$$

не зависит от слов  $\alpha^{(j)} \neq 0$  и  $\gamma^{(j)} \neq 0$  и равна  $(2^{n_a} - 1)^{-1}$ .

С л е д с т в и е из л е м м ы 5.1. Пусть столбец  $\gamma^{(j)}$  получен из ненулевого столбца  $\alpha^{(j)}$  в результате умножения его на невырожденную случайную матрицу  $H_0^{(j)}$ , и пусть для некоторого  $s$  элемент  $\gamma_{s,j}$  отличен от нуля. Тогда каждый из оставшихся элементов  $\gamma_{i,j}$ ,  $i=0, m$ ,  $i \neq s$ , может быть любым (в том числе и нулевым) элементом поля  $GF(2^{a_i})$  с одной и той же (для каждого  $i$ ) вероятностью  $2^{-a_i}$ .

Рассмотрим произвольную систему вложенных кодов, порождаемых невырожденной случайной матрицей  $H_0^{(j)}$ . Ненулевое слово является кодовым словом некоторого подкода со скоростью передачи  $a/n_a$ ,  $a=1, n_a$  тогда и только тогда, когда выполняется условие  $H_0^{(j)}\alpha^{(j)}=\gamma^{(j)}$ , где столбец  $\gamma^{(j)}$  в последних (нижних)  $n_a-a$  позициях содержит нулевые символы. Так как слово  $\alpha^{(j)}$  ненулевое (а значит, и  $\gamma^{(j)} \neq 0$ ), то согласно следствию из леммы 5.1 вероятность выполнения указанного условия равна  $P_j(w)=2^{-(n_a-a)}$ . Это выражение для вероятности  $P_j(w)$  позволяет легко найти производящую функцию  $\psi_j(z)$  среднего спектра весов ненулевых кодовых слов рассматриваемого случайного подкода.

Согласно формуле (5.1) и учитывая, что  $B(w)=C_{n_a}^w$ , получаем при  $w \neq 0$   $\bar{N}(w)=2^{-(n_a-a)}C_{n_a}^w \leq 2^{-(n_a-a)}2^{n_a H(w/n_a)}$ , так что

$$\psi_j(z) = \sum_{w=1}^{n_a} \bar{N}(w) z^w = 2^{-(n_a-a)} \sum_{w=1}^{n_a} C_{n_a}^w z^w = 2^{-(n_a-a)} [(z+1)^{n_a} - 1].$$

Выбирая в качестве верхней оценки  $\psi_j(z)$  функцию  $\Psi_j(z) = (z+1)^{n_a} 2^{-(n_a-a)}$  и используя выражения (5.3) и (5.6), получаем  $P(d \leq n_a \delta) \leq 2^{n_a \{H(\delta) - 1 + a/n_a\}}$ , откуда следует, что  $\delta^*(a/n_a) = \delta_{\text{ВГ}}(a/n_a)$ .

Таким образом, нижняя граница величины  $\delta(a/n_a)$  для любого подкода, определяемого невырожденной случайной матрицей  $H_0^{(j)}$ , совпадает с границей ВГ. Кроме того, так как доля «плохих» подкодов  $\xi = P\{d \leq (\delta^* - \varepsilon)n_a\}$  при  $n_a \rightarrow \infty$  убывает экспоненциально по  $n_a$ , то доля «хороших» подкодов экспоненциально по  $n_a$  стремится к единице. Отсюда следует (см. приложение П.5.2), что среди «хороших» подкодов существуют подкоды с «хорошим» спектром весов, т. е. такие, для которых

$$N(w) = 0 \quad \text{при} \quad 1 \leq w < n_a \delta_{\text{ВГ}}(a/n_a);$$

$$N(w) \leq f(n_a) 2^{n_a \{H(w/n_a) - 1 + a/n_a\}} \quad \text{при} \quad n_a \delta_{\text{ВГ}}(a/n_a) \leq w \leq n_a,$$

где  $f(n_a) \geq A n_a$ .

При этом вероятность невыполнения последнего условия  $P\{N(w) > f(n_a) \bar{N}(w)\} \leq (1 - \delta_{\text{ВГ}}(a/n_a) + \varepsilon) (n_a/f(n_a))$ . Так как полученные результаты справедливы для всех значений  $a=1, n_a$ , то вероятность, что хотя бы для одного из подкодов вложенной системы, определяемых значением  $a$ , кодовое расстояние оказывается меньше, чем  $\delta_{\text{ВГ}}(a/n_a) - \varepsilon$ , а  $N(w) > f(n_a) 2^{n_a \{H(w/n_a) - 1 + a/n_a\}}$ , не пре-

восходит соответственно величины  $n_a \max_a 2^{n_a \{H(\delta_{\text{ВГ}}(a/n_a) - \varepsilon) - 1 + a/n_a\}}$  и  $n_a \max_a \{1 - \delta_{\text{ВГ}}(a/n_a) + \varepsilon\} n_a / f(n_a)$ . Первая из этих величин экспоненциально стремится к нулю, а вторая оказывается меньше единицы, если  $f(n_a) = n_a^2$  и  $a < n_a$ , и стремится к нулю, если  $f(n_a) = n_a^\alpha$ , где  $\alpha > 2$ .

Таким образом, при  $n_a \rightarrow \infty$  почти все невырожденные случайные матрицы  $H_0^{(j)}$  определяют такие вложенные системы кодов, для которых каждый подкод имеет кодовое расстояние, достигающее границы ВГ, и «хороший» (с коэффициентом  $f(n_a) = n_a^\alpha$ ,  $\alpha > 2$ ) спектр весов  $N(w)$ .

### 5.2.2. Ансамбль невырожденных треугольных матриц

Рассмотрим случай, когда матрицы  $H_0^{(j)}$  выбираются из множества всех невырожденных двоичных нижних треугольных матриц. Так как все диагональные элементы таких матриц равны единице, а все остальные элементы произвольны, то общее число указанных матриц  $S = 2^{n_a(n_a-1)/2}$ . В данном случае имеется весьма простой случайный алгоритм построения матриц  $H_0^{(j)}$ , обеспечивающий как невырожденность, так и равновероятность получающихся на его основе матриц. Этот алгоритм состоит в том, что все элементы матрицы, расположенные под диагональными, выбираются случайно и независимо с вероятностью  $1/2$  из элементов поля GF(2). В силу независимости и равновероятности этих элементов условие  $H_0^{(j)} \alpha^{(j)} = \gamma^{(j)}$ , где  $\alpha^{(j)}$  и  $\gamma^{(j)}$  — ненулевые столбцы, причем последние  $n_a - a$  элементов столбца  $\gamma^{(j)}$  нулевые, сводится к выполнению  $n_a - a$  независимых проверочных соотношений, которые в матричной форме имеют вид  $H_a^{(j)} \alpha^{(j)} = 0$ , где  $H_a^{(j)}$  — матрица, получаемая из матрицы  $H_0^{(j)}$  отбрасыванием ее верхних  $a$  строк.

Каждое из этих проверочных соотношений для произвольного фиксированного ненулевого столбца  $\alpha^{(j)}$  выполняется с вероятностью  $1/2$ . В силу независимости проверочных соотношений вероятность выполнения всех  $n_a - a$  соотношений равна  $2^{-(n_a-a)}$ . Но отсюда следует, что все результаты, полученные в разд. 5.2.1 для произвольных невырожденных матриц, сохраняются и для невырожденных нижних треугольных матриц.

### 5.2.3. Ансамбль элементов поля GF( $2^{n_a}$ )

Рассмотрим случай, когда матрицы  $H_0^{(j)}$  выбираются из множества матриц, умножение которых на столбец  $\gamma^{(j)}$  эквивалентно умножению некоторого ненулевого элемента  $g_0^{(j)}$  поля GF( $2^{n_a}$ ) на элемент  $\gamma^{(j)}$  этого же поля, для которого столбец  $\gamma^{(j)}$  является двоичной формой записи.

В этом случае условие  $H_0^{(j)} \alpha^{(j)} = \gamma^{(j)}$  эквивалентно условию  $g_0^{(j)} \alpha^{(j)} = \gamma^{(j)}$ , где  $\alpha^{(j)}$  так же, как и  $\gamma^{(j)}$ , трактуется как элемент поля GF( $2^{n_a}$ ). Так как всего имеется  $2^{n_a} - 1$  ненулевых элементов



поля  $GF(2^a)$ , то общее число рассматриваемых матриц  $H^{(j)}$  равно  $S = 2^{na} - 1$ , т. е. оно значительно уступает и числу невырожденных треугольных и числу невырожденных произвольных матриц.

Так же, как и для произвольных невырожденных матриц, будем предполагать, что для каждого  $j$  элемент  $g_0^{(j)}$  (а значит, и матрица  $H_0^{(j)}$ ) выбирается независимо и с равной вероятностью из множества всех ненулевых элементов поля  $GF(2^{na})$ . Таким образом, теперь условие, что произвольный, но фиксированный элемент  $\alpha^{(j)}$  является кодовым словом соответствующего подкода, определяемого элементом  $g_0^{(j)}$ , состоит в том, что произведение случайно выбранного элемента  $g_0^{(j)}$  на элемент  $\alpha^{(j)} \neq 0$  равно элементу  $\gamma^{(j)} \neq 0$ , в двоичной записи которого последние  $n_a - a$  символов нулевые.

Так как для фиксированного  $\alpha^{(j)} \neq 0$  произведение  $g_0^{(j)}\alpha^{(j)}$  определяет единственный элемент  $\gamma^{(j)}$ , причем для различных  $g_0^{(j)}$  получаем различные элементы  $\gamma^{(j)} \neq 0$ , то в силу равновероятного выбора  $g_0^{(j)}$  получаем равновероятные различные значения  $g_0^{(j)}\alpha^{(j)}$ . Но число всех различных ненулевых произведений  $g_0^{(j)}\alpha^{(j)}$  равно  $2^{na} - 1$ , а число всех ненулевых элементов  $\gamma^{(j)}$ , двоичное представление которых содержит в последних  $n_a - a$  позициях нулевые символы, равно  $2^a - 1$ , следовательно, вероятность выполнения условия  $g_0^{(j)}\alpha^{(j)} = \gamma^{(j)}$  равна  $P_j(w) = (2^a - 1)/(2^{na} - 1) < 2^{-(n_a - a)}$ .

Таким образом, верхняя оценка  $P_j(w)$  в данном случае совпадает со значением  $P_j(w)$ , полученным для произвольных и треугольных невырожденных матриц. Но это значит, что и теперь сохраняются все результаты, полученные в разд. 5.2.1.

#### 5.2.4. Неслучайные внутренние коды

В заключение остановимся на случае, когда внутренние коды являются неслучайными. Тогда, как уже отмечалось выше, для всех  $j$  можно выбрать одну и ту же матрицу  $G_0$  (или, что то же самое, матрицу  $H_0 = G_0^{-1}$ ), порождающую наилучшую в том или ином смысле вложенную систему внутренних кодов.

Рассмотрим столбец  $\alpha^{(j)}$  длины  $n_a$ , символы которого, начиная снизу, разбиты на  $m + 1$  слов  $\alpha_{i,j}$  по  $a_i$ ,  $i = \overline{0, m}$ , символов в каждом. Выделим некоторые  $\nu$  из этих слов, соответствующих произвольному набору индексов  $i: (i_1, i_2, \dots, i_\nu)$ , где  $0 < i_1 < i_2 < \dots < i_\nu \leq m$ ,  $\nu = \overline{1, m}$ , и обозначим через  $A_{i_1 \dots i_\nu}$  множество слов  $\alpha^{(j)} = G_0 \gamma^{(j)}$ , где  $\gamma^{(j)}$  — любой столбец длины  $n_a$ , у которого ненулевые символы могут быть только в словах  $\gamma_{i,j}$ , соответствующих набору  $(i_1, \dots, i_\nu)$ . Тогда множество  $A_{i_1 \dots i_\nu}$  представляет собой линейный двоичный код с  $a_{i_1} + a_{i_2} + \dots + a_{i_\nu}$  информационными символами, размещенными в словах  $\gamma_{i_1,j}, \gamma_{i_2,j}, \dots, \gamma_{i_\nu,j}$ , для которого справедливо следующее утверждение (доказательство его приведено в приложении П.5.4.).

**Утверждение 5.2.** Существует такая невырожденная матрица  $G_0$ , что для любых  $v = \overline{1, m}$  и любого набора  $(i_1, i_2, \dots, i_v)$  в коде  $P_{i_1 \dots i_v}$  число кодовых слов  $N_{i_1 \dots i_v}(w)$  веса  $w > 0$  удовлетворяет условию

$$N_{i_1 \dots i_v}(w) \leq n_a^{2^{2m}} C_{n_a}^w 2^{-\left(n_a - \sum_{s=1}^v a_{i_s}\right)}. \quad (5.16)$$

В дальнейшем предполагается, что неслучайная матрица  $H_0$ , определяющая ансамбль  $\Gamma$ , выбрана так, что  $G_0 = H_0^{-1}$  удовлетворяет условию утверждения 5.2.

### § 5.3. Ансамбли внешних кодов

#### 5.3.1. Ансамбль внешних кодов, определяемый канонической проверочной матрицей

Рассмотрим вопрос о вероятности того, что некоторое фиксированное слово  $\gamma_i$  над полем  $\text{GF}(2^{a_i})$  является кодовым словом случайно выбранного  $i$ -го внешнего кода. Начнем с линейных случайных внешних  $(n_b, b_i)$  кодов, определяемых случайной проверочной матрицей размеров  $(n_b - b_i) \times n_b$  над полем  $\text{GF}(2^{a_i})$ . Так как при кодировании информационного слова  $(\mu_{i1}, \mu_{i2}, \dots, \mu_{ib_i}, 0, \dots, 0)$   $i$ -м внешним кодом  $(n_b, b_i)$  мы хотим сохранить неизменными информационные символы  $\mu_{ij}$ ,  $j = \overline{1, b_i}$ , то проверочную матрицу следует выбирать в канонической форме  $\|P_i E_{n_b - b_i}\|$ , где  $E_{n_b - b_i}$  — единичная матрица порядка  $n_b - b_i$ ,  $P_i$  — случайная матрица размеров  $(n_b - b_i) \times b_i$ . Все элементы матрицы  $P_i$  выбираются случайно (независимо и с равной вероятностью) из множества всех элементов поля  $\text{GF}(2^{a_i})$  (т. е. с вероятностью  $2^{-a_i}$ ).

Интересующая нас вероятность  $P_i(w)$  принадлежности некоторого фиксированного слова  $\gamma_i$  внешнему коду из рассматриваемого ансамбля определяется следующей леммой, доказательство которой приведено в приложении П. 5.5.

**Лемма 5.2.** Вероятность того, что произвольное ненулевое фиксированное слово  $\gamma_i$  над полем  $\text{GF}(2^{a_i})$  веса  $w > 0$  является кодовым словом случайно выбранного  $i$ -го внешнего кода, удовлетворяет неравенству

$$P_i(w) \leq 2^{-a_i(n_b - b_i)}. \quad (5.17)$$

#### 5.3.2. Ансамбль кодов РС

Под ансамблем кодов РС будем понимать множество случайных кодов  $(n_b, b_i)$  над полем  $\text{GF}(2^{a_i})$ , которые получаются из кода РС (или одной из его модификаций) умножением каждого кодового слова на случайную диагональную матрицу, диагональные эле-

менты которой выбираются случайно (независимо и с равной вероятностью) из множества всех ненулевых элементов поля  $GF(2^{a_i})$ . Каждый такой код, который будем называть случайным кодом РС или кодом РС со случайным преобразованием, определяется матрицей

$$A = \begin{pmatrix} g_1 & & 0 \\ & g_2 & \\ & & \ddots \\ 0 & & & g_{n_b} \end{pmatrix},$$

где  $g_j \neq 0 \in GF(2^{a_i})$ .

Так как при умножении матрицы  $A$  на кодовое слово кода РС каждый нулевой символ этого слова переходит в нулевой, а каждый ненулевой символ переходит в ненулевой, то спектр весов любого случайного кода РС совпадает со спектром весов исходного (неслучайного) кода РС.

Отсюда, в частности, следует, что все случайные коды РС из ансамбля, определяемого матрицами  $A$ , имеют одно и то же кодовое расстояние  $d_{b_i} = n_b - b_i + 1$ . Что касается основного вопроса о вероятности принадлежности некоторого фиксированного слова  $\gamma_i$  случайному коду РС, то ответ на него дается следующей леммой, доказательство которой приведено в приложении П.5.6.

**Лемма 5.3.** Вероятность того, что произвольное ненулевое фиксированное слово  $\gamma_i$  над полем  $GF(2^{a_i})$  веса  $w > 0$  является кодовым словом случайного кода РС  $-(n_b, b_i)$ , удовлетворяет условию

$$\begin{aligned} P_i(w) &= 0, & \text{если } 0 < w \leq n_b - b_i; \\ P_i(w) &\leq e2^{-a_i(n_b - b_i)}, & \text{если } n_b - b_i < w. \end{aligned} \quad (5.18)$$

### 5.3.3. Неслучайный код РС

В заключение рассмотрим случай, когда в качестве внешних кодов выбираются неслучайные коды РС  $-(n_b, b_i)$  над полем  $GF(2^{a_i})$ . Тогда возникает вопрос о вероятности  $P_i(w)$  принадлежности случайно выбранного слова  $\gamma_i$  веса  $w > 0$  над полем  $GF(2^{a_i})$  этому неслучайному коду РС. Пусть все символы  $\gamma_{i,j} \in GF(2^{a_i})$  слово  $\gamma_i$  независимы и равновероятны, т. е. все они независимо выбираются из всех элементов поля  $GF(2^{a_i})$  с вероятностью  $2^{-a_i}$ . В этом случае имеет место следующая лемма, доказательство которой приведено в приложении П.5.6.

**Лемма 5.4.** Вероятность того, что случайно выбранное слово  $\gamma_i$  над полем  $GF(2^{a_i})$  длины  $n_b$ , веса  $w > 0$  является кодовым словом неслучайного кода РС  $-(n_b, b_i)$ , удовлетворяет условию

$$\begin{aligned} P_i(w) &= 0, & \text{если } 0 < w \leq n_b - b_i; \\ P_i(w) &\leq e2^{-a_i(n_b - b_i)}, & \text{если } n_b - b_i < w. \end{aligned} \quad (5.19)$$

## § 5.4. Производящие функции среднего спектра весов случайных каскадных кодов

### 5.4.1. Вероятность принадлежности произвольного слова случайному каскадному коду

Как уже отмечалось выше, основной характеристикой ансамбля каскадных кодов является вероятность того, что некоторое двоичное ненулевое слово  $\alpha$  размеров  $n_a \times n_b$  является кодовым словом случайного каскадного кода из данного ансамбля. Однако эта вероятность существенно зависит от характера матриц  $H_0^{(j)}$  и внешних кодов  $(n_b, b_i)$  определяющих ансамбль, а также от числа ненулевых столбцов слова  $\alpha$ , а при использовании только нижних треугольных матриц  $H_0^{(j)}$  также и от количества верхних нулевых блоков  $\alpha_i$ ,  $i = m - k + 1, m$ .

Для большинства из ансамблей каскадных кодов, приведенных в табл. 5.1, на основании результатов § 5.2 и 5.3 и при помощи соотношений (5.12) и (5.13) легко получить удобные для дальнейшего использования верхние оценки этих вероятностей, которые в предположении, что  $b_1 < b_2 < \dots < b_m$ , определяются следующими утверждениями, доказательства которых приведены в приложении П.5.7.

**Утверждение 5.3.** Вероятность  $P_l(w)$  того, что произвольное ненулевое ( $w > 0$ ) двоичное слово  $\alpha$  размеров  $n_a \times n_b$ , содержащее  $l$  ненулевых и  $n_b - l$  нулевых столбцов, является кодовым словом случайного каскадного кода из ансамбля I, удовлетворяет условиям

$$P_l(w) = 0, \text{ если } 1 \leq l \leq n_b - b_m;$$

$$P_l(w) \leq m(2e)^m 2^{-\left(n_a - \sum_{s=1}^m a_s\right)l - \sum_{s=1}^m a_s(n_b - b_s)}, \quad (5.20)$$

если  $n_b - b_i + 1 \leq l \leq n_b - b_{i-1}$ .

**Утверждение 5.4.** Вероятность  $P_l(w)$  того, что произвольное ненулевое ( $w > 0$ ) двоичное слово  $\alpha$  размеров  $n_a \times n_b$ , содержащее  $l$  ненулевых и  $n_b - l$  нулевых столбцов, является кодовым словом случайного каскадного кода из ансамбля II, удовлетворяет условию

$$P_l(w) = m2^m \sum_{i=1}^m 2^{-(n_a - a_i)l - (n_b - b_i)a_i}, \text{ если } 1 \leq l \leq n_b - b_m;$$

$$P_l(w) \leq m2^m 2^{-\left(n_a - \sum_{s=1}^m a_s\right)l - \sum_{s=1}^m a_s(n_b - b_s)}, \text{ если } n_b - b_i + 1 \leq l \leq n_b - b_{i-1}. \quad (5.21)$$

**Утверждение 5.5.** Вероятность  $P_l^{(k)}(w)$  того, что произвольное ненулевое ( $w > 0$ ) двоичное слово  $\alpha$  размеров  $n_a \times n_b$ , содержащее  $l$  ненулевых и  $n_b - l$  нулевых столбцов, у которого верхние  $k$  блоков  $\alpha_s$ ,  $s = \overline{m-k+1, m}$ , нулевые, а блок  $\alpha_{m-k}$  ненулевой, является кодовым словом случайного каскадного кода из ансамбля III, удовлетворяет условию

$$P_l^{(k)}(w) = 0, \text{ если } 1 \leq l \leq n_b - b_{m-k};$$

$$P_l^{(k)}(w) \leq (2e)^m 2^{-\left(n_a - \sum_{s=1}^{m-k} a_s\right)l - \sum_{s=1}^{m-k} a_s(n_b - b_s)}, \quad (5.22)$$

если  $n_b - b_i + 1 \leq l \leq n_b - b_{i-1}$ ,  $i = \overline{1, m-k}$ .

**Утверждение 5.6.** Вероятность  $P_l^{(k)}(w)$  того, что произвольное ненулевое ( $w > 0$ ) двоичное слово  $\alpha$  размеров  $n_a \times n_b$ , содержащее  $l$  ненулевых,  $n_b - l$  нулевых столбцов, у которого верхние  $k$  блоков  $\alpha_s$ ,  $s = \overline{m-k+1, m}$ , нулевые, а блок  $\alpha_{m-k}$  ненулевой, является кодовым словом случайного каскадного кода из ансамбля IV, удовлетворяет условию

$$P_l^{(k)}(w) \leq m 2^m \sum_{i=1}^{m-k} 2^{-\left(n_a - \sum_{s=m-k+1}^m a_{s-a_i}\right)l - (n_b - b_i)a_i},$$

если  $1 \leq l \leq n_b - b_{m-k}$ ; (5.23)

$$P_l^{(k)}(w) \leq m 2^m 2^{-\left(n_a - \sum_{s=1}^{m-k} a_s\right)l - \sum_{s=i}^{m-k} a_s(n_b - b_s)},$$

если  $n_b - b_i + 1 \leq l \leq n_b - b_{i-1}$ .

Следует отметить, что утверждение 5.3 справедлива также для ансамблей I<sup>a</sup>, I<sup>b</sup> и I<sup>c</sup>, а утверждения 5.4 и 5.5 справедливы соответственно для ансамблей II<sup>a</sup> и III<sup>a</sup>.

Что касается ансамблей I<sup>r</sup>, II<sup>b</sup>, V, VI, VII и VIII, то из них мы рассмотрим только ансамбли I<sup>r</sup> и II<sup>b</sup>, для которых было доказано утверждение 5.2.

Для изучения ансамбля I<sup>r</sup> введем множества  $\mathfrak{A}_{i_1, \dots, i_\nu}$ , каждое из которых состоит из всех таких и только таких двоичных слов  $\alpha$  ( $i_1, \dots, i_\nu$ ) размеров  $n_a \times n_b$ , которые определяются произведением  $\alpha(i_1, \dots, i_\nu) = G_0 \gamma(i_1, \dots, i_\nu)$ , где  $G_0 = H_0^{-1}$ , а  $\gamma(i_1, \dots, i_\nu)$  — любое двоичное слово размеров  $n_a \times n_b$ , у которого ровно  $\nu$  горизонтальных блоков  $\gamma_{i_1}, \gamma_{i_2}, \dots, \gamma_{i_\nu}$  ненулевые, а все остальные блоки размеров  $a_i \times n_b$  нулевые, причем  $1 \leq i_1 < i_2 < \dots < i_\nu = m$ . Ясно, что для каждого фиксированного  $\nu$  число различных множеств  $\mathfrak{A}_{i_1, \dots, i_\nu}$ , равно  $C_m^\nu$ , так что число всех таких множеств  $\nu = \overline{1, m}$  равно  $2^m - 1$ . В этом случае справедливо следующее утверждение, доказательство которого приведено в приложении П.5.8.

**Утверждение 5.7.** Вероятность  $P_l(i_1, \dots, i_v, w)$  того, что любое фиксированное слово из множества  $\mathcal{A}_{i_1, \dots, i_v}$ , содержащее  $l$  ненулевых и  $n_b - l$  нулевых столбцов, является кодовым словом каскадного кода из ансамбля  $\Gamma^v$ , удовлетворяет условию

$$P_l(i_1, \dots, i_v, w) \leq e^v 2^{-\sum_{s=1}^v a_{i_s}(n_b - b_{i_s})}. \quad (5.24)$$

Утверждение 5.7 остается справедливым и для ансамбля  $\Pi^v$  с той только разницей, что множитель  $e^v$  можно заменить единицей.

#### 5.4.2. Производящие функции среднего спектра весов случайных каскадных кодов

Приведенные в предыдущем разделе оценки вероятностей  $P_l(w)$ ,  $P_l^{(k)}(w)$  и  $P_l(i_1, \dots, i_v, w)$  позволяют оценить производящие функции  $\psi(z)$  среднего спектра весов кодовых слов случайных каскадных кодов, принадлежащих первым 11 ансамблям, приведенным в табл. 5.1. Эти оценки определяются следующими утверждениями, доказательства которых приведены в приложениях П.5.9—П.5.11.

**Утверждение 5.8.** Производящая функция среднего по ансамблю спектра весов кодовых слов случайных каскадных кодов из ансамблей  $I$ ,  $I^a$ ,  $I^b$  и  $I^s$  при  $z > 0$  удовлетворяет неравенству

$$\psi(z) \leq \Psi(z) = m (2e)^m \sum_{i=1}^m [(1+z)^{n_a} + 2^{(1-R_{ai})n_a}]^{n_b} \cdot 2^{-(1-R_i)n}, \quad (5.25)$$

где  $R_{ai} = \frac{1}{n_a} \sum_{s=1}^m a_s$ ,  $R_i = \sum_{s=1}^m (R_{as} - R_{a,s+1}) R_{bs}$ ,  $R_{bs} = b_s/n_b$ ,  $R_{a,m+1} = 0$ ,  $R_1 = R$ .

**Утверждение 5.9 (П.5.9).** Производящая функция среднего по ансамблю спектра весов кодовых слов случайных каскадных кодов из ансамблей  $\Pi$  и  $\Pi^a$  при  $z > 0$  удовлетворяет неравенству

$$\begin{aligned} \psi(z) \leq \Psi(z) = m 2^m \sum_{i=1}^m [(1+z)^{n_a} + 2^{(1-R_{ai})n_a}]^{n_b} 2^{-(1-R_i)n} + \\ + m 2^n \sum_{i=1}^m [(1+z)^{n_a} + 2^{(1-\Delta R_{ai})n_a}]^{n_b} 2^{-(1-\Delta R_i)n}, \end{aligned} \quad (5.26)$$

где  $\Delta R_{ai} = R_{ai} - R_{a,i+1}$ ,  $\Delta R_i = R_i - R_{i+1} = (R_{ai} - R_{a,i+1}) R_{bi}$ .

**Утверждение 5.10 (П.5.10).** Производящая функция среднего по ансамблю спектра весов кодовых слов случайных каскадных кодов из ансамблей  $\Pi$  и  $\Pi^a$  при  $z > 0$  удовлетворяет неравенству

$$\psi(z) \leq \Psi(z) = m(2e)^m \sum_{k=0}^{m-1} \sum_{i=1}^{m-k} [(1+z)^{(1-R_a, m-k+1)n_a} + 2^{(1-R_{ai})n_a}]^{n_b} 2^{-(1-R_i+R_{m-k+1-R_a, m-k+1})n}, \quad (5.27)$$

где  $R_{m+1} = 0$ .

**Утверждение 5.11 (П.5.10).** Производящая функция среднего по ансамблю спектра весов кодовых слов случайных каскадных кодов из ансамбля IV при  $z > 0$  удовлетворяет неравенству

$$\begin{aligned} \psi(z) \leq \Psi(z) = m2^m \sum_{k=0}^{m-1} \sum_{i=1}^{m-k} [(1+z)^{(1-R_a, m-k+1)n_a} + 2^{(1-R_{ai})n_a}]^{n_b} 2^{-(1-R_i+R_{m-k+1-R_a, m-k+1})n} + \\ + m2^m \sum_{k=0}^{m-1} \sum_{i=1}^{m-k} [(1+z)^{(1-\Delta R_a, m-k+1)n_a} + 2^{(1-\Delta R_{ai})n_a}]^{n_b} 2^{-(1-\Delta R_i)n}. \end{aligned} \quad (5.28)$$

**Утверждение 5.12 (П.5.11).** Производящая функция среднего по ансамблю спектра весов кодовых слов случайных каскадных кодов из ансамблей I<sup>r</sup> и II<sup>6</sup>, для которых, кроме условия  $b_i < b_{i+1}$ , выполняется условие  $a_i \leq a_{i+1}$ ,  $i = \overline{1, m}$ , при  $z > 0$  удовлетворяет неравенству

$$\psi(z) \leq \Psi(z) = (2e)^m (n_a^2 2^m)^{n_b} \sum_{i=1}^m [(1+z)^{n_a} + 2^{(1-R_{ai})n_a}]^{n_b} 2^{-(1-R_i)n}. \quad (5.29)$$

Что касается ансамблей V, VI, VII и VIII, то они рассматриваться не будут, так как для неслучайных нижних треугольных матриц и неслучайных элементов поля GF( $2^a$ ) остается открытым вопрос о справедливости утверждения, подобного утверждению 5.2.

## § 5.5. Оценка кодового расстояния случайных каскадных кодов

### 5.5.1. Оценка кодового расстояния случайных каскадных кодов из ансамблей типа I

Для ансамблей типа I (т. е. для ансамблей I, I<sup>a</sup>, I<sup>6</sup>, I<sup>s</sup> и I<sup>r</sup>) верхняя оценка  $\Psi(z)$  производящей функции  $\psi(z)$  среднего спектра весов кодовых слов при  $z > 0$  может быть представлена в виде  $\Psi(z) = k_1(n, n_a, n_b) \sum_{i=1}^m \Psi_i(z)$ , где в соответствии с (5.25)

$$\Psi_i(z) = [(1+z)^{n_a} + 2^{(1-R_{ai})n_a}]^{n_b} 2^{-(1-R_i)n}. \quad (5.30)$$

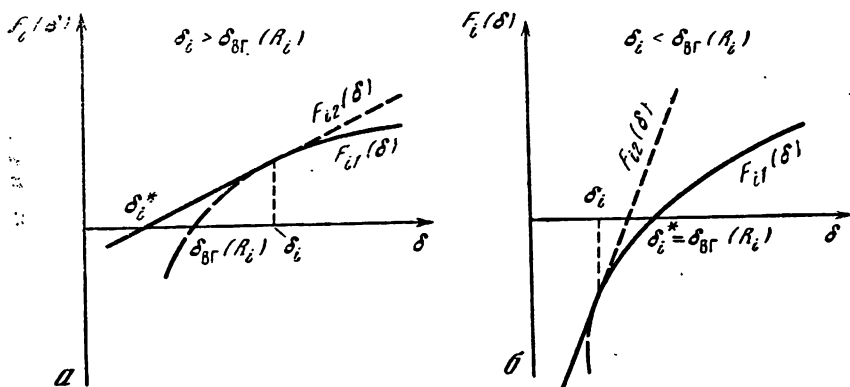


Рис. 5.1. График функции  $F_i(\delta)$

$a - \delta_i > \delta_{ВГ}(R_i)$ ;  $б - \delta_i < \delta_{ВГ}(R_i)$

Причем для ансамблей I, I<sup>a</sup>, I<sup>b</sup> и I<sup>c</sup> коэффициент  $k_1(m, n_a, n_b) = m(2e)^m$ , а для ансамбля I<sup>r</sup> коэффициент  $k_1(m, n_a, n_b) = (2e)^m (n_a^2 2^m)^{n_b}$ . Используя соотношение (5.11), получаем

$$\begin{aligned} P(d \leq n\delta) &\leq k_1(m, n_a, n_b) \sum_{i=1}^m \inf_{0 < z < 1} \{\Psi_i(z)/z^{n\delta}\} = \\ &= k_1(m, n_a, n_b) \sum_{i=1}^m 2^{-(1-R_i)n} \inf_{0 < z < 1} \{[(z^{-\delta} + z^{1-\delta})^{n_a} + \\ &\quad + (z^{-\delta} 2^{1-R_{ai}})^{n_a}]^{n_b}\}. \end{aligned} \quad (5.31)$$

Детальный анализ правой части (5.31) приводит к следующему утверждению, доказательство которого приведено в приложении П.5.12.

**Утверждение 5.13.** Вероятность  $P(d \leq n\delta)$  того, что случайный каскадный код из ансамблей типа I имеет кодовое расстояние  $d \leq n\delta$ , оценивается сверху выражением

$$P(d \leq n\delta) \leq \sum_{i=1}^m 2^{\{F_i(\delta) + 1/n_a + \log_2 k_1(m, n_a, n_b)/n\}}, \quad (5.32)$$

где

$$F_i(\delta) = \begin{cases} F_{i1}(\delta) = H(\delta) - (1 - R_i) & \text{при } \delta \geq \delta_i; \\ F_{i2}(\delta) = -\delta \log_2(2^{1-R_{ai}} - 1) - R_{ai} + R_i & \text{при } \delta < \delta_i, \end{cases} \quad (5.33)$$

причем  $\delta_i = 1 - 2^{-(1-R_{ai})}$ , а прямая  $F_{i2}(\delta)$  представляет собой касательную к кривой  $F_{i1}(\delta)$ . Таким образом, график функции  $F_i(\delta)$  имеет вид, показанный на рис. 5.1.

На рис. 5.1<sup>a</sup> показан случай, когда  $\delta_i > \delta_{ВГ}(R_i)$ , а на рис. 5.1<sup>б</sup> — случай, когда  $\delta_i < \delta_{ВГ}(R_i)$ , где  $\delta_{ВГ}(R_i) = \delta_{i1}^*$  — корень уравнения  $F_{i1}(\delta) = 0$ .



Обозначим через  $\delta_i^*$  корень уравнения  $F_i(\delta) = 0$  и введем наименьший из этих корней

$$\delta^* = \min_i \{\delta_i^*\}. \quad (5.34)$$

Так как на отрезке  $0 \leq \delta \leq 1/2$  каждая из функций  $F_i(\delta)$ ,  $i = \overline{1, m}$ , возрастает, приходим к выводу, что при  $\delta < \delta^*$  все величины  $F_i(\delta) < 0$ , а значит, для всех  $i$ ,  $i = \overline{1, m}$ ,  $2^{nF_i(\delta)} < 1$ . Заменяя оценку (5.32) более грубой оценкой

$$\begin{aligned} P(d \leq n\delta) &\leq m \max_i \{2^{n[F_i(\delta)+1/n_a+\log_2 k_1(m, n_a, n_b)/n]}\} = \\ &= \max_i \{2^{n[F_i(\delta)+(\log_2 m k_1(m, n_a, n_b)+n_b)/n]}\}. \end{aligned} \quad (5.35)$$

и учитывая, что при  $n_a \rightarrow \infty$  и  $n_b \rightarrow \infty$   $(\log_2 m k_1(m, n_a, n_b) + n_b)/n \rightarrow 0$  как при  $k_1(m, n_a, n_b) = m(2e)^m$ , так и при  $k_1(m, n_a, n_b) = (2e)^m (n_a^2)^{mn_b}$ , приходим к выводу, что при  $P(d \leq n\delta) < 1$ . Но это значит, что среди случайных каскадных кодов из ансамблей типа I существуют такие, кодовое расстояние которых удовлетворяет условию  $d \geq n(\delta^* - \epsilon)$ , где  $\epsilon$  — сколь угодно малое число.

Таким образом, величина  $\delta^*$ , определяемая из (5.34), представляет собой границу асимптотически достижимого на ансамблях типа I отношения кодового расстояния  $d$  к длине кода  $n$ . Более того, как следует из (5.35), доля таких каскадных кодов в каждом из ансамблей типа I экспоненциально по  $n$  стремится к единице. Величину  $\delta^*$  для каскадных кодов из ансамблей типа I, которая зависит от скорости передачи  $R$  порядка каскадного кода и его структуры, будем обозначать  $\delta^* = \delta^*(R, m)$ .

Для вычисления величины  $\delta^*(R, m)$  введем корни  $\delta_{i1}^*$  и  $\delta_{i2}^*$  соответственно уравнений  $F_{i1}(\delta) = 0$  и  $F_{i2}(\delta) = 0$ . Как следует из (5.33),  $\delta_{i1}^* = \delta_{\text{ВГ}}(R_i)$ ;  $\delta_{i2}^* = (R_i - R_{ai})/\log_2(2^{1-R_{ai}} - 1)$ . Причем в силу выпуклости кривой  $F_{i1}(\delta)$   $\delta_{i2}^* \leq \delta_{\text{ВГ}}(R_i)$ . Тогда

$$\delta_i^* = \begin{cases} \delta_{i1}^*, & \text{если } \delta_i \leq \delta_{\text{ВГ}}(R_i); \\ \delta_{i2}^*, & \text{если } \delta_i > \delta_{\text{ВГ}}(R_i). \end{cases}$$

Учитывая, что в соответствии с определением величины  $\delta_i$  условие  $\delta_i \leq \delta_{\text{ВГ}}(R_i)$  эквивалентно условию  $R_{ai} \geq \log_2 2(1 - \delta_{\text{ВГ}}(R_i))$ , а условие  $\delta_i > \delta_{\text{ВГ}}(R_i)$  эквивалентно условию  $R_{ai} < \log_2 2(1 - \delta_{\text{ВГ}}(R_i))$ , окончательно получаем

$$\delta_i^* = \begin{cases} \delta_{\text{ВГ}}(R_i), & \text{если } R_{ai} \geq \log_2 2(1 - \delta_{\text{ВГ}}(R_i)); \\ (R_i - R_{ai})/\log_2(2^{1-R_{ai}} - 1), & \text{если } R_{ai} < \log_2 2(1 - \delta_{\text{ВГ}}(R_i)), \end{cases} \quad (5.36)$$

причем согласно (5.34)  $\delta^*(R, m) = \min_i \{\delta_i^*\}$ .

### 5.5.2. Условия достижимости границы ВГ

Соотношение (5.35) позволяет вычислить величины  $\delta_i^*$  для каскадных кодов заданной структуры, причем так как для  $i=1$ ,  $R_i=R$   $\delta_{i2}=(R-R_{a1})/\log_2(2^{1-R_{a1}}-1) \leq \delta_{\text{ВГ}}(R)$ , то  $\delta_1^* \leq \delta_{\text{ВГ}}(R)$ . Причем равенство имеет место лишь при условии, что  $R_{a1}=1+\log_2(1-\delta_{\text{ВГ}}(R))$ . Это значит, что  $\delta^*(R, m)$  не может превысить границы ВГ, которая определяется равенством  $\delta^*(R, m)=\delta_{\text{ВГ}}(R)$ . Для выяснения условий, при которых для каскадных кодов из ансамблей типа I величина  $\delta^*(R, m)$  достигает границы ВГ, обратимся снова к выражению (5.36) и к рис. 5.2, на котором приведены графики функций  $F_{i1}(\delta)$  и  $F_{i2}(\delta)$  для двух значений  $i$  ( $i=1$  и  $i>1$ ). Так как при  $i>1$  в силу условия  $R_i < R$  следует, что  $\delta_{i1}^* > \delta_{\text{ВГ}}(R)$ , то  $\delta_{i2}^*$ , которое меньше чем  $\delta_{\text{ВГ}}(R_i)$ , может быть меньше, равно или больше, чем  $\delta_{\text{ВГ}}(R)$ .

Отсюда непосредственно следует, что для достижения границы ВГ необходимо и достаточно выполнение следующих условий:

- 1)  $R_{a1} \geq \log_2 2(1 - \delta_{\text{ВГ}}(R))$ , при этом  $\delta_1^* = \delta_{\text{ВГ}}(R)$ ;
- 2) для каждого  $i > 1$  либо

$$R_{ai} \geq \log_2 2(1 - \delta_{\text{ВГ}}(R_i)), \quad (5.37)$$

при этом  $\delta_i^* = \delta_{\text{ВГ}}(R_i) > \delta_{\text{ВГ}}(R)$ , либо  $(R_i - R_{ai})/\log_2(2^{1-R_{ai}} - 1) \geq \delta_{\text{ВГ}}(R)$ , при этом  $\delta_{\text{ВГ}}(R) \leq \delta_i^* < \delta_{\text{ВГ}}(R_i)$ .

Следует отметить, что достаточные, но не необходимые условия достижения границы ВГ можно представить одним и тем же для всех  $i=1, m$  неравенством

$$(R_i - R_{ai})/\log_2(2^{1-R_{ai}} - 1) \geq \delta_{\text{ВГ}}(R), \quad i=\overline{1, m}. \quad (5.38)$$

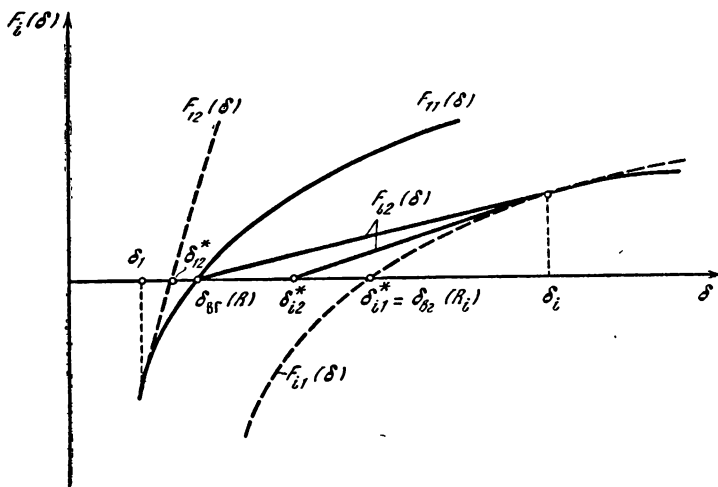


Рис. 5.2. Графики функций  $F_{i1}(\delta)$  и  $F_{i2}(\delta)$

Введем также условия достижимости границы ВГ в предельной форме, когда для всех  $i$ ,  $i = \overline{1, m}$ ,  $\delta_i^* = \delta_{\text{ВГ}}(R)$ , а  $R_{a1}$  принимает наименьшее значение.

Эти условия имеют вид

$$1) R_{a1} = \log_2 2(1 - \delta_{\text{ВГ}}(R));$$

$$2) (R_i - R_{ai}) / \log_2(2^{1-R_{ai}} - 1) = \delta_{\text{ВГ}}(R), \quad i = \overline{2, m}.$$

Учитывая, что первое условие совпадает со вторым при  $i = 1$ , последние равенства можно заменить одним выражением

$$(R_i - R_{ai}) / \log_2(2^{1-R_{ai}} - 1) = \delta_{\text{ВГ}}(R), \quad i = \overline{1, m}. \quad (5.39)$$

### 5.5.3. Оценка кодового расстояния и условия достижимости границы ВГ для случайных каскадных кодов из других ансамблей

Рассмотрим теперь ансамбль типа II (т. е. ансамбли II, II<sup>a</sup> и II<sup>b</sup>), для которых в соответствии с (5.26) представим верхнюю оценку  $\Psi(z)$  производящей функции среднего спектра весов при  $z > 0$  в виде суммы  $2m$  слагаемых

$$\Psi(z) = k_2(m, n_a, n_b) \sum_{i=1}^m (\Psi_i(z) + \Psi_i^*(z)), \quad (5.40)$$

где  $\Psi_i(z)$  определяется равенством (5.30), а  $\Psi_i^*(z)$  получается из  $\Psi_i(z)$  заменой  $R_{ai}$  на  $\Delta R_{ai} = R_{ai} - R_{ai+1}$  и  $R_i$  на  $\Delta R_i = R_i - R_{i+1}$ . Коэффициент  $k_2(m, n_a, n_b) = m2^m$  для ансамблей II и II<sup>a</sup> и  $k_2(m, n_a, n_b) = 2^m(n_a^2 2^m)^{n_b}$  для ансамбля II<sup>b</sup>.

Если применить тот же метод оценки выражения  $\inf_{0 < z < 1} \{\Psi(z)/z^{n_b}\}$ ,

что и в разд. 5.5.1, то из выражения (5.40) и результатов разд. 5.5.1 и 5.5.2 непосредственно следует, что граница асимптотически достижимого на указанных ансамблях кодового расстояния определяется  $\delta^*$ , где  $\delta^* = \min_i \{\delta_i^*, \mu_i^*\}$ , здесь  $\delta_i^*$  — введенный в разд. 5.5.2 корень функции  $F_i(\delta)$ , определяемой выражением (5.33), а  $\mu_i^*$  — корень функции  $F_i^*(\delta)$ , получаемой из  $F_i(\delta)$  заменой  $R_{ai}$  на  $\Delta R_{ai}$  и  $R_i$  на  $\Delta R_i$ . При этом величина  $\delta_i$ , фигурирующая в (5.33), для функции  $F_i^*(\delta)$  определяется равенством  $\delta_i = 1 - 2^{-(1-\Delta R_{ai})}$ . Но это значит, что достаточные условия достижимости границы ВГ для ансамблей II, II<sup>a</sup> и II<sup>b</sup> состоят из  $2m$  условий, из которых первые  $m$  совпадают с условиями (5.38) достижимости границы ВГ для случайных кодов из ансамблей типа I, а остальные  $m$  имеют вид

$$R_i - R_{i+1} - R_{ai} + R_{a_{i+1}} / \log_2(2^{1-R_{ai}+R_{a_{i+1}}} - 1) \geq \delta_{\text{ВГ}}(R), \quad i = \overline{1, m}. \quad (5.41)$$

Однако в силу равенства  $R_{a, m+1} = R_{m+1} = 0$  последнее условие (5.41) совпадает с последним условием (5.38), поэтому условия (5.41) надо рассматривать только для  $i = \overline{1, m-1}$ .

В тех случаях, когда справедливы равенства (5.39), имеет место следующее утверждение, доказательство которого приведено в приложении II. 5.13.

**Утверждение 5.14.** Если для случайных кодов из ансамблей типа II первые  $m$  условий достижения границы ВГ выполняются в предельной форме (5.39), то дополнительные  $m - 1$  условий (5.41) также выполняются.

Перейдем теперь к рассмотрению случайных каскадных кодов из ансамблей III и III<sup>a</sup>, которые определяются случайными невырожденными нижними треугольными матрицами  $H_0^{(j)}$  и кодами РС (случайными или неслучайными).

Для этих ансамблей функцию  $\Psi(z)$ , определяемую равенством (5.27), представим в виде

$$\Psi(z) = k_3(m) \sum_{k=0}^{m-1} \sum_{i=1}^{m-k} \Psi_{ik}(z),$$

где  $k_3(m) = m(2e)^m$ , а  $\Psi_{ik}(z) = [(1+z)^{(1-R_{ai}, m-k+1)n_a} + 2^{(1-R_{ai})n_a}]^{n_b} \times 2^{-(1-R_{ai}+R_{m-k+1}-R_{a, m-k+1})n}$ ,  $k = \overline{0, m-1}$ ,  $i = \overline{1, m-k}$ ,  $R_{m+1} = R_{a, m+1} = 0$ . Учитывая, что  $(1+z)^{(1-R_{ai}, m-k+1)n_a} + 2^{(1-R_{ai})n_a} \leq 2 \max \{(1+z)^{(1-R_{ai}, m-k+1)n_a}; 2^{(1-R_{ai})n_a}\}$ , в соответствии с выражением (5.11) получаем следующую оценку для  $P(d \leq n\delta)$ :

$$P(d \leq n\delta) \leq 2^{n_b} k_3(m) \sum_{k=0}^{m-1} \sum_{i=1}^{m-k} 2^{-(1-\bar{R}_i)n} \inf_{0 < \varepsilon < 1} \{(z^{-\delta} + z^{1-\delta})^n; (z^{-\delta} 2^{1-\bar{R}_{ai}})^n\},$$

$$\text{где } \bar{n} = (1 - R_{m-k+1})n, \quad \bar{R}_{ai} = (R_{ai} - R_{a, m-k+1})/(1 - R_{a, m-k+1}), \quad \bar{\delta} = \delta/(1 - R_{a, m-k+1}), \quad \bar{R}_i = (R_i - R_{m-k+1})/(1 - R_{a, m-k+1}). \quad (5.42)$$

Таким образом, с учетом новых обозначений мы приходим к задаче, подробно рассмотренной в разд. 5.5.1 и 5.5.2. Тогда, полностью повторяя рассуждения, проведенные при исследовании случайных каскадных кодов из ансамблей типа I, получаем следующее правило определения оценки величины  $\delta^*(R)$  для случайных каскадных кодов из ансамблей III и III<sup>a</sup>. Для каждой пары  $(i, k)$ ,  $k = \overline{0, m-1}$ ,  $i = \overline{1, m-k}$ , вычисляем  $\bar{\delta}_{ik} = 1 - 2^{-(1-\bar{R}_{ai})}$  и находим  $\bar{\delta}_{ik}^*$  из равенства

$$\bar{\delta}_{ik}^* = \begin{cases} \delta_{\text{ВГ}}(\bar{R}_i), & \text{если } \bar{\delta}_{ik} \leq \delta_{\text{ВГ}}(\bar{R}_i); \\ (\bar{R}_i - \bar{R}_{ai})/\log_2(2^{1-\bar{R}_{ai}} - 1), & \text{если } \bar{\delta}_{ik} > \delta_{\text{ВГ}}(\bar{R}_i). \end{cases}$$

Этим значениям  $\bar{\delta}_{ik}^*$  соответствуют  $\delta_{ik}^* = (1 - R_{a, m-k+1})\bar{\delta}_{ik}^*$ , из которых выбираем наименьшее  $\delta^* = \min_{(i, k)} \delta_{ik}^* = \min_{(i, k)} \{(1 - R_{a, m-k+1})\bar{\delta}_{ik}^*\}$ .

Отсюда непосредственно приходим к условиям достижения границы ВГ для случайных каскадных кодов из ансамблей III и III<sup>a</sup>. Эти условия после замены  $\bar{R}_i$  и  $\bar{R}_{ai}$  их значениями (5.42) принимают следующий вид.

Для каждой пары  $(k, i)$ ,  $k = \overline{0, m-1}$ ,  $i = \overline{1, m-k}$ :

1) либо  $\delta_{ik} \leq \delta_{\text{ВГ}}((R_i - R_{m-k+1})/(1 - R_{a, m-k+1}))$  и

$$(1 - R_{a, m-k+1}) \delta_{\text{ВГ}}((R_i - R_{m-k+1})/(1 - R_{a, m-k+1})) \geq \delta_{\text{ВГ}}(R); \quad (5.43)$$

2) либо  $\delta_{ik} > \delta_{\text{ВГ}}((R_i - R_{m-k+1})/(1 - R_{a, m-k+1}))$  и  $(R_{a, m-k+1} - R_{m-k+1} - R_{ai} + R_i) / \log_2 \{2^{1-(R_{ai}-R_{a, m-k+1})/(1-R_{a, m-k+1})} - 1\} \geq \delta_{\text{ВГ}}(R)$ .

Следует отметить, что  $\delta^*$  не может быть больше, чем  $\delta_{\text{ВГ}}(R)$ , так как при  $k=0$  получаем значения  $\delta_{i0}^* = \delta_i^*$ , рассмотренные в разд. 5.5.1. Более того, как было показано в гл. 3, для каскадных кодов любой структуры, определяемых нижними треугольными матрицами  $H_0$ , при  $m \rightarrow \infty$  верхняя оценка  $\delta^{(n)}(R)$  величины  $\delta(R)$  не достигает границы ВГ, т. е.  $\delta^{(n)}(R, \infty) < \delta_{\text{ВГ}}(R)$ .

Следовательно, для каждого значения  $R$ , начиная с некоторого  $m$ , условия (5.43) достижимости границы ВГ выполнены быть не могут. Что касается ансамбля IV, то легко видеть, что определение величины  $\delta^*$  для случайных каскадных кодов из этого ансамбля осуществляется точно так же, как и для кодов из ансамблей типа II. При этом, кроме замены (5.42), использованной при изучении ансамблей типа III, необходимо в соответствии с выражением (5.28) ввести еще дополнительную замену  $\Delta \bar{R}_{ai} = \Delta R_{ai}/(1 - R_{a, m-k+1})$ ;  $\Delta \bar{R}_i = \Delta R_i/(1 - R_{a, m-k+1})$ . В дальнейшем величину  $\delta^*$  для ансамблей типа II, так же как и для ансамблей типа I, будем обозначать  $\delta^*(R, m)$ . Для ансамблей III, III<sup>a</sup> и IV, определяемых нижними треугольными матрицами  $H_0$ , эту величину  $\delta^*$  будем обозначать  $\delta^*(R, m)$ .

## § 5.6. Оценка потенциальных корректирующих свойств каскадных кодов различного порядка

### 5.6.1. Каскадные коды первого порядка

Полученные в § 5.5 результаты позволяют достаточно просто вычислить величину  $\delta^*$ , которая характеризует при  $n \rightarrow \infty$  потенциально достижимое кодовое расстояние каскадных кодов при заданной заранее их структуре, т. е. при заданном наборе скоростей передачи  $R_{ai}$ ,  $R_{bi}$ ,  $i = \overline{1, m}$ .

Кроме того, возможны постановка и решение обратной задачи, заключающейся в нахождении такой структуры (или класса структур), при которой для заданного  $R$  достигается максимальное значение  $\delta^*$ , например, когда достигается граница ВГ, которая, как было показано, не может быть превзойдена.

Начнем с рассмотрения простейшего случая каскадных кодов первого порядка, для которых оценка кодового расстояния и условия достижения границы ВГ не зависят от того, к какому из ансамблей относятся эти коды. Действительно, для ансамблей типа III и IV возможно только одно значение параметра  $k$  (это  $k=0$ ), при котором все формулы, определяющие  $\delta^*$ , совпадают с аналогич-

ными выражениями соответственно для  $R_{a1}, R_{b1}$  кодов из ансамблей типа I и II. Что касается различия между кодами из ансамблей типа I и II, то оно также не сказывается на окончательных результатах, так как при  $m=1$   $\Delta R_{a1}=R_{a1}$  и  $\Delta R_1=R_1=R$ , что приводит к совпадению величин  $\delta^*$  и условий достижимости границы ВГ.

Для каскадных кодов первого порядка ( $m=1, R=R_1=R_m$ ) приходим к следующим результатам:

$$\delta^*(R, 1) = \begin{cases} \delta_{ВГ}(R), & \text{если } R_{a1} \geq \\ \geq \log_2 2(1 - \delta_{ВГ}(R)); & \\ (R - R_{a1})/\log_2(2^{1-R_{a1}} - 1) < \delta_{ВГ}(R), & \\ \text{если } R_{a1} < \log_2 2(1 - \delta_{ВГ}(R)), & \end{cases} \quad (5.44)$$

где  $R=R_{a1}R_{b1}$ .

Таким образом, условие достижимости границы ВГ в данном случае имеет вид  $R_{a1} \geq \log_2 2(1 - \delta_{ВГ}(R))$ , а его предельная форма определяется равенством

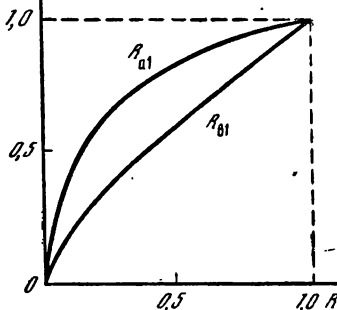
$$R_{a1} = \log_2 2(1 - \delta_{ВГ}(R)). \quad (5.45)$$

Выражение (5.44) позволяет для каждой скорости передачи  $R$  при заданной структуре ( $R_{a1}$  или  $R_{b1}$ ) каскадного кода первого порядка найти величину  $\delta^*(R, 1)$ . Равенство (5.45) определяет наименьшее значение  $R_{a1}$ , т. е. предельную структуру, при которой достигается граница ВГ. Значения  $R_{a1}$ , определяемые (5.45) и  $R_{b1} = R/R_{a1}$ , приведены в табл. 5.2 и на рис. 5.3.

Таблица 5.2

$R$	$R_{a1}$	$R_{b1}$	$R$	$R_{a1}$	$R_{b1}$
0,0000	0,0000	0,0000	0,3902	0,7655	0,5097
0,0072	0,1375	0,0526	0,5310	0,8480	0,6262
0,0290	0,2630	0,1104	0,7136	0,9260	0,7706
0,0651	0,3785	0,1742	0,9192	0,9855	0,9327
0,1187	0,4854	0,2446	0,9546	0,9928	0,9615
0,1887	0,5850	0,3226	0,9792	0,9971	0,9820
0,2781	0,6781	0,4101	1,0000	1,0000	1,0000

Рис. 5.3. Зависимости предельных значений  $R_{a1}$  и  $R_{b1}$  от скорости передачи  $R$ , при которых достигается граница ВГ



## 5.6.2. Каскадные коды второго порядка

При исследовании случайных каскадных кодов второго порядка ограничимся лишь кодами из ансамблей типа I и типа III, отличающихся характером матриц  $H_0^{(j)}$ . Для каскадных кодов второго

порядка, принадлежащих ансамблям типа I, имеем  $\delta^*(R, 2) = \delta^* = \min \{\delta_1^*, \delta_2^*\}$ , где

$$\delta_1^* = \begin{cases} \delta_{\text{ВГ}}(R), & \text{если } R_{a1} \geq \log_2 2(1 - \delta_{\text{ВГ}}(R)); \\ (R - R_{a1})/\log_2(2^{1-R_{a1}} - 1) < \delta_{\text{ВГ}}(R), & \\ \text{если } R_{a1} < \log_2 2(1 - \delta_{\text{ВГ}}(R)); \end{cases} \quad (5.46)$$

$$\delta_2^* = \begin{cases} \delta_{\text{ВГ}}(R_2), & \text{если } R_{a2} \geq \log_2 2(1 - \delta_{\text{ВГ}}(R_2)); \\ (R_2 - R_{a2})/\log_2(2^{1-R_{a2}} - 1), & \text{если } R_{a2} < \log_2 2(1 - \delta_{\text{ВГ}}(R_2)); \end{cases}$$

$$R = (R_{a1} - R_{a2})R_{b1} + R_{a2}R_{b2}; \quad R_2 = R_{a2}R_{b2}. \quad (5.47)$$

Таким образом, условия достижимости границы ВГ в данном случае имеют вид

$$\begin{aligned} 1. & R_{a1} \geq \log_2 2(1 - \delta_{\text{ВГ}}(R)); \quad R_{a2} \geq \log_2 2(1 - \delta_{\text{ВГ}}(R)). \\ 2. & \text{Либо, если } R_{a2} < \log_2 2(1 - \delta_{\text{ВГ}}(R_2)), \text{ то } (R_2 - R_{a2})/\log_2(2^{1-R_{a2}} - 1) \geq \\ & \geq \delta_{\text{ВГ}}(R). \end{aligned} \quad (5.48)$$

Предельная форма условий достижения границы ВГ, когда  $\delta_1^* = \delta_2^* = \delta_{\text{ВГ}}(R)$ , определяется равенствами

$$R_{a1} = \log_2 2(1 - \delta_{\text{ВГ}}(R)), \quad (R_2 - R_{a2})/\log_2(2^{1-R_{a2}} - 1) = \delta_{\text{ВГ}}(R). \quad (5.49)$$

Как следует из условий (5.49) и равенств (5.47), существует бесконечное множество структур каскадных кодов второго порядка (составляющих ансамбли типа I), для которых выполняются условия достижимости границы ВГ в предельной форме. При этом лишь один из параметров, определяющих структуру каскадного кода, а именно  $R_{a1}$ , однозначно зависит от скорости передачи  $R$ . Остальные параметры для каждого  $R$  могут изменяться в достаточно широких пределах. Полную определенность структуры можно получить, добавляя к (5.47) и (5.49) некоторое дополнительное условие, например весьма естественное с практической точки зрения требование  $R_{a1} = 2R_{a2}$ , при котором оба внешних кода являются кодами РС над одним и тем же полем.

В этом случае получаем

$$\begin{aligned} R_{a1} &= \log_2 2(1 - \delta_{\text{ВГ}}(R)); \quad R_{a2} = R_{a1}/2; \\ R_{b2} &= 1 + \delta_{\text{ВГ}}(R) \log_2(2^{1-R_{a2}} - 1)/R_{a2}; \\ R_{b1} &= R/R_{a2} - R_{b2}, \end{aligned} \quad (5.50)$$

так что для каждого  $R$  последовательно находим сначала  $R_{a1}$ , затем  $R_{a2}$ ,  $R_{b2}$  и  $R_{b1}$ . Результаты соответствующих расчетов приведены в табл. 5.3.

Таблица 5.3

$R$	$R_{a1}$	$R_{a2}$	$R_{b1}$	$R_{b2}$	$\delta^*(R, 2)$	$\delta^*(R, 2) = \delta_{ВГ}(R)$	$\delta^*(R, 2)/\delta_{ВГ}(R)$
0,0000	0,0000	0,0000	0,0000	0,0000	0,5000	0,5000	1,000
0,0072	0,1375	0,0688	0,0273	0,0775	0,4408	0,4500	0,980
0,0290	0,2630	0,1315	0,0606	0,1599	0,3851	0,4000	0,963
0,0651	0,3785	0,1893	0,0969	0,2470	0,3321	0,3500	0,949
0,1187	0,4854	0,2427	0,1500	0,3391	0,2814	0,3000	0,938
0,1887	0,5850	0,2925	0,2090	0,4361	0,2325	0,2500	0,930
0,2781	0,6781	0,3391	0,2820	0,5381	0,1849	0,2000	0,924
0,3902	0,7655	0,3828	0,3741	0,6452	0,1384	0,1500	0,923
0,5310	0,8480	0,4240	0,4946	0,7578	0,0925	0,1000	0,925
0,7136	0,9260	0,4630	0,6654	0,8759	0,0465	0,050	0,934
0,9192	0,9855	0,4928	0,8906	0,9747	0,0095	0,0100	0,952
0,9546	0,9928	0,4964	0,9357	0,9873	0,0048	0,0050	0,960
1,0000	1,0000	0,5000	1,0000	1,0000	0,0000	0,0000	—

Для каскадных кодов второго порядка, принадлежащих ансамблям типа III,  $\delta^*(R, 2) = \delta^* = \min \{\delta_1^*, \delta_2^*, \delta_{11}^*\}$ , где  $\delta_1^*$  и  $\delta_2^*$  те же, что и для кодов из ансамблей типа I, т. е. определяются выражениями (5.46), а

$$\delta_{11}^* = \begin{cases} (1 - R_{a2}) \delta_{ВГ}((R - R_2)/(1 - R_{a2})), & \text{если} \\ (R_{a1} - R_{a2})/(1 - R_{a2}) \geq \log_2 2 [1 - \delta_{ВГ}((R - R_2)/(1 - R_{a2}))]; \\ (R - R_{a1} - R_2 + R_{a2})/\log_2 \{2^{1-(R_{a1}-R_{a2})/(1-R_{a2})} - 1\}, & \text{если} \\ (R_{a1} - R_{a2})/(1 - R_{a2}) < \log_2 2 [1 - \delta_{ВГ}((R - R_2)/(1 - R_{a2}))]. \end{cases}$$

Величина  $\delta^*(R, 2)$ , подсчитанная для каскадных кодов, структура которых приведена в табл. 5.3, для всех  $R$  оказывается меньше, чем  $\delta_{ВГ}(R)$ . Ее значения и сравнение с  $\delta^*(R, 2) = \delta_{ВГ}(R)$  приведены в последних трех столбцах табл. 5.3.

Из выражений, определяющих  $\delta_1^*$ ,  $\delta_2^*$ ,  $\delta_{11}^*$ , следует, что для ансамблей типа III условия достижения границы ВГ состоят из условий (5.49) и дополнительного условия 3) либо  $(R_{a1} - R_{a2})/(1 - R_{a2}) \geq \log_2 2 [1 - \delta_{ВГ}((R - R_2)/(1 - R_{a2}))]$  и  $(1 - R_{a2}) \times < \delta_{ВГ}((R - R_2)/(1 - R_{a2})) \geq \delta_{ВГ}(R)$ , либо  $(R_{a1} - R_{a2})/(1 - R_{a2}) < \log_2 2 [1 - \delta_{ВГ}((R - R_2)/(1 - R_{a2}))]$  и  $(R - R_{a1} - R_2 + R_{a2})/\log_2 \times \times \{2^{1-(R_{a1}-R_{a2})/(1-R_{a2})} - 1\} \geq \delta_{ВГ}(R)$ . Соответственно предельная форма этих условий, когда  $\delta_1^* = \delta_2^* = \delta_{11}^* = \delta_{ВГ}(R)$ , определяется равенствами (5.49) и одним из дополнительных равенств:

если  $(R_{a1} - R_{a2})/(1 - R_{a2}) \geq \log_2 2 [1 - \delta_{ВГ}((R - R_2)/(1 - R_{a2}))]$ , то  $(1 - R_{a2}) \delta_{ВГ}((R - R_2)/(1 - R_{a2})) = \delta_{ВГ}(R)$ ;

если  $(R_{a1} - R_{a2})/(1 - R_{a2}) < \log_2 2 [1 - \delta_{ВГ}((R - R_2)/(1 - R_{a2}))]$ , то  $(R - R_{a1} - R_2 + R_{a2})/\log_2 \{2^{1-(R_{a1}-R_{a2})/(1-R_{a2})} - 1\} = \delta_{ВГ}(R)$ .

Вопрос о возможности выполнения условий достижимости границы ВГ в предельной форме для случайных каскадных кодов второго порядка из ансамблей типа III исследуем для скоростей пе-



редачи  $R=0,20496$ ,  $R=0,50008$  и  $R=0,80561$ , при которых соответственно  $\delta_{\text{ВГ}}(R)=0,2400$ ;  $\delta_{\text{ВГ}}(R)=0,1100$  и  $\delta_{\text{ВГ}}(R)=0,0300$ .

Как показали проведенные расчеты, для всех трех скоростей передачи и всех возможных значений  $R_{a2}$  ( $0 < R_{a2} < R_{a1}$ ) имеет место неравенство  $(R_{a1} - R_{a2})/(1 - R_{a2}) < \log_2 (1 - \delta_{\text{ВГ}}((R - R_2)/(1 - R_{a2})))$ , так что  $\delta_{11}^*$  определяется выражением  $\delta_{11}^* = (R - R_{a1} - R_2 + R_{a2})/\log_2 \{2^{1 - (R_{a1} - R_{a2})/(1 - R_{a2})} - 1\}$ , правая часть которого во всех случаях оказывается меньше, чем  $\delta_{\text{ВГ}}(R)$ . Но это значит, что среди каскадных кодов второго порядка, принадлежащих ансамблям типа III, при выбранных трех скоростях передачи нет таких, для которых условие достижимости границы ВГ выполняется в предельной форме.

### 5.6.3. Каскадные коды порядка $m > 2$

При  $m > 2$  ограничимся рассмотрением каскадных кодов, для которых при всех  $R$  выполняется условие  $R_{ai} = R_{a1}(m - i + 1)/m$ . В этом случае все внешние коды  $B_i$ ,  $i=1, m$ , являются кодами РС над одним и тем же полем.

Тогда для случайных каскадных кодов из ансамблей типа I имеем  $\delta^*(R, m) = \delta^* = \min_i \{\delta_i^*\}$ , где

$$\delta_i^* = \begin{cases} \delta_{\text{ВГ}}(R_i), & \text{если } R_{a1}(m - i + 1)/m \geq \log_2 2(1 - \delta_{\text{ВГ}}(R_i)); \\ (R_i - R_{a1}(m - i + 1)/m)/\log_2 [2^{1 - R_{a1}(m - i + 1)/m} - 1], & \\ \text{если } R_{a1}(m - i + 1)/m < \log_2 2(1 - \delta_{\text{ВГ}}(R_i)), \end{cases} \quad (5.51)$$

$$R_i = R_{a1}(R_{bi} + R_{b, i+1} + \dots + R_{bm})/m.$$

Таким образом, условия достижимости границы ВГ принимают вид

$$1) R_{a1} \geq \log_2 2(1 - \delta_{\text{ВГ}}(R));$$

$$2) \text{ для } i = \overline{2, m}: \text{ либо } R_{ai} \geq \log_2 2(1 - \delta_{\text{ВГ}}(R_i)), \text{ либо } (R_i - R_{a1}(m - i + 1)/m)/\log_2 [2^{1 - R_{a1}(m - i + 1)/m} - 1] \geq \delta_{\text{ВГ}}(R).$$

В предельной форме, когда  $R_{ai}$  принимает наименьшее значение и  $\delta_i^* = \delta_{\text{ВГ}}(R)$  для всех  $i = \overline{1, m}$ , эти условия определяются равенствами  $R_{a1} = \log_2 2(1 - \delta_{\text{ВГ}}(R))$ ,

$$R_i = R_{a1}(m - i + 1)/m + \delta_{\text{ВГ}}(R) \log_2 (2^{1 - R_{a1}(m - i + 1)/m} - 1). \quad (5.52)$$

Учитывая соотношения (5.51), последние  $m - 1$  соотношений легко разрешить относительно  $R_{bi}$ :

$$R_{bi} = 1 + \delta_{\text{ВГ}}(R) m \log_2 [(2^{1 - R_{a1}(m - i)/m} - 1)/(2^{1 - R_{a1}(m - i - 1)/m} - 1)]/R_{a1}, \\ i = \overline{2, m}.$$

Что касается величины  $R_{b1}$ , то она определяется очевидным равенством

$$R_{b1} = Rm/R_{a1} - \sum_{i=2}^m R_{bi},$$

вытекающим из условия  $R = R_1$ .

Величины  $R_{a1}$ ,  $R_{bi}$ ,  $i = \overline{2, m}$ , полностью характеризующие структуру каскадного кода, при условии, что  $R_{ai} = R_{a1}(m - i + 1)/m$ , для которой достигается граница ВГ при  $m = 3, 5$  и  $10$ , приведены в табл. 5.4—5.6.

Таблица 5.4

$R$	$\delta_{ВГ}(R)$	$R_{a1}$	$R_{b1}$	$R_{b2}$	$R_{b3}$	$\xi^*(R, 3)/\delta_{ВГ}(R)$
0,0000	0,50	0,0000	0,0000	0,0000	0,0000	1,0000
0,0072	0,45	0,1375	0,0852	0,0537	0,0189	0,9726
0,0290	0,40	0,2630	0,1741	0,1150	0,0421	0,9496
0,0659	0,35	0,3785	0,2664	0,1846	0,0715	0,9300
0,1187	0,30	0,4854	0,3621	0,2632	0,1084	0,9140
0,1887	0,25	0,5850	0,4609	0,3518	0,1552	0,9015
0,2781	0,20	0,6781	0,5627	0,4515	0,2160	0,8928
0,3902	0,15	0,7655	0,6677	0,5640	0,2975	0,8886
0,5310	0,10	0,8480	0,7755	0,6910	0,4120	0,8906
0,7136	0,05	0,9260	0,8863	0,8352	0,5903	0,9027
0,9192	0,01	0,9855	0,9770	0,9652	0,8560	0,9329
0,9546	0,005	0,9928	0,9885	0,9826	0,9136	0,9423
1,0000	0,000	1,0000	1,0000	1,0000	1,0000	—

Примечание.  $m = 3$ .

Таблица 5.5

$R$	$\delta_{ВГ}(R)$	$R_{a1}$	$R_{b1}$	$R_{b2}$	$R_{b3}$	$R_{b4}$	$R_{b5}$	$\xi^*(R, 5)/\delta_{ВГ}(R)$
0,0000	0,500	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	1,0000
0,0072	0,450	0,1375	0,0913	0,0731	0,0538	0,0333	0,0116	0,9668
0,0290	0,400	0,2630	0,1849	0,1522	0,1154	0,0737	0,0259	0,9386
0,0659	0,350	0,3785	0,2806	0,2372	0,1854	0,1227	0,0451	0,9139
0,1187	0,300	0,4854	0,3784	0,3282	0,2646	0,1819	0,0698	0,8930
0,1887	0,250	0,5850	0,4779	0,4250	0,3539	0,2537	0,1025	0,8759
0,2781	0,200	0,6781	0,5792	0,5277	0,4543	0,3416	0,1475	0,8629
0,3902	0,150	0,7655	0,6822	0,6365	0,5672	0,4505	0,2120	0,8550
0,5310	0,100	0,8480	0,7867	0,7514	0,6944	0,5874	0,3111	0,8546
0,7136	0,050	0,9260	0,8926	0,8725	0,8378	0,7640	0,4863	0,8681
0,9192	0,010	0,9855	0,9784	0,9740	0,9659	0,9466	0,7987	0,9094
0,9546	0,005	0,9928	0,9892	0,9870	0,9828	0,9729	0,8757	0,9230
1,0000	0,000	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000	—

Примечание.  $m = 5$ .

Таблица 5.6

$R$	$\delta_{\text{БГ}}(R)$	$R_{61}$	$R_{62}$	$R_{63}$	$R_{64}$	$R_{65}$	$R_{66}$	$R_{67}$	$R_{68}$	$R_{69}$	$R_{70}$	$\delta^*(R, 10)/\delta_{\text{БГ}}(R)$
0,0000	0,500	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	0,0000	1,0000
0,0072	0,450	0,1375	0,0958	0,0782	0,0691	0,0596	0,0498	0,0397	0,0294	0,0188	0,0062	0,9623
0,0290	0,400	0,2630	0,1926	0,1608	0,1436	0,1252	0,1057	0,08486	0,06260	0,03886	0,0130	0,9303
0,0659	0,350	0,3785	0,2906	0,2490	0,2255	0,1996	0,1713	0,1400	0,1053	0,06673	0,0234	0,9012
0,1187	0,300	0,4854	0,3896	0,3422	0,3142	0,2826	0,2467	0,2056	0,1581	0,1027	0,0370	0,8760
0,1887	0,250	0,5850	0,4894	0,4401	0,4099	0,3746	0,3332	0,2837	0,2237	0,1495	0,0555	0,8544
0,2781	0,200	0,6781	0,5901	0,5428	0,5127	0,4764	0,4322	0,3770	0,3063	0,2125	0,0825	0,8365
0,3902	0,150	0,7655	0,6916	0,6502	0,6228	0,5888	0,5457	0,4891	0,4118	0,3000	0,1240	0,8233
0,5310	0,100	0,8480	0,7938	0,7622	0,7405	0,7128	0,6760	0,6250	0,5497	0,4276	0,1946	0,8174
0,7136	0,050	0,9260	0,8966	0,8788	0,8662	0,8494	0,8261	0,7918	0,7362	0,6301	0,3424	0,8274
0,9192	0,010	0,9855	0,9793	0,9754	0,9726	0,9687	0,9631	0,9544	0,9389	0,9031	0,6944	0,8790
0,9546	0,005	0,9928	0,9896	0,9877	0,9862	0,9843	0,9814	0,9769	0,9688	0,9496	0,8020	0,8982

Если обратиться теперь к каскадным кодам этой же структуры, но принадлежащим ансамблям типа III, то к выражениям (5.52), отвечающим  $k=0$ , следует добавить полученные в разд. 5.5.3 соотношения для  $\delta_{ik}^*$ ,  $k=\overline{1, m-1}$ ,  $i=\overline{1, m-k}$ , и в качестве  $\delta^*(R, m)$  выбрать  $\delta^*(R, m) = \min \{\delta_{\text{ВГ}}(R), \delta_{ik}^*\}$ . Нетрудно убедиться, что в данном случае при всех  $R$ ,  $k=\overline{1, m-1}$ ,  $i=\overline{1, m-k}$ ,

$$\delta_{ik}^* = \frac{R_{a1}}{m} \frac{(m-k-i+1) - (R_{b1} + R_{b, i+1} + \dots + R_{b, m-k})}{-\log_2 [2^{1-R_{a1}(m-k-i+1)/(m-kR_{a1})} - 1]}$$

и принимает наименьшее значение при  $k=m-1$  и  $i=1$ . Поэтому для определения  $\delta^*(R, m)$  нет необходимости вычислять  $\delta_{ik}^*$  для всех  $i$  и  $k$ . Достаточно найти лишь

$$\delta_{1, m-1}^* = R_{a1} (1 - R_{b1}) m^{-1} \{-\log_2 [2^{1-R_{a1}/(m-(m-1)R_{a1})} - 1]\}^{-1} \quad (5.53)$$

и положить  $\delta^*(R, m) = \min \{\delta_{\text{ВГ}}(R), \delta_{1, m-1}^*\}$ .

Вычисления, проведенные по формуле (5.53), показали, что  $\delta_{1, m-1}^* < \delta_{\text{ВГ}}(R)$ , так что окончательно имеем  $\delta^*(R, m) = \delta_{1, m-1}^*$ . Значения  $\delta(R, m)$  и отношение  $\delta^*(R, m)/\delta^*(R, m) = \delta^*(R, m)/\delta_{\text{ВГ}}(R)$  для  $m=3, 5$  и  $10$  приведены в табл. 5.4—5.6. Как видно из этих таблиц и табл. 5.3, для каждого  $R$  ( $0 < R < 1$ ) отношение  $\delta^*(R, m)/\delta_{\text{ВГ}}(R)$  убывает с увеличением порядка  $m$  каскадного кода. При фиксированном  $m$  это отношение достигает минимума при средних значениях  $R$  ( $0,39 < R < 0,55$ ).

#### 5.6.4. Каскадные коды бесконечного порядка

Переходя к рассмотрению предельного случая, когда  $m \rightarrow \infty$ , так же, как и в гл. 3, обозначим  $R_{a1} = x$ , а  $R_{b1} = y$ . Тогда для случайных каскадных кодов бесконечного порядка из ансамблей

типа I имеем  $\delta^*(R, m) = \delta^* = \min_{0 \leq x \leq x_0} \{\delta_x^*\}$ , где  $x_0 = R_{a1}$ ;  $R_x = \int_0^x y dx$ ;

$$R_{x_0} = R,$$

$$\delta_x^* = \begin{cases} \delta_{\text{ВГ}}(R_x) & \text{при } x \geq \log_2 2(1 - \delta_{\text{ВГ}}(R_x)); \\ (R_x - x)/\log_2(2^{1-x} - 1) & \text{при } x < \log_2 2(1 - \delta_{\text{ВГ}}(R_x)). \end{cases}$$

Таким образом, условия достижимости границы ВГ принимают вид

1)  $x_0 \geq \log_2 2(1 - \delta_{\text{ВГ}}(R))$ ;  
2) для всех  $x < x_0$  либо  $x \geq \log_2 2(1 - \delta_{\text{ВГ}}(R_x))$ , либо, если  $x < \log_2 2(1 - \delta_{\text{ВГ}}(R_x))$ ,  $(R_x - x)/\log_2(2^{1-x} - 1) \geq \delta_{\text{ВГ}}(R)$ , а их предельная форма, когда при всех  $x$  —  $\delta_x^* = \delta_{\text{ВГ}}(x)$ , определяется равенствами

$$\begin{aligned} x_0 &= \log_2 2(1 - \delta_{\text{ВГ}}(R)), \\ (R_x - x)/\log_2(2^{1-x} - 1) &= \delta_{\text{ВГ}}(R). \end{aligned} \quad (5.54)$$

Так как при  $x=x_0$  первое и второе равенства эквивалентны, то можно ограничиться одним выражением, которое запишем в виде

$$\left( \int_0^x y dx - x \right) \Big| \log_2 (2^{1-x} - 1) = \delta_{\text{ВГ}}(R), \quad 0 \leq x \leq x_0. \quad (5.55)$$

Равенство (5.55) позволяет определить предельную структуру каскадных кодов бесконечного порядка из ансамблей типа I, для которых достигается граница ВГ.

Для нахождений этой структуры, т. е. для определения функции  $y=y(x)$ , перепишем (5.55) в виде

$$\int_0^x y dx - x = \delta_{\text{ВГ}}(R) \log_2 (2^{1-x} - 1),$$

после дифференцирования по  $x$  и простых преобразований получаем

$$y = 1 - \delta_{\text{ВГ}}(R) 2^{1-x} / (2^{1-x} - 1). \quad (5.56)$$

Отсюда с учетом равенства (5.54) следует, что при  $x=x_0$ ,  $y=y_0=0$ ; кроме того, при  $x=0$   $y(0)=y_{\text{max}}=1-2\delta_{\text{ВГ}}(R)$ . Напомним, что коды бесконечного порядка структуры (5.56) рассматривались в гл. 3, где эта структура была названа структурой  $C$ . Было показано, что для каскадных кодов бесконечного порядка структуры  $C$ , определяемых произвольной невырожденной матрицей  $H_0$ , верхняя оценка  $\delta_c^{(p)}(R, \infty)$  совпадает с границей ВГ.

Таким образом, для этих кодов получаем  $\delta_c^*(R, \infty) = \delta_c^{(p)}(R, \infty) = \delta_{\text{ВГ}}(R)$ . Учитывая, что  $\delta_c^*(R, \infty)$  представляет собой оценку величины  $\delta(R)$ , достижимую в ансамбле случайных каскадных кодов, а  $\delta_c^{(p)}(R, \infty)$  является верхней оценкой (превзойти которую  $\delta(R)$  не может), приходим к весьма важному выводу о том, что среди каскадных кодов бесконечного порядка, определяемых невырожденными матрицами  $H_0^{(j)}$ , есть такие (это коды структуры  $C$ ), для которых величина  $\delta(R)$  асимптотически (при  $n_a \rightarrow \infty$  и  $n_b \rightarrow \infty$ ) точно совпадает с границей ВГ, т. е. таких, для которых  $\delta(R) = \delta_{\text{ВГ}}(R)$ .

Следует отметить, что это единственный из известных в настоящее время случай корректирующих двоичных блочных кодов, для которых асимптотически точно известно кодовое расстояние, совпадающее с границей ВГ.

Рассмотрим теперь каскадные коды бесконечного порядка из ансамблей типа III, для которых в соответствии с принятыми в этом разделе обозначениями имеем

$$\delta^*(R, \infty) = \delta^* = \min_{\substack{0 \leq x \leq x_0 \\ 0 \leq t \leq x}} \{\delta_x^*, t\},$$

где

$$\delta_{x,t}^* = \begin{cases} (1-t)\delta_{\text{ВГ}} \left( (1-t)^{-1} \int_t^x y dx \right) \\ \text{при } (x-t)/(1-t) \geq \log_2 2 \left( 1 - \delta_{\text{ВГ}} \left( (1-t)^{-1} \int_t^x y dx \right) \right); \\ \left( \int_t^x y dx - x + t \right) \left| \log_2 (2^{1-(x-t)/(1-t)} - 1) \right| \\ \text{при } (x-t)/(1-t) < \log_2 2 \left( 1 - \delta_{\text{ВГ}} \left( (1-t)^{-1} \int_t^x y dx \right) \right). \end{cases} \quad (5.57)$$

Как было показано в гл. 3, для каскадных кодов бесконечного порядка, определяемых невырожденными нижними треугольными матрицами  $H_{(j)}^{(s)}$ , верхняя оценка  $\xi^{(s)}(R, \infty)$  величины  $\delta(R)$  при любой структуре каскадного кода не достигает границы ВГ. Поэтому ясно, что в рассматриваемом случае при любой структуре (в том числе и при структуре  $C$ )  $\delta_c^*(R, \infty) < \delta_{\text{ВГ}}(R)$ . В то же время несомненный интерес представляет значение  $\delta^*(R, \infty)$  для каскадных кодов, структура которых максимизирует верхнюю оценку кодового расстояния. Такая структура была найдена в разд. 3.4.4 и названа структурой  $B$ .

Структура  $B$  определяется равенством  $y = 1 - 2\xi_B^{(s)}(R, \infty)/(1-x)$ , где верхняя оценка  $\xi_B^{(s)}(R, \infty) < \delta_{\text{ВГ}}(R)$  приведена в табл. 3.11.

Можно показать, что для структуры  $B$  при всех  $x$  и  $0 < t \leq x$

$$(x-t)/(1-t) < \log_2 2 \left( 1 - \delta_{\text{ВГ}} \left( (1-t)^{-1} \int_t^x y dx \right) \right),$$

так что величины  $\delta_{x,t}^*$  в соответствии с (5.57) определяются равенством

$$\delta_{x,t}^* = \left( \int_t^x (1 - 2\xi_B^{(s)}(R, \infty)/(1-x)) dx - x + t \right) \left| \log_2 (2^{1-(x-t)/(1-t)} - 1) \right|,$$

которое после интегрирования и простых преобразований принимает вид  $\delta_{x,t}^* = 2\xi_B^{(s)}(R, \infty) \ln(1 - (x-t)/(1-t)) / \log_2 (2^{1-(x-t)/(1-t)} - 1)$ . Последнее выражение принимает наименьшее значение при  $(x-t)/(1-t) = 0$ , причем  $\min_{(x,t)} \{\delta_{x,t}^*\} = \xi_B^{(s)}(R, \infty)$ .

Таким образом, в данном случае получаем  $\delta_B^*(R, \infty) = \xi_B^{(s)}(R, \infty) < \delta_{\text{ВГ}}(R)$ . Это означает, что и ансамбли типа III содержат каскадные коды бесконечного порядка такой структуры (структуры  $B$ ),

для которых асимптотически точно известно кодовое расстояние. При этом в данном случае (в отличие от ансамблей типа I) это кодовое расстояние не достигает границы ВГ.

Как показали проведенные расчеты для всех  $R$ :  $0 < R < 1$   $\delta_C^*(R, \infty) < \delta_B^*(R, \infty)$ . Сравнение  $\delta_C^*(R, \infty)$  и  $\delta_B^*(R, \infty)$  с  $\delta_{ВГ}(R)$  приведено в табл. 5.7.

Таблица 5.7

$R$	$\delta_{ВГ}(R)$	$\delta_C^*(R, \infty) / \delta_{ВГ}(R)$	$\delta_B^*(R, \infty) / \delta_{ВГ}(R)$	$R$	$\delta_{ВГ}(R)$	$\delta_C^*(R, \infty) / \delta_{ВГ}(R)$	$\delta_B^*(R, \infty) / \delta_{ВГ}(R)$
0,0000	0,500	1,000	1,000	0,3902	0,150	0,782	0,866
0,0072	0,450	0,958	0,981	0,5310	0,100	0,760	0,844
0,0290	0,400	0,921	0,962	0,7136	0,050	0,740	0,838
0,0659	0,350	0,888	0,943	0,9192	0,010	0,725	0,774
0,1187	0,300	0,858	0,924	0,9540	0,005	0,723	0,758
0,1887	0,250	0,830	0,905	1,0000	0,000	0,721	0,732
0,2780	0,200	0,805	0,887				

#### 5.6.5. Оценка экспоненты вероятности ошибочного декодирования

Потенциальные корректирующие свойства кода, характеризующие вероятностью ошибочного декодирования в ДСК без памяти, реализуются при декодировании по минимуму расстояния.

При изучении вероятности ошибочного декодирования в ДСК без памяти ограничимся рассмотрением случайных каскадных кодов только из ансамблей типа I, для которых в разд. 5.4.2 были найдены оценки производящей функции среднего спектра весов.

Используя выражение (5.5) и повторяя рассуждения разд. 5.5.1, получаем для каскадных кодов из ансамблей типа I следующую оценку:

$$\bar{N}(n\omega) \leq \sum_{i=1}^m \inf_{0 < z} \{ \Psi_i(z) / z^{n\omega} \} \leq \sum_{i=1}^m 2^{n[F_i(\omega) + (n\delta_i + \log_2 k_i(m, n_{ai}, n_{bi})) / n]}, \quad (5.58)$$

где  $\omega = w/n \leq 0,5$ ,  $\bar{N}(n\omega)$  — среднее по ансамблю число кодовых слов веса  $\omega n = w > 0$ ,

$$F_i(\omega) = \begin{cases} F_{i1}(\omega) = H(\omega) - (1 - R_i) & \text{при } \omega \geq \omega_i; \\ F_{i2}(\omega) = -\omega \log_2(2^{1-R_{ai}} - 1) - R_{ai} + R_i & \text{при } \omega < \omega_i, \end{cases} \quad (5.59)$$

$$\omega_i = 1 - 2^{-(1-R_{ai})}.$$

Дальнейшее исследование спектра весов будем проводить лишь для кодов, у которых выполнены условия достижения границы ВГ, так что  $\omega \geq \delta_{ВГ}(R)$ .

При этих ограничениях легко видеть, что  $F_1(\omega) \geq F_i(\omega)$ ,  $i=2, m$ . Следовательно, из (5. 58) и (5. 59), учитывая, что  $R_1=R$ , получаем

$$\bar{N}(n\omega) \leq m 2^{n[H(\omega) - (1-R) + (n_b + \log_2 k_1(m, n_a, n_b))/n]}. \quad (5. 60)$$

Нетрудно убедиться в том, что (5. 60) имеет место и при  $\omega \geq 0,5$ . Отсюда непосредственно вытекает следующее утверждение.

**Утверждение 5.15.** В ансамблях (типа I) случайных каскадных кодов произвольного порядка, для которых выполняются условия достижимости границы ВГ, существуют каскадные коды со спектром весов, удовлетворяющим условиям

$$N(n\omega) = 0 \quad \text{при} \quad 0 < \omega < \delta_{\text{ВГ}}(R);$$

$$N(n\omega) \leq 2^{n[H(\omega) - (1-R) + o(1)]} \quad \text{при} \quad \omega \geq \delta_{\text{ВГ}}(R).$$

Из утверждения 5.15 следует, что такие коды в ДСК без памяти будут иметь экспоненту вероятности ошибки, соответствующую утверждению 1.2 (гл. 1), т. е. экспоненту  $E_0(R)$ , лучшую из известных.

Особый интерес представляют каскадные коды бесконечного порядка структуры  $C$ . Для них, с одной стороны, достижимы границы ВГ и экспонента  $E_0(R)$ . С другой стороны, среди них нет кодов, которые асимптотически превышали бы границу ВГ, а следовательно, они не могут иметь экспоненту, асимптотически лучшую, чем экспонента  $E_0(R)$ . Таким образом, граница ВГ и экспонента  $E_0(R)$  асимптотически точно описывают потенциальные корректирующие свойства каскадных кодов бесконечного порядка структуры  $C$  из ансамблей типа I.

## § 5.7. Сравнение потенциальных и реализуемых корректирующих свойств каскадных кодов

### 5.7.1. Принципы сравнения потенциальных и реализуемых характеристик

При сравнении потенциальных и реализуемых при каскадном декодировании корректирующих свойств каскадных кодов особую роль играют ансамбли случайных каскадных кодов, для которых внутренние коды определяются неслучайной матрицей  $G_0$  (или  $H_0 = G_0^{-1}$ ), одной и той же для всех  $j$ , а внешние коды представляют собой случайные коды РС.

Дело в том, что для каскадных кодов из таких ансамблей известны характеристики как внешних, так и внутренних кодов, что позволяет для каждого кода из ансамбля оценить реализуемые при каскадном декодировании корректирующие характеристики. Таким образом, в этом случае мы можем сравнивать между собой потенциальные и реализуемые корректирующие свойства одних и тех же каскадных кодов. В то же время ясно, что выбирая в ка-



честве кодирующей матрицы неслучайную матрицу, нельзя ожидать сколько-нибудь интересных результатов, не подчиняя ее специальным ограничениям. Так же, как и при выборе в качестве внешних неслучайных кодов мы останавливались на весьма «хороших» кодах РС, так и теперь при выборе неслучайных внутренних кодов будем в качестве матрицы  $G_0$  выбирать такую, которая гарантирует достаточно хороший спектр весов кодовых слов внутренних кодов. Кроме того, матрица  $G_0$  должна быть такой, чтобы для определяемых ею ансамблей каскадных кодов можно было оценить средние по ансамблю (т. е. потенциально достижимые) корректирующие свойства. Всем этим требованиям отвечает матрица  $G_0$ , удовлетворяющая условиям утверждения 5.2, приведенного в разд. 5.2.4.

Таким образом, сопоставление потенциальных и реализуемых свойств каскадных кодов может быть проведено для случайных кодов, составляющих ансамбль  $I^r$  и определяемых неслучайной матрицей  $H_0 = G_0^{-1}$  и случайным кодом РС.

Учитывая, что корректирующие свойства каскадных кодов зависят также и от их структуры, сравнение потенциальных и реализуемых характеристик следует производить для кодов одинаковой структуры.

В качестве характерных структур выберем структуру, максимизирующую реализуемое кодовое расстояние каскадного кода (структура  $A$ ) и структуру, максимизирующую потенциально достижимое кодовое расстояние (структура  $C$ ).

Что касается порядка  $m$  каскадных кодов, то для сокращения объема ограничимся двумя крайними случаями:  $m=1$  и  $m=\infty$ .

### 5.7.2. Каскадные коды первого порядка

Для каскадных кодов первого порядка, определяемых внутренним кодом с кодовым расстоянием, лежащим на границе ВГ, и внешним кодом, являющимся случайным кодом РС, потенциально достижимое кодовое расстояние определяется величиной

$$\delta^*(R, 1) = \begin{cases} \delta_{\text{ВГ}}(R), & \text{если } R_{a1} \geq \log_2 2(1 - \delta_{\text{ВГ}}(R)); \\ (R - R_{a1}) / \log_2(2^{1-R_{a1}} - 1), & \text{если } R_{a1} < \log_2 2(1 - \delta_{\text{ВГ}}(R)). \end{cases}$$

Реализуемое кодовое расстояние такого кода при использовании каскадного декодирования, как было показано в гл. 4, совпадает с нижней оценкой кодового расстояния, которая определяется величиной  $\delta^{(n)}(R, 1) = (1 - R/R_{a1}) \delta_{\text{ВГ}}(R_{a1})$ . Величины  $R_{a1}$  и  $R_{b1}$ , характеризующие структуру  $A$ , максимизирующую  $\delta^{(n)}(R, 1)$  (заимствованные из табл. 3.1), показаны на рис. 5.4. Как видно из этого рисунка, для структуры  $A$ , при всех  $R$ ,  $0 < R < 1$ ,  $R_{a1} < R_{b1}$ , в то время как для структуры  $C$ , максимизирующей  $\delta^*(R, 1)$  (см. рис. 5.3),  $R_{a1} > R_{b1}$ . Результаты расчетов  $\delta^*(R, 1)$  и  $\delta^{(n)}(R, 1)$  для структур  $A$  и  $C$  приведены на рис. 5.5, из которого видно, что различие между  $\delta_a^*(R, 1)$  и  $\delta_1^{(n)}(R, 1)$  немного

меньше, чем между  $\delta_c^*(R, 1) = \delta_{\text{ВГ}}(R)$  и  $\delta_c^{(n)}(R, 1)$ , причем  $\delta_c^{(n)}(R, 1) < \delta_A^{(n)}(R, 1)$ .

Сравнение потенциально достижимой и реализуемой экспоненты вероятности ошибки в ДСК без памяти проведем лишь для кодов структуры  $C$ , для которой, как было показано в разд. 5.7.1, потенциально достижимая экспонента совпадает с экспонентой  $E_0(R)$ :  $E_c^*(R, 1) = E_0(R)$ .

Реализуемая при каскадном декодировании экспонента  $E^{(n)}(R, 1)$  в соответствии с результатами гл. 4 определяется равенством  $E^{(n)}(R, 1) = (1 - R/R_{a1}) E_0(R_{a1})$ , справедливым для каскадных кодов первого порядка любой структуры, в том числе и структур  $A$  и  $C$ . Сравнение  $E_c^*(R, 1)$  с  $E_c^{(n)}(R, 1)$  дано на рис. 5.6, на котором приведена также реализуемая экспонента для структуры  $A$   $E_A^{(n)}(R, 1)$ , которая при всех  $R$  ( $0 < R < 1$ ) превосходит экспоненту  $E_c^{(n)}(R, 1)$ .

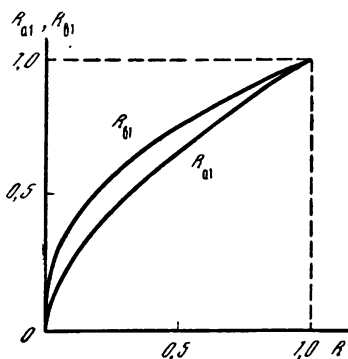


Рис. 5.4. Зависимость значений  $R_{a1}$  и  $R_{a2}$ , соответствующих структуре  $A$ , от скорости передачи  $R$

### 5.7.3. Каскадные коды бесконечного порядка -

Для каскадных кодов бесконечного порядка структуры  $C$ , как было показано в разд. 5.4.6,  $\delta_c^*(R, \infty) = \delta_{\text{ВГ}}(R)$ , т. е. потенциально достижимое кодовое расстояние достигает границы ВГ. Реализуемое при каскадном декодировании кодовое расстояние, совпадающее с его нижней оценкой  $\delta_c^{(n)}(R, \infty)$ , в соответствии с результатами гл. 3 для каскадных кодов бесконечного порядка структуры  $C$  определяется равенством  $\delta_c^{(n)}(R, \infty) = \delta_{\text{ВГ}}(x_0)$ , где  $x_0 = \log_2 \times \times (1 - \delta_{\text{ВГ}}(R))$ .

Что касается каскадных кодов бесконечного порядка структуры  $A$ , то для них, как было показано в гл. 3, верхняя и нижняя оценки кодового расстояния асимптотически совпадают, и так как во всех случаях  $\delta^{(n)}(R, m) \leq \delta^*(R, m) \leq \delta^{(n)}(R, m)$ , то отсюда следует, что для структуры  $A$   $\delta_A^{(n)}(R, \infty) = \delta_A^*(R, \infty)$ , где в соответствии с результатами гл. 3  $\delta_A^{(n)}(R, \infty) = \delta_{\text{ВГ}}(x_0)$ , причем теперь скорости передачи  $R$  и  $x_0 = R_{a1}$  связаны соотношением

$$R = x_0 - \delta_{\text{ВГ}}(x_0) \int_0^{x_0} \frac{dx}{\delta_{\text{ВГ}}(x)}.$$

Таким образом, для каскадных кодов бесконечного порядка структуры  $A$  реализуемое при каскадном декодировании кодовое расстояние совпадает с потенциально достижимым, которое, в свою очередь, является асимптотически истинным кодовым расстоянием.

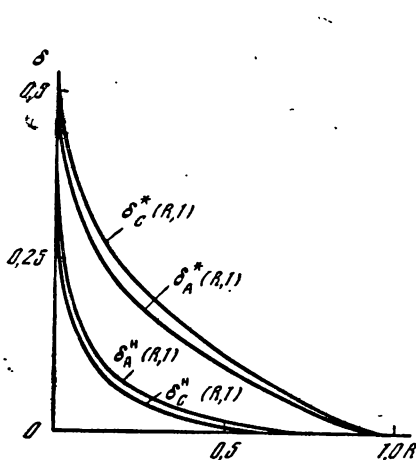


Рис. 5.5. Нижние и средние оценки кодового расстояния каскадных кодов первого порядка структур  $A$  и  $C$

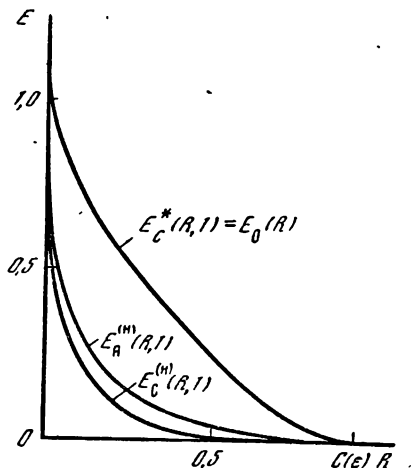


Рис. 5.6. Нижние оценки экспоненты вероятности неправильного декодирования каскадных кодов первого порядка структур  $A$  ( $E_A^{(n)}(R, 1)$ ) и  $C$  ( $E_C^{(n)}(R, 1)$ ) и среднее по ансамблю значение экспоненты вероятности неправильного декодирования структуры  $C$  ( $E_C^*(R, 1)$ ) в ДСК без памяти с  $\epsilon=0,01$

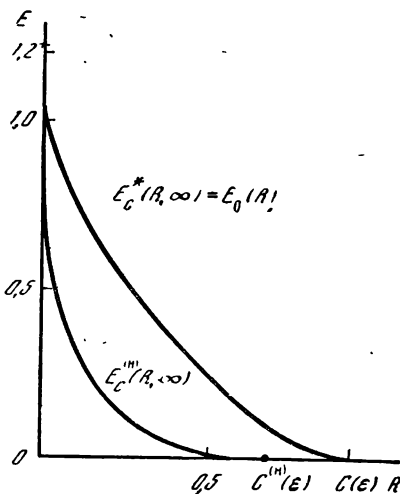
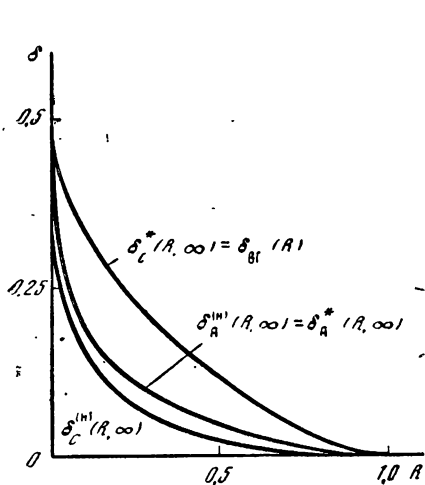


Рис. 5.7. Нижние и средние по ансамблю оценки кодового расстояния каскадного кода бесконечного порядка структур  $A$  и  $C$

Рис. 5.8. Средняя по ансамблю ( $E_C^*(R, \infty)$ ) и реализуемая при каскадном декодировании ( $E_C^{(n)}(R, \infty)$ ) экспоненты вероятности неправильного декодирования каскадных кодов бесконечного порядка структуры  $C$  в ДСК без памяти с  $\epsilon=0,01$

Отсюда следует, что для каскадных кодов структуры  $A$  достаточно большого порядка следует использовать только каскадное декодирование, которое значительно проще декодирования по максимуму правдоподобия. Результаты соответствующих расчетов приведены на рис. 5.7.

Потенциально достижимая экспонента вероятности ошибки в ДСК без памяти для каскадных кодов бесконечного порядка структуры  $C$ , как было указано в разд. 5.7.1, совпадает с экспонентой  $E_0(R)$  и является асимптотически точной. Таким образом,  $E_c^*(R, \infty) = E_0(R)$ . Реализуемая при каскадном декодировании экспонента в соответствии с результатами гл. 4 определяется равенством  $E_c^{(n)}(R, \infty) = E_0(x_0)$ ,  $0 \leq R \leq C^{(n)}(\epsilon)$ , где  $x_0 = \log_2(2 \times \times (1 - \delta_{\text{вг}}(R)))$ ,  $C^{(n)}(\epsilon) = 1 - H(1 - 2^{-(1-\epsilon)})$ ,  $C(\epsilon)$  — пропускная способность ДСК без памяти.

Результаты соответствующих расчетов в предположении, что вероятность одиночной ошибки в ДСК без памяти равна  $\epsilon = 0,01$ , представлены на рис. 5.8.

## ПРОБЛЕМЫ СЛОЖНОСТИ В ТЕОРИИ КОРРЕКТИРУЮЩИХ КОДОВ

---

По-видимому, многие специалисты согласятся, что основными проблемами теории корректирующих кодов являются построение кодов с хорошими корректирующими свойствами, кодирование и декодирование таких кодов. При этом исследователи уже давно не удовлетворялись лишь описанием методов построения, кодирования и декодирования, а пытались оценить и сложность этих методов (хотя бы на интуитивном уровне понимания сложности). Но только в последнее время проблемы сложности стали выдвигаться на первый план, и сейчас с полным правом их можно отнести к стержневым проблемам теории корректирующих кодов. Конечно, традиционные вопросы и вопросы сложности сильно переплетены, что оказывается весьма полезным, ибо, как часто случается, разнообразие подходов привело к значительным успехам и в той и в другой области. При этом, к сожалению, сложные постановки задач не имеют той завидной четкости и строгости традиционных задач. Отсутствие универсальной меры привело к большому разнообразию уже введенных количественных характеристик сложности. Такое разнообразие хотя и отражает истинное положение дел (каждого исследователя волнует своя сложность), но затрудняет сравнение различных результатов. Качественные и количественные выводы могут быть сделаны лишь на основании малого числа заранее выбранных и строго определенных количественных характеристик сложности.

Цель настоящей главы — осмыслить и по возможности строго и единообразно изложить достижения и успехи в решении «сложностных» проблем теории двоичных блочных кодов. При этом будет подчеркнута существенная роль каскадных методов в решении этих задач. Заметим, однако, что в существенной степени полученные результаты носят асимптотический характер — качественные выводы верны лишь при больших кодовых длинах, и, к сожалению, мало точных утверждений можно сделать о конкретных кодах фиксированной длины, хотя именно эта задача практически наиболее важна. Но это общее свойство «сложностных» вопросов любой теории, так как при фиксированных длинах надо учитывать слишком много частных случаев, оказывающих влияние на асимптотические результаты.

Для большей четкости и определенности сузим круг рассматриваемых проблем, ограничиваясь только случаем двоичных блочных кодов и только кодовым расстоянием и экспонентой вероятности неправильного декодирования в канале без памяти в качестве характеристик корректирующей способности в канале без памяти, а также проанализируем далеко не все меры слож-

ности, которые могли бы быть использованы в теории кодирования.

Опишем вкратце последовательность изложения материала. В § 6.1 вводятся основные понятия и определения, используемые при анализе проблемы сложности в теории кодирования. Проблемы задания последовательности асимптотически «хороших» кодов и сложности реализации их кодирования и декодирования при оценке корректирующих свойств кратностью исправляемых ошибок исследованы в § 6.2. Случай оценки корректирующих свойств вероятностью ошибочного декодирования исследован в § 6.3.

В целом в настоящей главе решается задача сложности реализации помехоустойчивого кодирования, которая позволяет определить место каскадных кодов в общей теории корректирующих кодов.

## § 6.1. Коды фиксированной длины

### 6.1.1. Кодирование и декодирование

В дальнейшем рассматриваются двоичные коды длины  $n$  со скоростью передачи  $R_n$  и с кодовым расстоянием  $d = \delta_n n$  или экспонентой вероятности неправильного декодирования  $E_n$  в ДСК без памяти с вероятностью ошибки в символе  $\epsilon$ . Для простоты изложения будем считать, что  $nR_n$  и  $n\delta_n$  — целое число. Множество кодовых слов будем обозначать через  $A(R_n, \delta_n, E_n)$ , а множество всех двоичных слов длины  $n$  — через  $\{0, 1\}^n$ .

Ясно, что множество кодовых слов  $A(R_n, \delta_n, E_n)$  может быть перенумеровано многими различными способами посредством множества  $\{0, 1\}^{nR_n}$  всех последовательностей длины  $nR_n$ . Любое взаимнооднозначное отображение

$$\varphi_n: \{0, 1\}^{nR_n} \leftrightarrow A(R_n, \delta_n, E_n) \quad (6.1)$$

назовем кодированием кода  $A(R_n, \delta_n, E_n)$ . Нетрудно видеть, что всего имеется  $2^{nR_n}$  различных кодирований фиксированного кода  $A(R_n, \delta_n, E_n)$ .

При исследовании декодирования ограничимся случаем, когда на вход декодера может поступить любое двоичное слово длины  $n$ . Поэтому под декодированием будем понимать некоторую функцию вида

$$\psi_n: \{0, 1\}^n \rightarrow A(R_n, \delta_n, E_n), \quad (6.2)$$

где выбор функции  $\psi_n$  определяется поставленной задачей. В дальнейшем ограничимся лишь следующими видами декодирования: декодирование по минимуму расстояния, декодирование с  $\gamma$ -реализацией кодового расстояния и декодирование с  $\gamma$ -реализацией экспоненты  $E_n$ .

Декодирование по минимуму расстояния задается любой функцией  $\psi_n$ , такой, что кодовое слово  $\psi_n(x)$  находится от принятого

слова  $x$  не дальше (в смысле расстояния Хэмминга), чем любое другое кодовое слово. Обозначим через  $\mathfrak{M}$  множество всех функций, задающих декодирование по минимуму расстояния. Очевидно, что  $\psi \in \mathfrak{M}$  тогда и только тогда, когда истинна формула

$$(\forall x: x \in \{0, 1\}^n) (\forall y: y \in A(R_n, \delta_n, E_n)) (d(x, \psi_n(x)) \leq d(x, y)), \quad (6.3)$$

где  $d(x, y)$  — расстояние Хэмминга между словами  $x$  и  $y$ . Напомним, что при декодировании по минимуму расстояния реализуется лучшая для данного кода экспонента вероятности неправильного декодирования  $E_n$ , а поэтому декодирование по минимуму расстояния будем также называть с  $\gamma=1$   $\gamma$ -реализацией экспоненты  $E_n$ .

Декодирование с  $\gamma$ -реализацией ( $0 \leq \gamma \leq 1$ ) кодового расстояния задается любой функцией  $\psi_n$ , такой, что кодовое слово  $\psi_n(x)$  совпадает с результатом декодирования по минимуму расстояния, когда расстояние от принятого слова  $x$  до  $\psi_n(x)$  менее, чем  $\gamma \delta_n n/2$ . Обозначим через  $\mathfrak{M}_\gamma$  множество всех функций, задающих декодирование с  $\gamma$ -реализацией кодового расстояния. Очевидно, что  $\psi_n \in \mathfrak{M}$  тогда и только тогда, когда истинна формула

$$(\forall x: x \in \{0, 1\}^n) (d(x, \psi'_n(x)) < \gamma \delta_n n/2) \Rightarrow (\psi_n(x) = \psi'_n(x)), \quad (6.4)$$

где  $\psi'_n \in \mathfrak{M}$ .

Отметим, что  $\mathfrak{M}_\gamma \supset \mathfrak{M}$  и из  $\gamma_1 < \gamma_2$  следует включение  $\mathfrak{M}_{\gamma_1} \supset \mathfrak{M}_{\gamma_2}$ . Декодирование с  $\gamma$ -реализацией экспоненты  $E_n$  задается любой функцией  $\psi_n$ , такой, что вероятность  $P_n$  неправильного декодирования удовлетворяет соотношению

$$P_n = \sum_{y \in A(R_n, \delta_n, E_n)} P(y) P(\psi(x) \neq y) \leq \exp\{-n E_n \gamma\}, \quad (6.5)$$

где  $P(y)$  — вероятность передачи кодового слова  $y$ , а  $P(\psi(x) \neq y)$  — вероятность, что  $\psi(x) \neq y$  при условии, что по каналу без памяти было передано кодовое слово  $y$ . Обозначим через  $\mathfrak{M}_\gamma^E$  множество всех функций, задающих декодирование с  $\gamma$ -реализацией экспоненты  $E_n$ . Отметим, что и в этом случае  $\mathfrak{M}_\gamma^E \supset \mathfrak{M}$  и из  $\gamma_1 < \gamma_2$  следует включение  $\mathfrak{M}_{\gamma_1}^E \supset \mathfrak{M}_{\gamma_2}^E$ .

### 6.1.2. Сложность кодирования и декодирования

Сложность кодирования и декодирования определим как сложность реализации соответствующих функций на схемах из функциональных элементов. Описание схемы из функциональных элементов и определение ее сложности даны в гл. 1.

Отметим, что для описания схемы (под описанием схемы понимается последовательность двоичных символов, которая однозначно определяет направленный граф и функциональные элементы в его вершинах) достаточно  $s(N+M+L(S)) \log(N+M+L(S))$  двоичных символов, где  $s$  — некоторая константа (так как все оценки в настоящей главе приводим с точностью до мультипли-

кативных констант, то всюду в дальнейшем эти константы будем обозначать одной и той же буквой  $c$ ). Действительно, всего в схеме  $N+M+L(S)$  вершин, их можно перенумеровать с помощью двоичных последовательностей длины  $c(N+M+L(S))$ . Чтобы описать схему для каждой вершины, мы должны указать, является ли она входной, выходной или функциональной; какой элемент в ней находится; из каких вершин в нее входят ребра. Поскольку и число входящих в вершину ребер, и число различных функциональных элементов ограничено, то каждая такая вершина требует для своего описания не более  $c \log(N+M+L(S))$  двоичных символов, а следовательно, и вся схема описывается посредством не более чем  $c(N+M+L(S)) \log(N+M+L(S))$  двоичных символов. Всюду в дальнейшем будем иметь в виду подобное описание схемы.

Рассмотрим теперь некоторый класс функций  $\Phi = \{f\}$ . В отличие от теории управляющих схем, в которой обычно интересуются реализацией всех функций из одного класса, а тем самым функцией с наиболее сложной реализацией, в теории кодирования интересуются реализацией какой-либо функции из данного класса, а тем самым функцией с наиболее простой реализацией, т. е. величиной

$$x(\Phi) = \min_{f \in \Phi} x_f. \quad (6.6)$$

К примеру, существует много кодирований кода  $A(R_n, \delta_n, E_n)$ . Нас, конечно, интересует кодирование этого кода, реализуемое с минимальной сложностью.

### 6.1.3. Система вложенных кодов

В этом разделе вновь возвращаемся к системе вложенных кодов, которая уже неоднократно исследовалась в предыдущих главах. В системе вложенных кодов речь идет уже не об отдельном коде длины  $n$ , а по существу о наборе кодов длины  $n$  со всеми возможными различными скоростями передачи

$$R_n^i = (n-i)/n, \quad i = \overline{1, n}, \quad (6.7)$$

и при этом  $A(R_n^i, \delta_n^i, E_n^i) \supset A(R_n^{i+1}, \delta_n^{i+1}, E_n^{i+1})$ . Поэтому имеют место неравенства  $\delta_n^i \leq \delta_n^{i+1}$ ,  $E_n^i \leq E_n^{i+1}$ . Обозначим через  $A_0^n$  систему вложенных кодов длины  $n$ , а через  $A_i^n$  — ее  $i$ -й подкод, т. е.  $A(R_n^i, \delta_n^i, E_n^i)$ .

Под кодированием системы вложенных кодов будем понимать любую взаимнооднозначную функцию  $\varphi_n: \{0, 1\}^n \rightarrow \{0, 1\}^n$ , такую, что все слова длины  $n$ , содержащие нули на последних  $i$  позициях для любого  $i$ , отображаются в слова кода  $A_i^n$ . Таким образом, функция  $\varphi_n$  задает кодирование сразу для всех кодов  $A_i^n$ ,  $i = \overline{1, n-1}$ , семейства.



Сложность кодирования системы вложенных кодов в соответствии с определениями разд. 6.1.2 будет определяться как

$$\kappa(\Phi_n) = \min_{\varphi_n \in \Phi_n} \kappa(\varphi_n), \quad (6.8)$$

где  $\Phi_n$  — множество всех функций  $\{\varphi_n\}$ , реализующих кодирование данной системы вложенных кодов.

Рассмотрим декодирование системы вложенных кодов. Каждый из подкодов  $A_i^n$  декодируется отдельно, но в то же время при декодировании подкода  $A_i^n$  мы, как правило, уже знаем результаты декодирования  $A_s^n$ ,  $s < i$ . Таким образом, под декодированием кода  $A_i^n$  будем понимать функцию

$$\psi_n : (0, 1)^n \times A_1^n \times A_2^n \times \dots \times A_{i-1}^n \rightarrow A_i^n, \quad (6.9)$$

где выбор функции  $\psi_n$  определяется поставленной задачей. Как и в разд. 6.1.1, ограничимся лишь следующими видами декодирования: декодирование по минимуму расстояния, декодирование с  $\gamma$ -реализацией кодового расстояния и декодирование с  $\gamma$ -реализацией экспоненты.

Во многих практически и теоретически интересных случаях декодирование системы вложенных кодов осуществляется последовательно, т. е. сначала декодируется  $A_1^n$ , потом  $A_2^n$  и т. д. Определим следующим образом декодирование в этом случае. Пусть  $x^1$  — принятое слово, а  $x^i$  определяется как

$$x^i = \begin{cases} x^{i-1}, & \text{если } \psi_n^{i-1}(x^{i-1}) \in A_i^n; \\ x^{i-1} + \psi_n^{i-1}(x^{i-1}), & \text{если } \psi_n^{i-1}(x^{i-1}) \notin A_i^n. \end{cases} \quad (6.10)$$

Декодирование по минимуму расстояния кода  $A_i^n$  будет задаваться любой функцией, такой, что кодовое слово  $\psi_n^i(x^i) \in A_i^n$  находится от слова  $x^i$  не дальше (в смысле расстояния Хэмминга), чем любое другое кодовое слово. Таким образом, если  $x^i$  считать «принятым» словом, то декодирование по минимуму расстояния в рассматриваемом случае совпадает с определенным в разд. 6.1.1. Аналогичное утверждение имеет место и относительно декодирования с  $\gamma$ -реализацией кодового расстояния или экспоненты неправильного декодирования.

Очевидно, что декодирование всей системы вложенных кодов заключается в следующем. Сначала декодируется код  $A_1^n$ , т. е. вычисляется значение  $\psi^1(x^1)$  и по формуле (6.10) определяется  $x^2$ , затем код  $A_2^n$  и т. д. При этом сложность  $\kappa(\psi)$  декодирования системы вложенных кодов определяется как

$$\kappa(\psi) = \sum_{i=1}^{n-1} [\kappa(\psi^i) + \kappa(x^i)], \quad (6.11)$$

где  $\kappa(\psi^i)$  — сложность декодирования кода  $A_i^n$ , а  $\kappa(x^i)$  — сложность вычисления  $x^i$  по формуле (6.10).

Отметим, что во всех рассматриваемых далее случаях  $x(\psi^i) \geq x(x^i)$ , поэтому вместо соотношения (6.11) будем пользоваться оценкой

$$x(\psi) \leq 2n \max_{1 \leq i \leq n} x(\psi^i). \quad (6.12)$$

Таким образом, сложность декодирования системы вложенных кодов будет определяться в основном сложностью декодирования того кода  $A_n$ , для которого она наибольшая.

## § 6.2. Последовательность кодов с асимптотически «хорошим» кодовым расстоянием

### 6.2.1. Задание последовательности

Теория кодирования посвящена исследованию не отдельных кодов, а по существу их последовательностей. В настоящем параграфе ограничимся лишь последовательностями кодов, у которых отношение кодового расстояния  $d$  к длине кода  $n$  не стремится к нулю при  $n \rightarrow \infty$  и любом значении скорости  $R$ ,  $0 < R < 1$ .

Объединение всех кодов бесконечной последовательности кодов  $A(R_n, \delta_n, E_n)$  назовем кодовым множеством  $A = \bigcup_{n=1}^{\infty} A(R_n, \delta_n, E_n)$ .

Таким образом, кодовое множество  $A$  является подмножеством множества  $E = \bigcup_{n=1}^{\infty} \{0, 1\}^n$  всех двоичных слов конечной длины.

Обозначим через  $N_A$  множество всех  $n$ , таких, что  $A(R_n, \delta_n, E_n)$  не пусто:  $N_A = \{n \mid A(R_n, \delta_n, E_n) \neq \emptyset\}$ . В настоящем параграфе будем рассматривать лишь такие кодовые множества  $A$ , у которых  $N_A$  бесконечно и существуют пределы  $R = \lim_{n \in N_A} R_n$ ,  $\delta = \lim_{n \in N_A} \delta_n$ .

В этом случае будем говорить, что кодовое множество  $A = A(R, \delta)$  имеет параметры  $R$  и  $\delta$ . Ради упрощения дальнейших записей будем считать, что начиная с некоторого  $n = n_0$  все  $R_n$  и  $\delta_n$  постоянны и равны соответственно  $R$  и  $\delta$ .

Нас будут интересовать лишь конструктивно задаваемые последовательности кодов. Конструктивность кодового множества  $A$  означает наличие алгоритма, позволяющего для любой точки  $x$  определить, принадлежит она множеству  $A$  или нет. Одна из наиболее принятых формализаций понятия алгоритма — машина Тьюринга (см. гл. 1). Всюду в дальнейшем под алгоритмом мы всегда подразумеваем машину Тьюринга.

Под заданием последовательности кодов будем понимать задание алгоритма для вычисления характеристической функции  $\chi_A$  кодового множества  $A$  (характеристическая функция множества  $A$  задается на  $E$  и равна единице на  $A$  и нулю в противном случае).

Из сказанного следует, что мы рассматриваем лишь рекурсивные кодовые множества, придавая тем самым интуитивному поня-

тию конструктивности общепринятый строгий и точный смысл. Параметры, определяющие сложность вычисления характеристической функции кода всего множества  $A$ , и будут параметрами, определяющими сложность задания последовательности кодов.

Исходя из условий, рассмотренных в гл. 1, будем интересоваться лишь одной количественной характеристикой алгоритма — временем вычислений на машине Тьюринга в зависимости от длины входной последовательности

$$T(n) = \max_{x: l(x)=n} T(x), \quad (6.13)$$

где  $l(x)$  — длина входной последовательности  $x$ ,  $T(x)$  — время вычислений для входной последовательности  $x$ . Кроме того, конкретные оценки будут выписаны для многоленточной машины Тьюринга.

Прежде всего укажем тривиальную оценку снизу времени вычислений для «хороших» кодовых множеств, т. е. множеств со строго положительными параметрами  $R$  и  $\delta$ .

Оценка снизу (тривиальная). Для всякой программы, задающей кодовое множество с параметрами  $R > 0$  и  $\delta > 0$ , при всех  $n \in N_A$  верно неравенство  $T(n) \geq cn$ .

Эта оценка следует из того, что машина Тьюринга за единицу времени может просмотреть лишь ограниченное число символов, а каждое кодовое слово должно быть просмотрено полностью. В самом деле, если некоторый символ кодового слова не просмотрен, то, заменяя этот символ на противоположный, получим новое слово, которое машина также отнесет к кодовым, что противоречит условию  $\delta > 0$ . К сожалению, других оценок снизу не известно. Прежде чем перейти к верхним оценкам времени вычислений для различных кодовых множеств, сделаем следующие замечания. Все эти верхние оценки получаются указанием соответствующих алгоритмов. Нигде не утверждается, что нет алгоритмов, время вычислений по которым растет гораздо медленнее (просто на сегодняшний день такие алгоритмы не известны). При этом, конечно, мы всегда будем давать лишь неформальные описания программ с некоторыми пояснениями, по которым формальные программы при желании всегда могут быть написаны.

Сложность задания кодовых множеств с кодовым расстоянием, соответствующим границе ВГ, по алгоритму Гилберта или алгоритму Варшавова приведена в утверждениях 1.3 и 1.4.

Сложность задания системы вложенных кодов, каждый из которых имеет кодовое расстояние, соответствующее границе ВГ, определяется следующим утверждением, доказанным в приложении П.6.1.

**Утверждение 6.1.** Сложность задания последовательности систем вложенных кодов при построении их по алгоритму, описанному при доказательстве теоремы 2.3, удовлетворяет соотношению

$$T(n) \leq cn^{2^{2n}}. \quad (6.14)$$

Итак, и алгоритм Гилберта, и алгоритм Варшамова, и алгоритм построения вложенной системы кодов (конечно, можно предложить и другие схожие алгоритмы) задают хорошие кодовые множества, но время вычислений растет экспоненциально с ростом  $n$ . С другой стороны, давно известны алгоритмы (к примеру, БЧХ-коды, коды РС, коды Рида—Маллера) со степенной сложностью вычислений, задающие, к сожалению, кодовые множества, один из параметров которых ( $R$  или  $\delta$ ) равен нулю. Длительное время оставалось неизвестным, существуют ли алгоритмы с неэкспоненциальным ростом времени вычислений, задающие кодовые множества со строго положительными параметрами  $R$  и  $\delta$ . Впервые положительный ответ на этот вопрос был получен каскадными методами в 1969 г. в работе [74]. До настоящего времени задачу построения асимптотически «хороших» кодовых множеств с неэкспоненциальной сложностью удается решать лишь каскадными методами.

Из большого разнообразия каскадных кодов ниже мы ограничимся лишь двумя крайними случаями: каскадными кодами первого порядка и каскадными кодами бесконечного порядка. Первые из них позволяют получить наименьшую из известных сложностей задания кодового множества с положительными  $R$  и  $\delta$ , а вторые — наилучшие из известных параметры  $R$  и  $\delta$  при неэкспоненциальной сложности задания кодового множества.

**Утверждение 6.2.** Существует кодовое множество  $A(R, \delta)$ , состоящее из каскадных кодов первого порядка, с параметрами  $R$  и  $\delta$ , удовлетворяющими соотношению

$$\delta(R) \geq \delta_1(R) = \max_{R_{a1} > \frac{1}{3}} \{H^{-1}(1 - R_{a1})(1 - R/R_{a1})\}, \quad (6.15)$$

где  $H^{-1}(y)$  — функция, обратная двоичной энтропии  $y = H(x)$  при  $x \in [0, 1/2]$ , и задающая его машина Тьюринга, такая, что

$$T(n) \leq cn^2 \log n. \quad (6.16)$$

Если в каскадном коде первого порядка в качестве внешнего кода использовать итерацию двух кодов РС [75] и применить быстрое умножение многочленов над конечными полями [10], то получим следующее утверждение.

**Утверждение 6.3.** Существует кодовое множество  $A(R, \delta)$ , состоящее из каскадных кодов первого порядка, с параметрами  $R$  и  $\delta$ , удовлетворяющими соотношению

$$\delta(R) \geq \delta_2(R) = \max_{R_{a1} \geq \frac{1}{2}} \{H^{-1}(1 - R_{a1})[1 - (R/R_{a1})^{1/2}]^2\}, \quad (6.17)$$

и задающая его машина Тьюринга, такая, что

$$T(n) \leq cn \log^4 n. \quad (6.18)$$

Эта сложностная оценка может быть еще улучшена, если в качестве внешних кодов использовать итерацию трех кодов РС

над простым полем, что в результате дает уже нелинейные двоичные каскадные коды, и применять соответствующее быстрое кодирование и декодирование кодов РС [3—6]. При этом, однако, еще ухудшается и оценка для  $\delta(R)$ , о чем свидетельствует следующее утверждение.

**Утверждение 6.4.** Существует нелинейное кодовое множество  $A(R, \delta)$ , состоящее из каскадных кодов первого порядка, с параметрами  $R$  и  $\delta$ , удовлетворяющими соотношению

$$\delta(R) \geq \delta_s(R) = \max_{R_{a1} \geq 1/4} \{H^{-1}(1 - R_{a1})[1 - (R/R_{a1})^{1/3}]^3\}, \quad (6.19)$$

и задающая его машина Тьюринга, такая, что

$$T(n) \leq cn \log^2 n. \quad (6.20)$$

Чтобы улучшить оценку для  $\delta(R)$ , можно использовать каскадные коды бесконечного порядка, что в соответствии со следующим утверждением, доказанным в приложении П.6.3, приведет к увеличению сложности задания.

**Утверждение 6.5.** Существует линейное кодовое множество  $A(R, \delta)$ , состоящее из каскадных кодов бесконечного порядка, с параметрами  $R$  и  $\delta$ , удовлетворяющими соотношению

$$R = 1 - H(\delta) - \delta \int_0^{1-H(\delta)} \frac{dx}{H^{-1}(1-x)}, \quad (6.21)$$

и задающая его машина Тьюринга, такая, что

$$T(n) \leq cn^{2 \log \log n / (1-H(\delta))} \log n. \quad (6.22)$$

Утверждения 6.2—6.5 задают различные каскадные кодовые множества с различными оценками для  $\delta$ . Чтобы показать, насколько ухудшаются оценки  $\delta$  в утверждениях 6.3 и 6.4 и улучшаются в утверждении 6.5, в табл. 6.1 приведены значения параметра  $\delta$  при некоторых скоростях передачи. Там же даны оценки ВГ для соответствующих скоростей передачи.

### 6.2.2. Задание последовательности кодов с кодированием

В предыдущем разделе мы рассмотрели безусловно интересный теоретический вопрос о сложности задания «хорошего» кодового множества. Теперь остановимся на практически более важном вопросе задания кодового множества вместе с кодированием и определим те количественные характеристики, которыми хотим оценивать простоту задания кодового множества с кодированием и самого кодирования.

Определим кодирование кодового множества как алгоритм, который каждому  $n \in N_A$  ставит в соответствие двоичное описание схемы из функциональных элементов, реализующих функцию

$\varphi_n$  (см. разд. 6.1.1). Введем следующие две численные характеристики: 1)  $\kappa_e(n)$  — сложность схемы (число функциональных

Таблица 6.1

$R$	$\delta_1(R, 1)$	$\delta_2(R, 1)$	$\delta_3(R, 1)$	$\delta_A(R, \infty)$	$\delta_{ВГ}(R)$
0,060	0,1427	0,0577	0,0142	0,2242	0,3570
0,132	0,1051	0,0239	0,0033	0,1508	0,2900
0,199	0,0735	0,0123	0,0012	0,1196	0,2440
0,272	0,0521	0,0071	0,0006	0,0914	0,2030
0,333	0,0373	0,0043	0,0003	0,0748	0,1740
0,406	0,0257	0,0025	0,0001	0,0576	0,1440
0,497	0,0157	0,0012	$5,3 \cdot 10^{-5}$	0,0411	0,1110
0,610	0,0078	0,0004	$1,4 \cdot 10^{-5}$	0,0255	0,0765
0,679	0,0047	0,0002	$5,1 \cdot 10^{-6}$	0,0187	0,0584
0,759	0,0025	0,0001	$1,4 \cdot 10^{-6}$	0,0115	0,0398
0,857	0,0007	$1,1 \cdot 10^{-5}$	$1,2 \cdot 10^{-7}$	0,0056	0,0222
0,917	0,0002	$2,0 \cdot 10^{-6}$	$1,1 \cdot 10^{-8}$	0,0023	0,0104

элементов в схеме), реализующей функцию  $\varphi_n$ ; 2)  $T_e(n)$  — сложность задания кодового множества с кодированием (время вычисления на машине Тьюринга двоичного описания этой схемы — число операций).

Заметим прежде всего, что

$$c\kappa_e(n) \log \kappa_e(n) \leq T_e(n), \quad (6.23)$$

так как машина Тьюринга должна, по крайней мере, напечатать двоичное описание схемы. Никаких обратных оценок не известно, и во многих примерах степенной рост  $\kappa_e(n)$  будет соседствовать с экспоненциальным ростом  $T_e(n)$ . Здесь уместно напомнить, что единожды вычисленная кодирующая схема может затем многократно использоваться, так что иногда имеет смысл затратить много времени  $T_e(n)$  на получение схемы малой сложности  $\kappa_e(n)$ , конечно, при условии, что численное значение  $T_e(n)$  технически и экономически приемлемо.

Отметим, что, как и ранее, мы будем давать лишь неформальное описание алгоритмов. Оценки сложности задания кодового множества с кодированием при использовании алгоритмов Гилберта и Варшамова приведены в гл. 1 (утверждения 1.3 и 1.4). Как уже отмечалось, переход от нелинейных к линейным кодовым множествам резко снижает сложность схем, реализующих кодирование. Еще больше можно снизить сложность  $\kappa_e(n)$ , если использовать класс псевдоциклических кодов.

**Утверждение 6.6.** Существует псевдоциклическое кодовое множество  $A(R, \delta)$  с параметрами  $R$  и  $\delta$ , удовлетворяющими границе ВГ, и такое его кодирование, что

$$\kappa_e(n) \leq cn \log^3 n; \quad T_e(n) \leq cn^2 2^n. \quad (6.24)$$

**Доказательство.** Для получения этих оценок достаточно вспомнить, что среди псевдоциклических кодов существуют коды, лежащие на границе ВГ [155], и для нахождения таких кодов перебором достаточно  $cn^2 2^n$  операций. Кодирование же псевдоциклических кодов сводится к перемножению многочленов над  $GF(2)$ , что может быть осуществлено на схеме из  $cn \log^3 n$  элементов [10].

Рассмотрим теперь кодирование последовательности систем вложенных кодов.

**Утверждение 6.7.** Существует такая последовательность систем вложенных кодов, у которой параметры  $R^i$  и  $\delta^i$  всех подкодов  $A_n^i$  удовлетворяют границе ВГ, и такое кодирование систем этой последовательности, что

$$x_e(n) \leq cn^2/\log n; \quad T_e(n) \leq cn2^{2^n}. \quad (6.25)$$

**Доказательство.** Этот результат получается непосредственной оценкой числа шагов по следующей неформальной программе. По алгоритму, описанному при доказательстве теоремы 2.3, строим кодирующую матрицу  $G_0$  системы вложенных кодов. В соответствии с утверждением 6.1 число операций не превосходит  $cn2^{2^n}$ . Используя кодирующую матрицу  $G_0$ , строим схему сложности  $cn^2/\log n$ , реализующую функцию  $\varphi_n$ , т. е. умножение матрицы порядка  $n$  на вектор (для описания ее достаточно  $cn^2 \log n$  операций).

К сожалению, во всех приведенных утверждениях сложность задания «хороших» кодовых множеств с кодированием остается слишком большой (экспоненциально растет с длиной кода). Однако, как и в предыдущем разделе, эта проблема решается применением каскадных кодовых множеств.

**Утверждение 6.8.** Существует кодовое множество  $A(R, \delta)$ , состоящее из каскадных кодов первого порядка, с параметрами  $R$  и  $\delta$ , удовлетворяющими соотношению (6.15), и такое его кодирование, что

$$x_e(n) \leq cn \log^4 n; \quad T_e(n) \leq cn^2 \log n. \quad (6.26)$$

**Доказательство.** Для получения этих оценок достаточно рассмотреть обычное кодирование каскадного кодового множества из утверждения 6.2. Это кодирование проводится в два этапа. Сначала используется для кодирования внешний код — код РС, что сводится к перемножению двух многочленов степени не более  $R_{b1} n_b$  и  $(1 - R_{b1}) n_b$  над полем  $GF(2^{R_{a1} n_a})$ . Согласно [10], это можно осуществить схемой сложности  $cn_b (\log n_b)^3 n_a^2$ , описание которой можно построить за  $cn_b (\log n_b)^4 n_a^2$  операций. Затем  $n_b$  двоичных последовательностей длины  $R_{a1} n_a$  кодируются внутренним кодом — линейным двоичным кодом длины  $n_a$ . Для этого согласно утверждению 1.4 достаточно  $n_b$  одинаковых схем сложности  $cn_a^2/\log n_a$ , описание которых можно построить

за  $cn_a 2^{(1-R_a)n_a}$  операций. Выражая теперь все приведенные оценки через длину кода  $n$  (напомним, что  $R_{a1} \geq 1/3$  в соответствии с (6.15)), получим утверждение 6.8.

Используя в каскадном коде в качестве внешнего кода итерацию двух одинаковых кодов Рида—Соломона, можно получить следующее утверждение (см. утверждение 6.3).

**Утверждение 6.9.** Существует кодовое множество  $A(R, \delta)$ , состоящее из каскадных кодов первого порядка, с параметрами  $R$  и  $\delta$ , удовлетворяющими соотношению (6.17), и такое его кодирование, что

$$x_e(n) \leq cn \log^4 n; \quad T_e(n) \leq cn \log^5 n. \quad (6.27)$$

Переходим, как и в утверждении 6.4, к трехмерной итерации кодов РС над простыми полями, тогда очевидным образом из утверждения 6.4 и работы [3] вытекает результат.

**Утверждение 6.10.** Существует нелинейное кодовое множество  $A(R, \delta)$ , состоящее из каскадных кодов первого порядка, с параметрами  $R$  и  $\delta$ , удовлетворяющими (6.19), и такое его кодирование, что

$$x_e(n) \leq cn \log^2 n; \quad T_e(n) \leq cn \log^3 n. \quad (6.28)$$

Как уже отмечалось, использование каскадных кодов бесконечного порядка позволяет существенно улучшить оценку  $\delta$  при фиксированном  $R$ . Сложность задания такого кодового множества с кодированием определяется следующим утверждением, доказанным в приложении П.6.4.

**Утверждение 6.11.** Существует линейное кодовое множество  $A(R, \delta)$ , состоящее из каскадных кодов бесконечного порядка с параметрами  $R$  и  $\delta$ , удовлетворяющими (6.21), и такое его кодирование, что

$$x_e(n) \leq cn \log^5 n \log \log n; \quad T_e(n) \leq cn^{2 \log \log n / (1-H(\delta))} \log n \log \log n. \quad (6.29)$$

Приведем теперь для сравнения тривиальные нижние оценки  $x_e(n)$  и  $T_e(n)$ . Очевидно, что для любого кодового множества с  $R > 0$  и  $\delta > 0$  и любого его кодирования имеют место неравенства

$$x_e(n) \geq cn; \quad T_e(n) \geq cn \log n. \quad (6.30)$$

Как видим, в приведенных выше результатах не достигается ни одна из нижних границ. Однако достижение по крайней мере первой из них в принципе возможно. Это непосредственно вытекает из работы [151], результат которой можно сформулировать в виде следующего утверждения.

**Утверждение 6.12.** Существует линейное кодовое множество  $A(R, \delta)$  с параметрами  $R$  и  $\delta$ , удовлетворяющими соотношению

$$\delta + \varepsilon = H^{-1}(1 - R), \quad (6.31)$$



где  $\varepsilon$  ( $0 < \varepsilon < \delta$ ) — любое фиксированное число, и такое его кодирование, что

$$x_\varepsilon(n) \leq c_1(\varepsilon)n; \quad T_\varepsilon(n) \leq c_2(\varepsilon)2^{c_3(\varepsilon)n \log n}, \quad (6.32)$$

где  $c_1(\varepsilon)$ ,  $c_2(\varepsilon)$  и  $c_3(\varepsilon)$  — величины, зависящие только от  $\varepsilon$ .

### 6.2.3. Задание последовательности кодов с декодированием

Аналогично кодированию определим декодирование как алгоритм, который позволяет для каждого  $n \in N_A$  вычислить на машине Тьюринга двоичное описание схемы, реализующей функцию  $\varphi_n$  (см. § 6.1). При декодировании, как и при кодировании, будем рассматривать следующие две численные характеристики:  $x_d(n)$  — сложность схемы, реализующей функцию  $\varphi_n$ ;  $T_d(n)$  — сложность задания кодового множества с декодированием (время вычисления на машине Тьюринга двоичного описания этой схемы — число операций). Как и ранее, будем давать лишь неформальное описание алгоритмов.

Рассмотрим декодирование по минимуму расстояния. Оценки сложности задания кодового множества с декодированием по минимуму расстояния при использовании алгоритмов Гилберта и Варшамова приведены в гл. 1 (утверждения 1.3 и 1.4).

Сложность декодирования последовательности систем вложенных кодов оценивается в соответствии со следующим утверждением, доказанным в приложении П.6.5.

**Утверждение 6.13.** Существует такая последовательность систем вложенных кодов, что параметры  $R^i$  и  $\delta^i$  всех подкодов  $A^i$  удовлетворяют границе ВГ, и такое декодирование по минимуму расстояния систем вложенных кодов, что

$$x_d(n) \leq cn^2n^{1/2}; \quad T_d(n) \leq cn2^{2n}. \quad (6.33)$$

При декодировании по минимуму расстояния мы впервые сталкиваемся со случаем, когда все оценки имеют экспоненциальный рост и не известны лучшие результаты ни для каких кодовых множеств с положительными параметрами  $R$  и  $\delta$ .

Рассмотрим декодирование  $\gamma$ -реализацией кодового расстояния. Ограничимся рассмотрением только таких множеств  $A(R, \delta)$ , для которых оценки сложности декодирования носят неэкспоненциальный характер. Как и при кодировании, это будут в основном каскадные методы.

**Утверждение 6.14.** Существует кодовое множество  $A(R, \delta)$ , состоящее из каскадных кодов первого порядка, с параметрами  $R$  и  $\delta$ , удовлетворяющими соотношению (6.15), и такое его декодирование с  $\gamma$ -реализацией кодового расстояния ( $\gamma = \delta_1(R)/\delta(R)$ ), где  $\delta_1(R)$  определяется соотношением (6.15), а  $\delta(R)$  — действительное отношение  $d/n$ , что

$$x_d(n) \leq cn^2; \quad T_d(n) \leq cn^2 \log n \quad (6.34)$$

(доказательство этого утверждения дано в приложении П.6.6).

Используя в каскадном коде в качестве внешнего кода итерацию двух одинаковых кодов РС, можно получить следующее утверждение (см. также утверждения 6.3 и 6.9).

**Утверждение 6.15.** Существует кодовое множество  $A(R, \delta)$ , состоящее из каскадных кодов первого порядка, с параметрами  $R$  и  $\delta$ , удовлетворяющее соотношению (6.17), и такое его декодирование с  $\gamma$ -реализацией кодового расстояния ( $\gamma = \delta_2(R)/\delta(R)$ ), что

$$x_d(n) \leq cn \log^5 n; \quad T_d(n) \leq cn \log^6 n. \quad (6.35)$$

Если же в каскадном коде в качестве внешних кодов использовать трехмерную итерацию кодов РС над простыми полями и результаты работы [6], то можно получить следующее утверждение (см. также утверждения 6.4 и 6.10).

**Утверждение 6.16.** Существует нелинейное кодовое множество  $A(R, \delta)$ , состоящее из каскадных кодов первого порядка, с параметрами  $R$  и  $\delta$ , удовлетворяющими (6.19), и такое его декодирование с  $\gamma$ -реализацией кодового расстояния ( $\gamma = \delta_3(R)/\delta(R)$ ), что

$$x_d(n) \leq cn \log^3 n; \quad T_d(n) \leq cn \log^4 n. \quad (6.36)$$

Как уже отмечалось, использование каскадных кодов бесконечного порядка позволяет существенно улучшить оценку  $\delta$  при фиксированном  $R$  (см. утверждения 6.5 и 6.11). Сложность задания такого кодового множества с декодированием определяется следующим утверждением, доказанным в приложении П.6.7.

**Утверждение 6.17.** Существует линейное кодовое множество  $A(R, \delta)$ , состоящее из каскадных кодов бесконечного порядка, с параметрами  $R$  и  $\delta$ , удовлетворяющими (6.21), и такое его декодирование с  $\gamma$ -реализацией кодового расстояния ( $\gamma \rightarrow 1$  при  $n \rightarrow \infty$ ), что

$$\begin{aligned} x_d(n) &\leq cn^{(1+\log \log n)/2(1-H(\delta))} \log n \log \log n, \\ T_d(n) &\leq cn^{2 \log \log n / (1-H(\delta))} \log n \log \log n. \end{aligned} \quad (6.37)$$

Наилучшая из известных на сегодняшний день оценка  $x_d(n)$  для декодирования с  $\gamma$ -реализацией кодового расстояния получена в работе [83]. Результаты этой работы в терминах задания кодового множества с декодированием можно сформулировать следующим образом.

**Утверждение 6.18.** Существует кодовое множество  $A(R, \delta)$ , содержащее низкоплотностные коды, с параметрами  $R$  и  $\delta$ , определяемыми соотношениями  $R \geq 1 - l/h$ , где  $l$  и  $h$  ( $4 < l < h$ ) — любые положительные целые числа, значение  $\delta$  определяется как корень уравнения

$$(l-1)H(x) + \frac{l}{h} \max_{0 < s < 1} \{ \log_2[(1+s)^h - (1-s)^h] - 1 + x \log_2 s \} = 0,$$

и такое его декодирование  $\gamma$ -реализацией кодового расстояния при  $\gamma \geq \rho_0/\delta$  ( $\rho_0 < 0.5$  — решение уравнения  $R=1-22 H(\rho)$ ), что  $x_d(n) \leq cn \log n$ ;  $T_d(n) \leq c2^{cn \log n}$ .

Подчеркнем, что для кодовых множеств с  $R > 0$  и  $\delta > 0$  нижняя тривиальная оценка  $x_d(n) \geq cn$  не получена ни для какого роста  $T_d(n)$ .

Отметим, что для положительных  $R$  и  $\delta$  пока только для каскадных кодовых множеств удается получить верхние оценки вида  $cn \log^a n$  одновременно для всех рассматриваемых в данном параграфе характеристик сложности. Более того, не известны «некаскадные» кодовые множества с  $R > 0$  и  $\delta > 0$ , у которых по крайней мере одна из характеристик сложности не росла бы экспоненциально. К сожалению, во всех каскадных кодовых множествах границы параметров  $R$  и  $\delta$  хуже границы ВГ, с которой принято сравнивать в подобных случаях корректирующие свойства кодов.

### § 6.3. Последовательность кодов с асимптотически «хорошей» экспонентой

#### 6.3.1. Система вложенных кодов

В настоящем параграфе вновь вернемся к задачам задания последовательности кодов с кодированием и декодированием, но уже в качестве основных характеристик кодового множества будем рассматривать не параметры  $R$  и  $\delta$ , а  $R$  и  $E$ , где  $R = \lim_{n \in N_A} R_n$ .

а  $E = \lim_{n \in N_A} E_n$ . В этом случае будем обозначать кодовое множество

через  $A(R, E)$  или  $A(R, \delta, E)$ , если известен и предел  $\delta = \lim_{n \in N_A} \delta_n$ . Уже говорилось, что  $E$  есть экспонента веро-

ятности неправильного декодирования в канале без памяти, которая для любого кода принимает максимальное значение при декодировании по минимуму расстояния. Кроме того, как следует из утверждения 1.4, существуют коды, для которых она положительна для всех скоростей, меньших пропускной способности  $(C)$ , и для этого достаточно, чтобы код имел спектр весов  $N(w)$ ,  $w=1, n$ , удовлетворяющий утверждению 1.3. При этом экспонента принимает наибольшее из известных значений, определяемое утверждением 1.4, которое в дальнейшем будем называть экспонентой или границей Галлагера и сравнивать с ней получаемые результаты, как это делалось с границей ВГ в предыдущем параграфе. Ниже асимптотически «хорошим» будем считать любое кодовое множество  $A(R, E)$ , когда имеет место  $R > 0$  и  $E > 0$  при  $R < C$ . Подчеркнем разницу в построении кодовых множеств  $A(R, \delta)$  и  $A(R, E)$ . При построении кодового множества  $A(R, \delta)$  по существу необходимо было лишь заботиться о том, чтобы вокруг каждого кодового слова не было других кодовых слов в сфере  $\delta n$ ,

что и гарантировалось, например, построением по алгоритму Варшамова или по алгоритму Гилберта. При построении  $A(R, E)$  нужно еще следить, чтобы вокруг каждого кодового слова не только слова наименьшего веса, но и слова других весов располагались соответствующим образом. Поэтому фактически всегда строится кодовое множество  $A(R, \delta, E)$ . Конечно, из существования таких кодовых множеств следует, что их всегда можно построить, выбирая посредством перебора всех кодов на каждой длине  $n \in N_A$  нужный код. Однако при этом число операций будет иметь порядок  $2^{an}$ . Как следует из приведенного ниже утверждения, доказанного в приложении П.6.8, эта задача решается более простым способом. При этом используются понятия и обозначения, введенные в § 6.2.

**Утверждение 6.19.** Существует такая последовательность систем вложенных кодов, что параметры  $R^i$ ,  $\delta^i$  и  $E^i$  всех подкодов  $A_n^i$  удовлетворяют границам ВГ и Галлагера, и существуют такие кодирование и декодирование по минимуму расстояния систем вложенных кодов, что

$$x_e(n) \leq cn^2; \quad x_d(n) \leq cn^2 2^{n/2}, \quad T_0(n) \leq cn^3 2^{2n}, \quad (6.38)$$

где  $T_0(n)$  характеризует сложность задания последовательности систем вложенных кодов с кодированием и декодированием.

Конечно, можно предложить и другие алгоритмы и схемы, но во всех известных случаях и сложность задания, и сложность декодирования по минимуму расстояния кодовых множеств с параметрами  $R > 0$  и  $\delta > 0$  будут иметь экспоненциальный характер. Например, модернизацией алгоритма Варшамова, т. е. когда при построении контролируется не только кодовое расстояние, но и следующие веса, можно получить следующее утверждение.

**Утверждение 6.20.** Существует такое линейное кодовое множество  $n(R, \delta, E)$ , что параметры  $R, \delta, E$  удовлетворяют границам ВГ и Галлагера, и такие кодирование и декодирование по минимуму расстояния, что

$$x_e(n) \leq cn^2 / \log n; \quad x_d(n) \leq cn \min \{2^{(1-R)n}; 2^{Rn}\}, \quad (6.39)$$

$$T_0(n) \leq cn^2 2^{(2-R)n}.$$

Сравнение утверждения 6.20 с утверждением 1.4 показывает, что необходимость при построении контролировать весь спектр весов увеличивает экспоненту числа операций при задании кода.

### 6.3.2. Каскадные кодовые множества

В настоящем разделе остановимся на  $\gamma$ -реализации экспоненты вероятности неправильного декодирования, которая имеет место при каскадном декодировании (см. гл. 4). При этом, как всюду, в этой главе ограничимся лишь случаями каскадных кодов первого и бесконечного порядков.

Отметим, что переход при каскадном декодировании от  $\gamma$ -реализации кодового расстояния к  $\gamma$ -реализации экспоненты связан лишь с «заменой» внутренних кодов с гарантируемым кодовым расстоянием на коды с гарантируемым спектром весов, т. е. все изменения в сложностных параметрах каскадных кодов будут в рассматриваемых случаях обусловлены изменениями сложностных параметров внутренних кодов. Учитывая это замечание и используя результаты утверждений 6.2, 6.5, 6.7, 6.11, 6.14, 6.17, 6.19 и 6.20, получаем следующие утверждения.

**Утверждение 6.21.** Существует линейное кодовое множество  $A(R, \delta, E)$ , состоящее из каскадных кодов первого порядка, с такими параметрами  $R, \delta$  и  $E$ , что  $R$  и  $\delta$  удовлетворяют (6. 15), а  $R$  и  $E$  удовлетворяют соотношению

$$E(R) \geq E_1(R) = \max_{R_{a1} \geq 1/3} E_0(R_{a1}) (1 - R/R_{a1}), \quad (6.40)$$

где  $E_0(R_{a1})$  — оценка Галлагера для экспоненты неправильного декодирования, и такие кодирование и каскадное декодирование с  $\gamma$ -реализацией экспоненты ( $\gamma \geq E_1(R)/E(R)$ ), что

$$\kappa_e(n) \leq cn \log^4 n; \quad \kappa_d(n) \leq cn^2; \quad T_0(n) \leq cn^4 \log n. \quad (6.41)$$

Использование в каскадном коде в качестве внешних кодов трехмерной итерации кодов РС над простыми полями дает следующее утверждение.

**Утверждение 6.22.** Существует нелинейное кодовое множество  $A(R, \delta, E)$ , состоящее из каскадных кодов первого порядка, с такими параметрами  $R, \delta$  и  $E$ , что  $R$  и  $\delta$  удовлетворяют (6. 19), а  $R$  и  $E$  удовлетворяют соотношению

$$E(R) \geq E'_1(R) = \max_{R_{a1} \geq 1/4} E_0(R_{a1}) (1 - (R/R_{a1})^{1/3}), \quad (6.42)$$

где  $E_0(R_{a1})$  — оценка Галлагера для экспоненты неправильного декодирования, и такие кодирование и каскадное декодирование с  $\gamma$ -реализацией экспоненты ( $\gamma \geq E'_1(R_{a1})/E(R)$ ), что

$$\kappa_e(n) \leq cn \log^2 n; \quad \kappa_d(n) \leq cn \log^3 n; \quad T_0(n) \leq cn \log^4 n. \quad (6.43)$$

**Утверждение 6.23.** Существует линейное кодовое множество  $A(R, \delta, E)$ , состоящее из каскадных кодов бесконечного порядка, с такими параметрами  $R, \delta$  и  $E$ , что  $R$  и  $\delta$  удовлетворяют (6. 21), а  $R$  и  $E$  удовлетворяют соотношению (см. гл. 4)

$$E(R) \geq E^{(u)}(R, \infty) = \max_{1 \geq x > R} \left\{ (x - R) \int_0^x \frac{dt}{E_0(t)} \right\}, \quad (6.44)$$

где  $E_0(t)$  — оценка Галлагера для экспоненты неправильного декодирования, и такие кодирование и каскадное декодирование с  $\gamma$ -реализацией экспоненты, что

$$\begin{aligned} \kappa_e(n) &\leq cn \log^5 n \log \log n; \quad \kappa_d(n) \leq cn^{(1+\log \log n)/2(1-H(\delta))}; \\ T_0(n) &\leq cn^{2 \log \log n / (1-H(\delta))}. \end{aligned} \quad (6.45)$$

Очевидно, что при  $\gamma$ -реализации экспоненты вероятности правильного декодирования решающее значение имеет алгоритм декодирования. Наилучшая из известных на сегодняшний день оценка для декодирования  $\gamma$ -реализацией экспоненты вероятности неправильного декодирования задается следующим утверждением, доказанным в приложении П.6.9.

**Утверждение 6.24.** Существует кодовое множество  $A(R, E)$ , содержащее каскадные коды с низкоплотностными кодами в качестве внешних, с параметрами  $R$  и  $E$ , удовлетворяющими соотношению

$$E = E(R) = \max_{R=R_{a1}R_{b1}} E_1(R_{a1}, \rho), \quad (6.46)$$

где  $R_{b1} = 1 - 22H(2\rho)$ ,  $E_1(R_{a1}, \rho) = \min_{\beta \geq \rho R_{a1}} \{\beta [E_0(R_{a1}) + F(\beta, \rho, R_{a1}, \epsilon)]\}$ ,

$$F(\beta, \rho, R_{a1}, \epsilon) =$$

$$= \begin{cases} 0 & \text{при } \epsilon > \frac{\rho R_{a1}}{2\beta}; \\ -H\left(\frac{\rho R_{a1}}{2\beta}\right) + \frac{\rho R_{a1}}{2\beta} \log_2 \epsilon + \left(1 - \frac{\rho R_{a1}}{2\beta}\right) \log_2 (1 - \epsilon) & \text{при } \epsilon \leq \frac{\rho R_{a1}}{2\beta}, \end{cases}$$

и такие его кодирование и декодирование с  $\gamma$ -реализацией экспоненты, что

$$\kappa_e(n) \leq cn^2/\log n; \quad \kappa_d(n) \leq cn \log n; \quad T_0(n) \leq c2^{\epsilon n \log n}. \quad (6.47)$$

Отметим, что для положительных  $R$  и  $E$  пока только для каскадных кодовых множеств удается получить верхние оценки вида  $cn \log^a n$  одновременно для всех рассматриваемых в данном параграфе характеристик сложности. Более того, не известны «некаскадные» кодовые множества с  $R > 0$  и  $E > 0$ , у которых по крайней мере одна из характеристик сложности не росла бы экспоненциально. К сожалению, во всех каскадных кодовых множествах просто реализуется лишь некоторая доля оценки Галлагера для экспоненты неправильного декодирования, с которой принято сравнивать в подобных случаях корректирующие свойства кодов.

## § 6.4. Заключение

Основным результатом настоящей главы является разработка сложных оценок применительно к корректирующим кодам, что позволяет с единой точки зрения рассмотреть многие системы корректирующих кодов и выделить из них те, реализация которых на сегодняшний день проще. Это дает возможность теоретически сравнивать классы кодов по важнейшим (с точки зрения практического использования) параметрам. Проведенные исследования показали, что

имеются три основные проблемы в теории кодирования: зада-

ние кода, кодирование и декодирование его, сложность решения которых определяет практическую и теоретическую ценность класса кодов;

задание кодов с наилучшими известными корректирующими свойствами (кодовым расстоянием, соответствующим границе ВГ, или экспонентой Галлагера) осуществляется посредством алгоритмов, оценки сложности которых растут экспоненциально с длиной кода;

- все линейные коды имеют степенной рост сложности кодирования (квадрат или менее) с длиной кода, однако задание таких кодов с кодированием имеет экспоненциальную сложность;

многие алгебраические коды (например, БЧХ, Гошпы) имеют степенную сложность задания, кодирования и декодирования, но асимптотически плохие корректирующие свойства;

на сегодняшний день только каскадными методами удастся получить степенной рост сложности решения одновременно всех трех задач теории кодирования и при этом асимптотически хорошие корректирующие свойства;

наименьший рост сложности решения одновременно всех трех задач при асимптотически хороших корректирующих свойствах имеет место у каскадных кодов первого порядка;

асимптотически наилучшие корректирующие свойства при неэкспоненциальном росте сложности решения одновременно всех трех задач имеют место у каскадных кодов бесконечного порядка.

Таким образом, исследование проблем сложности в теории корректирующих кодов показывает, что на сегодняшний день каскадные коды представляют собой уникальный среди корректирующих кодов класс кодов, в котором удастся при малом (степенном) росте сложности решить проблемы задания кодов, кодирования и декодирования их и достичь при этом асимптотически хороших корректирующих свойств.

## ПРИЛОЖЕНИЕ П.1

### П.1.1. Доказательство теоремы 1.5.

Рассмотрим обмен между вероятностями ошибки и стирания применительно к двоичным линейным блочным кодам. Пусть произвольный двоичный линейный блочный код используется в ДСК без памяти с вероятностью ошибки при передаче каждого символа  $\epsilon < 0,5$ . Передаваемое кодовое слово  $a_0$  обозначим через  $\bar{x}_0 = (x_{01}, x_{02}, \dots, x_{0n})$ , а все остальные кодовые слова  $a$  через  $\bar{x}_i = (x_{i1}, x_{i2}, \dots, x_{in})$ ,  $i = \overline{1, M-1}$ , где  $M$  — число всех кодовых слов. В силу линейности кода можно считать, что  $\bar{x}_0$  — нулевое кодовое слово, такое, что все  $x_{0j} = 0$ ,  $j = \overline{1, n}$ .

Принятое, т. е. искаженное ошибками, слово  $\hat{a}$  обозначим через  $\bar{y} = (y_1, y_2, \dots, y_n)$ , где  $y_j$  так же как и  $x_{ij}$ ,  $i = \overline{0, M}$ , являются элементами поля GF(2).

Результатом декодирования с гарантией, т. е. в соответствии с условием

$$P(\bar{y} | \bar{x}_0) \geq e^{\nu n} P(\bar{y} | \bar{x}_i), \quad (\text{П.1.1})$$

будет либо некоторое слово  $\bar{x}'_0$ , либо никакого слова. При этом при коэффициенте гарантии  $\nu > 0$  может быть осуществлено одно из следующих трех событий:

1. С о б ы т и е А. Выдача переданного слова  $\bar{x}'_0 = \bar{x}_0$  (правильное декодирование), когда условие (П.1.1) выполняется для слова  $\bar{x}_0$ .

2. С о б ы т и е Б. Выдача кодового слова  $\bar{x}'_0 \neq \bar{x}_0$  (ошибочное декодирование), когда условие (П.1.1) выполняется для некоторого кодового слова  $\bar{x}'_0$ , отличного от  $\bar{x}_0$ .

3. С о б ы т и е В. Стирание, когда условие (П.1.1) не выполняется ни для какого кодового слова.

Очевидно, что событие  $B \cup B$  (т. е. ошибка или стирание) имеет место, если хотя бы для одного  $i \neq 0$   $\ln P(\bar{y} | \bar{x}_0) - \ln P(\bar{y} | \bar{x}_i) \geq \nu n$ . Следовательно,

$$P(B \cup B) = P\left\{\bigcup_{i \neq 0} (\text{событие, когда } \xi_i - \xi_0 \leq \nu n)\right\}, \quad (\text{П.1.2})$$

где  $\xi_i = -\ln P(\bar{y} | \bar{x}_i)$ ,  $i = \overline{0, M-1}$ , причем  $P(B \cup B) = P(B) + P(B)$ .

Что касается события Б, то оно имеет место, когда для некоторого  $i_1 \neq 0$  и для всех  $i \neq i_1$  (включая и  $i = 0$ ) выполняется неравенство  $P(\bar{y} | \bar{x}_{i_1}) \geq e^{\nu n} P(\bar{y} | \bar{x}_i)$ , т. е.  $P(B) = \left\{\bigcup_{i_1 \neq 0} \bigcap_{i \neq i_1} (\text{событие, когда } \xi_{i_1} - \xi_i \leq -\nu n)\right\}$ . Но так как  $P\left\{\bigcap_{i \neq i_1} (\text{событие, когда } \xi_{i_1} - \xi_i \leq -\nu n)\right\} \leq P(\text{событие, когда } \xi_{i_1} - \xi_0 \leq -\nu n)$ , то после замены  $i_1$  на  $i$  получаем

$$P(B) \leq P\left\{\bigcup_{i \neq 0} (\text{событие, когда } \xi_i - \xi_0 \leq -\nu n)\right\}. \quad (\text{П.1.3})$$



Учитывая, что в канале без памяти

$$P(\bar{y} | \bar{x}_i) = \prod_{j=1}^n P(y_j | x'_{ij}), \quad i = \overline{0, M-1},$$

$$\text{имеем } \xi_i = \sum_{j=1}^n \xi_{ij},$$

где

$$\xi_{ij} = -\ln P(y_j | x_{ij}) = \begin{cases} -\ln(1 - \epsilon), & \text{если } y_j = x_{ij}; \\ -\ln \epsilon, & \text{если } y_j \neq x_{ij}, \end{cases}$$

причем  $\xi_{ij}$  являются независимыми случайными величинами.

Наиболее простой способ оценки вероятностей  $P(B \cup B)$  и  $P(B)$  состоит в замене в выражениях (П.1.2) и (П.1.3) вероятности объединения событий (соответствующих различным  $i \neq 0$ ) суммой вероятностей этих событий.

Однако, учитывая, что указанные события, вообще говоря, совместны, может оказаться, что при больших значениях  $\xi_0$  они будут осуществляться для слишком большого числа значений  $i$ , что может привести к чрезмерному завышению оценок. Поэтому для величины  $\xi_0$  введем некоторый порог  $\beta n$  ( $\beta > 0$ ) и рассмотрим отдельно случаи, когда  $\xi_0 \leq \beta n$  и  $\xi_0 > \beta n$ .

Для  $\xi_0 \leq \beta n$  будем считать приемлемой замену вероятности объединения суммой вероятностей. Для  $\xi_0 > \beta n$  такую замену будем считать недопустимой.

Соотношения (П.1.2) и (П.1.3) запишем в виде  $P(B \cup B) = P_1 + P_2$ ,  $P(B) = P_1^* + P_2^*$ , где  $P_1 = P$  (событие, когда  $\xi_0 \leq \beta n$  и  $\xi_i - \xi_0 \leq \nu n$ ),  $P_2 = P$  (событие, когда  $\xi_0 > \beta n$  и  $\xi_i - \xi_0 \leq \nu n$ ),  $P_1^* = P$  (событие, когда  $\xi_0 \leq \beta n$  и  $\xi_i - \xi_0 \leq -\nu n$ ),  $P_2^* = P$  (событие, когда  $\xi_0 > \beta n$  и  $\xi_i - \xi_0 \leq -\nu n$ ).

В соответствии со сказанным выше для  $P_1$  и  $P_1^*$  используем оценки  $P_1 \leq \sum_{i \neq 0} P\{\xi_0 \leq \beta n, \xi_i - \xi_0 \leq \nu n\}$ ,  $P_1^* \leq \sum_{i \neq 0} P\{\xi_0 \leq \beta^* n, \xi_i - \xi_0 \leq -\nu n\}$ .

Что касается вероятностей  $P$  и  $P_2^*$ , то для них воспользуемся тривиальными оценками:  $P_2 \leq P(\xi_0 > \beta n)$ ,  $P_2 \leq P(\xi_0 > \beta^* n)$ .

Таким образом, получаем  $P(B \cup B) \leq \sum_{i \neq 0} P(\xi_0 \leq \beta n, \xi_i - \xi_0 \leq \nu n) + P(\xi_0 > \beta n)$ ,  $P(B) \leq \sum_{i \neq 0} P(\xi_0 \leq \beta^* n, \xi_i - \xi_0 \leq -\nu n) + P(\xi_0 > \beta^* n)$ . Для оценки правых частей последних неравенств воспользуемся двумя леммами, доказательство которых приведено в работе [51].

**Лемма П.1.** Пусть  $Z = \sum_{j=1}^n z_j$  — сумма  $n$  независимых дискретных случайных величин с производящей функцией моментов каждой из них  $g_j(s) = \sum_{z_j} e^{sz_j} P(z_j)$ , где  $P(z_j)$  — распределения вероятностей случайной величины  $z_j$ . Тогда для любого  $z_0$  справедливо неравенство

$$P(Z > z_0 n) \leq e^{-nz_0 s} \prod_{j=1}^n g_j(s)$$

при всех  $s \geq 0$ , для которых  $g_j(s)$  существует. Если  $g_j(s) = g(s)$  не зависит от  $j$ , то эта оценка принимает вид  $P(Z > z_0 n) \leq e^{-nz_0 s} g^n(s)$ .

Лемма II.2. Пусть  $Z = \sum_{j=1}^n z_j$ , а  $U = \sum_{j=1}^w u_j$ , где  $w \leq n$ , а  $(z_j, u_j)$  —  $n$  независимых пар дискретных случайных величин с производящей функцией моментов каждой из пар  $g_j(r, t) = \sum_{(z_j, u_j)} e^{rz_j + tu_j} P(z_j, u_j)$ , где  $P(z_j, u_j)$  — распределение вероятности пары  $(z_j, u_j)$ . Тогда для любых значений  $z_0$  и  $u_0$  справедливо неравенство

$$P(Z \leq z_0 n, U \leq u_0 n) \leq e^{-n(z_0 r + u_0 t)} \prod_{j=1}^w g_j(r, t) \prod_{j=w+1}^n g_j(r, 0)$$

для всех  $r \leq 0$  и  $t \leq 0$ , таких, что  $g_j(r, t)$  существует. Если  $g_j(r, t) = g(r, t)$  не зависит от  $j$ , то это неравенство принимает вид  $P(Z \leq z_0 n, U \leq u_0 n) \leq e^{-n(z_0 r + u_0 t)} g^w(r, t) g^{n-w}(r, 0)$ . В нашем случае  $z_j = \xi_{0j}$ ,  $Z = \xi_0$ ,  $u_j = \xi_{1j} - \xi_{0j}$ ,  $U = \xi_1 - \xi_0$ . Кроме того, при оценке вероятности  $P(B \cup B)$   $z_0 = \beta$ ,  $u_0 = \nu$ , а при оценке вероятности  $P(B)$   $z_0 = \beta^*$ ,  $u_0 = -\nu$ . В соответствии с определением случайных величин  $\xi_{0j}$  и  $\xi_{1j}$  распределение вероятностей случайных величин  $z_j$  и пар случайных величин  $(z_j, u_j)$  не зависит от  $j$  и имеет вид, приведенный в табл. П.1.1 и П.1.2.

Таблица П.1.1

$z_j$	$-\ln(1 - \epsilon)$	$-\ln \epsilon$
$P(z_j)$	$1 - \epsilon$	$\epsilon$

Таблица П.1.2

$(z_j, u_j)$	$(-\ln(1 - \epsilon), \ln(1 - \epsilon) - \ln \epsilon)$	$(-\ln \epsilon, \ln \epsilon - \ln(1 - \epsilon))$
$P(z_j, u_j)$	$1 - \epsilon$	$\epsilon$

Причем  $w$  — число позиций, в которых кодовое слово  $\bar{x}_i$  отличается от переданного кодового слова  $\bar{x}_0$ , т. е. хеммингово расстояние между словами  $\bar{x}_i$  и  $\bar{x}_0$ .

Отсюда следует, что производящие функции моментов  $g(s)$  и  $g(r, t)$  имеют вид  $g(s) = e^{-s \ln(1 - \epsilon)} (1 - \epsilon) + e^{-s \ln \epsilon} \epsilon = (1 - \epsilon)^{1-s} + \epsilon^{1-s}$ ,  $g(r, t) = e^{-r \ln(1 - \epsilon) + t(\ln(1 - \epsilon) - \ln \epsilon)} (1 - \epsilon) + e^{-r \ln \epsilon + t(\ln \epsilon - \ln(1 - \epsilon))} \epsilon = (1 - \epsilon)^{1-r+t} \epsilon^{-t} + (1 - \epsilon)^{-t} \epsilon^{1-r+t}$ , следовательно,  $g(r, 0) = (1 - \epsilon)^{1-r} + \epsilon^{1-r} = g(r)$ .

Таким образом, для каждого кодового слова  $x_i$ , отличающегося от слова  $x_0$  в  $w$  позициях, согласно лемме II.2 имеем  $P(\xi_0 \leq \beta n, \xi_1 - \xi_0 \leq \nu n) \leq e^{-n(\beta r + \nu t)} g^w(r, t) g^{n-w}(r)$ ,  $P(\xi_0 \leq \beta^* n, \xi_1 - \xi_0 \leq -\nu n) \leq e^{-n(\beta^* r - \nu t)} g^w(r, t) \times g^{n-w}(r)$ . Но в силу линейности кода таких слов имеется ровно  $N(w)$

(причем  $N(w) = 0$  для  $1 \leq w < d$ ), тогда, используя еще и лемму П.1, приходим к следующей оценке для вероятностей:

$$P(B \cup B) \leq e^{-n\beta s} g^n(s) + e^{-n(\beta r + \nu t)} \sum_{w=d}^n N(w) g^w(r, t) g^{n-w}(r), \quad (\text{П.1.4})$$

$$P(B) \leq e^{-n\beta^* s} g^n(s) + e^{-n(\beta^* r - \nu t)} \sum_{w=d}^n N(w) g^w(r, t) g^{n-w}(r)$$

для любых  $s \geq 0$ ,  $r \leq 0$  и  $t \leq 0$ , при которых  $g(s)$ ,  $g(r)$  и  $g(r, t)$  существуют.

Учитывая, что при  $0 < w < d$  величина  $N(w) = 0$ , сумму, стоящую в правой части последних выражений, можно представить в виде

$$\sum_{w=d}^n N(w) g^w(r, t) g^{n-w}(r) = g^n(r) \sum_{w=1}^n N(w) (g(r, t)/g(r))^w =$$

$$= g^n(r) \psi_R(g(r, t)/g(r)),$$

где  $\psi_R(z)$  — производящая функция спектра весов ненулевых кодовых слов. Тогда соотношения (П.1.4) принимают вид

$$P(B \cup B) \leq e^{-n\beta s} g^n(s) + e^{-n(\beta r + \nu t)} g^n(r) \psi_R(g(r, t)/g(r)).$$

$$P(B) \leq e^{-n\beta^* s} g^n(s) + e^{-n(\beta^* r - \nu t)} g^n(r) \psi_R(g(r, t)/g(r)). \quad (\text{П.1.5})$$

Так как правая часть каждого из выражений (П.1.5) содержит сумму двух изменяющихся экспоненциально по  $n$  слагаемых, то при  $n \rightarrow \infty$  минимизация оценок для  $P(B \cup B)$  и  $P(B)$  достигается при равенстве этих экспонент. Исходя из последнего условия, получаем следующие оптимальные значения порогов:

$$\beta = \frac{1}{s-r} \left[ \ln g(s) - \ln g(r) - \frac{1}{n} \ln \psi_R(g(r, t)/g(r)) + \nu t \right],$$

$$\beta^* = \frac{1}{s-r} \left[ \ln g(s) - \ln g(r) - \frac{1}{n} \ln \psi_R(g(r, t)/g(r)) - \nu t \right].$$

Подставляя найденные значения порогов в (П.1.5), получаем следующие оценки:

$$P(B \cup B) \leq 2 \exp \left\{ -n \left[ F(R, s, r, t) + \frac{st}{s-r} \nu \right] \right\},$$

$$P(B) \leq 2 \exp \left\{ -n \left[ F(R, s, r, t) - \frac{st}{s-r} \nu \right] \right\}, \quad (\text{П.1.6})$$

где

$$F(R, s, r, t) = \frac{r}{s-r} \ln g(s) - \frac{s}{s-r} \ln g(r) -$$

$$- \frac{s}{s-r} \frac{1}{n} \ln \psi_R\left(\frac{g(r, t)}{g(r)}\right). \quad (\text{П.1.7})$$

Заметим, что в этом выражении зависимость  $F(R, s, r, t)$  от  $R$  определяется зависимостью производящей функции  $\psi_R(z)$  от скорости передачи  $R$ . Дальнейшая оптимизация оценок (П.1.6) сводится к максимизации их экспонент по параметрам  $s \geq 0$ ,  $r \leq 0$  и  $t \leq 0$ . При этом оптимизация каждого из выра-

жений (П.1.6) проводится независимо от другого, так что  $s$ ,  $r$  и  $t$ , оптимизирующие эти выражения, могут быть различными для каждого из них.

Таким образом, получаем

$$\begin{aligned} P(B \cup V) &\leq 2 \exp \{-n E_1(R, v)\}, \\ P(B) &\leq 2 \exp \{-n E_2(R, v)\}, \end{aligned} \quad (\text{П.1.8})$$

где  $E_1(R, v)$  и  $E_2(R, v)$  — результат оптимизации экспонент (П.1.6). Но точная оптимизация (П.1.6) по  $s \geq 0$ ,  $r \leq 0$  и  $t \leq 0$  во многих интересных случаях практически неосуществима. Поэтому ограничимся рассмотрением случая, когда параметры  $s$ ,  $r$  и  $t$  выбираются из условия максимизации функции  $F(R, s, r, t)$ , определяемой равенством (П.1.7), или, что то же самое, максимизацией (П.1.6) при  $v=0$ . Но в этом случае

$$E_1(R, 0) = E_2(R, 0) = E(R) \quad (\text{П.1.9})$$

представляет собой оценку экспоненты вероятности ошибки при декодировании по максимуму правдоподобия. Это значит, что вместо оптимальных значений  $s$ ,  $r$ ,  $t$  мы используем такие, которые обеспечивают наилучшую оценку экспоненты  $E(R)$ . Обозначим их соответственно через  $s_0$ ,  $r_0$ ,  $t_0$ . Такой способ выбора параметров назовем частичной оптимизацией. При этом из (П.1.6), (П.1.8) и (П.1.9) получаем

$$\begin{aligned} P(B \cup V) &\leq 2 \exp \left\{ -n \left[ E(R) + \frac{s_0 t_0}{s_0 - r_0} v \right] \right\}, \\ P(B) &\leq 2 \exp \left\{ -n \left[ E(R) - \frac{s_0 t_0}{s_0 - r_0} v \right] \right\}. \end{aligned} \quad (\text{П.1.10})$$

Из (П.1.10) с учетом того, что обычно при  $v > 0$   $P(B) \ll P(B \cup V)$ , и что  $P(B \cup V) = P(B) + P(V)$ , т. е.  $P(V) \approx P(B \cup V)$ , получаем доказательство теоремы 1.5.

## П.1.2. Доказательство утверждения 1.1

Как было показано в приложении П.1.1, экспонента вероятности ошибок при декодировании по максимуму правдоподобия  $E(R)$  оценивается как

$$E(R) \geq \max_{\substack{s \geq 0 \\ r \leq 0 \\ t \leq 0}} F(R, s, r, t), \quad (\text{П.1.11})$$

где  $F(R, s, r, t)$  определяется равенством (П.1.7). Заметим, что производящая функция весов  $\psi_R(R)$  есть возрастающая по  $s \geq 0$  функция. Поэтому, как следует из (П.1.7), максимизация  $F(R, s, r, t)$  по  $t$  соответствует минимизации по  $t$  функции  $g(r, t)$ , определенной в (1.10) теоремы 1.5. Эту функцию  $g(r, t)$  можно представить в виде  $g(r, t) = [\varepsilon^{(1-r+t)/2} (1-\varepsilon)^{-t/2} - (1-\varepsilon)^{(1-r+t)/2} \varepsilon^{-t/2}]^2 + 2[\varepsilon(1-\varepsilon)]^{(1-r)/2}$ . Отсюда следует, что  $g(r, t)$  достигает минимума при условии, что  $(1-r+t)/2 = -t/2$  или  $t = (r-1)/2$ , который равен

$$\min_{t \leq 0} g(r, t) = 2[\varepsilon(1-\varepsilon)]^{(1-r)/2}. \quad (\text{П.1.12})$$

Учитывая, что оценка (П.1.11) справедлива при любом  $r \leq 0$ , выбираем  $r = 2s - 1$  (некоторая аргументация такого выбора будет дана в приложении

П.1.3). Обозначая через  $F(R, s)$  функцию  $F(R, s, r, t)$  при максимизирующем ее значении  $t=(r-1)/2$  и выбранном  $r=2s-1$ , получаем

$$F(R, s) = \frac{2s-1}{1-s} \ln(\epsilon^{1-s} + (1-\epsilon)^{1-s}) - \frac{s}{1-s} \ln(\epsilon^{2(1-s)} + (1-\epsilon)^{2(1-s)}) - \frac{s}{1-s} \frac{1}{n} \psi_R \left( \frac{2(\epsilon(1-\epsilon))^{1-s}}{\epsilon^{2(1-s)} + (1-\epsilon)^{2(1-s)}} \right). \quad (\text{П.1.13})$$

При этом в силу ограничения  $s \geq 0$  и  $r \leq 0$  имеем

$$0 \leq s \leq 1/2. \quad (\text{П.1.14})$$

Функция  $F(R, s)$  является уравнением однопараметрического семейства кривых с параметром  $s$ . Нас интересует огибающая, расположенная выше всех кривых этого семейства. Иными словами, оптимизация по  $s$  сводится к построению огибающей для семейства (П.1.13). Проще всего уравнение огибающей записывается в параметрическом виде двух уравнений, одним из которых является (П.1.13), а другое имеет вид

$$\partial F(R, s) / \partial s = 0. \quad (\text{П.1.15})$$

Эту огибающую (при допустимых значениях  $s$ ) примем в качестве оценки для экспоненты  $E(R)$ .

Обозначим через  $C_1$  скорость передачи, соответствующую той точке огибающей, при которой  $s=0$ . Согласно (П.1.13) в этой точке

$$E(R) = E(C_1) = 0. \quad (\text{П.1.16})$$

В силу условия (П.1.14) огибающую можно принимать за  $E(R)$  лишь пока  $s \leq 1/2$ . Скорость передачи, соответствующую точке огибающей, в которой  $s=1/2$ , обозначим через  $R_*$ . При  $R < R_*$  положим  $s=1/2$  и согласно (П.1.13) получим

$$E(R) = F\left(R, \frac{1}{2}\right) = -\frac{1}{n} \ln \psi_R(2\sqrt{\epsilon(1-\epsilon)}), \quad (\text{П.1.17})$$

что завершает доказательство утверждения 1.1.

### П.1.3. Доказательство утверждения 1.2

Применим утверждение 1.1 для оценки экспоненты  $E(R)$  в случае кодов с хорошим спектром весов, определяемым теоремой 1.3, т. е.

$$N(w) = \begin{cases} 1 & \text{при } w=0; \\ 0 & \text{при } 0 < w < n\delta_{\text{ВГ}}; \\ nC_n^w 2^{-(1-R)n} & \text{при } \delta_{\text{ВГ}}n \leq w \leq n. \end{cases} \quad (\text{П.1.18})$$

Производящая функция в этом случае оценивается как

$$\psi_R(z) \leq n 2^{-(1-R)n} \sum_{w=\delta_{\text{ВГ}}n}^n C_n^w z^w. \quad (\text{П.1.19})$$

Очевидно, что во всех случаях  $z \geq 0$  оценка  $\psi_R(z)$  только усилится, когда суммирование начнем с  $w=0$ , т. е.

$$\psi_R(z) \leq n 2^{-(1-R)n} \sum_{w=0}^n C_n^w z^w = n 2^{-(1-R)n} (1+z)^n. \quad (\text{П.1.20})$$

Однако оценка (П.1.20) становится слишком грубой при таких значениях  $z$ , когда максимальный член  $C_n^w z^w$  будет при  $w \leq n\delta_{\text{ВГ}} = d$ . В этом случае, учитывая, что максимальным в (П.1.19) является член  $C_n^d z^d$ , воспользуемся следующей очевидной оценкой:

$$\psi_R(z) \leq n2^{-(1-R)n} C_n^d z^d (n-d) < n^2 2^{-(1-R)n} C_n^d z^d. \quad (\text{П.1.21})$$

Учитывая, что  $R = 1 - H(\delta_{\text{ВГ}})$ ,  $d = n\delta_{\text{ВГ}}$  и  $C_n^d \leq 2^{nH(\delta_{\text{ВГ}})}$ , оценку (П.1.21) после элементарных преобразований можно представить в виде

$$\psi_R(z) \leq n^2 z^{n\delta_{\text{ВГ}}}. \quad (\text{П.1.22})$$

Обозначим через  $R_0$  скорость передачи, при которой обе оценки (П.1.20) и (П.1.22) приводят к одному и тому же значению  $E(R_0)$ . Тогда для  $R < R_0$  можно применить оценку (П.1.22), которая приводит к более высокому значению  $E(R)$ , нежели оценка (П.1.20), а для  $R > R_0$  можно применить только оценку (П.1.20).

Легко проверить, что, используя утверждение 1.1 применительно к оценкам (П.1.20) и (П.1.22), мы непосредственно придем к теореме 1.4, т. е. получим, что  $E(R) = E_0(R)$ .

Однако в рассматриваемом случае можно доказать оптимальность условия  $r = 2s - 1$ , принятого при доказательстве утверждения 1.1. Для этого обратимся к выражению (П.1.7) для  $F(R, s, r, t)$ . Обозначая  $F(R, s, r, t)$  при оптимальном значении параметра  $t = -(1-r)/2$  через  $F(R, s, r)$ , после замены производящей функции  $\psi_R(z)$  оценками (П.1.20) и (П.1.22) получаем:

$$\begin{aligned} \text{при } R \geq R_0, \\ F(R, s, r) = \frac{s}{s-r} (1-R) \ln 2 + \frac{r}{s-r} \ln (\epsilon^{1-s} + (1-\epsilon)^{1-s}) - \\ - \frac{2s}{s-r} \ln \left( \epsilon^{\frac{1-r}{2}} + (1-\epsilon)^{\frac{1-r}{2}} \right) - \frac{s}{s-r} \frac{\ln n}{n}; \end{aligned} \quad (\text{П.1.23})$$

при  $R \leq R_0$

$$\begin{aligned} F(R, s, r) = \frac{r}{s-r} \ln (\epsilon^{1-s} + (1-\epsilon)^{1-s}) - \delta_{\text{ВГ}} \ln \left( 2 (\epsilon (1-\epsilon))^{\frac{1-r}{s}} \right) - \\ - \frac{s}{s-r} (1-\delta_{\text{ВГ}}) \ln (\epsilon^{1-r} + (1-\epsilon)^{1-r}) - \frac{2s}{s-r} \frac{\ln n}{n}. \end{aligned} \quad (\text{П.1.24})$$

Величина  $R_0$  определяется из условия равенства правых частей выражений (П.1.23) и (П.1.24), которое после соответствующих преобразований и при  $n \rightarrow \infty$  принимает вид

$$\begin{aligned} H(\delta_{\text{ВГ}}) \ln 2 + \delta_{\text{ВГ}} \ln (2 (\epsilon (1-\epsilon))^{(1-r)/2}) + (1-\delta_{\text{ВГ}}) \ln (\epsilon^{1-r} + (1-\epsilon)^{1-r}) - \\ - 2 \ln (\epsilon^{(1-r)/2} + (1-\epsilon)^{(1-r)/2}) = 0. \end{aligned} \quad (\text{П.1.25})$$

Введем вспомогательный параметр  $x = s/(s-r)$ , тогда для  $R > R_0$  в соответствии с (1.23) получаем

$$\begin{aligned} F(R, s, r) = F_1(R, s, x) = x(1-R) \ln 2 - (1-x) \ln (\epsilon^{1-s} + (1-\epsilon)^{1-s}) - \\ - 2x \ln \left( \epsilon^{\frac{1}{2}(1-s+s/x)} + (1-\epsilon)^{\frac{1}{2}(1-s+s/x)} \right). \end{aligned}$$

Вычисляя производную по  $s$ , находим

$$\frac{\partial F_1(R, s, x)}{\partial s} = -(1-x)(\varepsilon/1-\varepsilon)^{1-s} \times \\ \times \frac{1 - (\varepsilon/1-\varepsilon)^{-\frac{1}{2}(1-s-s/x)}}{(1 + (\varepsilon/1-\varepsilon)^{1-s}) \left(1 + (\varepsilon/(1-\varepsilon))^{\frac{1}{2}(1-s+s/x)}\right)} \ln \frac{1-\varepsilon}{\varepsilon}.$$

Отсюда следует, что  $\partial F_1(R, s, x)/\partial s = 0$  при  $s = x/(1+x)$ , причем для  $s < x/(1+x)$   $\partial F_1(R, s, x)/\partial s > 0$ , а для  $s > x/(1+x)$   $\partial F_1(R, s, x)/\partial s < 0$ , так что при  $s = x/(1+x)$  величина  $F_1(R, s, x)$  достигает максимума по параметру  $s$ .

Подставляя вместо  $x$  его значение, получаем  $s = (1+r)/2$  или  $r = 2s-1$ . Так как  $r \leq 0$ , а  $s \geq 0$ , то приходим к следующему диапазону изменения параметров  $s$  и  $r$ :  $0 \leq s \leq 1/2$ ;  $-1 \leq r \leq 0$ .

Таким образом, при  $R \geq R_0$  получаем два участка: первый, когда  $C_1 \geq R \geq R_*$ , на котором  $r = 2s-1$  и  $0 \leq s \leq 1/2$ , и второй, когда  $R_* > R \geq R_0$ , на котором  $r=0$  и  $s=1/2$ . На первом участке, заменяя  $r$  его значением, получаем

$$E(R) = F(R, s, 2s-1) = \frac{s}{1-s} (1-R) \ln 2 - \\ - \frac{1}{1-s} \ln (\varepsilon^{1-s} + (1-\varepsilon)^{1-s}). \quad (\text{П. 1. 26})$$

Последующая оптимизация по  $s$  приводит к построению огибающей однопараметрического семейства кривых (П.1.26), зависящего от параметра  $s$ . В результате соответствующих преобразований получаем параметрические уравнения, связывающие  $E(R)$  и  $R$ , одним из которых является уравнение (П. 1. 26), а второе имеет вид  $R = 1 - H(\varepsilon^{1-s}/(\varepsilon^{1-s} + (1-\varepsilon)^{1-s}))$ .

При  $s=0$   $E(R)=0$ , а  $R=C_1=1-H(\varepsilon)$ , так что для кодов с хорошим спектром весов  $C_1$  совпадает с пропускной способностью канала  $C$ . На втором участке, подставляя в  $F(R, s, r)$  значения  $r=0$  и  $s=1/2$ , получаем  $E(R) = (1-R) \ln 2 - \ln(1 + 2\sqrt{\varepsilon(1-\varepsilon)})$ . Точка  $R=R_*$ , разделяющая первый и второй участки, определяется равенством  $R_* = 1 - H(\sqrt{\varepsilon}/(\sqrt{\varepsilon} + \sqrt{1-\varepsilon}))$ . Точка  $R_0$ , ограничивающая слева второй участок (на котором  $r=0$ , а  $s=1/2$ ), определяется соотношением (П. 1. 25), которое после замены  $r=0$ ,  $s=1/2$  принимает вид  $H(\delta_{\text{ВГ}}) \ln 2 - \ln(1 + 2\sqrt{\varepsilon(1-\varepsilon)}) = -\delta_{\text{ВГ}} \ln(2\sqrt{\varepsilon(1-\varepsilon)})$  или  $-\delta_{\text{ВГ}} \ln \delta_{\text{ВГ}} - (1-\delta_{\text{ВГ}}) \ln(1-\delta_{\text{ВГ}}) - \ln(1 + 2\sqrt{\varepsilon(1-\varepsilon)}) + \delta_{\text{ВГ}} \ln(2\sqrt{\varepsilon(1-\varepsilon)}) = 0$ . Переписывая это равенство в виде

$$\delta_{\text{ВГ}} \left( \ln \left( 2\sqrt{\varepsilon(1-\varepsilon)} - \ln \frac{\delta_{\text{ВГ}}}{1-\delta_{\text{ВГ}}} \right) - (\ln(1 + 2\sqrt{\varepsilon(1-\varepsilon)}) - \right. \\ \left. - \ln \left( 1 + \frac{\delta_{\text{ВГ}}}{1-\delta_{\text{ВГ}}} \right) \right) = 0,$$

получаем очевидное решение  $\delta_{\text{ВГ}}/(1-\delta_{\text{ВГ}}) = 2\sqrt{\varepsilon(1-\varepsilon)}$ , откуда следует, что  $R_0 = 1 - H(2\sqrt{\varepsilon(1-\varepsilon)}/(1 + 2\sqrt{\varepsilon(1-\varepsilon)}))$ .

Учитывая, что при  $R < R_0$  функция  $F(R, s, r)$  определяется равенством (П.1.24) и что в точке  $R=R_0$  имеют место равенства  $r=0, s=1/2$ , примем значения параметров  $r$  и  $s$  одни и те же для всех  $R < R_0$ . Тогда для  $R \leq R_0$  получаем  $E(R) = -\delta_{\text{ВГ}} \ln(2\sqrt{\epsilon(1-\epsilon)})$ , где  $\delta_{\text{ВГ}}$  — оценка Варшавова—Гилберта в точке  $R$ , что завершает доказательство утверждения 1.2.

## ПРИЛОЖЕНИЕ П.2

### П.2.1. Доказательство утверждения 2.1

Слово  $\beta$  будем строить поэтапно:

на первом шаге определяем элементы  $\beta_{ij}$  для  $j = \overline{1, b_1}, i = \overline{1, m}$ , с последующим кодированием слова  $\mu_1 + \beta_1$  кодом  $B_1$ , в результате чего получаем слово  $\gamma_1$ ;

на втором шаге определяем элементы  $\beta_{ij}$  для  $j = \overline{b_1 + 1, b_2}, i = \overline{2, m}$ , с последующим кодированием слова  $\mu_2 + \beta_2$  кодом  $B_2$ , в результате чего получаем слово  $\gamma_2$ ;

на  $s$ -м шаге определяем  $\beta_{ij}$  для  $j = \overline{b_{s-1} + 1, b_s}, i = \overline{s, m}$ , с последующим кодированием слова  $\mu_s + \beta_s$  кодом  $B_s$ , в результате чего получаем слово  $\gamma_s$ ;

на последнем,  $m$ -м шаге определяем  $\beta_{mj}$  для  $j = \overline{b_{m-1} + 1, b_m}$  с последующим кодированием слова  $\mu_m + \beta_m$  кодом  $B_m$ , в результате чего получаем слово  $\gamma_m$ .

Таким образом, после выполнения всех  $m$  шагов получаем не только слово  $\beta$ , но и соответствующее слову  $\mu + \beta$  вспомогательное слово  $\gamma$ .

На первом шаге ( $j = \overline{1, b_1}$ ) условия (2.14), налагаемые на слово  $\beta$ , записываются в виде

$$G_{11} \begin{pmatrix} \mu_{mj} + \beta_{mj} \\ \vdots \\ \mu_{1j} + \beta_{1j} \end{pmatrix} = \begin{pmatrix} \mu_{mj} \\ \vdots \\ \mu_{1j} \end{pmatrix}. \quad (\text{П. 2. 1})$$

Равенство (П. 2. 1) представляет собой систему уравнений относительно неизвестных  $\beta_{ij}$ , в которой элементы  $\mu_{ij}$  являются известными.

Если матрица  $G_{11}$  невырождена, то эта система имеет решение, и притом единственное:

$$\begin{pmatrix} \mu_{mj} + \beta_{mj} \\ \vdots \\ \mu_{1j} + \beta_{1j} \end{pmatrix} = G_{11}^{-1} \begin{pmatrix} \mu_{mj} \\ \vdots \\ \mu_{1j} \end{pmatrix}, \quad j = \overline{1, b_1}.$$

Используя код  $B_1$ , кодируем слово  $\mu_1 + \beta_1$  и получаем слово  $\gamma_1$ , причем  $\gamma_{1j} = \mu_{1j} + \beta_{1j}$  для  $j = \overline{1, b_1}$ . На втором шаге ( $j = \overline{b_1 + 1, b_2}$ ) условия (2.14) записываются в виде

$$G_{22} \begin{pmatrix} \mu_{mj} + \beta_{mj} \\ \vdots \\ \mu_{2j} + \beta_{2j} \end{pmatrix} + \begin{pmatrix} Q_{m1} \\ \vdots \\ Q_{21} \end{pmatrix} \|\gamma_{1j}\| = \begin{pmatrix} \mu_{mj} \\ \vdots \\ \mu_{2j} \end{pmatrix}. \quad (\text{П. 2. 2})$$



Равенство (П. 2. 2) представляет собой систему уравнений относительно неизвестных  $\beta_{ij}$ , в которой  $\mu_{ij}$  и  $\gamma_{1j}$  являются известными ( $\gamma_{1j}$  было вычислено на первом шаге).

Если матрица  $G_{22}$  невырождена, то эта система имеет решение, и притом единственное:

$$\begin{pmatrix} \mu_{mj} + \beta_{mj} \\ \vdots \\ \mu_{2j} + \beta_{2j} \end{pmatrix} = G_{22}^{-1} \begin{pmatrix} \mu_{mj} \\ \vdots \\ \mu_{2j} \end{pmatrix} + G_{22}^{-1} \begin{pmatrix} Q_{m1} \\ \vdots \\ Q_{21} \end{pmatrix} \|\gamma_{1j}\|, \quad j = \overline{b_1 + 1, b_2}.$$

Используя код  $B_2$ , кодируем слово  $\mu_2 + \beta_2$  и получаем слово  $\gamma_2$ , причем  $\gamma_{2j} = \mu_{2j} + \beta_{2j}$  для  $j = \overline{1, b_2}$ . На  $s$ -м шаге ( $j = b_{s-1} + 1, b_s$ ) условия (2. 14) записываются в виде

$$G_{ss} \begin{pmatrix} \mu_{mj} + \beta_{mj} \\ \vdots \\ \mu_{sj} + \beta_{sj} \end{pmatrix} + \begin{pmatrix} Q_{m, s-1} \dots Q_{m, 1} \\ \vdots \\ Q_{s, s-1} \dots Q_{s, 1} \end{pmatrix} \cdot \begin{pmatrix} \gamma_{s-1, j} \\ \vdots \\ \gamma_{1j} \end{pmatrix} = \begin{pmatrix} \mu_{mj} \\ \vdots \\ \mu_{sj} \end{pmatrix}. \quad (\text{П. 2. 3})$$

Равенство (П. 2. 3) представляет собой систему уравнений относительно  $\beta_{ij}$ , в которой  $\mu_{ij}$  и  $\gamma_{ij}$  являются известными (элементы  $\gamma_{ij}$  вычислены на предыдущих  $s - 1$  шагах).

Если матрица  $G_{ss}$  невырождена, то эта система имеет решение, и притом единственное:

$$\begin{pmatrix} \mu_{mj} + \beta_{mj} \\ \vdots \\ \mu_{sj} + \beta_{sj} \end{pmatrix} = G_{ss}^{-1} \begin{pmatrix} \mu_{mj} \\ \vdots \\ \mu_{sj} \end{pmatrix} + G_{ss}^{-1} \begin{pmatrix} Q_{m, s-1} \dots Q_{m1} \\ \vdots \\ Q_{s, s-1} \dots Q_{s1} \end{pmatrix} \cdot \begin{pmatrix} \gamma_{s-1, j} \\ \vdots \\ \gamma_{1, j} \end{pmatrix},$$

$$j = \overline{b_{s-1} + 1, b_s}. \quad (\text{П. 2. 4})$$

Используя код  $B_s$ , кодируем слово  $\mu_s + \beta_s$  и получаем слово  $\gamma_s$ , причем  $\gamma_{sj} = \mu_{sj} + \beta_{sj}$  для  $j = \overline{1, b_s}$ . Наконец, на последнем,  $m$ -м шаге ( $j = \overline{b_{m-1} + 1, b_m}$ ) условия (2. 14) записываются в виде

$$Q_{mm} (\mu_{mj} + \beta_{mj}) - \begin{pmatrix} Q_{m, m-1} \dots Q_{m1} \\ \vdots \\ \gamma_{1j} \end{pmatrix} = \mu_{mj}. \quad (\text{П. 2. 5})$$

Равенство (П. 2. 5) представляет собой уравнение относительно  $\beta_{mj}$ , в котором  $\mu_{mj}$  и  $\gamma_{ij}$  являются известными (элементы  $\gamma_{ij}$  вычислены на предыдущих  $(m - 1)$ -х шагах).

Если матрица  $Q_{mm} = G_{mm}$  невырождена, то это уравнение имеет решение, и притом единственное:

$$\mu_{mj} + \beta_{mj} = Q_{mm}^{-1} \mu_{mj} + Q_{mm}^{-1} \begin{pmatrix} Q_{m, m-1} \dots Q_{m1} \\ \vdots \\ \gamma_{1, j} \end{pmatrix}, \quad j = \overline{b_{m-1} + 1, b_m}.$$

Используя код  $B_m$ , кодируем слово  $\mu_m + \beta_m$  и получаем слово  $\gamma_m$ , причем  $\gamma_{mj} = \mu_{mj} + \beta_{mj}$  для  $j = \overline{1, b_m}$ .

Предположим теперь, что среди матриц  $G_{ij}$ ,  $i = \overline{1, m}$ , хотя бы одна, например  $G_{ss}$ , является вырожденной. Так как элементы  $\mu_{ij}$  информационного слова  $\mu$  принимают все возможные значения из поля  $\text{GF}(2^{a_i})$ , то наряду со словами  $\mu$ , для которых система (П. 2. 3) будет иметь более одного решения, найдутся и такие, для которых эта система окажется несовместной. Но для таких нельзя построить слова  $\alpha$ , такого, чтобы  $\alpha_{ij} = \mu_{ij}$ ,  $j = \overline{1, b_i}$ ,  $i = \overline{1, m}$ . Следовательно, если матрица  $G_{ss}$  вырождена, то построение систематического каскадного кода оказывается невозможным.

При изложении схемы определения элементов  $\beta_{ij}$  слова  $\beta$  предполагалось, что  $b_1 < b_2 < \dots < b_m$ . Однако легко видеть, что эта схема остается справедливой и при любом соотношении между величинами  $b_i$ , меняется только порядок кодирования кодами  $B_i$ . Именно если  $b_{i_1} < b_{i_2} < \dots < b_{i_m}$ , то сначала рассматриваем  $j = \overline{1, b_{i_1}}$ , затем  $j = \overline{b_{i_1} + 1, b_{i_2}}$  и т. д. до  $j = \overline{b_{i_{m-1}} + 1, b_{i_m}}$ , последовательно определяя соответствующие элементы  $\beta_{ij}$ , и при помощи кодов  $B_{i_1} B_{i_2} \dots B_{i_m}$  находим слова  $\gamma_{i_1} \gamma_{i_2} \dots \gamma_{i_m}$ .

## П. 2. 2. Систематическое кодирование для треугольной кодирующей матрицы

Если  $G_0$  — невырожденная нижняя треугольная матрица, то соотношения (П. 2. 3) существенно упрощаются.

Действительно, так как в этом случае  $Q_{is} = 0$ , если  $s < i$ , то (П. 2. 3) принимает вид, вообще не содержащий элементов  $\gamma_{ij}$ :

$$G_{ss} \begin{pmatrix} \mu_{mj} + \beta_{mj} \\ \vdots \\ \mu_{sj} + \beta_{sj} \end{pmatrix} = \begin{pmatrix} \mu_{mj} \\ \vdots \\ \mu_{sj} \end{pmatrix}, \quad j = \overline{b_s + 1, b_s}, \quad s = \overline{1, m}. \quad (\text{П. 2. 6})$$

Это значит, что слово  $\beta$  и вспомогательное информационное слово  $\mu + \beta$  можно определять без использования внешних кодов  $B_i$  или что эти слова не зависят от характера внешних кодов, а целиком определяются кодирующей матрицей  $G_0$ .

Используя клеточную форму записи матрицы  $G_0$  (2. 17), заменим выражение (П. 2. 3) следующими уравнениями:

$$T_{mm}(\mu_{mj} + \beta_{mj}) = \mu_{mj},$$

$$Q_{m-1, m}(\mu_{mj} + \beta_{mj}) + T_{m-1, m-1}(\mu_{m-1, j} + \beta_{m-1, j}) = \mu_{m-1, j},$$

$$\vdots \quad \quad \quad \vdots \quad \quad \quad \vdots \quad \quad \quad \vdots \quad \quad \quad \vdots$$

$$Q_{s, m}(\mu_{mj} + \beta_{mj}) + \dots + Q_{s, s+1}(\mu_{s+1, j} + \beta_{s+1, j}) + T_{ss}(\mu_{sj} + \beta_{sj}) = \mu_{sj},$$

где  $j = \overline{b_{s-1} + 1, b_s}$ .

Из этих уравнений непосредственно получаем

$$\mu_{mj} + \beta_{mj} = T_{mm}^{-1} \mu_{mj},$$

$$\mu_{m-1, j} + \beta_{m-1, j} = T_{m-1, m-1}^{-1} \mu_{m-1, j} + T_{m-1, m-1}^{-1} Q_{m-1, m}(\mu_{mj} + \beta_{mj}),$$

$$\vdots \quad \quad \quad \vdots \quad \quad \quad \vdots \quad \quad \quad \vdots \quad \quad \quad \vdots$$

$$\mu_{sj} + \beta_{sj} = T_{ss}^{-1} \mu_{sj} + \dots + T_{ss}^{-1} Q_{sm}(\mu_{mj} + \beta_{mj}).$$

(П. 2. 7)

Так как переход от шага  $s$  к шагу  $s + 1$  соответствует лишь отбрасыванию последнего из уравнения (П. 2. 7) при сохранении всех предшествующих

ему уравнений и изменению интервала  $j = \overline{b_{s-1} + 1, b_s}$  на интервал  $j = \overline{b_s + 1, b_{s+1}}$ , то это значит, что каждое из уравнений (П. 2. 7) определяет соответствующий ему элемент  $\mu_{sj} + \beta_{sj}$  для всех  $j = \overline{1, b_s}$  при условии, что сначала определяется  $\mu_{mj} + \beta_{mj}$  для  $j = \overline{1, b_m}$ , затем  $\mu_{m-1, j} + \beta_{m-1, j}$  для  $j = \overline{1, b_{m-1}}$  и т. д. до  $\mu_{1j} + \beta_{1j}$  для  $j = \overline{1, b_1}$ .

Если же все  $T_{ii} = E_{a_i}$  — единичные матрицы порядка  $a_i$ , то выражения (П. 2. 7) еще более упрощаются и принимают вид

$$\begin{aligned} \beta_{mj} &= 0, \\ \beta_{m-1, j} &= Q_{m-1, m} \mu_{mj}, \\ &\vdots \\ &\vdots \end{aligned} \quad (П. 2. 8)$$

$$\beta_{sj} = Q_{s, s+1} (\mu_{s+1, j} + \beta_{s+1, j}) + \dots + Q_{s, m-1} (\mu_{m-1, j} + \beta_{m-1, j}) + Q_{sm} \mu_{mj},$$

$$\vdots$$

$$\beta_{1j} = Q_{12} (\mu_{2j} + \beta_{2j}) + \dots + Q_{1, m-1} (\mu_{m-1, j} + \beta_{m-1, j}) + Q_{1m} \mu_{mj},$$

где при определении элементов  $\beta_{sj}$  величина  $j$  меняется от 1 до  $b_s$ .

### П. 2.3. Построение матрицы $H_0$ для системы вложенных кодов БЧХ

Если  $i$ -й внутренний код  $A_i$  является кодом БЧХ, проверочный многочлен которого  $h_i(x)$ , то проверочная матрица этого кода имеет вид

$$H_{*i} = \begin{pmatrix} x & h_i(x) \\ x^2 & h_i(x) \\ \vdots & \vdots \\ \sum_{s=0}^{i-1} a_s^{-1} & h_i(x) \end{pmatrix}.$$

Таким образом, задача построения матрицы  $H_0$  сводится к тому, как, зная многочлены  $h_1(x)$ ,  $h_2(x)$ , ...,  $h_m(x)$ , построить матрицу, из которой в результате отбрасывания первых  $a_m + a_{m-1} + \dots + a_1$  строк получаем матрицу  $H_i$ , эквивалентную матрице  $H_{*i}$ ,  $i = \overline{1, m}$ , т. е. такую, из которой матрица  $H_{*i}$  может быть получена при помощи элементарных преобразований строк.

Для решения этой задачи рассмотрим вспомогательную матрицу

$$H_{*0} = \begin{pmatrix} & \frac{1}{x} \\ & \vdots \\ & x^{a_m-1} \\ x & h_m^*(x) \\ & h_m^*(x) \\ & \vdots \\ & \sum_{s=0}^{m-1} a_s^{-1} \\ & h_m^*(x) \end{pmatrix},$$

где  $h_m^*(x) = h_m(x)$ .

Если отбросить первые  $a_m$  строк матрицы  $H_{*0}$ , то получим матрицу  $H_{*t}$ , которая определяет код  $A_m$ .

Покажем, что матрицу  $H_{*0}$  при помощи элементарных преобразований строк можно привести к такой матрице  $H_0$ , что, отбрасывая у нее первые  $a_m + a_{m-1} + \dots + a_t$  строк, получим матрицу, эквивалентную матрице  $H_{*t}$ , т. е. матрицу, определяющую код, эквивалентный по кодовому расстоянию (т. е. с тем же кодовым расстоянием  $d_{at}$ ) коду  $A_t$ , отвечающему матрице  $H_{*t}$ .

Действительно, рассмотрим многочлен  $h_{m-1}^*(x)$  степени  $a_{m-1}$   $h_{m-1}^*(x) = \beta_{m-1,0} + \beta_{m-1,1}x + \dots + \beta_{m-1,a_{m-1}-1}x^{a_{m-1}-1} + x^{a_{m-1}}$ , где  $\beta_{m-1,i} \in \text{GF}(2)$ . Тогда, умножая  $(a_m + v)$ -ю строку матрицы  $H_{*0}$  на коэффициент  $\beta_{m-1,v}$ ,  $v = \overline{1, a_{m-1} - 1}$ , и прибавляя полученные таким образом строки к каждой строке матрицы  $H_{*0}$  начиная со строки  $a_m + a_{m-1} + 1$ , получим матрицу (П. 2. 9)

$$\left( \begin{array}{c} 1 \\ x \\ \vdots \\ x^{a_{m-1}-1} \\ h_m^*(x) \\ h_m^*(x) \\ \vdots \\ x^{a_{m-1}-1} h_m^*(x) \\ h_m^*(x) h_{m-1}^*(x) \\ \vdots \\ \sum_{s=0}^{m-2} a_s-1 \\ x^{s=0} h_m^*(x) h_{m-1}^*(x) \end{array} \right) \quad \cdot \quad (\text{П. 2. 9})$$

$$\left( \begin{array}{c} 1 \\ x \\ \vdots \\ x^{a_{m-1}-1} \\ h_m(x) \\ h_m(x) \\ \vdots \\ x^{a_{m-1}-1} h_m(x) \\ h_{m-1}(x) \\ x h_{m-1}(x) \\ \vdots \\ x^{a_{m-1}-1} h_{m-1}(x) \\ h_{m-2}(x) \\ x h_{m-2}(x) \\ \vdots \\ x^{a_0-1} h_1(x) \end{array} \right) \quad \cdot \quad (\text{П. 2. 10})$$

Далее рассмотрим многочлен  $h_{m-2}^*(x)$  степени  $a_{m-2}$   $h_{m-2}^*(x) = \beta_{m-2,0} + \beta_{m-2,1}x + \dots + \beta_{m-2,a_{m-2}-1}x^{a_{m-2}-1} + x^{a_{m-2}}$  и применим описанные операции к матрице (П. 2. 9) начиная с  $(a_m + a_{m-1} + a_{m-2} + 1)$ -й строки. С полученной таким образом матрицей повторим те же операции применительно к многочлену  $h_{m-3}^*(x)$  и т. д. В результате приведем матрицу  $H_{*0}$  к виду (П. 2. 10), где  $h_i(x)$  определяется выражением (2. 27).

Так же как на  $i$ -м этапе построения матрицы  $H_0$  первые ее  $a_m + a_{m-1} + \dots + a_{m-i+1}$  строк остаются неизменными и не используются в преобразованиях остальных строк, следует, что, отбрасывая в матрице  $H_0$   $a_m + a_{m-1} + \dots + a_{m-i+1}$  первых строк, получим матрицу  $H_t$ , эквивалентную матрице  $H_{*t}$ .

Таким образом, матрица (П. 2. 10) является искомой проверочной матрицей  $H_0$ , определяющей систему вложенных кодов БЧХ.

## П.2.4. Доказательство теорем 2.3 и 2.4

В соответствии со способом кодирования внутренним кодером и выбранной нумерацией внутренних кодов кодовые слова кода  $A$ , получаются в результате умножения столбцов вспомогательного слова на матрицу  $G_0$ , т. е.  $\alpha^{(j)} = G_0 \gamma^{(j)}$ , где  $\alpha^{(j)}$  — кодовое слово кода  $A$ , (вектор-столбец), а  $\gamma^{(j)}$  — вектор-столбец, у которого  $n_1 - v$  нижних символов нулевые, а остальные произвольные. Следовательно,  $\alpha^{(j)}$  является линейной комбинацией над полем  $GF(2)$  тех столбцов матрицы  $G_0$ , номера которых не превосходят  $n_a - v$ . Другими словами, код  $A$ , является линейным пространством, порождаемым первыми  $n_a - v$  столбцами матрицы  $G_0$ .

Учитывая сказанное, матрицу  $G_0$  будем строить столбец за столбцом, т. е., переходя от кода  $A$ , к коду  $A_{v-1}$ . В качестве первого столбца выберем любой столбец веса  $n_a/2$ . Пусть уже выбраны первые  $n_a - v$  столбцов матрицы  $G_0$ , т. е. уже построен код  $A_v$ , удовлетворяющий условию теоремы. Тогда в качестве следующего,  $(n_a - v + 1)$ -го столбца выберем любое слово того смежного класса кода  $A_v$ , минимальный представитель которого имеет наибольший вес  $w_m$ . Тогда кодовое расстояние  $d_{a, v-1}$  кода  $A_{v-1}$  (представляющего собой объединение кода  $A_v$  с выбранным смежным классом) будет равно  $d_{a, v-1} = \min \{d_{a_v}, w_m\}$ . Если  $w_m \geq d_{a_v}$ , то  $d_{a, v-1} = d_{a_v}$ , и код  $A_{v-1}$  удовлетворяет условию теоремы, так как  $R_{a_{v-1}} > R_{a_v}$ . Если же  $w_m < d_{a_v}$ , то  $d_{a, v-1} = w_m$ .

Но число смежных классов  $2^{r_{a,v}}$  кода  $A_v$ , где  $r_{a,v}$  — число проверочных символов кода  $A_v$ , удовлетворяет неравенству

$$2^{r_{a,v}} \leq \sum_{w=1}^{w_m} C_{n_a}^w = \sum_{w=1}^{d_{a,v-1}} C_{n_a}^w \leq 2^{n_a H(d_{a, v-1})},$$

которое следует из того, что любое слово веса  $w \leq w_m$  принадлежит одному из смежных классов и любой смежный класс содержит слово, вес которого не превосходит  $w_m$ .

Так как  $r_{a,v} = r_{a, v-1} + 1 = n_a(1 - R_{a, v-1}) + 1 = n_a H(\delta_{BG}(R_{a, v-1})) + 1$ , то из последнего неравенства следует, что  $n_a H(\delta_{BG}(R_{a, v-1})) + 1 \leq n_a H(\delta_{a, v-1})$  или  $\delta_{a, v-1} > \delta_{BG}(R_{a, v-1})$ , т. е. что код  $A_{v-1}$ , так же как и код  $A_v$ , удовлетворяет условию теоремы. Так как единственное ненулевое кодовое слово кода  $A_{n_a-1}$  совпадает с первым столбцом матрицы  $G_0$ , вес которого по условию равен  $n_a/2$ , то и этот код также удовлетворяет условию теоремы (так как его кодовое расстояние достигает границы ВГ). Последнее утверждение завершает доказательство теоремы 2.3. Перед доказательством теоремы 2.4 докажем следующую лемму.

**Лемма 2.1.** Среди смежных классов любого двоичного линейного кода длины  $n$  с  $r$  проверочными символами найдется по меньшей мере  $S \geq (2^r - 2n)/n$  смежных классов, спектр весов которых удовлетворяет неравенству

$$N(w) \leq n C_n^{2^r - w}, \quad w = \overline{1, n}, \quad (\text{П. 2.11})$$

где  $N(w)$  — число слов веса  $w$  в смежном классе.

**Доказательство.** Пусть  $\lambda(w)$  — доля смежных классов, для которых число слов веса  $w$  —  $N(w)$  не удовлетворяет условию (П.2.11).

Так как число смежных классов равно  $2^r - 1$ , а общее число слов веса  $w$  равно  $C_n^w$  и любое слово входит не более чем в один смежный класс, то для любого  $w$  справедливо очевидное неравенство

$$\lambda(w) (2^r - 1) n \frac{C_n^w}{2^r} \leq C_n^w,$$

откуда  $\lambda(w) \leq 2^r / (2^r - 1)$  при  $w = \overline{1, n-1}$ , причем  $\lambda(0) = 0$  и  $\lambda(n) \leq 1 / (2^r - 1)$ .

Таким образом, число смежных классов, для которых хотя бы для одного  $w$  не выполняется условие (П.2.11), не более чем

$$(2^r - 1) \sum_{w=1}^n \lambda(w) \leq (2^r - 1) \left\{ \frac{n-1}{n} \frac{2^r}{2^r - 1} + \frac{1}{2^r - 1} \right\} = \frac{n-1}{n} 2^r + 1,$$

следовательно, при всех  $w = \overline{1, n}$

$$S \geq 2^r - 1 - \left\{ 2^r \frac{n-1}{n} + 1 \right\} = \frac{2^r - 2n}{n},$$

что и требовалось доказать.

**Доказательство теоремы 2.4.** Учитывая замечания, сделанные в начале доказательства теоремы 2.3, будем, как и в этой теореме, строить матрицу  $G_0$ , определяющую систему вложенных кодов  $A_v$ ,  $v = \overline{1, n_a - 1}$ , удовлетворяющих условию

$$N(w) \leq n_a C_{n_a}^w 2^{-r_{a,v}} = n_a C_{n_a}^w 2^{-v} \quad (\text{П. 2. 12})$$

столбец за столбцом. Здесь в качестве первого столбца выберем любой столбец, вес которого равен  $n_a/2$ . Пусть уже выбраны первые  $n_a - v$  столбцов матрицы  $G_0$ , т. е. построен код  $A_v$ , удовлетворяющий условию (П.2.12). Тогда в качестве следующего  $(n_a - v + 1)$ -го столбца выберем любое слово смежного класса кода  $A_v$ , в котором число слов  $N'_v(w)$  удовлетворяет условию  $N'_v(w) \leq n_a C_{n_a}^w 2^{-v}$ ,  $w = \overline{1, n_a}$ .

Как следует из леммы 2.1, такой смежный класс (при  $r_{a,v} > \log_2 3n_a$ ) существует.

Учитывая, что спектр весов кода  $A_{v-1}$  представляет собой сумму спектра весов кода  $A_v$  и выбранного смежного класса  $N_{v-1}(w) = N_v(w) + N'_v(w) \leq n_a C_{n_a}^w 2^{-v} + n_a C_{n_a}^w 2^{-v} = n_a C_{n_a}^w 2^{-v+1}$ , видим, что  $N_{v-1}(w)$  удовлетворяет условию (П. 2. 12).

Так как при  $v = n_a - 1$  условие (П. 2. 12) выполняется очевидным образом, то для всех  $v > \log_2 3n_a$  приходим к неравенству  $N_v(w) \leq n_a C_{n_a}^w 2^{-n_a(1-R_{a,v})}$ . После замены  $C_{n_a}^w$  на  $2^{n_a H(w/n_a)}$  и  $1 - R_{a,v}$  на  $H(\delta_{\text{ВГ}}(R_{a,v}))$  получаем  $N_v(w) \leq n_a 2^{n_a(H(w/n_a) - H(\delta_{\text{ВГ}}(R_{a,v})))}$ .

Отсюда видно, что при достаточно больших  $n_a$  для  $w/n < \delta_{\text{ВГ}}(R_{a,v})$  величина  $N_v(w) < 1$ , т. е.  $N_v(w) = 0$ . Учитывая также, что  $N_v(0) = 1$ , приходим к теореме 2.4.

## П.2.5. Доказательство теорем 2.5 и 2.6

Доказательство теорем 2.5 и 2.6 почти полностью совпадает с доказательством теорем 2.3 и 2.4. Отличие состоит лишь в том, что в качестве первого столбца матрицы  $G_0$  выбирается любое слово веса  $n_a/2$  при дополнительном условии, чтобы его первый символ равнялся единице. Затем после выбора  $(n_a - \nu)$ -го столбца, который производится так же, как и при доказательстве теорем 2.3 и 2.4, выполняются преобразования, при помощи которых этот столбец приводится к такому виду, что верхние его  $n_a - \nu$  символов равны нулю (что достигается добавлением к этому столбцу соответствующих столбцов из числа первых  $n_a - \nu$ ), а  $(n_a - \nu + 1)$ -й символ равен единице.

Последнее условие, если оно не выполняется сразу, достигается перестановкой  $(n_a - \nu + 1)$ -й строки с любой строкой большего номера, у которой в  $(n_a - \nu + 1)$ -м столбце стоит единица. Учитывая, что добавление к  $(n_a - \nu + 1)$ -му столбцу предшествующих столбцов соответствует выбору в качестве этого столбца другого слова из того же самого смежного класса, а перестановка строк не меняет спектра весов ни в коде, ни в смежном классе, приходим к выводу, что если в матрице  $G_0$  уже построены  $n_a - \nu$  нужных нам столбцов, то можно построить и  $(n_a - \nu + 1)$ -й столбец.

Отметим также, что если построена треугольная матрица  $G_0$ , удовлетворяющая условиям теорем 2.5 и 2.6, то элементарными преобразованиями только  $a_i$ ,  $i = 0, \overline{n_a - 1}$ , рядом стоящих столбцов (что не изменяет множества кодовых слов кода  $A_{i+1}$ ) ее можно привести к специальной треугольной матрице.

Таким образом, теоремы 2.5 и 2.6 справедливы и для специальной треугольной матрицы, определяющей систему из  $m$  вложенных кодов  $A_i$  со скоростями передачи  $R_{A_i} = (a_i + a_{i+1} + \dots + a_m)/n_a$ .

## П.2.7. Доказательство теорем 2.7 и 2.8

Доказательство теоремы 2.7. Покажем сначала, что теорема справедлива для некоторого фиксированного  $\nu$ . Обозначим через  $J_\nu$  множество всех ненулевых элементов  $\gamma$  поля  $GF(2^{n_a})$ , таких, у которых последние  $\nu$  символов (в двоичной записи) равны нулю, а через  $J_\nu^{-1}$  — множество всех элементов  $\mu$ , обратных элементам из множества  $J_\nu$ . Выделим теперь множество  $\Omega_\nu$  элементов  $\omega$ , вес которых (в двоичной записи) меньше, чем число  $d_{a_\nu}$ , определяемое неравенствами

$$\sum_{i=1}^{d_{a_\nu}-1} C_{n_a}^i \leq 2^\nu / n_a < \sum_{i=1}^{d_{a_\nu}} C_{n_a}^i,$$

и построим множество  $U_\nu$ , элементы которого и представляют собой все возможные (различные) произведения элементов  $\omega \in \Omega_\nu$ , и  $\mu \in J_\nu^{-1}$ , т. е.  $u = \omega \mu$ . Тогда любой ненулевой элемент  $g \in U_\nu$ , где  $U_\nu$  — дополнение  $U_\nu$  до множества всех ненулевых элементов поля  $GF(2^{n_a})$ , порождает код с кодовым расстоянием  $d_{a_\nu}$ , таким, что  $\sum_{i=1}^{d_{a_\nu}} C_{n_a}^i > 2^\nu / n_a$ ,  $H^-$  или  $H(d_{a_\nu}/n_a) >$

П.2.6. Таблица элементов поля GF (2<sup>7</sup>)

Таблица П.2.1

Степень	Представление многочленом	Представление вектором
0	1	(0 0 0 0 0 0 1)
1	$x$	(0 0 0 0 0 1 0)
2	$x^2$	(0 0 0 0 1 0 0)
3	$x^3$	(0 0 0 1 0 0 0)
4	$x^4$	(0 0 1 0 0 0 0)
5	$x^5$	(0 1 0 0 0 0 0)
6	$x^6$	(1 0 0 0 0 0 0)
7	$x^3+1$	(0 0 0 1 0 0 1)
8	$x^4+x$	(0 0 1 0 0 1 0)
9	$x^5+x^2$	(0 1 0 0 1 0 0)
10	$x^6+x^3$	(1 0 0 1 0 0 0)
11	$x^5+x^3+1$	(0 0 1 1 0 0 1)
12	$x^5+x^4+x$	(0 1 1 0 0 1 0)
13	$x^6+x^5+x^2$	(1 1 0 0 1 0 0)
14	$x^6+1$	(1 0 0 0 0 0 1)
15	$x^3+x+1$	(0 0 0 1 0 1 1)
16	$x^4+x^2+x$	(0 0 1 0 1 1 0)
17	$x^5+x^3+x^2$	(0 1 0 1 1 0 0)
18	$x^6+x^4+x^3$	(1 0 1 1 0 0 0)
19	$x^5+x^4+x+1$	(0 1 1 1 0 0 1)
20	$x^6+x^5+x^2+x$	(1 1 1 0 0 1 0)
21	$x^6+x^5+x^3+x^2+1$	(1 1 0 1 1 0 1)
22	$x^6+x^4+x+1$	(1 0 1 0 0 1 1)
23	$x^5+x^3+x^2+x+1$	(0 1 0 1 1 1 1)
24	$x^6+x^4+x^3+x^2+x$	(1 0 1 1 1 1 0)
25	$x^5+x^4+x^2+1$	(0 1 1 0 1 0 1)
26	$x^6+x^5+x^3+x$	(1 1 0 1 0 1 0)
27	$x^6+x^4+x^3+x^2+1$	(1 0 1 1 1 0 1)
28	$x^5+x^4+x+1$	(0 1 1 0 0 1 1)
29	$x^6+x^5+x^2+x$	(1 1 0 0 1 1 0)
30	$x^6+x^2+1$	(1 0 0 0 1 0 1)
31	$x+1$	(0 0 0 0 0 1 1)
32	$x^2+x$	(0 0 0 0 1 1 0)
33	$x^3+x^2$	(0 0 0 1 1 0 0)
34	$x^4+x^3$	(0 0 1 1 0 0 0)
35	$x^5+x^4$	(0 1 1 0 0 0 0)
36	$x^6+x^5$	(1 1 0 0 0 0 0)
37	$x^6+x^3+1$	(1 0 0 1 0 0 1)
38	$x^4+x^3+x+1$	(0 0 1 1 0 1 1)
39	$x^5+x^4+x^2+x$	(0 1 1 0 1 1 0)
40	$x^6+x^5+x^3+x^2$	(1 1 0 1 1 0 0)
41	$x^6+x^4+1$	(1 0 1 0 0 0 1)
42	$x^5+x^3+x+1$	(0 1 0 1 0 1 1)
43	$x^6+x^4+x^2+x$	(1 0 1 0 1 1 0)
44	$x^5+x^2+1$	(0 1 0 0 1 0 1)
45	$x^6+x^3+x$	(1 0 0 1 0 1 0)
46	$x^4+x^3+x^2+1$	(0 0 1 1 1 0 1)
47	$x^5+x^4+x^3+x$	(0 1 1 1 0 1 0)
48	$x^6+x^5+x^5+x^2$	(1 1 1 0 1 0 0)
49	$x^6+x^5+1$	(1 1 0 0 0 0 1)
50	$x^6+x^3+x+1$	(1 0 0 1 0 1 1)
51	$x^4+x^3+x^2+x+1$	(0 0 1 1 1 1 1)



Таблица П.2.1 (продолжение)

Степень	Представление многочленом	Представление вектором
52	$x^5+x^4+x^3+x^2+x$	(0 1 1 1 1 1 0)
53	$x^6+x^5+x^4+x^3+x^2$	(1 1 1 1 1 0 0)
54	$x^6+x^5+x^4+1$	(1 1 1 0 0 0 1)
55	$x^6+x^5+x^3+x+1$	(1 1 0 1 0 1 1)
56	$x^6+x^4+x^3+x^2+x+1$	(1 0 1 1 1 1 1)
57	$x^5+x^4+x^2+x+1$	(0 1 1 0 1 1 1)
58	$x^6+x^5+x^3+x^2+x$	(1 1 0 1 1 1 0)
59	$x^6+x^5+x^2+1$	(1 0 1 0 1 0 1)
60	$x^5+x+1$	(0 1 0 0 0 1 1)
61	$x^6+x^2+x$	(1 0 0 0 1 1 0)
62	$x^2+1$	(0 0 0 0 1 0 1)
63	$x^3+x$	(0 0 0 1 0 1 0)
64	$x^4+x^2$	(0 0 1 0 1 0 0)
65	$x^5+x^3$	(0 1 0 1 0 0 0)
66	$x^6+x^4$	(1 0 1 0 0 0 0)
67	$x^5+x^3+1$	(0 1 0 1 0 0 1)
68	$x^6+x^4+x$	(1 0 1 0 0 1 0)
69	$x^5+x^3+x^2+1$	(0 1 0 1 1 0 1)
70	$x^6+x^4+x^3+x$	(1 0 1 1 0 1 0)
71	$x^5+x^4+x^3+x^2+1$	(0 1 1 1 1 0 1)
72	$x^6+x^5+x^4+x^3+x$	(1 1 1 1 1 0 1 0)
73	$x^6+x^5+x^4+x^3+x^2+1$	(1 1 1 1 1 0 1 1)
74	$x^6+x^5+x^4+x+1$	(1 1 1 0 0 1 1)
75	$x^6+x^5+x^3+x^2+x+1$	(1 1 0 1 1 1 1)
76	$x^6+x^4+x^2+x+1$	(1 0 1 0 1 1 1)
77	$x^5+x^2+x+1$	(0 1 0 0 1 1 1)
78	$x^6+x^3+x^2+x$	(1 0 0 1 1 1 0)
79	$x^4+x^2+1$	(0 0 1 0 1 0 1)
80	$x^5+x^3+x$	(0 1 0 1 0 1 0)
81	$x^6+x^4+x^2$	(1 0 1 0 1 0 0)
82	$x^5+1$	(0 1 0 0 0 0 1)
83	$x^6+x$	(1 0 0 0 0 1 0)
84	$x^3+x^2+1$	(0 0 0 1 1 0 1)
85	$x^4+x^3+x$	(0 0 1 1 0 1 0)
86	$x^5+x^4+x^2$	(0 1 1 0 1 0 0)
87	$x^6+x^5+x^3$	(1 1 0 1 0 0 0)
88	$x^6+x^4+x^3+1$	(1 0 1 1 0 0 1)
89	$x^5+x^4+x^3+x+1$	(0 1 1 1 0 1 1)
90	$x^6+x^5+x^4+x^2+x$	(1 1 1 0 1 1 0)
91	$x^6+x^5+x^2+1$	(1 1 0 0 1 0 1)
92	$x^6+x+1$	(1 0 0 0 0 1 1)
93	$x^3+x^2+x+1$	(0 0 0 1 1 1 1)
94	$x^4+x^3+x^2+x$	(0 0 1 1 1 1 0)
95	$x^5+x^4+x^3+x^2$	(0 1 1 1 1 0 0)
96	$x^6+x^5+x^4+x^3$	(1 1 1 1 1 0 0 0)
97	$x^6+x^5+x^4+x^3+1$	(1 1 1 1 0 0 1)
98	$x^6+x^5+x^4+x^3+x+1$	(1 1 1 1 0 1 1)
99	$x^6+x^5+x^4+x^3+x^2+x+1$	(1 1 1 1 1 1 1)
100	$x^6+x^5+x^4+x^2+x+1$	(1 1 1 0 1 1 1)
101	$x^6+x^5+x^2+x+1$	(1 1 0 0 1 1 1)
102	$x^6+x^3+x+1$	(1 0 0 0 1 1 1)
103	$x^2+x+1$	(0 0 0 0 1 1 1)
104	$x^3+x^2+x$	(0 0 0 1 1 1 0)
105	$x^4+x^3+x^2$	(0 0 1 1 1 0 0)

Таблица П.2.1 (окончание)

Степень	Представление многочленом	Представление вектором
106	$x^5 + x^4 + x^3$	(0 1 1 1 0 0 0)
107	$x^6 + x^5 + x^4$	(1 1 1 0 0 0 0)
108	$x^6 + x^5 + x^3 + 1$	(1 1 0 1 0 0 1)
109	$x^6 + x^4 + x^3 + x + 1$	(1 0 1 1 0 1 1)
110	$x^5 + x^4 + x^3 + x^2 + x + 1$	(0 1 1 1 1 1 1)
111	$x^6 + x^5 + x^4 + x^3 + x^2 + x$	(1 1 1 1 1 1 0)
112	$x^6 + x^5 + x^4 + x^2 + 1$	(1 1 1 0 1 0 1)
113	$x^6 + x^5 + x + 1$	(1 1 0 0 0 1 1)
114	$x^6 + x^3 + x^2 + x + 1$	(1 0 0 1 1 1 1)
115	$x^4 + x^3 + x + 1$	(0 0 1 0 1 1 1)
116	$x^5 + x^3 + x^2 + x$	(0 1 0 1 1 1 0)
117	$x^6 + x^4 + x^3 + x^2$	(1 0 1 1 1 0 0)
118	$x^5 + x^4 + 1$	(0 1 1 0 0 0 1)
119	$x^6 + x^5 + x$	(1 1 0 0 0 1 0)
120	$x^6 + x^3 + x^2 + 1$	(1 0 0 1 1 0 1)
121	$x^4 + x + 1$	(0 0 1 0 0 1 1)
122	$x^5 + x^2 + x$	(0 1 0 0 1 1 0)
123	$x^6 + x^3 + x^2$	(1 0 0 1 1 0 0)
124	$x^4 + 1$	(0 0 1 0 0 0 1)
125	$x^5 + x$	(0 1 0 0 0 1 0)
126	$x^6 + x^2$	(1 0 0 0 1 0 0)
127	1	(0 0 0 0 0 0 1)

$> 1 - R_a, -\log_2 n_a/n_a$ . Действительно, пусть  $\gamma$  — любой элемент множества  $J$ , тогда для любых  $\mu \in J_v^{-1}$  и  $\omega \in Q$ , имеем  $g\gamma \neq \mu\omega$ . Но для любого  $\gamma \in J$ , найдется  $\mu = \gamma^{-1} \in J_v^{-1}$ , значит,  $g\gamma \neq \omega$ . Следовательно, вес элемента  $g\gamma$  не менее, чем  $d_a$ .

Убедимся теперь в справедливости теоремы одновременно для всех  $v = \overline{1, n_a - 1}$ . Для этого построим множество

$$U = \bigcup_{v=1}^{n_a-1} U_v.$$

Ясно, что любой элемент  $g \in U$  (т. е.  $g \notin U$ ) порождает систему вложенных кодов, для каждого из которых  $R_{a_v} = (n_a - v)/n$  и  $d_{a_v}$  удовлетворяют условию теоремы. Поэтому для завершения доказательства теоремы 2.7 остается показать, что множество  $U$  не является пустым. Так как мощности множеств  $J_v$ ,  $J_v^{-1}$ ,  $Q_v$ ,  $U_v$  соответственно удовлетворяют условиям  $|J_v| = |J_v^{-1}| = 2^{n_a - v} - 1$ ;  $|Q_v| \leq 2v/n_a$ ;  $|U_v| \leq (2^{n_a - v} - 1) 2v/n_a \leq (2^{n_a} - 1)/n_a$ , то

$$|U| \leq \sum_{v=1}^{n_a-1} |U_v| \leq \left(1 - \frac{1}{n_a}\right) (2^{n_a} - 1) \text{ и, следовательно, мощность множества}$$

$|U| > (2^{n_a} - 1)/n_a$ , что и доказывает теорему. Перед доказательством теоремы 2.8 докажем следующую лемму.

**Лемма 2.2.** Число  $M_v(w)$  ненулевых элементов поля  $GF(2^{n_a})$ , порождающих коды со скоростью передачи  $R_{a_v} = (n_a - v)/n_a$  и числом  $N_v(w)$  кодовых слов веса  $w$ , таким, что  $N_v(w) > n_a^2 C_{n_a}^w 2^{-v}$ , не превосходит величины  $M_v(w) \leq 2^{n_a} (1 - 2^{-(n_a - v)})/n_a^2$ .

Доказательство леммы 2.2. Составим таблицу из  $C_{n_a}^w$  строк и  $2^{n_a}-1$  столбцов, столбцы которой пронумерованы всеми ненулевыми элементами  $g \in \text{GF}(2^{n_a})$ , а строки теми элементами  $\alpha$  того же поля, вес которых (в двоичной записи) равен  $w$ . На пересечении каждой строки и столбца поставим единицу, если  $\alpha g = \gamma$ , где  $\gamma$  — элемент поля  $\text{GF}(2^{n_a})$ , такой, у которого последние  $v$  символов (в двоичной записи) равны нулю, и нуль — в противном случае. Другими словами, ставим единицу тогда и только тогда, когда  $\alpha$  является кодовым словом (веса  $w$ ) кода со скоростью передачи  $R_{\alpha} = (n_a - v)/n_a$ , порождаемого элементом  $g$ . Так как при заполнении каждой строки рассматривается произведение фиксированного ненулевого элемента на все ненулевые элементы поля  $\text{GF}(2^{n_a})$ , то в результате пробегаются (но в другом порядке) также все ненулевые элементы этого поля. Учитывая, что число ненулевых элементов  $\gamma$  равно  $2^{n_a-v}-1$ , приходим к выводу, что каждая строка таблицы содержит ровно  $2^{n_a-v}-1$  единиц, а значит, вся таблица содержит  $N_w = C_{n_a}^w (2^{n_a-v}-1)$  единиц.

Рассмотрим теперь такие  $M_w(w)$  столбцов, в которых число единиц больше, чем  $n_a^2 C_{n_a}^w 2^{-v}$ . Эти столбцы соответствуют элементам  $g$ , порождающим коды со спектром весов, удовлетворяющим условию леммы.

Общее число  $L_w$  единиц в этих  $M_w(w)$  столбцах удовлетворяет очевидным неравенствам  $M_w(w) n_a^2 C_{n_a}^w 2^{-v} \leq L_w \leq N_w$ , откуда  $M_w(w) n_a^2 C_{n_a}^w 2^{-v} \leq N_w = C_{n_a}^w (2^{n_a-v}-1)$  или  $M_w(w) \leq 2^{n_a} (1 - 2^{-(n_a-v)})/n_a^2$ , что и требовалось доказать.

Доказательство теоремы 2.8. Обозначим через  $M$  число всех ненулевых элементов  $g \in \text{GF}(2^{n_a})$ , порождающих систему вложенных кодов, такую, что хотя бы для одного кода  $A$ , со скоростью передачи  $R_{\alpha} = (n_a - v)/n_a$ ,  $v = \overline{1, n_a - 1}$ , спектр весов  $N_w(w)$ ,  $w = \overline{1, n_a}$ , удовлетворяет неравенству хотя бы для одного значения  $w$ ,  $w = \overline{1, n_a}$ ,  $N_w(w) > n_a^2 C_{n_a}^w 2^{-v}$ .

Значения  $M$  оцениваются сверху как

$$M = \sum_{v=1}^{n_a-1} \sum_{w=1}^{n_a} M_w(w) \leq \sum_{v=1}^{n_a-1} \sum_{w=1}^{n_a} 2^{n_a} (1 - 2^{-(n_a-v)})/n_a^2 < \frac{n_a-1}{n_a} (2^{n_a}-1).$$

Но тогда число элементов  $g$ , порождающих коды, спектр весов которых удовлетворяет условию

$$N_w(w) \leq n_a^2 C_{n_a}^w 2^{-v}, \quad v = \overline{1, n_a-1}, \quad w = \overline{1, n_a}, \quad (\text{П. 2. 13})$$

равно  $2^{n_a}-1-M \geq (2^{n_a}-1)(1 - (n_a-1)/n_a) = (2^{n_a}-1)/n_a$ , и так как  $(2^{n_a}-1)/n_a > 1$  при  $n_a > 1$ , то элементы  $g$ , для которых выполняется условие (П. 2. 13), существуют.

После замены  $C_{n_a}^w$  на  $2^{n_a H(w/n_a)}$  и  $v/n_a = 1 - R_{\alpha}$ , на  $H(\delta_{\text{ВГ}}(R_{\alpha}))$  из (П. 2. 13) получаем  $N_w(w) \leq 2^{n_a} 2^{n_a \{H(w/n_a) - H(\delta_{\text{ВГ}}(R_{\alpha}))\}}$ , и так как при достаточно больших  $n_a$  для  $w < n_a \delta_{\text{ВГ}}(R_{\alpha})$  величина  $N_w(w) < 1$ , то для этих  $w$   $N_w(w) = 0$ . Учитывая также, что  $N_w(0) = 1$ , получаем неравенства (2. 34), т. е. приходим к теореме 2.8.

## ПРИЛОЖЕНИЕ П.3

### П.3.1. Доказательство утверждения 3.3

Рассмотрим каскадный код порядка  $m$  с нижней оценкой кодового расстояния  $\delta_n(R, m)$  и скоростью передачи  $R$ . Как всегда предполагаем, что в качестве внутренних и внешних кодов выбраны наилучшие из известных кодов (см. разд. 3.1.1). Напомним, что параметры  $R$  и  $\delta_n(R, m)$  определяются равенствами

$$R = \sum_{i=1}^m (R_{a_i} - R_{a, i+1}) R_{b_i}, \quad \delta^{(n)}(R, m) = \min_i \delta_i^{(n)}, \quad (\text{П. 3. 1})$$

где  $\delta_i^{(n)} = (1 - R_{b_i}) \delta_{\text{ВГ}}(R_{a_i})$ .

Рассмотрим построение каскадного кода порядка  $m+1$ , удовлетворяющего утверждению 3.3. При этом его параметры в отличие от параметров исходного кода будем отмечать штрихом.

Для нового кода порядка  $m+1$  положим

$$R'_{a_i} = R_{a_i} \text{ и } R'_{b_i} = R_{b_i} \text{ при } i \leq s,$$

$$R'_{a_i} = \frac{1}{2} (R_{a_s} + R_{a, s+1}) \text{ и } R'_{b_i} = 1 - \delta_s^{(n)} / \delta_{\text{ВГ}}(R'_{a, s+1}) \text{ при } i = s+1, \quad (\text{П. 3. 2})$$

$$R'_{a_i} = R_{a, i-1} \text{ и } R'_{b_i} = R_{b, i-1} \text{ при } i = s+1.$$

Схема преобразования исходного кода порядка  $m$  в новый код порядка  $m+1$  показана на рис. П.3.1.

Указанный выбор внутренних и внешних кодов приводит к равенствам

$$\delta_i^{(n)} = \delta_i^{(n)} \text{ при } i \leq s;$$

$$\delta_i^{(n)} = \delta_{\text{ВГ}}(R'_{a, s+1}) (1 - R'_{b, s+1}) = \delta_s^{(n)} \text{ при } i = s+1;$$

$$\delta_i^{(n)} = \delta_{i-1}^{(n)} \text{ при } i > s+1,$$

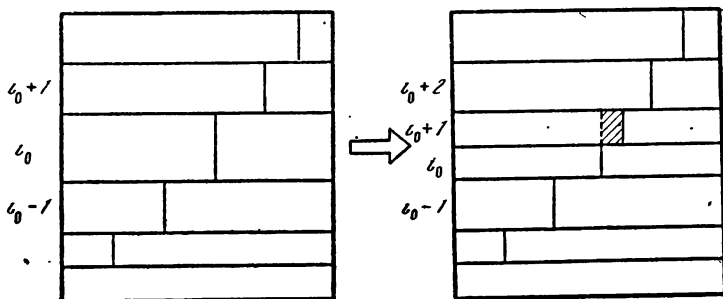


Рис. П.3.1. Схема преобразования каскадного кода порядка  $m$  в код порядка  $m+1$

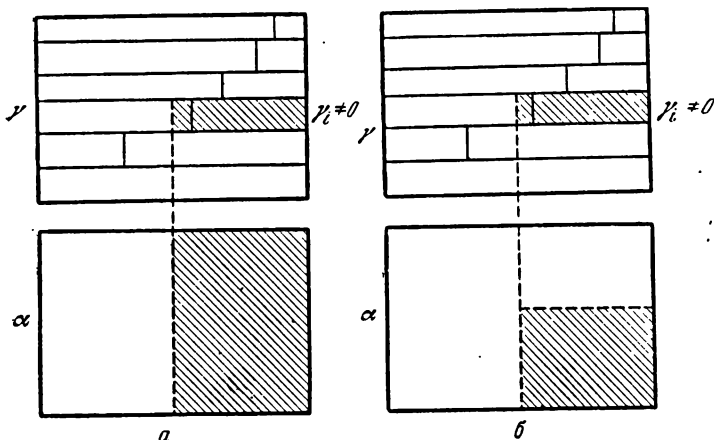


Рис. П.3.2. Схематическое представление распределения ненулевых символов (заштрихованная область) в слове каскадного кода в случае произвольной (а) и нижней треугольной (б) кодирующей матрицы  $G_0$

из которых согласно (П.3.1) следует, что  $\delta^{(n)}(R', m+1) = \min_i \delta_i^{(n)} = \min_i \delta^{(n)} = \delta^{(n)}(R, m)$ .

Таким образом при указанном построении каскадного кода порядка  $m+1$  нижняя оценка его кодового расстояния осталась такой же, как и у исходного кода порядка  $m$ .

Вычислим теперь скорость передачи  $R' = \sum_{i=1}^{m+1} (R'_{ai} - R'_{ai+1}) R'_{bi}$ . Подставляя в это соотношение равенства (П.3.2), после элементарных преобразований получаем  $R' - R = 1/2 (R_{as} - R_{a, s+1}) (R'_{b, s+1} - R'_{bs})$ , что, впрочем, ясно из рис. П.3.1.

Так как  $R_{as} > R_{a, s+1}$ ,  $R'_{b, s+1} = 1 - \delta_s^{(n)}/\delta_{BF}(R'_{a, s+1}) > 1 - \delta_s^{(n)}/\delta_{BF}(R_{as}) = R_{bs}$ , получаем  $R' - R > 0$ , что и завершает доказательство утверждения 3.3.

Аналогичным образом можно показать, что и для каскадных кодов НЗ можно, увеличивая порядок  $m$ , увеличить скорость передачи  $R$ , не изменяя нижних оценок степеней защиты.

### П.3.2. Доказательство утверждения 3.4

Рассмотрим подмножество  $V_i$  кодовых слов  $\alpha$  каскадного кода, которым соответствуют информационные слова  $\mu$ , удовлетворяющие следующим условиям:

$$\left. \begin{aligned} \mu_s &= 0 \text{ для всех } s \neq i, \\ \mu_{ij} &= 0 \text{ для } j \leq x_i, \\ \mu_{ij} &\text{ произвольны для } j > x_i, \end{aligned} \right\} 0 \leq x_i \leq b_i - 1. \quad (\text{П.3.3})$$

Тогда множество рассматриваемых вспомогательных слов  $\gamma$  и соответствующих им кодовых слов  $\alpha$  (учитывая, что код  $B_i$  — систематический, а  $G_0$  — квадратная матрица) имеют вид, показанный на рис. П.3.2, т. е. все символы слов  $\alpha$  вне заштрихованного прямоугольника равны нулю, а сам заштрихованный прямоугольник является кодовым словом двоичного линейного кода  $V_i$ , мощность которого  $|V_i| = 2^{a_i(b_i - x_i)}$ .

Так как все первые  $x_i$  столбцов любого слова  $\alpha \in V_i$  равны нулю, то фактическая длина слов кода  $V_i$  определяется как

$$n_i^* = n = n_a x_i = n_a (n_b - x_i), \quad (\text{П. 3. 4})$$

а его скорость передачи

$$r_i = a_i (b_i - x_i) / n_a (n_b - x_i). \quad (\text{П. 3. 5})$$

Кодовое расстояние  $d_i^*$  кода  $V_i$ , как и любого двоичного линейного блочного кода, удовлетворяет условию

$$d_i^* \leq n_i^* \delta_B(r_i), \quad (\text{П. 3. 6})$$

где  $\delta_B(r_i)$  — любая из верхних оценок величины  $d/n$  для двоичного линейного блочного кода.

Так как код  $V_i$  при любом  $i, i = \overline{1, m}$ , является подкодом исходного каскадного кода, то кодовое расстояние последнего удовлетворяет очевидному соотношению

$$d \leq \min_i \{d_i^*\}. \quad (\text{П. 3. 7})$$

Соотношение (П.3.7) задает ограничение сверху на кодовое расстояние  $d$  каскадного кода. Для улучшения этой верхней оценки следует по возможности минимизировать  $d_i^*$ , что можно сделать надлежащим выбором фактической длины  $n_i^*$  и скорости передачи  $r_i$  кодов  $V_i$ .

Из (П.3.4) и (П.3.6) получаем

$$d_i^* \leq n (1 - x_i/n_b) \delta_B(r_i). \quad (\text{П. 3. 8})$$

Но из (П.3.5) имеем

$$\frac{x_i}{n_b} = \frac{r_i - a_i b_i / n_a n_b}{r_i - a_i / n_a} = \frac{r_i - (R_{a,i} - R_{a,i+1}) R_{b,i}}{r_i - (R_{a,i} - R_{a,i+1})}. \quad (\text{П. 3. 9})$$

Подставляя (П.3.9) в (П.3.8), имеем

$$d_i^* \leq n \delta_B(r_i) (R_{a,i} - R_{a,i+1}) (1 - R_{b,i}) / (R_{a,i} - R_{a,i+1} - r_i). \quad (\text{П. 3. 10})$$

Из (П.3.10) следует, что минимизацию  $d_i^*$  можно получить надлежащим выбором  $r_i$ . Из (П.3.5) следует, что выбор  $r_i$  связан с выбором  $x_i$ , которое в силу (П.3.3) может изменяться от 0 до  $b_{i-1}$ , что соответствует изменению  $r_i$  от  $(R_{a,i} - R_{a,i+1}) R_{b,i}$  до  $(R_{a,i} - R_{a,i+1}) / n_b$ .

Таким образом, минимизируя (П.3.10) по всем возможным значениям  $r_i$  и подставляя результат в (П.3.5), получаем (3.16), что и завершает доказательство утверждения 3.4.

# П.3.4. Характеристики каскадных кодов первого порядка

Таблица П.3.1

$b_1$	$d_{b1}$	$d^{(n)}$	$k$	$d_{БЧХ}$	$k_{БЧХ}$	$b_1$	$d_{b1}$	$d^{(n)}$	$k$	$d_{БЧХ}$	$k_{БЧХ}$
33	1	16	165	—	—	16	18	288	80	—	—
32	1	32	160	248	162	15	19	304	75	376	75
31	3	48	155	—	—	14	20	320	70	—	—
30	4	64	150	252	152	13	21	336	65	380	65
29	5	80	145	—	—	12	22	352	60	—	—
28	6	96	140	254	142	11	23	368	55	384	55
27	7	112	135	—	—	10	24	384	50	—	—
26	8	128	130	256	132	9	25	400	45	400	45
25	9	144	125	342	122	8	26	416	40	—	—
24	10	160	120	344	120	7	27	432	35	448	35
23	11	176	115	—	—	6	28	448	30	—	—
22	12	192	110	348	110	5	29	464	25	480	25
21	13	208	105	—	—	6	30	480	20	—	—
20	14	224	100	352	100	3	31	496	15	496	15
19	15	240	95	—	—	2	32	512	10	512	10
18	16	256	90	364	90	1	33	528	5	—	—
17	17	272	85	368	85						

Примечание.  $p=1$ ,  $a_1=5$ ,  $d_{a1}=16$ .

Таблица П.3.2

$b_1$	$d_{b1}$	$d^{(n)}$	$k$	$d_{БЧХ}$	$k_{БЧХ}$	$b_1$	$d_{b1}$	$d^{(n)}$	$k$	$d_{БЧХ}$	$k_{БЧХ}$
33	1	12	330	—	—	17	17	204	170	—	—
32	2	24	320	184	317	16	18	216	160	248	162
31	3	36	310	188	307	15	19	228	150	252	152
30	4	48	300	—	—	14	20	240	140	254	142
29	5	60	290	192	287	13	21	252	130	256	132
28	6	72	280	—	—	12	22	264	120	344	120
27	7	84	270	208	267	11	23	276	110	348	110
26	8	96	260	214	257	10	24	288	100	352	100
25	9	108	250	216	247	9	25	300	90	364	90
24	10	120	240	220	237	8	26	312	80	—	—
23	11	132	230	222	227	7	27	324	70	—	—
22	12	144	220	—	—	6	28	336	60	—	—
21	13	156	210	—	—	5	29	348	50	—	—
20	14	168	200	236	202	4	30	360	40	—	—
19	15	180	190	—	—	3	31	372	30	—	—
18	16	192	180	240	182	2	32	384	20	—	—
						1	33	396	10	512	10

Примечание.  $p=2$ ,  $a_1=10$ ,  $d_{a1}=12$ .

Таблица П.3.3

$b_1$	$d_{b1}$	$d^{(a)}$	$k$	$d_{БЧХ}$	$k_{БЧХ}$	$b_1$	$d_{b1}$	$d^{(a)}$	$k$	$d_{БЧХ}$	$k_{БЧХ}$
33	1	8	495	120	492	16	18	144	240	—	—
32	2	16	480	—	—	15	19	152	225	222	227
31	3	24	465	—	—	14	20	160	210	—	—
30	4	32	450	—	—	13	21	168	195	—	—
29	5	40	435	—	—	12	22	176	180	240	182
28	6	48	420	152	422	11	23	184	165	248	162
27	7	56	405	—	—	10	24	192	150	252	152
26	8	64	390	—	—	9	25	200	135	256	132
25	9	72	375	—	—	8	26	208	120	342	122
24	10	80	360	—	—	7	27	216	105	—	—
3	11	88	345	176	347	6	28	224	90	364	90
22	12	96	330	—	—	5	29	232	75	376	75
21	13	104	315	184	317	4	30	240	60	—	—
20	14	112	300	—	—	3	31	248	45	440	45
19	15	120	285	192	287	2	32	256	30	—	—
18	16	128	270	208	267	1	33	264	15	496	15
17	17	136	255	214	257						

Примечание.  $\mu=3$ ,  $a_1=15$ ,  $d_{a1}=8$ .

Таблица П.3.4

$b_1$	$d_{b1}$	$d^{(a)}$	$k$	$d_{БЧХ}$	$k_{БЧХ}$	$b_1$	$d_{b1}$	$d^{(a)}$	$k$	$d_{БЧХ}$	$k_{БЧХ}$
33	1	6	660	80	657	16	18	108	320	184	317
32	2	12	640	—	—	15	19	114	300	—	—
31	3	18	620	90	617	14	20	120	280	—	—
30	4	24	600	—	—	13	21	126	260	214	257
29	5	30	580	—	—	12	22	132	240	220	237
28	6	36	560	104	562	11	23	138	220	—	—
27	7	42	540	—	—	10	24	144	200	236	202
26	8	48	520	112	522	9	25	150	180	240	182
25	9	54	500	118	502	8	26	156	160	248	162
24	10	60	480	—	—	7	27	162	140	254	142
23	11	66	460	—	—	6	28	168	120	344	120
22	12	72	440	148	442	5	29	174	100	352	100
21	13	78	420	152	422	4	30	180	80	—	—
20	14	84	400	—	—	3	31	186	60	—	—
19	15	90	380	166	382	2	32	192	40	—	—
18	16	96	360	—	—	1	33	198	20	—	—
17	17	102	340	—	—						

Примечание.  $\mu=4$ ,  $a_1=20$ ,  $d_{a1}=6$ .



Таблица П.3.5

$b_1$	$d_{b1}$	$d^{(n)}$	$k$	$d_{БЧХ}$	$k_{БЧХ}$	$b_1$	$d_{b1}$	$d^{(n)}$	$k$	$d_{БЧХ}$	$k_{БЧХ}$
33	1	4	825	—	—	16	18	72	400	—	—
32	2	8	800	48	797	15	19	76	375	—	—
31	3	12	775	—	—	14	20	80	350	176	347
30	4	16	750	58	747	13	21	84	325	—	—
29	5	20	725	—	—	12	22	88	300	—	—
28	6	24	700	—	—	11	23	92	275	—	—
27	7	28	675	—	—	10	24	96	250	216	247
26	8	32	650	84	647	9	25	100	225	222	227
25	9	36	625	88	627	8	26	104	200	236	202
24	10	40	600	—	—	7	27	108	175	—	—
23	11	44	575	102	572	6	28	112	150	252	152
22	12	48	550	—	—	5	29	116	125	342	122
21	13	52	525	112	522	4	30	120	100	352	100
20	14	56	500	118	502	3	31	124	75	376	75
19	15	60	475	124	472	2	32	128	50	—	—
18	16	64	450	—	—	1	33	132	25	480	25
17	17	68	425	152	422						

Примечание.  $\mu = 5$ ,  $a_1 = 25$ ,  $d_{a1} = 4$ .

Таблица П.3.6

$b_1$	$d_{b1}$	$d^{(n)}$	$k$	$d_{БЧХ}$	$k_{БЧХ}$	$b_1$	$d_{b1}$	$d^{(n)}$	$k$	$d_{БЧХ}$	$k_{БЧХ}$
33	1	2	990	—	—	16	18	36	480	—	—
32	2	4	960	—	—	15	19	38	450	—	—
31	3	6	930	20	932	14	20	40	420	152	422
30	4	8	900	—	—	13	21	42	390	—	—
29	5	10	870	32	872	12	22	44	360	—	—
28	6	12	840	40	837	11	23	46	330	—	—
27	7	14	810	—	—	10	24	48	300	—	—
26	8	16	780	—	—	9	25	50	270	208	267
25	9	18	750	58	747	8	26	52	240	220	237
24	10	20	720	64	717	7	27	54	210	—	—
23	11	22	690	74	687	6	28	56	180	240	182
22	12	24	660	80	657	5	29	58	150	252	152
21	13	26	630	88	627	4	30	60	120	344	120
20	14	28	600	—	—	3	31	62	90	364	90
19	15	30	570	102	572	2	32	64	60	—	—
18	16	32	540	—	—	1	33	66	30	—	—
17	17	34	510	—	—						

Примечание.  $\mu = 6$ ,  $a_1 = 30$ ,  $d_{a1} = 2$ .

### П.3.5. Значения интеграла $I(x)$

Таблица П.3.7

$x$	$\delta_{\text{ВГ}}(x)$	$I(x)$	$x$	$\delta_{\text{ВГ}}(x)$	$I(x)$
0,000000	0,500	0,000000	0,2398	0,220	0,8040
0,000003	0,499	0,000006	0,2491	0,215	0,8464
0,000012	0,498	0,000024	0,2585	0,210	0,8909
0,000072	0,495	0,000145	0,2682	0,205	0,9375
0,000289	0,490	0,000585	0,2780	0,200	0,9863
0,000649	0,485	0,001325	0,2882	0,195	1,0376
0,0012	0,480	0,0024	0,2985	0,190	1,0913
0,0018	0,475	0,0037	0,3091	0,185	1,1477
0,0026	0,470	0,0054	0,3199	0,180	1,2070
0,0035	0,465	0,0074	0,3310	0,175	1,2693
0,0046	0,460	0,009	0,3423	0,170	1,3349
0,0059	0,455	0,0125	0,3539	0,165	1,4040
0,0072	0,450	0,0155	0,3657	0,160	1,4768
0,0087	0,445	0,0189	0,3778	0,155	1,5536
0,0104	0,440	0,0227	0,3902	0,150	1,6347
0,0122	0,435	0,0268	0,4028	0,145	1,7205
0,0142	0,430	0,0313	0,4158	0,140	1,8114
0,0163	0,425	0,0363	0,4290	0,135	1,9077
0,0185	0,420	0,0416	0,4426	0,130	2,0101
0,0209	0,415	0,0474	0,4564	0,125	2,1189
0,0235	0,410	0,0535	0,4706	0,120	2,2349
0,0262	0,405	0,0602	0,4852	0,115	2,3587
0,0290	0,400	0,0672	0,5001	0,110	2,4912
0,0320	0,395	0,0748	0,5154	0,105	2,6332
0,0352	0,390	0,0828	0,5310	0,100	2,7860
0,0385	0,385	0,0913	0,5471	0,095	2,9507
0,0420	0,380	0,1004	0,5635	0,090	3,1288
0,0456	0,375	0,1099	0,5804	0,085	3,3222
0,0493	0,370	0,1200	0,5978	0,080	3,5329
0,0532	0,365	0,1307	0,6157	0,075	3,7636
0,0573	0,360	0,1419	0,6341	0,070	4,0174
0,0615	0,355	0,1538	0,6530	0,065	4,2982
0,0659	0,350	0,1662	0,6726	0,060	4,6110
0,0705	0,345	0,1793	0,6927	0,055	4,9622
0,0752	0,340	0,1930	0,7136	0,050	5,3602
0,0800	0,335	0,2074	0,7352	0,045	5,8161
0,0851	0,330	0,2226	0,7577	0,040	6,3457
0,0902	0,325	0,2384	0,7811	0,035	6,9713
0,0956	0,320	0,2550	0,8056	0,030	7,7267
0,1011	0,315	0,2724	0,8313	0,025	8,6657
0,1068	0,310	0,2906	0,8586	0,020	9,8819
0,1127	0,305	0,3096	0,8876	0,015	11,558
0,1187	0,300	0,3296	0,9192	0,010	14,126
0,1249	0,295	0,3504	0,9546	0,005	19,070
0,1313	0,290	0,3721	0,9792	0,002	26,676
0,1445	0,280	0,4188	0,9886	0,001	33,235
0,1585	0,270	0,4696	0,9938	0,0005	40,489
0,1733	0,260	0,5252	0,9973	0,0002	51,142
0,1887	0,250	0,5859	0,9985	0,0001	60,006
0,2049	0,240	0,6522	0,9998	0,00001	94,426
0,2220	0,230	0,7247			

### П.3.3. Доказательство утверждения 3.6

Нижняя оценка  $\delta_A^{(n)}(R, m)$  определяется соотношением

$$\delta_A^{(n)}(R, m) = (1 - R_{bi}) \delta_{BG}(R_{ai}), \quad i = \overline{1, m}. \quad (\text{П. 3. 11})$$

Так как (П. 3. 11) имеет место для всех  $i$ , то в силу того, что  $R_{ai} > R_{a, i+1}$  и  $\delta_{BG}(R_{ai}) < \delta_{BG}(R_{a, i+1})$ , из него следует, что  $R_{bi} < R_{b, i+1}$ . Следовательно, в (3. 16) минимум будет иметь место при  $i = m$ , т. е.

$$\delta_A^{(n)}(R, m) = (1 - R_{bm})/2. \quad (\text{П. 3. 12})$$

Умножая (П. 3. 12) на  $2\delta_{BG}(R_{am})$ , получаем

$$\delta_A^{(n)}(R, m) 2\delta_{BG}(R_{am}) = (1 - R_{bm}) \delta_{BG}(R_{am}). \quad (\text{П. 3. 13})$$

Учитывая, что правая часть (П.3.13) в силу (П.3.11) равна  $\delta_A^{(n)}(R, m)$ , из (П.3.13) очевидным образом получаем (3.22), что завершает доказательство утверждения.

### П.3.6. Доказательство утверждения 3.11

Чтобы максимизировать скорость передачи

$$R = \int_0^{x_0} f(x) dx,$$

надо для каждого  $x$  ( $0 < x < x_0$ ) выбирать максимально возможное значение  $f(x)$ . Но из (3.60) следует, что  $\delta_B^{(n)}(R, \infty) \leq \frac{1}{2}(1 - f(x))(1 - x)$ , откуда  $f(x) \leq 1 - 2\delta_B^{(n)}(R, \infty)/(1 - x)$ .

Знак равенства в последнем выражении определяет максимально возможное значение  $f(x)$ , что и завершает доказательство утверждения.

### П.3.7. Доказательство утверждения 3.13

Подставляя (3.66) в выражение для скорости передачи, имеем

$$R = x_0 - \delta_B^{(n)}(R, \infty) \int_0^{x_0} 2^{1-x} (2^{1-x} - 1)^{-1} dx,$$

откуда после интегрирования получаем  $R = x_0 - \delta_B^{(n)}(R, \infty) \log_2(2^{1-x_0} - 1)$ . Подставляя в это выражение вместо  $x_0$  его значение  $x_0 = 1 + \log_2(1 - \delta_B^{(n)}(R, \infty))$ , после элементарных преобразований получаем  $R = 1 - H(\delta_B^{(n)}(R, \infty))$  или  $\delta_B^{(n)}(R, \infty) = \delta_{BG}(R)$ , что и завершает доказательство утверждения.

## ПРИЛОЖЕНИЕ П.4

### П.4.1. Доказательство леммы 4.2

Оценим наименьшее число ошибок  $t$ , которое при использовании процедуры  $\psi_t^k(z_t)$  может привести к тому, что все  $\tilde{\gamma}_t^k \in \tilde{\Gamma}(t)$  окажутся неправильными ( $\tilde{\gamma}_t^k \neq \gamma_t$ ,  $k = \overline{1, z_t}$ ). Для этого необходимо, чтобы для всех кри-

териев  $T_k^{(i)}$  число ошибок  $e_k$  и стираний  $\tau_k$  в словах  $\hat{1}_i^k$  удовлетворяло условию

$$2e_k + \tau_k \geq d_{bi}. \quad (\text{П. 4. 1})$$

Обозначим через  $N_s$  число столбцов  $\hat{a}^{(j)}(i-1)$  в слове  $\hat{a}(i-1)$ , в каждом из которых содержится ровно  $s \leq n_a$  ошибок. Тогда общее число ошибок  $t$  в слове  $\hat{a}(i-1)$  равно

$$t = \sum_{s=1}^{n_a} sN_s. \quad (\text{П. 4. 2})$$

В соответствии с определением  $\hat{1}_i^k$  (см. П.3 процедуры  $\psi_i^q(z_i)$ )

$$e_k + \tau_k = \sum_{s=T_k^{(i)}+1}^{n_a} N_s, \quad e_k \leq \sum_{s=d_{ai}-T_k^{(i)}}^{n_a} N_s, \quad \tau_k \geq \sum_{s=T_k^{(i)}+1}^{d_{ai}-T_k^{(i)}-1} N_s \quad (\text{П. 4. 3})$$

Таким образом, задача сводится к нахождению наименьшего значения, определяемого из (П.4.2), при котором для всех значений  $T_k^{(i)}$ ,  $k=1, z_i$ , одновременно выполняются условия (П.4.1) и (П.4.3). В силу линейности этих условий указанная задача является типичной задачей линейного программирования. Известно, что в этом случае решение находится на границе, что соответствует замене неравенств в условиях (П.4.1) и (П.4.3) строгими равенствами.

Учитывая, что  $T_k^{(i)} < T_{k+1}^{(i)}$  и, следовательно,  $e_k \leq e_{k+1}$  и  $\tau_k \geq \tau_{k+1}$ , получаем

$$\begin{aligned} e_1 &= \sum_{s=d_{ai}-T_1^{(i)}}^{n_a} N_s, & e_{k+1} - e_k &= \sum_{s=d_{ai}-T_{k+1}^{(i)}}^{d_{ai}-T_k^{(i)}-1} N_s, \quad k=1, z_i-1, \\ (\tau_k - \tau_{k+1}) - (e_{k+1} - e_k) &= \sum_{s=T_k^{(i)}+1}^{T_{k+1}^{(i)}} N_s, \quad k=1, z_i-1, \\ \tau_{z_i} &= \sum_{s=T_{z_i}^{(i)}+1}^{d_{ai}-T_{z_i}^{(i)}-1} N_s. \end{aligned} \quad (\text{П. 4. 4})$$

Заметим, что условия (П.4.4) состоят из  $2z_i$  условий с неперекрывающимися индексами. При этом задача минимизации числа ошибок  $t$  сводится к задаче минимизации числа ошибок на каждом из  $2z_i$  диапазонов изменения  $s$ . На любом из них задача сводится к выбору такого набора величин  $N_s$ , который минимизирует  $\sum sN_s$  при заданном значении суммы  $\sum N_s$ . В силу линейности формы и условия  $\sum N_s = \text{const}$  минимум достигается на границе, т. е. в данном случае, когда все  $N_s$ , кроме одного, равны нулю. При этом ясно, что ненулевым следует выбирать  $N$  с наименьшим номером  $s$ .

Таким образом, приходим к набору  $N_s$ , где  $s \in S = \{T_1^{(i)} + 1, \dots, T_{z_i}^{(i)} + 1, d_{ai} - T_{z_i}^{(i)}, \dots, d_{ai} - T_1^{(i)}\}$ , а все остальные  $N_s$ ,  $s \notin S$ , полагаем равными нулю. Тогда согласно (П. 4. 4) получаем

$$\begin{aligned} e_1 &= N_{d_{ai}-T_1^{(i)}}, & e_{k+1} - e_k &= N_{d_{ai}-T_{k+1}^{(i)}}; \\ \tau_k - \tau_{k+1} &= N_{T_k^{(i)}+1} + |N_{d_{ai}-T_{k+1}^{(i)}}| = N_{T_k^{(i)}+1} + e_{k+1} - e_k; \\ \tau_{z_i} &= N_{T_{z_i}^{(i)}+1}. \end{aligned} \quad (\text{П. 4. 5})$$

Подставляя определяемые (П. 4. 5) значения  $N_s$ ,  $s \in S$  в (П. 4. 4) и учитывая, что для  $s \notin S$   $N_s = 0$ , получаем

$$t = \sum_{k=1}^{x_i-1} \{(\tau_k - \tau_{k+1}) - (e_{k+1} - e_k)\} (T_k^{(i)} + 1) + \tau_{x_i} (T_{x_i}^{(i)} + 1) + \\ + \sum_{k=1}^{x_i-1} (e_{k+1} - e_k) (d_{a_i} - T_{k+1}^{(i)}) + e_1 (d_{a_i} - T_1^{(i)}). \quad (\text{П. 4. 6})$$

Как уже указывалось выше в условии (П. 4. 1), надо знак неравенства заменить знаком равенства, т. е. положить  $2e_k + \tau_k = d_{b_i}$ . Отсюда следует, что

$$\tau_k = d_{b_i} - 2e_k \quad \text{при } 2e_k \leq d_{b_i},$$

$$\tau_k = 0 \quad \text{при } 2e_k > d_{b_i}.$$

В силу условия  $\tau_k \geq \tau_{k+1}$  при  $\tau_k = 0$  разность  $\tau_k - \tau_{k+1} = 0$ . Но в этом случае минимум (П. 4. 6) достигается при наименьшем значении  $e_k$ , при котором  $\tau_k = 0$ , т. е. при

$$e_k = \left\lceil \frac{d_{b_i} + 1}{2} \right\rceil, \quad \text{где } [X] \text{ — целая часть } X.$$

Отсюда следует, что при минимизации (П. 4. 6) достаточно рассмотреть лишь случай

$$e_k \leq \left\lceil \frac{d_{b_i} + 1}{2} \right\rceil, \quad k = \overline{1, z_i}, \quad \text{полагая в нем } \tau_k - \tau_{k+1} = 2(e_{k+1} - e_k).$$

Тогда после элементарных преобразований выражения (П. 4. 6) находим

$$t = d_{b_i} (T_{x_i}^{(i)} + 1) + e_1 (T_2^{(i)} - 2T_1^{(i)} - 1) + \sum_{k=2}^{x_i-1} e_k (T_{k+1}^{(i)} - 2T_k^{(i)} + T_{k-1}^{(i)}) + \\ + e_{x_i} (d_{a_i} - 3T_{x_i}^{(i)} + T_{x_i-1}^{(i)} - 1),$$

$$\text{где } 0 \leq e_1 \leq e_2 \leq \dots \leq e_{x_i} \leq \left\lceil \frac{d_{b_i} + 1}{2} \right\rceil.$$

Так как  $t$  является линейной функцией переменных  $e_k$ , то наименьшее значение  $t$  может достигаться в одной или нескольких граничных точках  $(e_1, e_2, \dots, e_{x_i})$ , которые имеют вид

$$\begin{pmatrix} 0, & 0, & \dots & 0, & 0 \end{pmatrix} \\ \begin{pmatrix} 0, & 0, & \dots & 0, & \left\lceil \frac{d_{b_i} + 1}{2} \right\rceil \end{pmatrix} \\ \vdots & \vdots & & \vdots & \vdots \\ \left\lceil \frac{d_{b_i} + 1}{2} \right\rceil, & \left\lceil \frac{d_{b_i} + 1}{2} \right\rceil, & \dots, & \left\lceil \frac{d_{b_i} + 1}{2} \right\rceil, & \left\lceil \frac{d_{b_i} + 1}{2} \right\rceil. \end{pmatrix}$$

Следовательно, минимальная величина  $t = t_i$  определяется равенством  $t_i = \min \{t\} = \min \{t_i^0, \dots, t_i^k, \dots, t_i^{x_i}\}$ , где

$$t_i^0 = d_{bi}(T_{zi}^{(i)} + 1); \quad t_i^1 = t_i^0 + (d_{ai} - 3T_{zi}^{(i)} + T_{zi-1}^{(i)} - 1) \left[ \frac{d_{bi} + 1}{2} \right];$$

$$t_i^k = t_i^{k-1} + (T_{zi-k+2}^{(i)} - 2T_{zi-k+1}^{(i)} + T_{zi-k}^{(i)}) \left[ \frac{d_{bi} + 1}{2} \right], \quad k = \overline{2, z_i - 1};$$

$$t_i^{z_i} = z_i^{z_i-1} + (T_{z_i}^{(i)} - 2T_{z_i-1}^{(i)} - 1) \left[ \frac{d_{bi} + 1}{2} \right].$$

Максимизируют же величину  $t_i$  такие значения  $T_k^{(i)}$ , при которых выполняются равенства  $t_i^0 = t_i^1 = \dots = t_i^{z_i}$ . Записывая эти равенства в виде  $t_i^k - t_i^{k+1} = 0$ , после очевидных преобразований получаем систему уравнений относительно  $T_k^{(i)}$

$$\begin{aligned} d_{ai} - 3T_{zi}^{(i)} + T_{zi-1}^{(i)} - 1 = 0, \quad T_{k+1}^{(i)} - 2T_k^{(i)} + T_{k-1}^{(i)} = 0, \quad k = \overline{2, z_i - 1}, \\ T_{z_i}^{(i)} - 2T_{z_i-1}^{(i)} - 1 = 0, \end{aligned} \quad (\text{П. 4. 7})$$

причем интересующая нас величина  $t_i$  равна

$$t_i = t_i^0 = (T_{zi}^{(i)} + 1) d_{bi}. \quad (\text{П. 4. 8})$$

Легко видеть, что второму соотношению (П. 4. 7) (при любом  $k$ ) удовлетворяет  $T_k^{(i)}$ , определяемое как

$$T_k^{(i)} = Ak + B, \quad (\text{П. 4. 9})$$

где  $A$  и  $B$  — произвольные постоянные. Подставляя (П. 4. 9) в первое и последнее уравнения (П. 4. 7), получаем систему уравнений относительно  $A$  и  $B$ , решая которую находим  $A = (d_{ai} + 1)/(2z_i + 1)$ ,  $B = -1$ , откуда следует, что  $T_k^{(i)} = k(d_{ai} + 1)/(2z_i + 1) - 1$  и, в частности,  $T_{z_i}^{(i)} = z_i(d_{ai} + 1)/(2z_i + 1) - 1$ . Подставляя это значение  $T_{z_i}^{(i)}$  в (П. 4. 8), окончательно получаем  $t_i = (d_{ai} + 1) d_{bi} z_i / (2z_i + 1)$ .

#### П. 4. 2. Доказательство леммы 4.3

Покажем сначала, что  $t(i, k_0) \leq t$ , где  $t < d_{ai} d_{bi} / 2$  — истинное число ошибок в принятом слове каскадного кода. Обозначим через  $t^j$  истинное

число ошибок в  $j$ -м столбце, тогда очевидно, что  $t = \sum_{j=1}^{n_b} t^j$ .

Пусть  $\hat{\gamma}_{ij} \neq \tilde{\gamma}_{ij}^{k_0} = \gamma_{ij}$  и  $\hat{\gamma}_{ij}$  не стерто. Это значит, что при декодировании внутреннего кода  $A_i$  было получено неправильное кодовое слово, расстояние до которого от принятого слова  $\hat{a}^{(j)}(i-1)$  равно  $\Delta_j(i)$ . Тогда расстояние до любого другого кодового слова кода  $A_i$ , в том числе и истинного, не меньше, чем  $d_{ai} - \Delta_j(i)$ .

Следовательно,  $d_{ai} - \Delta_j(i) = t_j(k_0) \leq t^j$ . Если же  $\hat{\gamma}_{ij} = \tilde{\gamma}_{ij}^{k_0}$  или  $\hat{\gamma}_{ij}$  — стирание, то расстояние от принятого слова  $\hat{a}^{(j)}(i-1)$  до любого кодового слова кода  $A_i$  (в том числе и истинного) не менее, чем  $\Delta_j(i)$ . Значит,  $\Delta_j(i) = t_j(k_0) \leq t^j$ .

Таким образом, во всех случаях имеем  $t_j(k_0) \leq t^j$ , что после суммирования по  $j$  приводит к неравенству  $t(i, k_0) \leq t < d_{ai} d_{bi} / 2$ . Покажем

теперь, что для любых  $\tilde{\gamma}_i^{k_1} \neq \tilde{\gamma}_i^{k_2}$  имеет место неравенство  $t(i, k_1) + t(i, k_2) \geq d_{ai}d_{bi}$ . Действительно, рассмотрим различные символы  $\tilde{\gamma}_{ij}^{k_1}$  и  $\tilde{\gamma}_{ij}^{k_2}$ , расположенные на одинаковых позициях различных кодовых слов  $\tilde{\gamma}_i^{k_1}$  и  $\tilde{\gamma}_i^{k_2}$  внешнего кода  $B_i$ . Если  $\tilde{\gamma}_{ij}^{k_1} \neq \tilde{\gamma}_{ij}^{k_2}$ , то возможен один из следующих четырех вариантов:

1)  $\hat{\gamma}_{ij}^{k_1}$  — стирание, в этом случае  $t_j(k_1) = t_j(k_2) = \Delta_j(i) = d_{ai}/2$ , так что  $t_j(k_1) + t_j(k_2) = d_{ai}$ .

Если же  $\hat{\gamma}_{ij}^{k_1}$  не стерто, то:

2)  $\tilde{\gamma}_{ij}^{k_1} = \hat{\gamma}_{ij}^{k_1}$ ,  $\tilde{\gamma}_{ij}^{k_2} \neq \hat{\gamma}_{ij}^{k_2}$ , в этом случае  $t_j(k_1) = \Delta_j(i)$ ,  $t_j(k_2) = d_{ai} - \Delta_j(i)$ , так что  $t_j(k_1) + t_j(k_2) = d_{ai}$ .

3)  $\tilde{\gamma}_{ij}^{k_1} \neq \hat{\gamma}_{ij}^{k_1}$ ,  $\tilde{\gamma}_{ij}^{k_2} = \hat{\gamma}_{ij}^{k_2}$ , в этом случае  $t_j(k_1) = d_{ai} - \Delta_j(i)$ ,  $t_j(k_2) = \Delta_j(i)$ , так что  $t_j(k_1) + t_j(k_2) = d_{ai}$ .

4)  $\tilde{\gamma}_{ij}^{k_1} \neq \hat{\gamma}_{ij}^{k_1}$ ,  $\tilde{\gamma}_{ij}^{k_2} \neq \hat{\gamma}_{ij}^{k_2}$  и  $\tilde{\gamma}_{ij}^{k_1} \neq \tilde{\gamma}_{ij}^{k_2}$  не стерто, в этом случае  $t_j(k_1) = t_j(k_2) = d_{ai} - \Delta_j(i)$ , где  $\Delta_j(i) < d_{ai}/2$ , так что  $t_j(k_1) + t_j(k_2) = 2d_{ai} - 2\Delta_j(i) > d_{ai}$ .

Таким образом, при  $\tilde{\gamma}_{ij}^{k_1} \neq \tilde{\gamma}_{ij}^{k_2}$  в любом случае имеем  $t_j(k_1) + t_j(k_2) \geq d_{ai}$ . Суммируя по  $j$  и учитывая, что слова  $\tilde{\gamma}_i^{k_1}$  и  $\tilde{\gamma}_i^{k_2}$  отличаются не менее чем в  $d_{bi}$  позициях, получаем

$$\sum_{j=1}^{n_b} t_j(k_1) + \sum_{j=1}^{n_b} t_j(k_2) = t(i, k_1) + t(i, k_2) \geq d_{ai}d_{bi}.$$

Так как  $k_1$  и  $k_2$  любые, то, полагая  $k_2 = k_0$ , для которого в соответствии с первой частью леммы  $t(i, k_0) < d_{ai}d_{bi}/2$ , имеем для  $k \neq k_0$   $t(i, k) \geq d_{ai}d_{bi} - t(i, k_0) > d_{ai}d_{bi}/2$ , что завершает доказательство леммы 4.3.

#### П.4.3. Доказательство леммы 4.4

Без ограничения общности можно считать, что пакет ошибок расположен в первых  $x$  столбцах. Пусть  $t^1$  и  $t^x$  — наибольшая возможная кратность ошибок соответственно в первом и  $x$ -м столбцах. Так как  $t^1$  может принимать  $n_a$  различных ненулевых значений, то достаточно рассмотреть эти  $n_a$  случаев.

Пусть  $t^1 \geq d_{ai}$ . Тогда в силу (4.11)  $x \leq v$ , так что  $e_k + \tau_k \leq v$ , а следовательно,  $2e_k + \tau_k \leq 2v$ .

Пусть  $d_{ai}/2 \leq t^{(1)} < d_{ai}$ . Тогда в силу (4.11) либо  $x \leq v$ , либо  $x = v + 1$ , причем в обоих случаях  $t^x \leq d_{ai} - t^1$ . Очевидно, что в первом случае лемма справедлива. Поэтому рассмотрим только второй случай, когда  $x = v + 1$ . Если  $T_k^{(i)} < t^x$ , то оба крайних столбца окажутся стерты, так что  $e_k \leq v - 1$ , и так как в этом случае  $e_k + \tau_k < v + 1$ , то получаем  $2e_k + \tau_k \leq 2v$ . Если  $T_k^{(i)} \geq t^x$ , то в последнем столбце ошибки будут исправлены, а поэтому  $e_k + \tau_k = v$ , так что снова выполняется условие  $2e_k + \tau_k \leq 2v$ .

Наконец, пусть  $1 \leq t^1 < d_a/2$ . Легко проверить, что в этом случае все возможные варианты сводятся к предыдущим, что и завершает доказательство леммы 4.4.

## П. 4.4. Доказательство леммы 4.5

Если длина одиночного пакета ошибок удовлетворяет условию  $l \leq l_i(t_{bi})$ , где  $t_{bi} = \left\lfloor \frac{d_{bi} - 1}{2} \right\rfloor$ , то, как следует из леммы 4.4, множество  $\tilde{\Gamma}(i)$  будет содержать только верные слова. Действительно, в этом случае для всех  $k$   $2e_k + \tau_k \leq 2t_{bi}$ , и все ошибки и стирания в словах  $\tilde{\gamma}_i^k$  будут исправлены  $i$ -м внешним кодом  $B_i$ . Поэтому следует рассмотреть лишь случаи, когда  $l_i(t_{bi}) < l < l_i^*$ . Как и в лемме 4.4, будем считать, что пакет ошибок расположен в первых  $x$  столбцах. Пусть  $t^{(1)}$  и  $t^x$  также обозначают наибольшую кратность ошибок в крайних столбцах, пораженных пакетом.

Пусть  $t^1 \geq d_{ai} - T\{i\}$ . Тогда  $x \leq t_{bi} + 1$ . При нечетном  $d_{bi}$  в силу (4.10) величина  $t^x \leq T_{ii}^{(i)}$ . При  $T_{ii}^{(i)} \geq t^x$  (а такие  $T_{ii}^{(i)}$  в силу условий леммы имеются) ошибки в крайнем правом столбце, пораженном пакетом ошибок, исправляются и, следовательно,  $e_k + \tau_k \leq t_{bi}$ . Но это значит, что  $\tilde{\Gamma}(i)$  содержит верное  $\tilde{\gamma}_i^k = \gamma_i^k$ . При четном  $d_{bi}$  в силу (4.10) величина  $t^x \leq d_{ai} - T\{i\} - 1$ . Тогда в первых  $x - 1 = t_{bi}$  столбцах могут быть как ошибки, так и стирания, а в последнем столбце, пораженном пакетом ошибок, только стирание. Поэтому  $2e_1 - \tau_1 \leq 2t_{bi} + 1$ , следовательно,  $\tilde{\Gamma}(i)$  содержит верное слово  $\tilde{\gamma}_i^{(1)} = \gamma_i$ .

Пусть теперь  $T_{ii}^{(i)} + 1 \leq t^{(1)} < d_{ai} - T\{i\}$ . Если  $d_{bi}$  нечетно, то нетрудно убедиться в том, что в обоих крайних столбцах, пораженных пакетом ошибок, число ошибок меньше, чем  $d_{ai} - T\{i\}$ . Следовательно, при  $T\{i\}$  получаем  $e_1 \leq t_{bi} - 1$ , а  $e_1 + \tau_1 \leq t_{bi} + 1$ , т. е.  $2e_1 + \tau_1 \leq 2t_{bi} < d_{bi}$ , значит,  $\tilde{\Gamma}(i)$  содержит верное слово  $\tilde{\gamma}_i^{(1)} = \gamma_i$ . Если  $d_{bi}$  четно, то в силу условия  $t^{(1)} < d_{ai} - T\{i\}$  в первом столбце может иметь место только стирание, поэтому (как уже отмечалось выше)  $2e_1 - \tau_1 \leq 2t_{bi} + 1 < d_{bi}$ . Следовательно,  $\tilde{\Gamma}(i)$  содержит верное слово  $\tilde{\gamma}_i^{(1)} = \gamma_i$ . Наконец, в случае, когда  $1 \leq t^1 \leq T_{ii}^{(i)}$ , все возможные варианты сводятся к предыдущим, что и завершает доказательство леммы 4.5.

## П.4.5. Доказательство леммы 4.6

Рассмотрим два слова  $\tilde{\gamma}_i^{k_0}$  и  $\tilde{\gamma}_i^k$ , которым в силу процедуры  $\psi_i^q(z_i)$  ставятся в соответствие параметры  $t(i, k_0)$  и  $t(i, k)$ .

При этом двум символам  $\tilde{\gamma}_{ij}^{k_0} \neq \tilde{\gamma}_{ij}^k$  соответствуют параметры  $t_j(k_0)$  и  $t_j(k)$ , такие, что  $t_j(k_0) + t_j(k) \geq d_{ai}$ . С другой стороны, два различных слова  $\tilde{\gamma}_i^{k_0}$  и  $\tilde{\gamma}_i^k$  будут различаться не менее чем в  $d_{bi}$  столбцах. Так как

$$t(i, k) = \sum_{j=1}^{n_b} t_j(k), \text{ получаем } t(i, k_0) + t(i, k) \geq d_{ai} d_{bi}.$$

Покажем теперь, что  $t(i, k_0) < d_{ai} d_{bi} / 2$ . Без ограничения общности будем предполагать, что пакет ошибок расположен в первых  $x$  столбцах. Кроме того, будем учитывать, что  $t_j(k_0) \leq t^x$  — истинное число ошибок в  $j$ -м столбце (см. доказательство леммы 4.3).

Пусть  $d_{bi}$  нечетно. В силу процедуры  $\psi_i^q(z_i)$   $t_j(k_0) \leq d_{ai}$  для  $j \leq x$  и  $t_j(k_0) = 0$  для  $j > x$ . Если  $x \leq t_{bi}$ , то  $t(i, k_0) < d_{ai} t_{bi} < d_{ai} d_{bi} / 2$ . Если  $x = t_{bi} + 1$  ( $x \geq t_{bi} + 2$  в этом случае невозможно), то в силу условия



леммы  $t^1 + t^x \leq d_{ai} + t_{ai}$ . Поэтому  $t_1(k_0) + t_x(k_0) \leq t^1 + t^x \leq d_{ai} + t_{ai}$ . Но  $t_j(k_0) \leq d_{ai}$  при  $j = 2, x-1$  и  $t_j(k_0) = 0$  при  $j > x$ . Отсюда

$$\begin{aligned} t(i, k_0) &= \sum_{j=1}^{n_b} t_j(k_0) \leq d_{ai} + t_{ai} + d_{ai}(x-2) = \\ &= d_{ai} + t_{ai} + d_{ai}(t_{bi} - 1) = d_{ai}t_{bi} + t_{ai} < d_{ai}d_{bi}/2, \end{aligned}$$

что завершает доказательство в случае нечетного  $d_{bi}$ . Случай четного  $d_{bi}$  доказывается аналогичным образом с учетом лишь того факта, что теперь  $t_1(k_0) + t_x(k_0) \leq 2d_{bi} - 1$ .

#### П.4.6. Доказательство леммы 4.7

Условно разделим на две части корректирующую способность  $i$ -го внешнего кода, которая, как известно, определяется его кодовым расстоянием  $d_{bi}$ . Часть этого расстояния, равную  $2\rho_i$ , будем использовать для исправления ошибок  $e'_k$  и стираний  $\tau'_k$ , обусловленных пакетами ошибок. Оставшуюся часть этого кодового расстояния, равную  $d_{bi} - 2\rho_i$ , будем использовать для исправления ошибок  $e''_k$  и стираний  $\tau''_k$ , обусловленных независимыми ошибками. Формально это соответствует требованию, чтобы при некотором  $T_k^{(i)}$  одновременно с неравенством  $2e_k + \tau_k \leq d_{bi}$ , где  $e_k = e'_k + e''_k$  и  $\tau_k = \tau'_k + \tau''_k$ , выполнялись неравенства

$$2e'_k + \tau'_k \leq 2\rho_i, \quad (\text{П. 4. 10})$$

$$2e''_k + \tau''_k < d_{bi} - 2\rho_i. \quad (\text{П. 4. 11})$$

Тогда из леммы 4.4 и соотношения (4.17) следует, что (П. 4.10) будет выполнено при всех  $T_k^{(i)}$ . В свою очередь из леммы 4.2 и соотношений (4.15) и (4.16) следует, что (П. 4.11) будет выполнено по крайней мере для одного значения  $T_k^{(i)}$ . Следовательно, множество  $\tilde{\Gamma}(i)$  будет содержать верное слово  $\tilde{\gamma}_i^k = \gamma_i$ , что завершает доказательство леммы.

#### П.4.7. Доказательство леммы 4.8

Рассмотрим два слова  $\tilde{\gamma}^k$  и  $\tilde{\gamma}_i^k$ . Нетрудно убедиться (см. доказательство леммы 4.6), что в силу процедуры  $\psi_i^q(z_i)$  имеют место неравенства

$$t(i, k_0) + t(i, k) \geq d_{ai}d_{bi}, \quad (\text{П. 4. 12})$$

$$t_j(k_0) \leq \min \{t^j; d_{ai}\}, \quad (\text{П. 4. 13})$$

где  $t^j$  — истинное число ошибок в  $j$ -м столбце.

Покажем теперь, что  $t(i, k_0) < d_{ai}d_{bi}/2$ . В силу определения величины  $t(i, k_0)$  можно представить как  $t(i, k_0) = t^*(i, k_0) + t'(i, k_0)$ . Здесь

$$\begin{aligned} t^*(i, k_0) &= \sum_{j \in I^*} t_j(k_0), \\ t'(i, k_0) &= \sum_{j \in I'} t_j(k_0), \end{aligned} \quad (\text{П. 4. 14})$$

где  $I^*$ ,  $I'$  — множество номеров столбцов, пораженных соответственно независимыми ошибками, пакетами ошибок.

Из (П. 4. 13), (П. 4. 14) и условий теоремы 4.3 непосредственно получаем

$$t^*(i, k_0) = \sum_{j \in J^*} t_j(k_0) \leq \sum_{j \in J^*} t^j = t < (d_{bt} - 2\rho_i) d_{at}/2. \quad (\text{П. 4. 15})$$

Параметр  $t'(i, k_0)$  представим в виде

$$t'(i, k_0) = \sum_{u=1}^v t^{(u)}(i, k_0), \quad (\text{П. 4. 16})$$

где  $t^{(u)}(i, k_0)$  — параметр, обусловленный только  $u$ -м пакетом ошибок.

Покажем, теперь, что в условиях леммы имеет место соотношение

$$t^{(u)}(i, k_0) \leq v_{ut} d_{at}. \quad (\text{П. 4. 17})$$

Без ограничения общности можно считать, что  $u$ -й пакет ошибок поразил первые  $x$  столбцов. В этом случае

$$t^{(u)}(i, k_0) = \sum_{j=1}^x t_j(k_0). \quad (\text{П. 4. 18})$$

Если  $x \leq v_{ut}$ , то из (П. 4. 18) с учетом (П. 4. 13) следует (П. 4. 17). Если  $x = v_{ut} + 1$  (случай  $x > v_{ut} + 1$  невозможен), то  $t^1 + t^x \leq d_{at}$  и  $t^j \leq d_{at}$ ,  $j = \overline{2, x-1}$ . Подставляя оценки  $t_j(k_0)$  в (П. 4. 18), получаем (П. 4. 17). Из (П. 4. 16) и (П. 4. 17) с учетом (4. 17) имеем

$$t'(i, k_0) \leq \sum_{u=1}^v v_{ut} d_{at} = \rho_i d_{at}. \quad (\text{П. 4. 19})$$

Неравенства (П. 4. 15), (П. 4. 19) и (П. 4. 12) доказывают лемму 4.8.

#### П.4.8. Доказательство леммы 4.9

Как было показано в гл. 1 (теорема 1.5 и утверждение 1.2), оценки экспонент вероятности ошибки  $E_e(R, v)$  и стирания  $E_\tau(R, v)$  соответственно равны  $E_e(R, v) = E_0(R) + h'v$ ,  $E_\tau(R, v) = E_0(R) - h'v$ ,  $v > 0$ . Однако эти оценки были получены в предположении, что слово, полученное в результате декодирования, удовлетворяет условию

$$\log_2 \{P(\hat{a}^{(j)}(i-1) | \hat{a}^{(j)}(i)) / P(\hat{a}^{(j)}(i-1) | x)\} \geq v n_a, \quad (\text{П. 4. 20})$$

где  $x \neq \hat{a}^{(j)}(i)$  — слово кода  $A_i$ , для которого вероятность  $P(\hat{a}^{(j)}(i-1) | x)$  максимальна.

В работе Форни [141 (теорема 1)] показано, что при любом критерии, отличном от (4. 35), имеют место следующие неравенства: если  $P_{ст} \geq P'_{ст}$ , то  $P_{ом} \leq P'_{ом}$ , где  $P_{ст}$  и  $P_{ом}$  получены в соответствии с критерием (4. 35), а  $P'_{ст}$  и  $P'_{ом}$  получены в соответствии с любым другим критерием.

Из сравнения критериев (4. 35) и (П. 4. 20) следует, что зона приема, соответствующая критерию (4. 35), содержится в зоне приема, соответствующей критерию (П. 4. 20) при всех значениях  $v$ . Отсюда вытекает справедливость леммы 4.9.

#### П.4.9. Доказательство леммы 4.10

Рассмотрим два случая  $\alpha^{(j)}(i) = \tilde{\alpha}^{(j)}(i)$  и  $\alpha^{(j)}(i) \neq \tilde{\alpha}^{(j)}(i)$ . Первый случай имеет место при  $v_i^j \geq v \geq 0$  и не произойдет при  $v_i^j < v$ . Отсюда следует, что вероятность события  $D_i^j$  оценивается вероятностью стирания при  $v = v_i^j$ , т. е. в соответствии с леммой 4.9 имеем  $P(D_i^j) \leq 2^{-n_a(E_0(R_{ai}) - h_i v_i^j)}$ . Тогда в соответствии с (4.31) получаем доказательство леммы 4.10 для этого случая.

Рассмотрим случай  $\alpha^{(j)}(i) \neq \tilde{\alpha}^{(j)}(i)$ , т. е. ошибочное декодирование. В начале покажем, что в этом случае  $v_i^j < 0$ . Пусть при некотором  $v \geq 0$  получено слово  $\tilde{\alpha}^{(j)}(i) \neq \alpha^{(j)}(i)$ . Из этого следует, что

$$\frac{P(\hat{\alpha}^{(j)}(i-1) | \tilde{\alpha}^{(j)}(i))}{\sum_{\substack{x \in A_i \\ x \neq \tilde{\alpha}^{(j)}(i)}} P(\hat{\alpha}^{(j)}(i-1) | x)} \geq 2^{n_a} \geq 1.$$

Тогда

$$\frac{P(\hat{\alpha}^{(j)}(i-1) | \alpha^{(j)}(i))}{\sum_{\substack{x \in A_i \\ x \neq \alpha^{(j)}(i)}} P(\hat{\alpha}^{(j)}(i-1) | x)} < 1.$$

Следовательно,  $v_i^j < 0$ . Тогда выберем  $v = -v_i^j$ . В этом случае  $P(D_i^j) \leq P_{\text{ом}}$ , для которой в соответствии с леммой 4.9 имеем  $P(D_i^j) \leq 2^{-n_a(E_0(R_{ai}) + h_i v)}$ . Учитывая, что по определению  $F_i^{(j)} = (E_0(R_{ai}) - h_i v_i^j) n_a$  и  $v = -v_i^j$ , получаем доказательство леммы 4.10 и в случае, когда  $\tilde{\alpha}^{(j)}(i) \neq \alpha^{(j)}(i)$ .

#### П.4.10. Доказательство леммы 4.11

Оценим наименьшее значение параметра  $F_i$ , при котором процедура  $\psi_i^k(z_i)$  может привести к тому, что все  $\hat{\gamma}_i^k \in \bar{\Gamma}(i)$  окажутся неверными. Для этого необходимо, чтобы для всех критериев  $T_k^{(i)}$  число ошибок  $e_k$  и стираний  $\tau_k$  в словах  $\hat{\gamma}_i^k$  удовлетворяло условию

$$2e_k + \tau_k \geq d_{bi}. \quad (\text{П. 4. 21})$$

Обозначим через  $N_s$  число столбцов  $\hat{\alpha}^{(j)}(i-1)$  в слове  $\hat{\alpha}(i-1)$ , в каждом из которых значение параметра  $F_i^{(j)} = s$ . В этом случае имеем очевидное равенство

$$F_i = \sum_{j=1}^{n_b} F_i^{(j)} = \sum_s s N_s. \quad (\text{П. 4. 22})$$

Отметим, что для любого принятого слова  $\hat{\alpha}(i-1)$  величина  $s$  принимает не более чем  $n_b$  значений.

В соответствии с определением  $\hat{\gamma}_i^k$  (см. п. 4 процедуры  $\psi_i^k(z_i)$ ) для того, чтобы слово  $\hat{\gamma}_i^k$  не содержало ни ошибок, ни стираний, надо, чтобы при всех  $j = \overline{1, n_b}$  выполнялись условия  $\hat{\alpha}^{(j)}(i) = \alpha^{(j)}(i)$  (т. е.  $\tilde{v}_i^j = v_i^j$ )

и  $v_i^j \geq T_k^{(i)}$ . Но в этом случае  $F_i^{(j)} = n_a(E_0(R_{ai}) - h_i v_i^j) \leq n_a(E_0(R_{ai}) - h_i T_k^{(i)})$ . Следовательно, ошибки или стирания будут иметь место только в тех столбцах, для которых  $s > n_a(E_0(R_{ai}) - h_i T_k^{(i)})$ , т. е.

$$e_k + \tau_k = \sum_{s > n_a(E_0(R_{ai}) - h_i T_k^{(i)})} N_s. \quad (\text{П. 4. 23})$$

Для того чтобы в слове  $\hat{r}_i^k$  произошла ошибка, надо, чтобы в соответствующем столбце выполнялись условия  $\hat{a}^{(j)}(i) \neq a^{(j)}(i)$ ,

$$\frac{1}{n_a} \log \frac{P(\hat{a}^{(j)}(i-1) | \hat{a}^{(j)}(i))}{\sum_{\substack{x \in A_i \\ x \neq \hat{a}^{(j)}(i)}} P(\hat{a}^{(j)}(i-1) | x)} \geq T_k^{(i)}. \quad (\text{П. 4. 24})$$

Но

$$\frac{\sum_{\substack{x \in A_i \\ x \neq \hat{a}^{(j)}(i)}} P(\hat{a}^{(j)}(i-1) | x)}{P(\hat{a}^{(j)}(i-1) | \hat{a}^{(j)}(i))} > \frac{P(\hat{a}^{(j)}(i-1) | a^{(j)}(i))}{\sum_{\substack{x \in A_i \\ x \neq a^{(j)}(i)}} P(\hat{a}^{(j)}(i-1) | x)}.$$

Следовательно, из (П. 4. 24) и из определения  $v_i^j$  получаем  $2^{-n_a T_k^{(i)}} > 2^{-n v_i^j}$  или

$$v_i^j < T_k^{(i)}. \quad (\text{П. 4. 25})$$

Но это значит, что ошибки в слове  $\hat{r}_i^k$  возможны только для тех  $j$ , для которых  $s = F_i^{(j)} = n_a(E_0(R_{ai}) - h_i v_i^j) > n_a(E_0(R_{ai}) + h_i T_k^{(i)})$ , т. е.

$$e_k \leq \sum_{s > n_a(E_0(R_{ai}) + h_i T_k^{(i)})} N_s. \quad (\text{П. 4. 26})$$

Из (П. 4. 26) и (П. 4. 23) вытекает, что

$$\tau_k \geq \sum_{s > n_a(E_0(R_{ai}) + h_i T_k^{(i)})} N_s. \quad (\text{П. 4. 27})$$

Таким образом, задача сводится к определению наименьшего значения  $F_i$ , определяемого равенством (П. 4. 22), при котором для всех  $T_k^{(i)}$ ,  $k=1, \dots, x_i$ , одновременно выполняются условия (П. 4. 21), (П. 4. 23), (П. 4. 26) и (П. 4. 27). В силу линейности этих условий указанная задача является типичной задачей линейного программирования. Известно, что в этом случае решение находится на границе, что соответствует замене неравенств в (П. 4. 26) и (П. 4. 27) равенствами.

Учитывая, что  $T_k^{(i)} < T_{k+1}^{(i)}$  и, следовательно,  $e_k \geq e_{k+1}$ ,  $\tau_k \leq \tau_{k+1}$ , получаем

$$e_{s_i} = \sum_{s > n_a(E_0(R_{ai}) + h_i T_{s_i}^{(i)})} N_s, \quad e_k - e_{k+1} = \sum_{s > n_a(E_0(R_{ai}) + h_i T_{k+1}^{(i)})} N_s.$$

$$\tau_{k+1} - \tau_k - (e_k - e_{k+1}) = \sum_{s > n_a(E_0(R_{ai}) - h_i T_k^{(i)})}^{n_a(E_0(R_{ai}) - h_i T_k^{(i)})} N_s,$$

$$\tau_1 = \sum_{s > n_a(E_0(R_{ai}) - h_i T_1^{(i)})}^{n_a(E_0(R_{ai}) + h_i T_1^{(i)})} N_s.$$

Заметим, что полученные условия состоят из  $2z_i$  условий с непрерывными индексами. При этом задача минимизации  $F_i$  сводится к задаче минимизации на каждом из  $2z_i$  диапазонов изменения  $s$ . Но на любом из них задача, в свою очередь, сводится к выбору такого набора величин  $N_s$ , который минимизирует  $\sum s N_s$  при заданном значении  $\sum N_s$ . В силу линейности формы и условия, что на каждом из диапазонов изменения задана,  $s \sum N_s$  минимум достигается на границе. Это значит, что в данном случае все  $N_s$ , кроме одного, следует положить равными нулю, а в качестве ненулевого выбрать  $N_s$  с наименьшим значением  $s$ .

Таким образом, приведенные выше условия принимают вид

$$e_{z_i} = N_{n_a(E_0(R_{ai}) + h_i T_{z_i}^{(i)})}, \quad e_k - e_{k+1} = N_{n_a(E_0(R_{ai}) + h_i T_k^{(i)})},$$

$$\tau_{k+1} - \tau_k - (e_k - e_{k+1}) = N_{n_a(E_0(R_{ai}) - h_i T_{k+1}^{(i)})}, \quad (\text{П. 4. 28})$$

$$\tau_1 = N_{n_a(E_0(R_{ai}) - h_i T_1^{(i)})}.$$

Разбивая сумму (П. 4. 22) на  $2z_i$  сумм с соответствующими диапазонами суммирования и подставляя в каждую из них минимизирующие значения  $N_s$ , определяемые (П. 4. 28), получаем

$$F_i = \tau_1 (E_0(R_{ai}) - h_i T_1^{(i)}) n_a + \sum_{k=1}^{z_i-1} (\tau_{k+1} - \tau_k - e_k + e_{k+1}) (E_0(R_{ai}) -$$

$$- h_i T_{k+1}^{(i)}) n_a + \sum_{k=1}^{z_i-1} (e_k - e_{k+1}) (E_0(R_{ai}) + h_i T_k^{(i)}) n_a +$$

$$+ e_{z_i} (E_0(R_{ai}) + h_i T_{z_i}^{(i)}) n_a. \quad (\text{П. 4. 29})$$

Как уже указывалось выше, для минимизации  $F_i$  знак неравенства в (П. 4. 21) надо заменить знаком равенства, т. е. положить  $2e_k + \tau_k = d_{bi}$ . Отсюда следует, что

$$\tau_k = d_{bi} - 2e_k, \text{ если } 2e_k \leq d_{bi}, \quad \tau_k = 0, \text{ если } 2e_k > d_{bi}.$$

В силу условия  $\tau_k \leq \tau_{k+1}$  при  $\tau_{k+1} = 0$  разность  $\tau_{k+1} - \tau_k = 0$ . Но в этом случае минимум (П. 4. 29) достигается при наименьшем значении  $e_k$ , при котором  $\tau_k = 0$ , т. е. при

$$e_k = \left\lceil \frac{d_{bi} + 1}{2} \right\rceil,$$

где  $[x]$  — целая часть  $x$ . Отсюда следует, что при минимизации (П. 4. 29) достаточно рассмотреть лишь случай, когда

$$e_k \leq \left\lceil \frac{d_{bi} + 1}{2} \right\rceil.$$

Тогда после элементарных преобразований выражения (П. 4. 29) получаем

$$F_i = d_{bi} (E_0 (R_{ai}) - h_i T_1^{(i)}) n_a + e_1 (3T_1^{(i)} - T_2^{(i)}) h_i n_a + \\ + h_i n_a \sum_{k=2}^{z_i-1} e_k (2T_k^{(i)} - T_{k+1}^{(i)} - T_{k-1}^{(i)}) + \\ + e_{z_i} (2h_i T_{z_i}^{(i)} - E_0 (R_{ai}) - h_i T_{z_i-1}^{(i)}) n_a.$$

Так как  $F_i$  является линейной функцией переменных  $e_k$ ,  $k = \overline{1, z_i}$ , то наименьшее значение  $F_i$  может достигаться в одной или нескольких граничных точках  $(e_1, e_2, \dots, e_{z_i})$ , которые имеют вид

$$\begin{pmatrix} 0, & 0, & \dots, & 0 \end{pmatrix}, \\ \begin{pmatrix} 0, & 0, & \dots, & [(d_{bi} + 1)/2] \end{pmatrix}, \\ \vdots \\ \begin{pmatrix} [(d_{bi} + 1)/2], & [(d_{bi} + 1)/2], & \dots, & [(d_{bi} + 1)/2] \end{pmatrix}.$$

Следовательно, минимальная величина  $F_i = F_i^*$  определяется равенством

$$F_i^* = \min \{F_i^{*0}, F_i^{*1}, \dots, F_i^{*z_i}\}, \text{ где}$$

$$F_i^{*0} = d_{bi} (E_0 (R_{ai}) - h_i T_1^{(i)}) n_a, F_i^{*1} = F_i^{*0} + (3T_1^{(i)} - T_2^{(i)}) h_i [(d_{bi} + 1)/2] n_a,$$

$$F_i^{*k} = F_i^{*k-1} + (2T_k^{(i)} - T_{k+1}^{(i)} - T_{k-1}^{(i)}) h_i [(d_{bi} + 1)/2] n_a, \quad k = \overline{2, z_i - 1},$$

$$F_i^{*z_i} = F_i^{*z_i-1} + (2h_i T_{z_i}^{(i)} - E_0 (R_{ai}) - h_i T_{z_i-1}^{(i)}) [(d_{bi} + 1)/2] n_a.$$

Максимизируют же величину  $F_i^*$  такие значения  $T_k^{(i)}$ , при которых выполняются равенства  $F_i^{*0} = F_i^{*1} = \dots = F_i^{*z_i}$ . Записывая эти равенства в виде  $F_i^{*k} - F_i^{*k-1} = 0$ , после очевидных преобразований получаем систему уравнений относительно  $T_k^{(i)}$

$$3T_1^{(i)} - T_2^{(i)} = 0, \quad 2T_k^{(i)} - T_{k+1}^{(i)} - T_{k-1}^{(i)} = 0; \quad k = \overline{2, z_i - 1},$$

$$2h_i T_{z_i}^{(i)} - E_0 (R_{ai}) - h_i T_{z_i-1}^{(i)} = 0. \quad (\text{П. 4. 30})$$

При этом искомая величина  $F_i^*$  равна

$$F_i^* = F_i^{*0} = d_{bi} n_a (E_0 (R_{ai}) - h_i T_1^{(i)}). \quad (\text{П. 4. 31})$$

Легко видеть, что второму соотношению (П. 4. 30) при любом  $k$  удовлетворяет величина  $T_k^{(i)}$ , определяемая равенством

$$T_k^{(i)} = Ak + B, \quad (\text{П. 4. 32})$$

где  $A$  и  $B$  — произвольные постоянные.

Подставляя (П. 4. 32) в первое и последнее соотношения (П. 4. 30), получаем систему уравнений относительно  $A$  и  $B$ , решая которую находим  $A = 2E_0 (R_{ai}) / (h_i (2z_i + 1))$ ;  $B = -E_0 (R_{ai}) / (h_i (2z_i + 1))$ , откуда следует, что

$$T_k^{(i)} = (2k + 1) / (h_i (2z_i + 1)). \quad (\text{П. 4. 33})$$

Подставляя (П. 4. 33) при  $k = 1$  в (П. 4. 31), получаем  $F_i^* = d_{bi} n_a E_0 (R_{ai}) \times \times 2z_i / (2z_i + 1)$ . Отсюда, учитывая, что  $d_{bi} = (1 - R_{bi}) n_b$  и  $n = n_a n_b$ , имеем

$$F_i^* = (1 - R_{bi}) E_0 (R_{ai}) n 2z_i / (2z_i + 1). \quad (\text{П. 4. 34})$$

Так как  $F_i^*$ , задаваемое (П. 4.34), при выборе критериев  $T_i^{(j)}$  согласно (П. 4.33) является наименьшим значением  $F_i$ , при котором в списке  $\tilde{\Gamma}(i)$  может не оказаться правильного слова, то получаем доказательство леммы 4.11.

#### П.4.11. Доказательство леммы 4.12

Сначала покажем, что  $E(i, k_0) \leq F_i < nE_0(R_{ai})(1 - R_{bi})$ . Пусть  $\gamma_{ij} = \tilde{\gamma}_{ij}^{k_0} \neq \hat{\gamma}_{ij}$  и  $\tilde{\gamma}_{ij}$  не стерто, где  $\hat{\gamma}_{ij}$  определяется (4.6) (см. п. 3 процедуры  $\psi_j^p(z_i)$ ). Это значит, что при декодировании внутреннего кода  $A_i$  было получено неправильное кодовое слово; т. е.  $\hat{\alpha}^{(j)}(i) \neq \alpha^{(j)}(i)$ . В силу П. 6 процедуры  $\psi_j^p(z_i)$  величина  $E_j(k_0)$  в этом случае определяется равенством  $E_j(k_0) = E_0(R_{ai}) + h_i \Delta_j(i) n_a$ , где

$$\Delta_j(i) = \frac{1}{n_a} \log_2 \frac{P(\hat{\alpha}^{(j)}(i-1) | \hat{\alpha}^{(j)}(i))}{\sum_{\substack{x \in A_i \\ x \neq \hat{\alpha}^{(j)}(i)}} P(\hat{\alpha}^{(j)}(i-1) | x)},$$

а параметр  $F_i^{(j)}$  — равенством  $F_i^{(j)} = (E_0(R_{ai}) - h_i v_i^j) n_a$ . Для выполнения неравенства  $E_j(k_0) \leq F_i^{(j)}$  необходимо и достаточно, чтобы

$$\Delta_j(i) \leq -v_i^j. \quad (\text{П. 4.35})$$

Неравенство (П. 4.35) с учетом определения  $\Delta_j^{(i)}$  и  $v_i^j$  может быть записано в виде неравенства

$$\frac{P(\hat{\alpha}^{(j)}(i-1) | \hat{\alpha}^{(j)}(i))}{\sum_{\substack{x \in A_i \\ x \neq \hat{\alpha}^{(j)}(i)}} P(\hat{\alpha}^{(j)}(i-1) | x)} \leq \frac{\sum_{\substack{x \in A_i \\ x \neq \alpha^{(j)}(i)}} P(\hat{\alpha}^{(j)}(i-1) | x)}{P(\hat{\alpha}^{(j)}(i-1) | \alpha^{(j)}(i))},$$

выполнение которого очевидно.

Пусть  $\tilde{\gamma}_{ij} = \hat{\gamma}_{ij}^{k_0}$ , тогда, чтобы выполнялось неравенство  $E_j(k_0) = (E_0(R_{ai}) - h_i \Delta_j(i)) n_a \leq F_i^{(j)} = (E_0(R_{ai}) - h_i v_i^j) n_a$ , необходимо и достаточно, чтобы  $\Delta_j(i) \geq v_i^j$  или

$$\frac{P(\hat{\alpha}^{(j)}(i-1) | \hat{\alpha}^{(j)}(i))}{\sum_{\substack{x \in A_i \\ x \neq \hat{\alpha}^{(j)}(i)}} P(\hat{\alpha}^{(j)}(i-1) | x)} \geq \frac{P(\hat{\alpha}^{(j)}(i-1) | \alpha^{(j)}(i))}{\sum_{\substack{x \in A_i \\ x \neq \alpha^{(j)}(i)}} P(\hat{\alpha}^{(j)}(i-1) | x)}.$$

Выполнение последнего неравенства очевидно при  $\hat{\alpha}^{(j)}(i) = \alpha^{(j)}(i)$ , а при  $\hat{\alpha}^{(j)}(i) \neq \alpha^{(j)}(i)$  оно вытекает из условия  $\Delta_j(i) \geq 0$ , что эквивалентно неравенству

$$P(\hat{\alpha}^{(j)}(i-1) | \hat{\alpha}^{(j)}(i)) \geq P(\hat{\alpha}^{(j)}(i-1) | \alpha^{(j)}(i)) + \\ + \sum_{\substack{x \in A_i \\ x \neq \hat{\alpha}^{(j)}(i) \\ x \neq \alpha^{(j)}(i)}} P(\hat{\alpha}^{(j)}(i-1) | x).$$

Если же  $\hat{\gamma}_{ij}$  — стирание, то  $E_j(k_0) = n_a E_0(R_{at})$ . Очевидно, что в этом случае  $v_i^j \leq 0$ , так что  $E_j(k_0) = n_a E_0(R_{at}) \leq n_a (E_0(R_{at}) - h_i v_i^j) = F_i^{(j)}$ . Таким образом, приходим к выводу, что во всех случаях  $E_j(k_0) \leq F_i^{(j)}$ . Отсюда

$$\text{следует, что } E(i, k_0) = \sum_{j=1}^{n_b} E_j(k_0) \leq \sum_{j=1}^{n_b} F_i^{(j)} = F_i < n E_0(R_{at}) (1 - R_{bt}).$$

Покажем теперь, что для любых двух слов  $\tilde{\gamma}_{ij}^{k_1} \neq \tilde{\gamma}_{ij}^{k_2}$  имеет место неравенство  $E(i, k_1) + E(i, k_2) \geq 2n E_0(R_{at}) (1 - R_{bt})$ . Действительно, рассмотрим различные символы  $\tilde{\gamma}_{ij}^{k_1}$  и  $\tilde{\gamma}_{ij}^{k_2}$ , расположенные на одинаковых позициях, различных кодовых слов  $\tilde{\gamma}_{ij}^{k_1}$  и  $\tilde{\gamma}_{ij}^{k_2}$  внешнего кода  $B_t$ . В этом случае возможен один из следующих четырех вариантов:

1)  $\hat{\gamma}_{ij}$  — стирание, тогда  $E_j(k_1) = E_j(k_2) = n_a E_0(R_{at})$ , отсюда  $E_j(k_1) + E_j(k_2) = 2n_a E_0(R_{at})$ ;

если же  $\hat{\gamma}_{ij}$  не стерто, то:

2)  $\tilde{\gamma}_{ij}^{k_1} = \hat{\gamma}_{ij}$ ,  $\tilde{\gamma}_{ij}^{k_2} \neq \hat{\gamma}_{ij}$ , тогда в силу процедуры  $\psi_j^p(z_i)$  имеем  $E_j(k_1) = (E_0(R_{at}) - h_i \Delta_j(i)) n_a$ ,  $E_j(k_2) = (E_0(R_{at}) + h_i \Delta_j(i)) n_a$ , отсюда  $E_j(k_1) + E_j(k_2) = 2n_a E_0(R_{at})$ ;

3)  $\tilde{\gamma}_{ij}^{k_1} \neq \hat{\gamma}_{ij}$ ,  $\tilde{\gamma}_{ij}^{k_2} = \hat{\gamma}_{ij}$ , тогда в силу процедуры  $\psi_j^p(z_i)$  имеем  $E_j(k_1) = (E_0(R_{at}) + h_i \Delta_j(i)) n_a$ ,  $E_j(k_2) = (E_0(R_{at}) - h_i \Delta_j(i)) n_a$ , отсюда  $E_j(k_1) + E_j(k_2) = 2n_a E_0(R_{at})$ ;

4)  $\tilde{\gamma}_{ij}^{k_1} \neq \hat{\gamma}_{ij}$ ,  $\tilde{\gamma}_{ij}^{k_2} \neq \hat{\gamma}_{ij}$ , тогда в силу процедуры  $\psi_j^p(z_i)$  имеем  $E_j(k_1) = (E_0(R_{at}) + h_i \Delta_j(i)) n_a$ ,  $E_j(k_2) = (E_0(R_{at}) + h_i \Delta_j(i)) n_a$ , отсюда  $E_j(k_1) + E_j(k_2) = 2n_a (E_0(R_{at}) + h_i \Delta_j(i)) \geq 2n_a E_0(R_{at})$ .

Таким образом, при  $\tilde{\gamma}_{ij}^{k_1} \neq \tilde{\gamma}_{ij}^{k_2}$  во всех случаях имеем  $E_j(k_1) + E_j(k_2) \geq 2n_a E_0(R_{at})$ . Суммируя по  $j$  и учитывая, что слова  $\tilde{\gamma}_{ij}^{k_1}$  и  $\tilde{\gamma}_{ij}^{k_2}$  отличаются

друг от друга не менее чем в  $d_{bt}$  позициях, получаем  $\sum_{j=1}^{n_b} (E_j(k_1) +$

$+ E_j(k_2)) \geq 2n_a E_0(R_{at}) d_{bt}$ . Учитывая, что  $\sum_{j=1}^{n_b} E_j(k) = E(i, k)$  и  $d_{bt} = n_b (1 - R_{bt})$ , окончательно имеем  $E(i, k_1) + E(i, k_2) \geq 2n E_0(R_{at}) (1 - R_{bt})$ .

Так как  $k_1$  и  $k_2$  любые, то, полагая  $k_2 = k_0$ , для которого, как было показано выше,  $E(i, k_0) < n E_0(R_{at}) (1 - R_{bt})$ , имеем для любого  $k \neq k_0$   $E(i, k) \geq 2n E_0(R_{at}) (1 - R_{bt}) - E(i, k_0) > n E_0(R_{at}) (1 - R_{bt})$ , что завершает доказательство леммы 4.12.



## ПРИЛОЖЕНИЕ П.5

### П.5.1. Доказательство соотношения (5.1)

Обозначим через  $b_k(w)$  число кодов из ансамбля, для которых выбранное  $k$ -е слово веса  $w$  является кодовым словом. Тогда

$$P_k(w) = b_k(w)/S, \quad k = \overline{1, B(w)}, \quad (\text{П.5.1})$$

где  $S$  — объем ансамбля.

Найдем теперь среднее по ансамблю число кодовых слов  $\bar{N}(w)$  веса  $w$ , равное

$$\bar{N}(w) = S^{-1} \sum_{s=1}^S N_s(w),$$

где  $N_s(w)$  — число кодовых слов веса  $w$  в  $s$ -м коде. Но  $\sum_{s=1}^S N_s(w) = \sum_{k=1}^{B(w)} b_k(w)$ , так что согласно (П.5.1)

$$\bar{N}(w) = S^{-1} \sum_{k=1}^{B(w)} b_k(w) = \sum_{k=1}^{B(w)} P_k(w).$$

### П.5.2. Доказательство утверждения 5.1

Обозначим  $\bar{N}_n(w)$  и  $\bar{N}_x(w)$  — среднее по ансамблю число кодовых слов веса  $w$  — соответственно в «плохих» и «хороших» кодах. Очевидно, что  $\bar{N}(w) = \xi \bar{N}_n(w) + (1 - \xi) \bar{N}_x(w)$  и, следовательно,  $(1 - \xi) \bar{N}_x(w) \leq \bar{N}(w)$  или  $\bar{N}_x(w) \leq \bar{N}(w)/(1 - \xi)$ .

Так как для любой случайной величины  $\bar{\vartheta}$  и ее среднего значения  $\bar{\vartheta}$

$$P(\bar{\vartheta} \geq a\bar{\vartheta}) < 1/a, \quad (\text{П.5.2})$$

то  $P\{N_x(w) \geq a\bar{N}(w)/(1 - \xi)\} \leq P\{N_x(w) \geq a\bar{N}_x(w)\} \leq 1/a$ .

Полагая  $a = (1 - \xi)f(n)$ , получаем  $P\{N_x(w) \geq f(n)\bar{N}(w)\} \leq [(1 - \xi)f(n)]^{-1}$ .

Таким образом, вероятность того, что для случайного кода, выбранного из подмножества только «хороших» кодов (данного ансамбля), для всех  $w > (\delta^* - \varepsilon)n$  имеет место неравенство  $N_x(w) \geq f(n)\bar{N}(w)$  и оценивается сверху выражением

$$Q \leq \sum_{w=(\delta^*-\varepsilon)n}^n P\{N_x(w) \geq f(n)\bar{N}(w)\} \leq (1 - \delta^* + \varepsilon)n/[(1 - \xi)f(n)].$$

Так как доля «плохих» кодов  $\xi < 1$ , то при  $k > 1$  и  $n \rightarrow \infty$  величина  $n/f(n) = n/An^k \rightarrow 0$ . Но это значит, что среди «хороших» кодов данного ансамбля при достаточно большой длине кода  $n$  найдутся такие (доля их равна  $1 - Q$ ), для которых  $N_x(w) < f(n)\bar{N}(w)$  при  $(\delta^* - \varepsilon)n < w \leq n$ .

Что касается величины  $N_x(w)$  при  $1 \leq w \leq (\delta^* - \varepsilon)n$ , то по самому определению «хороших» кодов эта величина равна нулю. Так как «хорошие» коды составляют часть всех кодов из данного ансамбля, то для  $k > 1$  утверждение 5.1 доказано.

Рассмотрим теперь случай  $k=1$ , когда  $f(n)=An$ , тогда  $Q \leq (1-\delta^*+\varepsilon)/((1-\xi)A)$ . Выбирая  $A$  достаточно большим, можно получить  $Q < 1$ , что завершает доказательство утверждения 5.1.

Заметим, что если при  $n \rightarrow \infty$  величина  $\xi \rightarrow 0$ , то утверждение 5.1 остается справедливым и при  $A=1$ .

### П.5.3. Доказательство леммы 5.1

Каждый элемент столбца  $\gamma^{(j)}$  представляет собой скалярное произведение над полем  $\text{GF}(2)$  соответствующего вектор-строки матрицы  $H_0^{(j)}$  на вектор-столбец  $\alpha^{(j)}$ , причем в силу невырожденности матрицы  $H_0^{(j)}$  столбцы  $\alpha^{(j)}$  и  $\gamma^{(j)}$  либо оба нулевые, либо оба ненулевые. Пусть  $\alpha^{(j)}$  и  $\gamma^{(j)}$  — два произвольных двоичных столбца длины  $n_a$ . Вычислим число всех невырожденных двоичных матриц  $H_0^{(j)}$  порядка  $n_a$ , удовлетворяющих равенству (5.5). Для этого введем множество  $M_1$  всех двоичных векторов длины  $n_a$ , скалярное произведение которых с вектором  $\alpha^{(j)}$  равно единице. Число таких векторов равно  $2^{n_a-1}$ . Действительно, если в векторе  $\alpha^{(j)}$  единицы расположены на  $r$  фиксированных позициях, то на оставшихся  $n_a-r$  позициях векторов из  $M_1$  можно разместить любые символы (как «0» так и «1»), так что число всех возможных вариантов равно  $2^{n_a-r}$ ; на оставшихся  $r$  позициях должно быть нечетное число единиц, расположенных в произвольном порядке, так что число вариантов их расположения равно  $\sum_r C_r^{s+1} = 2^{r-1}$ .

Следовательно, общее число векторов, образующих множество  $M_1$ , равно  $2^{n_a-r}2^{r-1} = 2^{n_a-1}$ . Скалярное произведение остальных  $2^{n_a-1}$  векторов, не входящих в множество  $M_1$  с вектором  $\alpha^{(j)}$ , будет равно нулю. Так как один из таких векторов нулевой, то общее число ненулевых векторов, скалярное произведение которых с вектором  $\alpha^{(j)}$  равно нулю, равняется  $2^{n_a-1}-1$ . Множество этих векторов назовем  $M_0$ . Очевидно (в силу свойств скалярного произведения над полем  $\text{GF}(2)$ ), что сумма нечетного числа векторов из  $M_1$  принадлежит  $M_1$ , а сумма четного числа векторов из  $M_1$  принадлежит  $M_0$ . В то же время сумма любого числа векторов из  $M_0$  принадлежит  $M_0$ .

Если вектор  $\gamma^{(j)}$  содержит  $k > 0$  единиц, то соответствующие  $k$  строк матрицы  $H_0^{(j)}$  следует выбирать из множества  $M_1$ . Первую из них можно выбрать  $2^{n_a-1}$  способом, вторую  $2^{n_a-1}-1$  способом, а после выбора  $v-1$  строк  $v$ -ю строку (чтобы обеспечить невырожденность матрицы  $H_0^{(j)}$ ) можно выбрать

$$2^{n_a-1} - \sum_{s=1}^{v-1} C_{s-1}^{2s-1} = 2^{n_a-1} - 2^{v-2}, \quad v = \overline{1, k},$$

способами.

Таким образом, имеется всего  $2^{n_a-1}(2^{n_a-1}-1)(2^{n_a-1}-2)\dots(2^{n_a-1}-2^{k-2})$  вариантов выбора, соответствующих  $k$  строк матрицы  $H_0^{(j)}$ . Остальные  $n_a-k$  строк матрицы  $H_0^{(j)}$  следует выбирать из множества  $M_0$ . Первую из них можно выбрать (учитывая свойства множества  $M_1$ )  $2^{n_a-1} - \sum_{s=1}^{k-1} C_s^{2s} = 2^{n_a-1} - 2^{k-2}$  способами, вторую  $2^{n_a-1} - 2^{k-1} \cdot 2$  способами, а  $\mu$ -ю  $2^{n_a-1} - 2^{k-1}2^{\mu-1}$  способами ( $\mu = \overline{1, n_a-k}$ ). Таким образом, имеется

всего  $(2^{n_{a-1}} - 2^{k-1})(2^{n_{a-1}} - 2^k) \dots (2^{n_{a-1}} - 2^{n_{a-2}})$  вариантов выбора соответствующих  $n_a - k$  строк матрицы  $H_0^{(j)}$ .

Отсюда следует, что число всех различных невырожденных матриц  $H_0^{(j)}$ , удовлетворяющих равенству (5.15), равно  $2^{n_{a-1}}(2^{n_{a-1}} - 1) \dots (2^{n_{a-1}} - 2^{k-2})(2^{n_{a-1}} - 2^{k-1}) \dots (2^{n_{a-1}} - 2^{n_{a-2}})$ , причем это число не зависит ни от вектора  $\alpha^{(j)} \neq 0$ , ни от вектора  $\gamma^{(j)} \neq 0$ .

Так как число всех различных невырожденных матриц  $H_0^{(j)}$  равно  $(2^{n_a} - 1)(2^{n_a} - 2)(2^{n_a} - 2^2) \dots (2^{n_a} - 2^{n_{a-1}})$ , то доля матриц, удовлетворяющих (5.15) при любых фиксированных (ненулевых)  $\alpha^{(j)}$  и  $\gamma^{(j)}$ , составляет

$$\frac{2^{n_{a-1}}(2^{n_{a-1}} - 1)(2^{n_{a-1}} - 2) \dots (2^{n_{a-1}} - 2^{n_{a-2}})}{(2^{n_a} - 1)(2^{n_a} - 2)(2^{n_a} - 2^2) \dots (2^{n_a} - 2^{n_{a-1}})} = \frac{1}{2^{n_a} - 1},$$

что и доказывает лемму 5.1.

#### П.5.4. Доказательство утверждения 5.2

Рассмотрим множество всех ненулевых двоичных слов длины  $n_a$ . Любое слово  $\alpha^{(j)}$  из этого множества принадлежит коду  $A_{i_1 \dots i_v}$ , тогда и только тогда, когда слово  $\gamma^{(j)} = G_0^{-1} \alpha^{(j)}$  имеет ненулевые символы только в наборе  $(i_1 \dots i_v)$ . Если слово  $\alpha^{(j)}$  фиксировано, а матрица  $G_0$  выбирается случайно из множества всех двоичных невырожденных матриц порядка  $n_a$ , то в соответствии с леммой 5.1 вероятность  $P_{i_1 \dots i_v}(w)$ , что слово веса  $w > 0$  принадлежит коду  $A_{i_1 \dots i_v}$ , порожденному матрицей  $G_0$ , определяется как

$$P_{i_1 \dots i_v}(w) = \left( \frac{\sum_{s=1}^v a_{i_s}}{2^{n_a} - 1} \right) / (2^{n_a} - 1) < 2^{-\left( n_a - \sum_{s=1}^v a_{i_s} \right)}$$

и не зависит от  $w > 0$ .

Следовательно, среднее по всем случайным кодам  $A_{i_1 \dots i_v}$  число кодовых слов  $\bar{N}_{i_1 \dots i_v}(w)$  веса  $w > 0$  равно

$$\bar{N}_{i_1 \dots i_v}(w) = C_{n_a}^w P_{i_1 \dots i_v}(w) < C_{n_a}^w 2^{-\left( n_a - \sum_{s=1}^v a_{i_s} \right)}.$$

В соответствии с (П.5.2) доля кодов  $\rho_{i_1 \dots i_v}(w)$ , у которых число кодовых слов веса  $w > 0$ ,  $N_{i_1 \dots i_v}(w)$  будет превышать среднее по всем кодам  $A_{i_1 \dots i_v}$  число кодовых слов того же веса  $\bar{N}_{i_1 \dots i_v}(w)$  в  $n_a^{2^m}$  раз, не превосходит величины  $\{n_a^{2^m}\}^{-1}$ .

Пусть  $\rho$  — доля матриц  $G_0$ , порождающих хотя бы один код  $A_{i_1 \dots i_v}$ , у которого хотя бы для одного  $w > 0$  и одного набора  $(i_1, \dots, i_v; i = \overline{1, m})$ , выполняется условие  $N_{i_1 \dots i_v}(w) > n_a^{2^m} \bar{N}_{i_1 \dots i_v}(w)$ . Очевидно, что

$$\rho \leq \sum_{v=1}^m \sum_{(i_1, \dots, i_v)} \sum_{w=1}^{n_a} \rho_{i_1 \dots i_v}(w).$$

Учитывая, что  $\rho_{i_1 \dots i_s}(w) \leq \{n^2 2^m\}^{-1}$  и что для фиксированного  $v \neq 0$  число различных наборов  $(i_1 \dots i_s)$  равно  $C_m^s$ , а общая сумма всех возможных наборов равна  $2^{m-1}$ , получаем  $\rho \leq n_a (2^m - 1) / [n_a^2 2^m] < (n_a)^{-1}$ . Следовательно, доля матриц  $G_0$ , не удовлетворяющих утверждению 5.2, меньше единицы и стремится к нулю при  $n_a \rightarrow \infty$ , что и завершает доказательство утверждения.

### П.5.5. Доказательство леммы 5.2

Обозначим  $\gamma_i = (\mu_i, \nu_i)$ , где  $\mu_i = (\gamma_{i1}, \gamma_{i2}, \dots, \gamma_{ib_i})$ ,  $\nu_i = (\gamma_i, b_{i+1}, \gamma_i, b_{i+2}, \dots, \gamma_i, n_b)$ . Если  $\mu_i = 0$ , а  $\nu_i \neq 0$ , то  $\gamma_i$  не может быть кодовым словом кода  $(n_b, b_i)$ , определяемого канонической проверочной матрицей. Если же  $\mu_i \neq 0$ , то  $\gamma_i$  является кодовым словом кода  $(n_b, b_i)$  тогда и только тогда, когда выполняются все  $n_b - b_i$  проверочных соотношений, определяемых матрицей  $\|P_i E_{n_b - b_i}\|$ . Но в силу алгоритма построения этой матрицы все коэффициенты каждого из проверочных соотношений (кроме последнего, равного единице) независимы и равновероятны, так что вероятность выполнения одного проверочного соотношения равна  $2^{-a_i}$ , а всех  $n_b - b_i$  соотношений равна  $2^{-a_i(n_b - b_i)}$ .

Таким образом,

$$P_i(w) = 0, \text{ если } \mu_i = 0, \nu_i \neq 0;$$

$$P_i(w) = 2^{-a_i(n_b - b_i)}, \text{ если } \mu_i \neq 0,$$

что и доказывает лемму 5.2.

### П.5.6. Доказательство лемм 5.3 и 5.4

Так как кодовое расстояние случайного кода РС- $(n_b, b_i)$  равно  $n_b - b_i + 1$ , то слово  $\gamma_i$ , вес которого  $w \leq n_b - b_i$ , не может быть кодовым словом этого кода. Пусть вес слова  $\gamma_i$  больше, чем  $n_b - b_i$ , тогда оно будет кодовым словом случайного кода РС, определяемого матрицей  $A$ , если слово  $\beta_i = A^{-1} \gamma_i$  является кодовым словом исходного (неслучайного) кода РС. Но в силу того что все диагональные (ненулевые) элементы матрицы  $A$  независимы и равновероятны, в слове  $\beta_i$ , вес которого, так же как и вес слова  $\gamma_i$ , равен  $w$ , возможны любые сочетания ненулевых символов. При этом все возможные сочетания равновероятны, а их общее число равно  $(2^{a_i} - 1)^w$ . В то же время, согласно [140], число слов кода РС веса  $w > n_b - b_i$  оценивается сверху величиной  $(2^{a_i} - 1)^{w - n_b + b_i}$ .

Следовательно, вероятность того, что слово  $\beta_i$  веса  $w > n_b - b_i$  является кодовым словом кода РС, удовлетворяет неравенству  $P_i(w) \leq (2^{a_i} - 1)^{w - n_b + b_i} / (2^{a_i} - 1)^w = (2^{a_i} - 1)^{-(n_b - b_i)}$ , но  $(2^{a_i} - 1)^{-(n_b - b_i)} = 2^{-a_i(n_b - b_i)} \times (1 - 2^{-a_i})^{-(n_b - b_i)} < 2^{-a_i(n_b - b_i)} e^{(n_b - b_i)/2^{a_i}}$ . Для кодов РС (в том числе укороченных и удлиненных)  $n_b \leq 2^{a_i} + 1$ , так что  $(n_b - b_i) 2^{-a_i} \leq (n_b - b_i) / (n_b - 1) \leq 1$ , если  $b_i > 0$ . Таким образом, если  $w > n_b - b_i$ , то  $P_i(w) \leq e 2^{-a_i(n_b - b_i)}$ , что и доказывает лемму 5.3.

Доказательство леммы 5.4 полностью совпадает с доказательством леммы 5.3 с той лишь разницей, что теперь нет необходимости рассматривать вспомогательное слово.

### П.5.7. Доказательство утверждений 5.3, 5.4, 5.5 и 5.6

Вероятность  $P_l(w)$  согласно (5.12) определяется равенством

$$P_l(w) = P(C_0) \sum_{i=1}^m P(D_i) \prod_{s \neq i}^m (P(C_s) + P(D_s)). \quad (\text{П.5.3})$$

В соответствии со следствием из леммы 5.1, если некоторое  $\gamma_i \neq 0$  (что имеет место, если произошло событие  $D_i$ ) для всех  $l \geq 1$ , вероятность  $P(C_s) = 2^{-a_s l}$ ,  $s \neq i$ ,  $s = \overline{0, m}$ .

При оценке вероятностей  $P(D_i)$  следует учитывать, что вес слова  $\gamma_i$  не может быть больше, чем  $l$ , поэтому, если  $l < n_b - b_i + 1$ , то  $P(D_i) = 0$ . Если же  $l > n_b - b_i$ , но вес слова  $\gamma_i$   $w < n_b - b_i + 1$ , то также  $P(D_i) = 0$ . Если же  $l \geq n_b - b_i + 1$  и  $w \geq n_b - b_i + 1$ , то согласно лемме 5.3  $P(D_i) \leq e 2^{-a_i(n_b - b_i)}$ .

Таким образом, имеем

$$P(D_i) = \begin{cases} 0, & \text{если } l < n_b - b_i + 1; \\ \leq e 2^{-a_i(n_b - b_i)}, & \text{если } l \geq n_b - b_i + 1. \end{cases}$$

Если  $l < n_b - b_m + 1$  (учитывая, что  $b_1 < b_2 < \dots < b_m$ ) для всех  $i = \overline{1, m}$  получаем  $P(D_i) = 0$ , следовательно,  $P_l(w) = 0$ . Таким образом, для каждого из диапазонов изменения  $l$ , определяемых условием  $n_b - b_i + 1 \leq l \leq n_b - b_{i-1}$ ,  $i = \overline{2, m+1}$ ,  $b_{m+1} = n_b$ , выражение (П.5.3) принимает вид

$$P_l(w) = \sum_{k=i}^m P(D_k) \prod_{s \neq k}^m (P(D_s) + P(C_s)) \prod_{s=0}^{i-1} P(C_s),$$

которое после замены  $P(D_k)$  на  $P(D_k) + P(C_k)$  оценивается неравенством

$$P_l(w) \leq (m - i + 1) \prod_{s=i}^m [P(D_s) + P(C_s)] \prod_{s=0}^{i-1} P(C_s), \quad i = \overline{1, m}.$$

Заменяя  $P(C_s)$  его значением, а  $P(D_s)$  — полученной выше оценкой, получаем

$$P_l(w) \leq (m - i + 1) \prod_{s=i}^m [e 2^{-a_s(n_b - b_s)} + 2^{a_s l}] \prod_{s=0}^{i-1} 2^{-a_s l}.$$

Но при указанных значениях  $l$   $2^{-a_s(n_b - b_s)} > 2^{-a_s l}$ , так что  $e 2^{-a_s(n_b - b_s)} + 2^{-a_s l} < 2e 2^{-a_s(n_b - b_s)}$ .

Таким образом,

$$P_l(w) \leq (m - i + 1) (2e)^{m-i+1} 2^{-\left(n_a - \sum_{s=1}^m a_s\right)l - \sum_{s=i}^m a_s(n_b - b_s)},$$

где  $n_b - b_i + 1 \leq l \leq n_b - b_{i-1}$ .

Замена множителя  $(m-i+1)(2e)^{m-i+1}$  большей величиной  $m(2e)^m$  завершает доказательство утверждения 5.3. Легко убедиться в том, что утверждение 5.3, доказанное для ансамбля каскадных кодов I, полностью сохраняется и для ансамблей I<sup>a</sup>, I<sup>b</sup> и I<sup>в</sup>. При доказательстве утверждения 5.4 оценка  $P_l(w)$  при  $n_b - b_i + 1 \leq l \leq n_b - b_{i-1}$  и  $i \leq m$  осуществляется так же, как и при доказательстве утверждения 5.3, с той только разницей, что для оценки  $P(D_i)$  следует использовать лемму 5.2, согласно которой  $P(D_i) \leq 2^{-a_i(n_b - b_i)}$ . Однако теперь при  $1 \leq l \leq n_b - b_m$  вероятность  $P(D_i) \neq 0$ , так как случайный код  $(n_b, b_i)$  может иметь кодовое расстояние  $d_{bi}$ , удовлетворяющее условию  $1 \leq d_{bi} \leq n_b - b_i$ . Согласно лемме 5.2 при всех  $l \geq 1$  вероятность  $P(D_i) \leq 2^{-a_i(n_b - b_i)}$ , и так как  $P(C_s) = 2^{-a_s l}$  (также для всех  $l \geq 1$ ), то, учитывая, что  $b_i > b_{i-1}$ , для случая  $1 \leq l \leq n_b - b_m$  приходим к неравенству  $P(C_s) \geq P(D_s)$ , так что произведение

$$\prod_{s \neq i}^m [P(C_s) + P(D_s)] \leq 2^{m-1} \prod_{s \neq i}^m P(C_s)$$

и, следовательно,

$$P_l(w) \leq 2^{m-1} \sum_{i=1}^m P(D_i) \prod_{s \neq i}^m P(C_s) P(C_0).$$

Таким образом, при  $1 \leq l \leq n_b - b_m$

$$P_l(w) \leq 2^{m-1} \sum_{i=1}^m 2^{-a_i(n_b - b_i)} 2^{-l \sum_{s \neq i}^m a_s} 2^{-l a_0} \leq m 2^m \sum_{i=1}^m 2^{-(n_b - b_i)a_i - (n_a - a_i)l},$$

что и завершает доказательство утверждения 5.4, которое остается справедливым и для ансамбля II<sup>a</sup>.

Доказательство утверждения 5.5 полностью совпадает с доказательством утверждения 5.3, только в процессе этого доказательства вместо соотношения (5.12) используется соотношение (5.13). Утверждение 5.5 остается справедливым и для ансамбля III<sup>a</sup>. Доказательство утверждения 5.6 полностью совпадает с доказательством утверждения 5.4 при замене в процессе доказательства соотношения (5.12) соотношением (5.13).

## П.5.8. Доказательство утверждения 5.7

Выбранное из множества  $\mathcal{A}_{i_1, \dots, i_v}$  слово  $\alpha(i_1 \dots i_v)$  является кодовым словом каскадного кода из ансамбля тогда и только тогда, когда все ненулевые блоки  $\gamma_{i_1}, \gamma_{i_2}, \dots, \gamma_{i_v}$  соответствующего им слова  $\gamma(i_1 \dots i_v)$  представляют собой кодовые слова внешних кодов  $B_{i_1}, B_{i_2}, \dots, B_{i_v}$ . Поэтому в силу независимости выбора внешних кодов вероятность  $P_l(i_1, \dots, i_v, w)$  определяется очевидным равенством

$$P_l(i_1, \dots, i_v, w) = \prod_{s=1}^v P_l(i_s, w).$$

где  $P_l(i_s, w)$  — вероятность того, что  $\gamma_{i_s}$  является ненулевым словом внешнего кода  $B_{i_s}$ . Если выбранное слово  $a(i_1, \dots, i_s)$  содержит  $l$  ненулевых и  $n_b - l$  нулевых столбцов, то, как следует из леммы 5.3,

$$P_l(i_s, w) = \begin{cases} 0, & \text{если } l \leq n_b - b_{i_s}; \\ \leq e^{2^{-a_{i_s}(n_b - b_{i_s})}} & \text{если } l > n_b - b_{i_s}. \end{cases}$$

Таким образом, для всех  $l > 0$  получаем для  $P_l(i_1, \dots, i_s, w)$  оценку сверху

$$P_l(i_1, \dots, i_s, w) \leq e^{2^{-\sum_{s=1}^s a_{i_s}(n_b - b_{i_s})}},$$

что и доказывает утверждение 5.7.

### II.5.9. Доказательство утверждений 5.8 и 5.9

Для ансамблей I, I<sup>a</sup>, I<sup>b</sup>, I<sup>c</sup> II и II<sup>a</sup> среднее, по ансамблю число кодовых слов веса  $w > 0$  в случайном каскадном коде

$$\bar{N}(w) = \sum_{l=1}^{n_b} M_l(w) P_l(w),$$

где  $M_l(w)$  — число всех двоичных слов размеров  $n_a \times n_b$  веса  $w > 0$ , содержащих  $l$  ненулевых и  $n_b - l$  нулевых столбцов.

В соответствии с утверждением 5.3 для ансамблей I, I<sup>a</sup>, I<sup>b</sup> и I<sup>c</sup> имеем

$$\bar{N}(w) \leq \sum_{i=1}^m m (2e)^m \sum_{l=n_b - b_{i_s} + 1}^{n_b - b_{i_s} - 1} M_l(w) 2^{-s_i(l)},$$

где

$$s_i(l) = \left( n_a - \sum_{s=1}^m a_s \right) l + \sum_{s=1}^m a_s (n_b - b_s). \quad (\text{II.5.4})$$

Величина  $M_l(w) = C_{n_b}^l Q_l(w)$ , где  $Q_l(w)$  — число всех слов  $a$  веса  $w > 0$ , содержащих  $l$  ненулевых и  $n_b - l$  нулевых столбцов, расположенных в некотором фиксированном порядке (например, первые  $l$  столбцов ненулевые). Величину  $Q_l(w)$  оценим тривиальным образом  $Q_l(w) \leq C_{n_a l}^w$ .

Таким образом,  $M_l(w) \leq C_{n_b}^l C_{n_a l}^w$  и для производящей функции  $\psi(z)$  среднего спектра весов

$$\psi(z) = \sum_{w=1}^n \bar{N}(w) z^w$$

при  $z \geq 0$  получаем

$$\begin{aligned} \psi(z) &\leq m (2e)^m \sum_{w=1}^n \sum_{i=1}^m \sum_{l=n_b - b_{i_s} + 1}^{n_b - b_{i_s} - 1} C_{n_b}^l C_{n_a l}^w 2^{-s_i(l)} z^w \leq \\ &\leq m (2e)^m \sum_{i=1}^m \sum_{l=n_b - b_{i_s} + 1}^{n_b - b_{i_s} - 1} C_{n_b}^l 2^{-s_i(l)} (1+z)^{n_a l}. \end{aligned}$$

Используя равенство (П. 5.4), последнее выражение можно представить в виде

$$\begin{aligned} \psi(z) &\leq m (2e)^m \sum_{i=1}^m 2^{-\sum_{s=i}^m a_s (n_b - b_s)} \sum_{l=n_b - b_{i+1}}^{n_b - b_i - 1} C_{n_b}^l (1+z)^{n_a l} 2^{-\left(n_a - \sum_{s=i}^m a_s\right) l} \leq \\ &\leq \Psi(z) = m (2e)^m \sum_{i=1}^m 2^{-\sum_{s=i}^m a_s (n_b - b_s)} \left[ (1+z)^{n_a} 2^{-\left(n_a - \sum_{s=i}^m a_s\right)} + 1 \right]^{n_b}. \end{aligned}$$

После очевидных преобразований получаем выражение (5.25).

Аналогичные результаты нетрудно получить и для ансамблей II и II<sup>a</sup>, определяемых произвольными невырожденными матрицами (или ненулевым элементом поля GF(2<sup>n<sub>a</sub></sup>)) и случайными внешними кодами (n<sub>b</sub>, b<sub>i</sub>). Используя утверждение 5.4, получаем выражение (5.26).

### П.5.10. Доказательство утверждений 5.10 и 5.11

Для ансамблей III, III<sup>a</sup> и IV среднее по ансамблю число кодовых слов веса w > 0 в случайном каскадном коде

$$\bar{N}(w) = \sum_{k=0}^m \sum_{l=1}^{n_b} M_{\{k\}}^{(w)}(w) P_{\{k\}}^{(w)}(w),$$

где M<sub>{k}</sub><sup>(k)</sup>(w) — число всех двоичных слов веса w > 0 размеров  $\left(n_a - \sum_{s=m-k+1}^m a_s\right) n_b$ , содержащих l ненулевых и n<sub>b</sub> - l нулевых столбцов.

Но M<sub>{k}</sub><sup>(k)</sup>(w) = C<sub>n<sub>b</sub></sub><sup>l</sup> Q<sub>{k}</sub><sup>(k)</sup>(w), где

$$Q_{\{k\}}^{(k)}(w) \leq C_{\left(n_a - \sum_{s=m-k+1}^m a_s\right) l}^w.$$

Тогда

$$\bar{N}(w) \leq \sum_{k=0}^m \sum_{l=1}^{n_b} C_{n_b}^l C_{(1-R a, m-k+1) n_a l}^w P_{\{k\}}^{(k)}(w).$$

Если в качестве внешних кодов выбираются коды РС (случайные или неслучайные), то, воспользовавшись утверждением 5.5, после достаточно громоздких, но совершенно простых преобразований для ансамблей III и III<sup>a</sup> получаем выражение (5.27).

Если же в качестве внешних кодов выбираются случайные (n<sub>b</sub>, b<sub>i</sub>) коды, то, воспользовавшись утверждением 5.6 для ансамбля IV, получаем выражение (5.28).

### П.5.11. Доказательство утверждения 5.12

Для ансамблей I<sup>r</sup> и II<sup>b</sup> среднее число  $\bar{N}_{i_1, \dots, i_r}(w)$  кодовых слов веса w > 0 каскадного кода из ансамбля, содержащихся в множестве  $\mathfrak{A}_{i_1, \dots, i_r}$ , определяется равенством

$$\bar{N}_{i_1, \dots, i_r}(w) = \sum_{l=1}^{n_b} M_l(i_1, \dots, i_r, w) P_l(i_1, \dots, i_r, w),$$



где  $M_l(i_1, \dots, i_v, w)$  — число всех слов веса  $w$  в множестве  $\mathcal{Q}_{i_1 \dots i_v}$ , имеющих  $l$  ненулевых и  $n_b - l$  нулевых столбцов.

Из определения множеств  $\mathcal{Q}_{i_1 \dots i_v}$  очевидным образом следует, что

$$\bar{N}(w) = \sum_{v=1}^m \sum_{(i_1, \dots, i_v)} \sum_{l=1}^{n_b} M_l(i_1, \dots, i_v, w) P_l(i_1, \dots, i_v, w),$$

следовательно, производящая функция

$$\psi(z) = \sum_{w=1}^{\infty} \bar{N}(w) z^w = \sum_{w=1}^{\infty} \sum_{v=1}^m \sum_{(i_1, \dots, i_v)} \sum_{l=1}^{n_b} M_l(i_1, \dots, i_v, w) P_l(i_1, \dots, i_v, w) z^w.$$

Учитывая, что  $M(i_1, \dots, i_v, w) = C_{n_b}^l Q(i_1 \dots i_v, w)$ , где  $Q(i_1, \dots, i_v, w)$  — число слов веса  $w$  в множестве  $\mathcal{Q}_{i_1 \dots i_v}$ , содержащих  $l$  ненулевых и  $n_b - l$  нулевых столбцов, расположенных в некотором фиксированном порядке, имеем

$$\psi(z) = \sum_{v=1}^m \sum_{(i_1, \dots, i_v)} \sum_{l=1}^{n_b} C_{n_b}^l \sum_{w=1}^{\infty} P_l(i_1, \dots, i_v, w) Q(i_1, \dots, i_v, w) z^w.$$

Заменяя в соответствии с утверждением 5.7 вероятность  $P_l(i_1 \dots i_v, w)$  ее верхней оценкой  $P_{i_1 \dots i_v}$ , которая не зависит ни от  $w > 0$ , ни от  $l$ , получаем для  $z \geq 0$

$$\psi(z) \leq \sum_{v=1}^m \sum_{(i_1, \dots, i_v)} e^{v2^{-\sum_{s=1}^v a_{i_s}(n_b - b_{i_s})}} \sum_{l=1}^{n_b} C_{n_b}^l \psi_{i_1 \dots i_v}^{(l)}(z),$$

где

$$\psi_{i_1 \dots i_v}^{(l)}(z) = \sum_{w=1}^{\infty} Q(i_1, \dots, i_v, w) z^w.$$

Для оценки  $\psi_{i_1 \dots i_v}^{(l)}(z)$  введем производящую функцию  $\omega_{i_1 \dots i_v}(z)$  числа кодовых слов внутреннего кода  $A_{i_1 \dots i_v}$ , определяемого матрицей  $G_0$ , удовлетворяющей условию (5.16) утверждения 5.2.

В соответствии с условием 5.2 для  $z \geq 0$  имеем

$$\begin{aligned} \omega_{i_1 \dots i_v}(z) &\leq n_a^{2^m} 2^{-\left(n_a - \sum_{s=1}^v a_{i_s}\right)} |(1+z)^{n_a} - 1| < \\ &< n_a^{2^m} 2^{-\left(n_a - \sum_{s=1}^v a_{i_s}\right)} (1+z)^{n_a}. \end{aligned}$$

Если теперь учесть, что вес слова, принадлежащего множеству  $\mathcal{Q}_{i_1 \dots i_v}$ , равен сумме весов каждого из его столбцов и что производящая функция числа слов, вес которых равен сумме весов соответствующих столбцов, равна произведению производящих функций числа этих столбцов, видим, что  $\psi_{i_1 \dots i_v}^{(l)}(z) = (\omega_{i_1 \dots i_v}(z))^l$ , так что производящая функция  $\psi(z)$  для  $z \geq 0$  удовлетворяет условию

$$\psi(z) \leq \sum_{\nu=1}^m \sum_{(i_1 \dots i_\nu)} e^{\nu 2^{-\sum_{s=1}^{\nu} a_{i_s} (n_b - b_{i_s})}} \left[ n_a^{2^{2m} 2^{-\left(n_a - \sum_{s=1}^{\nu} a_{i_s}\right)}} (1+z)^{n_a} + 1 \right]^{n_b} < \\ < e^m (n_a^{2^{2m}})^{n_b} \sum_{\nu=1}^m \sum_{(i_1 \dots i_\nu)} 2^{-\left(n - \sum_{s=1}^{\nu} a_{i_s} b_{i_s}\right)} \left[ (1+z)^{n_a} + 2^{-n_a - \sum_{s=1}^{\nu} a_{i_s}} \right]^{n_b}.$$

Для дальнейшего упрощения полученной оценки, кроме обычного условия  $b_1 < b_2 < \dots < b_m$ , примем дополнительное условие  $a_1 \leq a_2 \leq \dots \leq a_m$ , которое включает наиболее интересный с практической точки зрения случай  $a_1 = a_2 = \dots = a_m$ .

При этих условиях, учитывая, что

$$2^{-\left(n - \sum_{s=1}^{\nu} a_{i_s} b_{i_s}\right)} \leq 2^{-\left(n - \sum_{s=m-\nu+1}^m a_s b_s\right)}, \\ 2^{-\left(n_a - \sum_{s=1}^{\nu} a_{i_s}\right)} \leq 2^{-\left(n_a - \sum_{s=m-\nu+1}^m a_s\right)},$$

получаем

$$\psi(z) \leq e^m (n_a^{2^{2m}})^{n_b} \sum_{\nu=1}^m C_m^{\nu} 2^{-\left(n - \sum_{s=m-\nu+1}^m a_s b_s\right)} \left[ (1+z)^{n_a} + 2^{-n_a - \sum_{s=m-\nu+1}^m a_s} \right]^{n_b}.$$

Заменяя  $C_m^{\nu}$  на  $2^m$  и обозначая  $m - \nu + 1 = i$ , окончательно приходим к выражению (5.29).

### П.5.12. Доказательство утверждения 5.13

Учитывая, что

$$(z^{-\delta} + z^{1-\delta})^{n_a} + (z^{-\delta} 2^{1-R_{a i}})^{n_a} \leq 2 \max \{ (z^{-\delta} + z^{1-\delta})^{n_a}; (z^{-\delta} 2^{1-R_{a i}})^{n_a} \},$$

имеем

$$\inf_{0 < \delta \leq 1} \{ [(z^{-\delta} + z^{1-\delta})^{n_a} + (z^{-\delta} 2^{1-R_{a i}})^{n_a}]^{n_b} \} \leq \\ \leq 2^{n_b} \inf_{0 < \delta \leq 1} \max \{ (z^{-\delta} + z^{1-\delta})^{n}; (z^{-\delta} 2^{1-R_{a i}})^{n} \}.$$

Введем величину  $\delta_i$ , определяемую равенством  $R_{a i} = \log_2 2(1 - \delta_i)$ , и рассмотрим график функции  $\varphi_i(z) = \max \{ (z^{-\delta} + z^{1-\delta})^n; (z^{-\delta} 2^{1-R_{a i}})^n \} = \max \{ (z^{-\delta} + z^{1-\delta})^n; (z^{-\delta} + z^{-\delta \delta_i / (1 - \delta_i)})^n \}$  при различных значениях параметра  $\delta_i$  (рис. П.5.1). Так как функция  $z^{-\delta} + z^{1-\delta}$  имеет минимум при  $z = z_{\min} = \delta / (1 - \delta)$ , равный  $2^{H(\delta)}$ , то в тех случаях, когда  $\delta_i < \delta$  (т. е. когда  $z_{\min} \geq \delta_i / (1 - \delta_i)$ ), функция  $\varphi_i(z)$  имеет минимум при  $z = z_{\min}$ , равный  $2^{H(\delta)n}$  (см. рис. П.5.1, а). Если же  $z_{\min} < \delta_i / (1 - \delta_i)$ , то функция  $\varphi_i(z)$  имеет минимум при  $z = \delta_i / (1 - \delta_i)$  (когда  $z^{-\delta} + z^{1-\delta} = z^{-\delta} + z^{-\delta \delta_i / (1 - \delta_i)}$ ), равный

$$\left[ \left( \frac{\delta_i}{1 - \delta_i} \right)^{-\delta} \frac{1}{1 - \delta_i} \right]^n = \left[ \frac{2^{1-R_{a i}}}{(2^{1-R_{a i}} - 1)^{\delta}} \right]^n = 2^{n[(1-R_{a i}) - \delta \log_2(2^{1-R_{a i}} - 1)]}.$$

(см. рис. П.5.1, б).

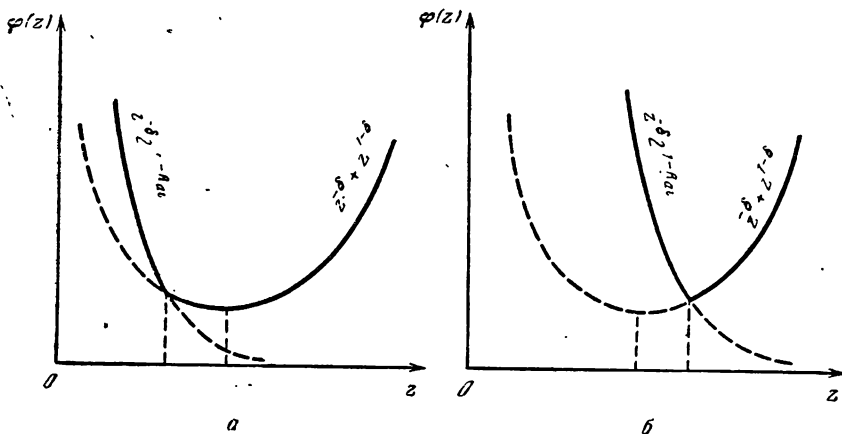


Рис. П.5.1. График функции  $\varphi_i(z)$  для случаев

$\alpha - z \min \geq \delta_i/(1 - \delta_i)$ ; б —  $z \min < \delta_i/(1 - \delta_i)$

Из полученных результатов непосредственно следует, что

$$\inf_{0 < z \leq 1} \left\{ \frac{\Psi_i(z)}{z^{n\delta}} \right\} \leq \begin{cases} 2^{n k_1}(m, n_a, n_b) 2^{n[H(\delta)-1+R_i]} & \text{при } \delta \geq \delta_i; \\ 2^{n k_1}(m, n_a, n_b) 2^{n[-\delta \log_2(2^{1-R_{at}}-1)-R_{at}+R_i]} & \text{при } \delta < \delta_i. \end{cases}$$

что и доказывает первую часть утверждения 5.13.

Покажем теперь, что прямая  $F_{i2}(\delta)$  является касательной к кривой  $F_{i1}(\delta)$  в точке  $\delta = \delta_i$ . Уравнение касательной в данном случае имеет вид  $y - F_{i1}(\delta_i) = F'_{i1}(\delta - \delta_i)$ . Учитывая, что  $F'_{i1}(\delta_i) = H'(\delta_i) = \log_2(1 - \delta_i) - \log_2 \delta_i$ , и подставляя вместо  $F_{i1}(\delta_i)$  его значение, имеем  $y = -\delta \log_2[\delta_i/(1 - \delta_i)] - \log_2(1 - \delta_i) - (1 - R_i) = -\delta \log_2(2^{1-R_{at}} - 1) - R_{at} + R_i = F_{i2}(\delta)$ , что и завершает доказательство утверждения 5.13.

### П.5.13. Доказательство утверждения 5.14

Учитывая равенства (5.39), представим левую часть условий (5.41) в виде

$$\begin{aligned} & \frac{R_{at} - R_i}{-\log_2(2^{1-R_{at}} - 1)} \frac{\log_2(2^{1-R_{at}} - 1)}{\log_2(2^{1-R_{at}+R_{a,i+1}} - 1)} - \\ & - \frac{(R_{a,i+1} - R_{i+1})}{-\log_2(2^{1-R_{a,i+1}} - 1)} \frac{\log_2(2^{1-R_{a,i+1}} - 1)}{\log_2(2^{1-R_{at}+R_{a,i+1}} - 1)} = \\ & = \delta_{\text{БГ}}(R) k(R_{at}, R_{a,i+1}), \end{aligned}$$

где  $k(R_{at}, R_{a,i+1}) = [\log_2(2^{1-R_{at}} - 1) - \log_2(2^{1-R_{a,i+1}} - 1)] / \log_2(2^{1-R_{at}+R_{a,i+1}} - 1)$ .

Введем обозначения:  $x = 2^{1-R_{at}}$ ,  $y = 2^{1-R_{a,i+1}}$ , так что  $0 < x < y < 2$ . Тогда

$$k(R_{at}, R_{a,i+1}) = [\log_2(x - 1) - \log_2(y - 1)] / \log_2(2x/y - 1) = 1 + \log_2[(x - 1)y / ((y - 1)(2x - y))] / \log_2(2x/y - 1).$$

После элементарных преобразований выражений  $(x-1)y/[(y-1)(2x-y)]$  и  $2x/y-1$  получаем  $k(R_{ai}, R_{a, i+1}) = 1 + \ln(1 - (y-x)(2-y)/((y-1) \times (2x-y)))/\ln(1 - 2(y-x)/y)$ . Так как при  $0 < x < y < 2$  справедливы неравенства  $0 < (y-x)(2-y)/[(y-1)(2x-y)] < 1$ ,  $0 < 2(y-x)/y < 1$ , то  $k(R_{ai}, R_{a, i+1}) > 1$ , что и доказывает утверждение 5.14.

## ПРИЛОЖЕНИЕ П.6

### П.6.1. Доказательство утверждения 6.1

Если мы знаем матрицу  $G_0$  порядка  $n$ , заданную систему вложенных кодов, то, чтобы для любого  $x \in \{0, 1\}^n$  убедиться, что  $x \in A_i^n$ , достаточно найти матрицу  $G_0^{-1} = H_0$  (порядка  $n^3$  операций, здесь и далее под операцией понимается число шагов машины Тьюринга), умножить  $H_0$  на  $x$  (порядка  $n^2$  операций) и убедиться, что последние  $i$  символов равны нулю (порядка  $n$  операций). Таким образом, число операций для вычисления характеристической функции любого  $A_i^n$  при знании  $G_0$  не более  $cn^3$ .

Оценим теперь сложность построения матрицы  $G_0$ . Для этого сначала выпишем все слова длины  $n$  так, чтобы они следовали в порядке возрастания весов, т. е. нулевое слово, затем все слова веса единицы, затем все слова веса два и т. д. Для этого достаточно  $cn2^n$  операций.

После того как в качестве первого столбца выбрано слово из одних единиц, получаем код, порождаемый этим столбцом и содержащий два слова: все нули и все единицы. В этом случае каждый смежный класс содержит лишь два слова (слово и его дополнение). Расположим эти смежные классы в порядке возрастания весов слов минимального веса в них. Для этого достаточно  $cn2^n$  операций.

Пусть теперь уже построено  $k_i = n - i$  столбцов матрицы  $G_0$  и выписаны на ленте код  $A_i^n$  и все смежные классы в порядке возрастания весов слов минимального веса в них. Обозначим через  $\{S_i^l\}$  код, а через  $\{S_i^l\}$  — смежный класс, задаваемый представителем  $S_i^l$  (не обязательно минимального веса), где  $l$  — номер смежного класса в порядке их выписывания. Тогда в качестве кода  $A_{i-1}^n$ , соответствующего уже  $k_i + 1$  столбцам матрицы  $G_0$ , возьмем множество

$$\{S_i^{-1}\} = \{S_i^1\} \cup \{S_{2i}^1\},$$

а в качестве  $(k_i + 1)$ -го столбца матрицы  $G_0$  — любое слово смежного класса  $\{S_{2i}^1\}$ . Вычеркнем оба эти множества  $\{S_i^1\}$  и  $\{S_{2i}^1\}$  из списка смежных классов. В качестве первого смежного класса кода  $A_{i-1}^n$ , т. е.  $\{S_{2i}^{-1}\}$ , возьмем множество

$$\{S_{2i}^{-1}\} = \{S_i^1\} \cup \{S_i^1 + S_{2i}^1\}$$

и вычеркнем оба этих смежных класса  $\{S_i^1\}$  и  $\{S_i^1 + S_{2i}^1\}$  из списка. Затем в качестве следующего смежного класса в новом списке возьмем первый из невычеркнутых смежных классов старого списка (пусть это будет  $\{S_i^1\}$ ) и найдем очередной по порядку смежный класс  $\{S_i^{-1}\}$  кода  $A_{i-1}^n$  по формуле

$$\{S_i^{-1}\} = \{S_i^1\} \cup \{S_i^1 + S_{2i}^1\}$$

и т. д., пока не выпишем все смежные классы кода  $A_{i-1}^n$ . При таком построении смежные классы кода  $A_{i-1}^n$  уже будут расположены в порядке возрастания весов слов минимального веса в них. Для выписывания списка смежных классов кода  $A_{i-1}^n$  достаточно числа операций  $cn2^{n2^{i-1}}$ . Таким образом, для построения матрицы  $G_0$  потребуется не более

$$\sum_{i=1}^n cn2^{n2^i} \leq cn2^{2^n}$$

операций, что завершает доказательство утверждения 6.1.

## П.6.2. Доказательство утверждения 6.2

Напомним, что длина  $n$  кода имеет вид  $n_a(2^{R_{a1}n_a} - 1)$ , т. е.  $N_A = \{n = n_a(2^{R_{a1}n_a} - 1) \mid n_a \text{ — любое целое положительное число}\}$ . В качестве внутреннего кода выбирается по алгоритму Варшавова (см. утверждение 1.4) двоичный код длины  $n_a$  со скоростью передачи  $R_{a1}$ . В качестве внешнего кода выбирается код РС длины  $n_b = 2^{R_{a1}n_a} - 1$  над полем  $\text{GF}(2^{R_{a1}n_a})$  с числом информационных символов  $R_{b1}n_b$ .

Рассмотрим теперь алгоритм вычисления характеристической функции  $\chi_A(x)$  на слове  $x = (x_1, x_2, \dots, x_n)$ . Вначале вычисляется, представимо ли  $n$  в виде  $n_a(2^{R_{a1}n_a} - 1)$  (число операций не превосходит  $c \log^3 n$ ). Если  $n$  представимо в таком виде (в противном случае  $\chi_A(x) = 0$ ), то по алгоритму Варшавова вычисляется проверочная матрица в систематическом виде, а следовательно, и порождающая матрица линейного кода длины  $n_a$  со скоростью передачи  $R_{a1}$  (число операций не превосходит  $cn_a^{32(1-R_{a1}n_a)}$ ). Для каждой подпоследовательности  $x_{(j-1)n_a+1}, x_{(j-1)n_a+2}, \dots, x_{jn_a}$ ,  $j = 1, 2, \dots, n_b$ , выясняется ее принадлежность коду Варшавова: если да, то  $R_{a1}n_a$  информационных символов образуют символ  $\gamma_{ij} \in \text{GF}(2^{R_{a1}n_a})$ , в противном случае  $\chi_A(x) = 0$  (число операций не превосходит  $cn_a^2 n_b$ ). Таким образом, мы получим  $\gamma_1 = (\gamma_{11}, \gamma_{12}, \dots, \gamma_{1n_b})$  слово длины  $n_b$  с символами из  $\text{GF}(2^{R_{a1}n_a})$ , и надо проверить, является ли оно словом кода РС. Как следует из утверждения 1.6, сложность задания кода РС, т. е. вычисления характеристической функции кода РС, требует не более  $cq^2 \log^2 q$  или  $cn_a^2 n_b^2$  числа операций.

Выражая все полученные оценки через длину  $n$ , получим утверждение 6.2.

## П.6.3. Доказательство утверждения 6.5

Для того чтобы убедиться, что слово  $x = (x_1, \dots, x_n)$  является кодовым словом обобщенного каскадного кода, нужно это слово записать в виде матрицы  $\alpha$  размера  $n_a \times n_b$ , умножить матрицу  $\alpha$  на матрицу  $H_0 = G_0^{-1}$  и в получившейся матрице  $\gamma = H_0 \alpha$  убедиться, что все  $\gamma_i$ ,  $i = \overline{0, m}$ , являются словами соответствующих внешних кодов.

Ограничимся рассмотрением лишь кодового множества  $A(R, \delta)$ , у которого каскадные коды имеют структуру  $A$ , длину  $n = n_a 2^{R_{a1}n_a \log_2 n_a}$ , порядок  $m = \log_2 n_a$  и в качестве внешних кодов используются коды РС над-

$\text{GF}(2^{R_{a1}n_a/\log_2 n_a})$ , где  $R_{a1} = 1 - H(\delta)$ . В соответствии с этим  $N_A = \{n = n_a 2^{R_{a1}n_a/\log_2 n_a} \mid n_a - \text{любое целое положительное число}\}$ .

Рассмотрим теперь алгоритм вычисления характеристической функции  $\chi_A(x)$  на слове  $x$ . Вначале вычисляется, представимо ли  $n$  в виде  $n_a 2^{R_{a1}n_a/\log_2 n_a}$  (число операций не превосходит  $c \log^a n$ , где  $a$  — некоторая постоянная). Если  $n$  представимо, то  $x$  записываем в виде матрицы  $n_a \times n_b$ , где  $n_b = 2^{R_{a1}n_a/\log_2 n_a}$ , и переходим к построению матрицы  $G_0$  или  $H_0 = G_0^{-1}$  (в противном случае  $\chi_A(x) = 0$ ).

Для построения матрицы  $G_0$  в соответствии с утверждением 6.1 достаточно  $cn_a 2^{2n_a}$  операций. Построение  $H_0 = G_0^{-1}$  потребует не более  $cn_a^3$  операций. Для умножения  $H_0$  на  $a$  нужно еще  $cn_a^2 n_b$  операций. Чтобы убедиться, что в полученном слове  $\gamma$  все  $\gamma_i$ ,  $i = 0, m$  — кодовые слова соответствующих кодов РС, т. е. для вычисления  $m$  характеристических функций кода РС над  $\text{GF}(q)$  ( $q = 2^{R_{a1}n_a/\log_2 n_a}$ ), в соответствии с утверждением 1.6 потребуется еще не более  $mcq^2 \log^2 q$  операций. Суммируя все полученные оценки и выражая их через  $n$ , получаем утверждение 6.5.

#### П.6.4. Доказательство утверждения 6.11

Для получения этих оценок достаточно рассмотреть обычное кодирование каскадного кодового множества из утверждения 6.5. Это кодирование проводится в два этапа: внешними, а затем внутренними кодами. Сначала проводится кодирование  $m = \log_2 n_a$  внешними кодами, т. е. кодами РС. Так как кодирование каждого кода РС сводится к перемножению двух многочленов степени не более  $n_b$  над полем  $\text{GF}(q)$ , где  $q = 2^{R_{a1}n_a/\log_2 n_a}$ , то, согласно [10], это можно осуществить схемой сложности  $cn_b \log^3 n_b n_a^2 (\log n_a)^{-2}$ . Следовательно, сложность схемы кодирования внешними кодами не более  $mcn_b (\log n_b)^3 n_a^2 (\log n_a)^{-2} = cn_b n_a^2 \log^3 n_b (\log n_a)^{-1}$ , а описание этой схемы можно построить за  $cn_b (\log n_b)^4 n_a^2 (\log n_a)^{-1}$  шагов на машине Тьюринга. В результате кодирования внешними кодами получается двоичная матрица  $\gamma$  размера  $n_a \times n_b$ . Затем  $n_b$  двоичных последовательностей длины  $n_a$ , т. е. столбцы матрицы  $\gamma$ , кодируются внутренними кодами, т. е. матрица  $G_0$  умножается на матрицу размера  $n_a \times n_b$ . Схема, реализующая такое умножение, имеет сложность не более  $cn_a^2 n_b$ , а сложность описания этой схемы при известной матрице  $G_0$  не более  $cn_a^2 n_b \log n_b$ .

Учитывая, что в соответствии с утверждением 6.1 для построения матрицы  $G_0$  потребуется не более  $cn_a 2^{2n_a}$  операций, и выражая все приведенные оценки через длину кода  $n$ , получаем утверждение 6.11.

#### П.6.5. Доказательство утверждения 6.13

Этот результат получается непосредственной оценкой необходимого числа шагов для вычисления на машине Тьюринга по следующей неформальной программе. По алгоритму, описанному при доказательстве теоремы 2.3, строим кодирующую  $G_0$  и проверочную  $H_0 = G_0^{-1}$  матрицы (число операций не более  $cn 2^{2n}$ ). Для каждого кода  $A_i^?$  с  $i \geq n/2$  строим все множество кодовых слов (достаточно  $cn 2^{2n/2}$  операций). Затем строится описание схемы декодирования каждого кода  $A_i^?$  по следующему принципу. Все кодовые слова раз-

бываются на пары, и строятся схемы, которые из пары кодовых слов выбирают и выдают на выход ближайшее к принятому. Следовательно, число кодовых слов, из которых следует выбирать ближайшее, сокращается вдвое. Эти слова опять попарно поступают на идентичные схемы, которые из каждой пары поступающих слов выбирают одно ближайшее к принятому, т. е. снова вдвое сокращается число слов, среди которых находится ближайшее к принятому. Продолжая подобным же образом, получим единственное слово, которое и есть результат декодирования по минимуму расстояния.

Таким образом, схема состоит из  $2^{Rn}$  идентичных схем, каждая из которых выбирает ближайшее только из двух слов и имеет сложность порядка  $n$ , т. е. сложность схемы декодирования одного кода  $A_i^n$  порядка  $n2^{Rn}$ , а всех кодов  $A_i^n$  не более  $cn2^{n/2}$ . Декодирование каждого из кодов  $A_i^n$ ,  $i < n/2$ , будем вести следующим образом:

а) слово-столбец  $x^i$  умножается слева на матрицу  $H_0$ , т. е.  $y = H_0 x^i$  (это реализуется схемой сложности  $cn^2$ , для описания которой достаточно  $cn^2 \log n$  операций);

б) нижние  $i$  символов рассматриваются как синдром, в соответствии со значением которого выбирается минимальный представитель смежного класса  $e$  (это реализуется схемой сложности не более  $cn2^i$ , описание которой можно получить за  $cn2^n$  операций);

в) в качестве результата декодирования выдается слово  $x^i + e$ , которое, как известно [23], есть ближайшее кодовое к принятому (это реализуется схемой сложности  $cn$ , для описания которой достаточно  $cn \log n$  операций). Таким образом, сложность схемы декодирования одного кода  $A_i^n$ ,  $i < n/2$ , не более  $cn2^{(1-R)n}$ , а всех кодов  $A_i^n$  не более  $cn2^{n/2}$ .

Суммируя все приведенные оценки сложности схемы декодирования и нахождения описания ее, получим утверждение 6.13.

#### П.6.6. Доказательство утверждения 6.14

Этот результат получается непосредственной оценкой необходимого числа операций для вычисления описания схемы декодирования на машине Тьюринга по следующей неформальной программе. Рассмотрим составной алгоритм каскадного декодирования. Он сводится к двум этапам: сначала все внутренние коды декодируются по минимуму расстояния, а затем внешний код (код РС) декодируется с исправлением ошибок и стираний. В соответствии с утверждением 1.4  $n_b$  внутренних кодов могут быть декодированы схемой сложности  $cn_b n_a^{2^{R_1} n_a}$ . Эти схемы могут быть описаны на машине Тьюринга не более чем за  $c(n_a 2^{(1-R_1)n_a} + n_b n_a^{2^{R_1} n_a} \log n)$  операций. Код РС декодируется посредством схемы, сложность которой не более  $cn_b^2 \log^2 n_b$ , описание которой может быть вычислено на машине Тьюринга за  $cn_b^2 \log^3 n_b$  операций. Выражая все полученные оценки через длину кода  $n$ , получаем утверждение 6.14.

#### П.6.7. Доказательство утверждения 6.17

Для получения этих оценок достаточно рассмотреть составное декодирование каскадного кода бесконечного порядка. Из гл. 3 и 4 следует, что оценка (6.21) асимптотически совпадает с кодовым расстоянием, а полный составной

алгоритм реализует его. Оценим теперь сложность схем декодирования и получения описания этих схем на машине Тьюринга. Напомним, что полный составной алгоритм каскадного декодирования состоит из  $m = \log_2 n_a$  шагов, каждый из которых реализуется в два этапа: сначала декодируются по минимуму расстояния все  $n_b$  соответствующих  $i=x$  внутренних кодов системы вложенных кодов, а затем осуществляется не более  $n_a$  попыток декодирования внешних кодов (кода РС) с исправлением ошибок и стираний.

Нетрудно убедиться, что в целом составной алгоритм каскадного кода сводится к декодированию по минимуму расстояния  $n_b$  систем вложенных кодов длины  $n_a$  и декодированию  $m$  различных кодов РС длины  $n_b$  с исправлением ошибок и стираний, причем каждый декодируется не более  $n_a$  раз. В соответствии с утверждением 6.13 системы вложенных кодов могут быть декодированы схемой сложности  $cn_b n_a^{2^{n_a/2}}$ , которая может быть описана на машине Тьюринга за  $cn_b n_a^{2^{n_a/2}} \log n + cn_a 2^{2^{n_a}}$  операций. Каждый код РС в соответствии с утверждением 1.6 декодируется посредством схемы сложности  $cn_b^2 \log^2 n_b$ , описание которой может быть получено на машине Тьюринга за  $cn_b^2 \log^3 n_b$  операций. Таким образом, общая сложность схемы декодирования равна  $cn_b n_a^{2^{n_a/2}} + cm n_a n_b^2 \log^2 n_b$ , а сложность получения описания этой схемы не более  $cn_b n_a^{n_a/2} \log n + cn_a 2^{2^{n_a}} + cm n_b^2 \log^3 n_b \log n_a$ .

Выражая все полученные оценки через длину кода  $n$ , получаем утверждение 6.17.

#### П.6.8. Доказательство утверждения 6.19

Для того чтобы вычислить характеристическую функцию кода  $A_i^{n_a}$ , построить схемы кодирования или декодирования (см. утверждения 6.1, 6.7 и 6.13), нужно знать кодирующую матрицу. Поэтому сначала оценим сложность построения этой матрицы, которую в соответствии с теоремой 2.4 будем строить следующим образом.

В качестве первого столбца возьмем любое слово веса  $n_a/2$ , т. е. получаем код, порождаемый этим столбцом и содержащий всего два слова (нулевое и первый столбец). Выпишем все смежные классы и их спектр весов (каждый смежный класс содержит два слова). Для этого достаточно  $cn_a 2^{2^{n_a}}$  операций.

Пусть теперь уже построено  $k_i = n_a - i$  столбцов матрицы  $G_0$  и выписаны на ленте код  $A_i^{n_a}$  и все его смежные классы со спектром весов. Выберем из смежных классов такой, спектр весов которого удовлетворяет лемме 2.1 (достаточно  $cn 2^{2^n}$  операций), и в качестве кода  $A_{i+1}^{n_a}$  возьмем объединение кода  $A_i^{n_a}$  с выбранным смежным классом. В качестве  $(k_i + 1)$ -го столбца матрицы  $G_0$  возьмем любое слово выбранного смежного класса. После этого построим все смежные классы кода  $A_{i+1}^{n_a}$ . Нетрудно убедиться, что для увеличения в матрице  $G_0$  столбцов на единицу достаточно  $cn_a^{2^{2^{n_a}}}$  операций. Следовательно, для построения всей матрицы  $G_0$  будет достаточно  $cn_a^{2^{2^{n_a}}}$  операций. Как следует из теоремы 2.4, каждый из кодов  $A_i^{n_a}$  будет удовлетворять оценкам ВГ и Галлагера.

Построение схем кодирования и декодирования по минимуму расстояния аналогично рассмотренным в утверждениях 6.7 и 6.13 и имеет те же оценки сложности, что завершает доказательство утверждения 6.19.



### П.6.9. Доказательство утверждения 6.24.

Рассмотрим построение и характеристики каскадных систем с низкоплотностными кодами в качестве внешних (в данном случае будем строить каскадный код первого порядка). Передаваемая информация, т. е.  $k$  двоичных информационных символов, кодируется низкоплотностным кодом длины  $n^* = k_a n_b$  ( $k_a$  и  $n_b$  — целые положительные числа) со скоростью передачи  $R_{b1} = k/n^*$ , который в дальнейшем будем называть внешним кодом. В результате получаем кодовое слово низкоплотностного кода, которое будем представлять в виде двоичной матрицы  $U$  размера  $k_a \times n_b$ , т. е.

$$U = (u^1, u^2, \dots, u^{n_b}), \quad (\text{П. 6. 1})$$

где  $u^j$  — двоичное слово-столбец длины  $k_a$ .

Пусть  $G_0$  — двоичная матрица размера  $n_a \times k_a$ , такая, что линейное пространство, порождаемое ее столбцами, образует линейный двоичный код со спектром весов, удовлетворяющим теореме 1.3. Тогда слово каскадного кода  $x$ , т. е. матрица размера  $n_a \times n_b$ , получается в результате умножения матрицы  $G_0$  на матрицу  $U$ , т. е.

$$x = G_0 U = (x^1, x^2, \dots, x^{n_b}), \quad (\text{П. 6. 2})$$

где  $x^j$  — вектор-столбец длины  $n_a$  (кодовое слово внутреннего кода).

Таким образом, получаем каскадный код первого порядка длины  $n = n_a n_b$  со скоростью передачи  $R = R_{a1} R_{b1}$  ( $R_{a1} = k_a/n_a$ ).

Условимся при  $R < C$ , где  $C$  — пропускная способность ДСК без памяти, скорости передачи внутреннего кода  $R_{a1}$  и внешнего кода  $R_{b1}$  выбирать так, что  $R_{a1} < C$ , а  $R_{b1} = R/R_{a1} < 1$ .

После передачи слова  $x$  по ДСК без памяти с вероятностью трансформации символа  $\varepsilon$  получаем слово  $y = (y^1, y^2, \dots, y^{n_b})$ , где  $y^j = x^j + e^j$ , а  $e^j$  — вектор ошибок в  $j$ -м столбце. Декодировать слово  $y$  будем следующим образом: сначала все  $y^j$ ,  $j = \overline{1, n_b}$ , декодируем в слова внутреннего кода по минимуму расстояния. В результате получим слово  $\hat{u} = (\hat{u}^1, \hat{u}^2, \dots, \hat{u}^{n_b})$ , где  $\hat{u}^j$  — информационные символы кодового слова внутреннего кода, полученного в результате декодирования  $y^j$ . Затем слово  $\hat{u}$  декодируется по описанному в работе [83] алгоритму декодирования в кодовое слово низкоплотностного кода, т. е. исправляется сочетание ошибок, если их кратность не превосходит  $pn^*$ .

Оценим теперь сложностные параметры такой каскадной системы. При этом длину  $n_a$  будем выбирать так, что  $R_{a1} n_a \leq \log_2 \log_2 n$ . Сложность задания такого каскадного кода будет оцениваться сложностями задания низкоплотностного кода и построения матрицы  $G_0$  порядка  $n_a$ . Из утверждения 6.18 следует, что сложность задания низкоплотностного кода оценивается как  $T(n) \leq c 2^{\varepsilon n^*} \log n^*$ , или, учитывая, что  $n^* = R_{a1} n$ , получаем

$$T(n) \leq c 2^{\varepsilon n \log n}, \quad (\text{П. 6. 3})$$

где  $c$  — некоторая постоянная. В силу утверждения 6.19 сложность построения «хорошей» кодирующей матрицы  $G_0$  оценивается как  $T(n) \leq c n_a^{2^2 n_a}$ , или, учитывая, что  $R_{a1} n_a \leq \log_2 \log_2 n$ , получаем

$$T(n) \leq c (\log_2 \log_2 n)^2 \log_2^2 n. \quad (\text{П. 6. 4})$$

Из (П.6.3) и (П.6.4) вытекает справедливость первого из соотношений (6.47). Справедливость второго из соотношений (6.47), т. е. оценки сложности кодирования, есть следствие линейности каскадного кода.

Сложность  $\kappa$  декодирования каскадного кода оценивается сверху суммой сложностей декодирования всех  $n_b$  внутренних кодов  $\kappa_a$  и сложности декодирования внешнего кода  $\kappa_b$ , т. е.  $\kappa = \kappa_a + \kappa_b$ . Так как сложность декодирования одного внутреннего кода не более  $cn_a 2^{R_{a1} n_a}$ , а число таких кодов  $n_b$ , то

$$\kappa_a \leq cn_a 2^{R_{a1} n_a} n_b = cn 2^{R_{a1} n_a}, \quad (\text{П. 6. 5})$$

где  $c$  — некоторая постоянная. Учитывая, что  $R_{a1} n_a \leq \log_2 \log_2 n$ , имеем

$$\kappa_a \leq cn \log n. \quad (\text{П. 6. 6})$$

Сложность  $\kappa_b$ , как следует из [83], имеет порядок роста  $n^* \log n^*$ . Учитывая, что  $n^* = k_a n_b = R_{a1} n$ , получаем

$$\kappa_b \leq cn \log n, \quad (\text{П. 6. 7})$$

где  $c$  — некоторая постоянная. Из (П.6.6) и (П.6.7) следует, что

$$\kappa = \kappa_a + \kappa_b \leq cn \log n. \quad (\text{П. 6. 8})$$

Таким образом, сложность декодирования рассмотренного каскадного кода первого порядка имеет такой же порядок роста с длиной кода, как и сложность декодирования низкоплотностного кода.

Неправильное декодирование рассмотренного выше каскадного кода может возникнуть, только если после декодирования всех внутренних кодов в слове  $\hat{u}$  будет больше, чем  $\rho n^*$  ошибок. Так как слова  $y^j$ ,  $j=1, n_b$ , декодируются по минимуму расстояния, то результат декодирования будет неправильным с вероятностью

$$P_a \leq \exp \{-n_a E_0(R_{a1})\}, \quad (\text{П. 6. 9})$$

где  $E_0(R_{a1})$  — экспонента вероятности ошибки при скорости передачи  $R_{a1}$ , определяемая в соответствии с теоремой 1.4 (оценка Галлагера).

Пусть число слов  $\hat{u}^j$  с ошибками равно  $b$ , тогда вероятность  $P_b$  того, что декодирование будет неправильным, мажорируется вероятностью того, что в слове  $\hat{u}$  будет более  $\rho n^*$  ошибок:

$$P_b \leq \sum_{b=1}^{n_b} C_{n_b}^b P_a^b (1 - P_a)^{n_b - b} P \{t \geq \rho n^* | b\}, \quad (\text{П. 6. 10})$$

где  $P \{t \geq \rho n^* | b\}$  — условная вероятность того, что в  $b$  фиксированных неправильно декодированных  $\hat{u}^j$  суммарное число ошибок больше  $\rho n^*$ . Очевидно, что  $P \{t \geq \rho n^* | b\} = 0$ , если  $b R_{a1} n_a < \rho n^*$ . При  $b R_{a1} n_a > \rho n^*$  вероятность  $P \{t \geq \rho n^* | b\}$  меньше вероятности того, что до декодирования в соответствующих словах  $y^*$  было больше  $\rho n^*/2$  ошибок (при декодировании по минимуму расстояния число ошибок в неправильно декодированном слове не более чем удваивается). Следовательно, получаем следующую оценку

$$P \{t \geq \rho n^* | b\} \leq \sum_{i \geq \rho n^*/2}^{b n_a} C_{b n_a}^i \varepsilon^i (1 - \varepsilon)^{b n_a - i}. \quad (\text{П. 6. 11})$$

Подставляя правую часть (П.6.11) в (П.6.10), имеем

$$P_b \leq \sum_{b > \rho n_b}^{n_b} C_{n_b}^b P_a^b (1 - P_a)^{n_b - b} \sum_{i \geq \rho n^*/2}^{bn_a} C_{n_a b}^i \varepsilon^i (1 - \varepsilon)^{n_a b - i}. \quad (\text{П. 6. 12})$$

Отсюда, обозначая через  $\beta = b/n$ , при  $n \rightarrow \infty$  и  $n_a \rightarrow \infty$  после элементарных преобразований выводим  $P_b \leq \exp \{-n E_1(R_{a1}, \rho)\}$ , где  $E_1(R_{a1}, \rho) = \min_{\beta \geq \rho R_{a1}} \{\beta [E_0(R_{a1}) + F(\beta, \rho, R_{a1}, \varepsilon)]\}$ ,

$$F(\beta, \rho, R_{a1}, \varepsilon) =$$

$$= \begin{cases} -H\left(\frac{\rho R_{a1}}{2\beta}\right) + \frac{\rho R_{a1}}{2\beta} \ln \varepsilon + \left(1 - \frac{\rho R_{a1}}{2\beta}\right) \ln (1 - \varepsilon) & \text{при } \varepsilon \leq \frac{\rho R_{a1}}{2\beta}; \\ 0 & \text{при } \varepsilon > \frac{\rho R_{a1}}{2\beta}. \end{cases}$$

Нетрудно убедиться, что при любых  $R < C$  экспонента  $E_1(R_{a1}, \rho) > 0$ , так как  $R_{a1} < C$ ,  $R_{b1} < 1$ , т. е.  $E_0(R_{a1}) > 0$ ,  $\rho > 0$ . С другой стороны, при фиксированном  $R$  скорости  $R_{a1}$  и  $R_{b1}$  следует выбирать так, чтобы максимизировать  $E_1(R_{a1}, \rho)$ , что завершает доказательство утверждения.

## ЛИТЕРАТУРА

1. Андрианов В. И., Сасковец В. Н. Дедиклические коды. — Кибернетика, 1965, № 1, с. 11—16.
2. Арутюнян Е. А. Оценка экспоненты вероятности ошибки для непрерывного канала без памяти. — Пробл. передачи информ., 1968, № 4, с. 37—48.
3. Афанасьев В. Б. Быстрое кодирование и обнаружение ошибок кодом Риды—Соломона. — В кн.: III Междунар. симпоз. по теории информации: Тез. докл. Москва; Таллин, 1973, ч. 2, с. 13—15.
4. Афанасьев В. Б. Вычисление значений и корней многочленов над конечным полем. — В кн.: Повышение верности передачи цифровой информации по дискретным каналам. М.: Наука, 1974, с. 49—55.
5. Афанасьев В. Б. Новые алгоритмы декодирования кодов Риды—Соломона. — В кн.: VI конф. по теории кодирования и передачи информации: Докл. Москва; Томск, 1975, ч. 2, с. 13—18.
6. Афанасьев В. Б. Сложность декодирования кодов Риды—Соломона. — В кн.: Труды Междунар. симпоз. по теории информации: Тез. докл. М., 1976, ч. 2, с. 10—13.
7. Бабкин В. Ф., Штарьков Ю. М. О применении корректирующих кодов в некоторых каналах. — В кн.: Передача цифровой информации по каналам с памятью. М.: Наука, 1970, с. 52—60.
8. Бассалыго Л. А. Новые верхние границы для кодов, исправляющих ошибки. — Пробл. передачи информ., 1965, № 4, с. 41—44.
9. Бассалыго Л. А. Формализация задачи о сложности задания кода. — Пробл. передачи информ., 1976, № 4, с. 105—106.
10. Бассалыго Л. А. Замечание о быстром умножении многочлена над полями Галуа. — Пробл. передачи информ., 1978, № 1, с. 101—102.
11. Бассалыго Л. А., Зяблов В. В., Пинскер М. С. Проблемы сложности в теории корректирующих кодов. — Пробл. передачи информ., 1977, № 3, с. 5—17.
12. Бассалыго Л. А., Зиновьев В. А., Зяблов В. В. и др. Границы для кодов с неравной защитой двух множеств сообщений. — Пробл. передачи информ., 1979, № 3, с. 40—49.
13. Берлекэмп Э. Алгебраическая теория кодирования: Пер. с англ. М.: Мир, 1971. 477 с.
14. Берман С. Д. К теории групповых кодов. — Кибернетика, 1967, № 1, с. 31—39.
15. Блос Э. Л. Видоизменение процедуры использования кодов Риды—Соломона для построения кодов исправляющих пакет ошибок. — В кн.: Теория передачи информации. М.: Наука, 1964, с. 32—34.
16. Блос Э. Л. Исправление ошибок и стираний кодами Боуза—Чоудхури. — Пробл. передачи информ., 1965, № 3, с. 12—19.
17. Блос Э. Л., Зяблов В. В. Каскадные итерированные коды и применение их для исправления пакетов ошибок. — В кн.: Передача дискретных сообщений по каналам с группирующимися ошибками. М.: Наука, 1972, с. 5—8.
18. Блос Э. Л., Зяблов В. В. О существовании линейных двоичных каскадных кодов с оптимальными корректирующими свойствами. — Пробл. передачи информ., 1973, № 4, с. 3—10.
19. Блос Э. Л., Зяблов В. В. Кодирование и декодирование обобщенного каскадного кода. — В кн.: III междунар. симпоз. по теории информации: Тез. докл. Москва; Таллин, 1973, ч. 2, с. 36—40.
20. Блос Э. Л., Зяблов В. В. Кодирование обобщенных каскадных кодов. — Пробл. передачи информ., 1974, № 3, с. 45—50.

21. Блох Э. Л., Зяблов В. В. Потенциальные и реализуемые корректирующие свойства каскадных кодов на основе кодов Риди—Соломона. — В кн.: Повышение верности передачи цифровой информации по дискретным каналам. М.: Наука, 1974, с. 5—17.
22. Блох Э. Л., Зяблов В. В. Составной алгоритм декодирования каскадного кода в канале без памяти. — В кн.: VI конф. по теории кодирования и передачи информации: Доклады. Москва; Томск, 1975, ч. 2, с. 19—24.
23. Блох Э. Л., Зяблов В. В. Обобщенные каскадные коды. М.: Связь, 1976. 240 с. с ил.
24. Блох Э. Л., Зяблов В. В. Оценка асимптотики кодового расстояния обобщенного каскадного кода. — В кн.: Кодирование и передача дискретных сообщений в системах связи. М.: Наука, 1976, с. 3—21.
25. Блох Э. Л., Зяблов В. В. Построение обобщенных каскадных кодов на базе кодов БЧХ. — В кн.: Кодирование и передача дискретных сообщений в системах связи. М.: Наука, 1976, с. 21—28.
26. Блох Э. Л., Зяблов В. В. Обобщенные каскадные коды. — В кн.: Вопросы кибернетики. Актуальные проблемы теории информации. М., Науч. совет по компл. пробл. «Кибернетика» АН СССР, 1977, вып. 29, с. 3—27.
27. Блох Э. Л., Зяблов В. В. Границы для кодового расстояния каскадных кодов. — В кн.: Вопросы кибернетики. Проблемы избыточности в информационных системах. М.: Науч. совет по компл. пробл. «Кибернетика» АН СССР, 1977, вып. 34, с. 48—60.
28. Блох Э. Л., Зяблов В. В. Экспонента вероятности ошибки при каскадном декодировании. — В кн.: VII Всесоюз. конф. по теории кодирования и передачи информации: Доклады. Москва; Вильнюс, 1978, ч. 2, с. 23—28.
29. Блох Э. Л., Зяблов В. В. Перспективные методы помехоустойчивого кодирования. — Электросвязь, 1978, № 6, с. 70—73.
30. Блох Э. Л., Зяблов В. В. Оценки корректирующих свойств ансамбля каскадных кодов бесконечного порядка. — В кн.: V междунар. симпоз. по теории информации: Тез. докл. Москва; Тбилиси, 1979, ч. 1, с. 49—52.
31. Блох Э. Л., Зяблов В. В. Случайные каскадные коды произвольного порядка. — В кн.: Построение и анализ систем передачи информации. М.: Наука, 1980, с. 3—13.
32. Блох Э. Л., Зяблов В. В. Обменные соотношения вероятности ошибки и стирания для двоичных линейных кодов. — В кн.: Построение и анализ систем передачи информации. М.: Наука, 1980, с. 26—34.
33. Блох Э. Л., Попов О. В., Турин В. Я. Модели источника ошибок в каналах передачи цифровой информации. М.: Связь, 1971. 312 с.
34. Бородин Л. Ф. Введение в теорию помехоустойчивого кодирования. М.: Сов. радио, 1968. 408 с. с ил.
35. Бояринов И. М. О кодах, исправляющих пакеты ошибок с ограниченной плотностью. — Пробл. передачи информ., 1973, № 1, с. 104—107.
36. Бояринов И. М. Об одной конструкции линейных кодов с неравной защитой информационных символов. — Пробл. передачи информ., 1980, № 2, с. 103—107.
37. Бояринов И. М. Метод декодирования прямых сумм произведений кодов и его применение. — Пробл. передачи информ., 1981, № 2, с. 39—51.
38. Бояринов И. М., Кацман Г. Л. О линейных кодах с неравной защитой символов. — В кн.: VII Всесоюз. симпоз. по проблеме избыточности в информационных системах: Тез. докл. Л., 1977, ч. 1, с. 66—70.
39. Бояринов И. М., Кацман Г. Л. Линейные коды с неравной защитой символов. — В кн.: Вопросы кибернетики. Проблемы избыточности в информационных системах. М.: Науч. совет по компл. пробл. «Кибернетика» АН СССР, 1977, вып. 34, с. 60—91.
40. Бояринов И. М., Кацман Г. Л. Две конструкции кодов с неравной защитой символов от группирующихся ошибок. — В кн.: VII Всесоюз. конф. по теории кодирования и передачи информации: Доклады. Москва; Вильнюс, 1978, с. 15—19.
41. Бояринов И. М., Кацман Г. Л. Класс оптимальных двоичных линейных кодов с неравной защитой информационных символов. — В кн.: V между-

- нар. симпози. по теории информации: Тез. докл. Москва; Тбилиси, 1979, ч. 1, с. 56—58.
42. *Варшавов Р. Р.* Оценка числа сигналов в кодах с коррекцией ошибок. — ДАН СССР, 1957, 117, № 5, с. 739—741.
  43. *Введенская Н. Д., Зяблов В. В.* Экспериментальное исследование исправления ошибок низкоплотностными кодами. — В кн.: VI конф. по теории кодирования и передачи информации: Доклады. Москва; Томск, 1975, ч. 2, с. 44—48.
  44. *Введенская Н. Д., Зяблов В. В.* Каскадные коды с проверкой на четность во внутреннем коде. — В кн.: VII Всесоюз. конф. по теории кодирования и передачи информации: Доклады. Москва; Вильнюс, 1978, ч. 2, с. 29—32.
  45. *Возенкрафт Дж. М., Рейфорен Б.* Последовательное декодирование: Пер. с англ. М.: Изд-во иностр. лит., 1963. 153 с.
  46. *Возенкрафт Дж. М., Джекобс И.* Теоретические основы техники связи: Пер. с англ. М.: Мир, 1969. 640 с.
  47. *Габидулин Э. М.* Границы для вероятности ошибки декодирования при использовании линейных кодов в каналах без памяти. — Пробл. передачи информ., 1967, № 2, с. 55—62.
  48. *Габидулин Э. М.* Об оценках вероятности ошибки для некоторых каналов с памятью. — Пробл. передачи информ., 1969, № 1, с. 40—46.
  49. *Габидулин Э. М., Коржик В. И.* Коды, исправляющие ошибки решетчатой конфигурации. — Изв. вузов. Радиоэлектроника, 1972, № 4, с. 492—498.
  50. *Габидулин Э. М., Сидоренко В. Р.* Об одной общей границе объема кода. — Пробл. передачи информ., 1976, № 4, с. 31—35.
  51. *Галлагер Р.* Коды с малой плотностью проверок на четность: Пер. с англ. М.: Мир, 1966. 144 с.
  52. *Галлагер Р.* Теория информации и надежная связь: Пер. с англ. М.: Сов. радио, 1974. 720 с.
  53. *Гоппа В. Д.* Новый класс линейных корректирующих кодов. — Пробл. передачи информ., 1970, № 3, с. 24—30.
  54. *Гоппа В. Д.* На неприводимых кодах достигается пропускная способность ДСК. — Пробл. передачи информ., 1974, № 1, с. 111—112.
  55. *Дадаев Ю. Г.* Арифметические коды, исправляющие ошибки. М.: Сов. радио, 1969. 168 с.
  56. *Дельсарт Ф.* Алгебраический подход к схемам отношений теории кодирования: Пер. с англ. М.: Мир., 1976. 134 с.
  57. *Думер И. И.* Исправление пакетов ошибок каскадными кодами. — В кн.: V всесоюз. школа-семинар по вычислительным сетям. Москва; Владивосток, 1980, ч. 4, с. 86—91.
  58. *Думер И. И.* О декодировании обобщенных каскадных кодов. — В кн.: V всесоюз. школа-семинар по вычислительным сетям. Москва; Владивосток, 1980, ч. 2, с. 92—95.
  59. *Емельянов Г. А., Шварцман В. О.* Передача дискретной информации и основы телеграфии. М.: Связь, 1973. 383 с.
  60. *Жегалов С. И.* Линейные блочные коды, исправляющие многократные пакеты ошибок и независимые ошибки. — Пробл. передачи информ., 1977, № 4, с. 54—61.
  61. *Жигулин Л. Ф., Зяблов В. В.* Экспонента вероятности ошибки в системе с обратной связью при использовании каскадного кода. — Пробл. передачи информ., 1973, № 1, с. 3—10.
  62. *Зайцев Г. В., Зиновьев В. А., Семаков Н. В.* Быстрое корреляционное декодирование блочных кодов. — В кн.: Кодирование и передача дискретных сообщений в системах связи. М.: Наука, 1976, с. 74—85.
  63. *Зигангиров К. Ш.* Процедуры последовательного декодирования. М.: Связь, 1974. 208 с.
  64. *Зиновьев В. А.* Обобщенные каскадные коды. — Пробл. передачи информ., 1976, № 1, с. 5—15.
  65. *Зиновьев В. А.* О корректирующих способностях обобщенных каскадных кодов. — В кн.: V всесоюз. школа-семинар по вычислительным сетям. Москва; Владивосток, 1980, ч. 4, с. 111—114.

66. *Зиновьев В. А., Зяблов В. В.* Декодирование нелинейных обобщенных каскадных кодов. — В кн.: IV междунар. симпоз. по теории информации: Тез. докл. М.; Л., 1976, ч. 2, с. 42—44.
67. *Зиновьев В. А., Зяблов В. В.* Исправление обобщенными каскадными кодами независимых ошибок при наличии пакетов. — В кн.: VII всесоюз. симпоз. по проблеме избыточности в информационных системах: Тез. докл. Л., 1977, ч. 1, с. 78—81.
68. *Зиновьев В. А., Зяблов В. В.* Декодирование нелинейных обобщенных каскадных кодов. — Пробл. передачи информ., 1978, № 2, с. 46—52.
69. *Зиновьев В. А., Зяблов В. В.* Исправление пакетов и независимых ошибок обобщенными каскадными кодами. — Пробл. передачи информ., 1979, № 2, с. 58—70.
70. *Зиновьев В. А., Зяблов В. В.* Коды с неравной защитой. — Пробл. передачи информ., 1979, № 3, с. 50—60.
71. *Зяблов В. В.* Кусочно-циклические коды и схема их декодирования по большинству. — Пробл. передачи информ., 1968, № 2, с. 31—37.
72. *Зяблов В. В.* Алгоритмы поэтапного декодирования итерированных и каскадных кодов. — В кн.: Передача цифровой информации по каналам с памятью. М.: Наука, 1970, с. 86—92.
73. *Зяблов В. В.* Анализ корректирующих свойств итерированных и каскадных кодов. — В кн.: Передача цифровой информации по каналам с памятью. М.: Наука, 1970, с. 76—85.
74. *Зяблов В. В.* Оценка сложности построения двоичных линейных каскадных кодов. — Пробл. передачи информ., 1971, № 1, с. 5—13.
75. *Зяблов В. В.* Сложность декодирования итерированных и каскадных кодов. — В кн.: Труды II Междунар. симпоз. по теории информации: Доклады. Цахкадзор, 1974, с. 83—87.
76. *Зяблов В. В.* Оптимизация алгоритмов каскадного декодирования. — Пробл. передачи информ., 1973, № 1, с. 26—32.
77. *Зяблов В. В.* Алгоритм декодирования двоичных БЧХ-кодов и реализующие его схемы. — В кн.: Передача дискретных сообщений по каналам с группирующимися ошибками. М.: Наука, 1972, с. 23—34.
78. *Зяблов В. В.* Исправление стираний в двоичных линейных кодах. — В кн.: Передача дискретных сообщений по каналам с группирующимися ошибками. М.: Наука, 1972, с. 34—38.
79. *Зяблов В. В.* Новая трактовка кодов для локализации ошибок, их корректирующие свойства и алгоритмы декодирования. — В кн.: Передача дискретных сообщений по каналам с группирующимися ошибками. М.: Наука, 1972, с. 8—18.
80. *Зяблов В. В., Афанасьев В. Б., Иванова Л. А., Шутиков И. В.* Результаты моделирования трехмерных кодов с локализацией ошибок. — В кн.: Передача дискретных сообщений по каналам с группирующимися ошибками. М.: Наука, 1972, с. 47—51.
81. *Зяблов В. В., Жигулин Л. Ф.* Улучшение экспоненты вероятности ошибки в системе с обратной связью при использовании каскадного кода. — В кн.: Повышение верности передачи цифровой информации по дискретным каналам. М.: Наука, 1974, с. 56—62.
82. *Зяблов В. В., Пинскер М. С.* Сложность декодирования низкоплотностных кодов при передаче по каналу со стираниями. — Пробл. передачи информ., 1974, № 1, с. 15—28.
83. *Зяблов В. В., Пинскер М. С.* Оценка сложности исправления ошибок низкоплотностными кодами Галлагера. — Пробл. передачи информ., 1975, № 1, с. 23—36.
84. *Зяблов В. В., Пинскер М. С.* Надежная передача информации при малой сложности декодирования. — В кн.: VI конф. по теории кодирования и передачи информации: Доклады. Москва; Томск, 1975, ч. 2, с. 64—69.
85. *Зяблов В. В., Пинскер М. С.* Коды с малой средней сложностью декодирования. — В кн.: IV междунар. симпоз. по теории информации: Тез. докл. М.; Л., 1976, ч. 2, с. 48—50.

86. *Зяблов В. В., Пинскер М. С.* Каскадное кодирование списками. — В кн.: V всесоюз. школа-семинар по вычислительным сетям. Москва; Владивосток, 1980, ч. 4, с. 115—120.
87. *Зяблов В. В., Самаров А. М., Хасьминский Р. З.* Задача оценивания при ограниченных ресурсах статистика. — Пробл. передачи информ., 1977, № 3, с. 32—44.
88. *Зяблов В. В., Штарьков Ю. М.* Сложность реализации алгоритмов автоматами. — В кн.: VI конф. по теории кодирования и передачи информации: Доклады. Москва; Томск, 1975, ч. 2, с. 70—76.
89. *Касами Т., Токура Н., Иадурс Е., Инагаки Я.* Теория кодирования: Пер. с яп. М.: Мир, 1978. 576 с.
90. *Кловский Д. Д.* Передача дискретных сообщений по радиоканалам. М.: Связь, 1969.
91. *Козлов Н. В.* Об ансамбле кодов с малой плотностью единиц в проверочной матрице. — Пробл. передачи информ., 1971, № 3, с. 107—109.
92. *Колесник В. Д.* Вероятностное декодирование мажоритарных кодов. — Пробл. передачи информ., 1971, № 3, с. 3—17.
93. *Колесник В. Д., Мирончиков Е. Т.* Некоторые циклические коды и схема декодирования по большинству проверок. — Пробл. передачи информ., 1965, № 2, с. 3—17.
94. *Колесник В. Д., Мирончиков Е. Т.* Декодирование циклических кодов. М.: Связь, 1968. 251 с.
95. *Колесник В. Д., Полтырев Г. Ш.* О сложности декодирования в дискретных постоянных каналах. — В кн.: Вопросы кибернетики. Актуальные проблемы теории информации. М.: Науч. совет по компл. пробл. «Кибернетика» АН СССР, 1977, вып. 29, с. 46—61.
96. *Колесник В. Д., Полтырев Г. Ш.* О сложности декодирования итерационных кодов. — В кн.: Вопросы кибернетики. Актуальные проблемы теории информации. М.: Науч. совет по компл. пробл. «Кибернетика» АН СССР, 1977, вып. 29, с. 62—78.
97. *Колмогоров А. Н.* Три подхода к определению понятия «количества информации». — Пробл. передачи информ., 1965, № 1, с. 3—11.
98. *Колмогоров А. Н.* К логическим основам теории информации и теории вероятностей. — Пробл. передачи информ., 1969, № 3, с. 3—7.
99. *Коржик В. И., Осмоловский С. А., Финк Л. М.* Универсальное стохастическое кодирование в системах с решающей обратной связью. — Пробл. передачи информ., 1974, № 4, с. 25—29.
100. *Коржик В. И., Финк Л. М.* Помехоустойчивое кодирование дискретных сообщений в каналах со случайной структурой. М.: Связь, 1975. 271 с.
101. *Котельников В. А.* Теория потенциальной помехоустойчивости. М; Л.: ГЭИ, 1956. 151 с.
102. *Крачковский В. Ю.* Сложность построения кодов, обладающих заданными корректирующими свойствами. — Пробл. передачи информ., 1980, № 1, с. 50—55.
103. *Кузнецов А. В.* Хранение информации в памяти из ненадежных элементов. — Пробл. передачи информ., 1973, № 3, с. 100—114.
104. *Левенштейн В. И.* О верхних оценках для кодов с фиксированным весом векторов. — Пробл. передачи информ., 1971, № 4, с. 3—12.
105. *Левенштейн В. И.* О минимальной избыточности двоичных кодов, исправляющих ошибки. — Пробл. передачи информ., 1974, № 2, с. 26—42.
106. *Левин Л. А.* Универсальные задачи перебора. — Пробл. передачи информ., 1973, № 3, с. 115—116.
107. *Луанов О. Б.* О синтезе некоторых классов управляющих схем. — В кн.: Проблемы кибернетики. М.: Наука Глав. ред. физ.-мат. лит., 1967, вып. 10, с. 63—97.
108. *Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А.* Теория кодов, исправляющих ошибки: Пер. с англ. М.: Связь, 1979. 774 с.
109. *Мальцев А. И.* Алгоритмы и рекурсивные функции. М.: Наука, 1965. 391 с.



110. *Марчуков А. С.* О суммировании произведений кодов. — Пробл. передачи информ., 1968, № 2, с. 11—20.
111. *Месси Дж.* Пороговое декодирование: Пер с англ. М.: Мир, 1966. 207 с.
112. *Мешковский К. А., Кириллов Н. Е.* Кодирование в технике связи. М.: Связь, 1966. 324 с.
113. *Овчинников В. В.* Обобщенные каскадные сверточно-блочные коды. — В кн.: VII всесоюз. симпоз. по проблеме избыточности в информационных системах: Тез. докл. Л., 1977, ч. 1, с. 106—108.
114. *Омзоре Х.* Экономический эффект от использования кодирования для источника и кодирования канала. — Пробл. передачи информ., 1977, № 2, с. 3—10.
115. *Питерсон У., Уэлдон Э.* Коды, исправляющие ошибки: Пер. с англ. М.: Мир, 1976. 594 с.
116. *Попов О. В.* О кодовой защите цифровой информации в стандартных телефонных каналах. — В кн.: III конф. по теории передачи и кодирования информации. Секция 2. М.: Науч. совет по компл. пробл. «Кибернетика» АН СССР, 1967.
117. *Попов О. В.* Об исправлении стираний циклическими кодами. — В кн.: Передача цифровой информации по каналам с памятью. М.: Наука, 1970, с. 111—124.
118. *Попов О. В.* Об исправлении ошибок кодами Вулфа—Элепаса. — В кн.: Передача дискретных сообщений по каналам с группирующимися ошибками. М.: Наука, 1972, с. 18—22.
119. *Попов О. В.* Коды с каскадной локализацией для исправления ошибок с переменным группированием. — В кн.: III междунар. симпоз. по теории информации: Тез. докл. Москва; Таллин, 1973, ч. 2, с. 131—136.
120. *Попов О. В.* Исправление группирующихся ошибок методом каскадной локализации. — В кн.: Повышение верности передачи цифровой информации по дискретным каналам. М.: Наука, 1974, с. 27—42.
121. *Попов О. В., Устинов Г. Н.* Коды с локализацией ошибок. — В кн.: Передача цифровой информации по каналам с памятью. М.: Наука, 1970, с. 71—85.
122. *Попов С. А.* Оценка эффективности каскадного кода на базе сверточного при различных способах декодирования. — В кн.: VII Всесоюз. конф. по теории кодирования и передачи информации: Доклады. Москва; Вильнюс, 1978, ч. 2, с. 130—133.
123. *Роджерс Х.* Теория рекурсивных функций и эффективная вычислимость: Пер. с англ. М.: Мир, 1972. 624 с.
124. *Руднева И. В.* Исследование параметров обобщенных каскадных кодов на основе кодов БЧХ. — В кн.: Кодирование и передача дискретных сообщений в системах связи. М.: Наука, 1976, с. 28—52.
125. *Руднева И. В.* Энергетическое усиление каскадных кодов. — В кн.: VII Всесоюз. конф. по теории кодирования и передачи информации: Доклады. Москва; Вильнюс, 1978, ч. 5, с. 153—158.
126. *Руднева И. В.* Оценка вероятности ошибки и стирания при декодировании линейных кодов в гауссовском канале. — В кн.: Построение и анализ систем передачи информации. М.: Наука, 1980, с. 33—42.
127. *Сагалович Ю. Л.* Кодирование состояний и надежность автоматов. М.: Связь, 1975. 208 с.
128. *Сагалович Ю. Л.* Каскадные коды состояний автомата. — Пробл. передачи информ., 1978, № 2, с. 75—85.
129. *Самойленко С. И.* Помехоустойчивое кодирование. М.: Наука, 1966. 239 с.
130. *Сидоренко В. Р.* Верхняя граница мощности  $g$ -х кодов. — Пробл. передачи информ., 1975, № 3, с. 14—20.
131. *Скворцов Э. Ф., Сулимов Ю. В.* Об одном подходе к вопросу декодирования кодов Боуза—Чоудхури—Хоквингема. — Пробл. передачи информ., 1976, № 4, с. 36—45.
132. *Скопинцев О. Д.* Кодирование обобщенных сверточно-блочных каскадных кодов. — В кн.: VII Всесоюз. конф. по теории кодирования и пе-

- редачи информации: Доклады. Москва; Вильнюс, 1978, ч. 2, с. 139—144.
133. Скопинцев О. Д., Попов С. А. О построении «хороших» систем вложенных сверточных кодов. — В кн.: V всесоюз. школа-семинар по вычислительным сетям. Москва; Владивосток, 1980, ч. 4, с. 145—150.
  134. Слоэн Н. Дж. А. Обзор конструктивной теории кодирования и таблицы кодов с наибольшими известными скоростями. — В кн.: Кибернетический сборник. Новая серия. М.: Мир, 1973, вып. 10, с. 5—82.
  135. Стиффлер Дж. Дж. Теория синхронной связи: Пер. с англ. М.: Связь, 1975. 488 с.
  136. Турин В. Я. Передача информации по каналам с памятью. М.: Связь, 1977. 248 с.
  137. Удалов А. П., Супрун Б. А. Избыточное кодирование при передаче сообщений двоичными кодами. М.: Связь, 1964. 270 с.
  138. Феллер В. Введение в теорию вероятностей и ее приложения: Пер. с англ. М.: Мир, 1967. Т. 1. 498 с.
  139. Финк Л. М. Теория передачи дискретных сообщений. М.: Сов. радио, 1970. 728 с.
  140. Форни Д. Каскадные коды: Пер. с англ. М.: Мир, 1970. 207 с.
  141. Форни Д. Экспоненциальные границы для ошибки в системах со стиранием, декодированием списком и решающей обратной связью. В кн.: Некоторые вопросы теории кодирования. М.: Мир, 1970, с. 166—204.
  142. Харкевич А. А. Борьба с помехами. М.: Наука, 1965. 275 с.
  143. Шеннон К. Е. Работы по теории информации и кибернетике. М.: Изд-во иностр. лит., 1963. 829 с.
  144. Элиас П. Безошибочное кодирование. — В кн.: Коды с обнаружением и исправлением ошибок. М.: Изд-во иностр. лит., 1956, с. 59—71.
  145. Юстесен Й. Класс конструктивных асимптотически хороших алгебраических кодов. — В кн.: Кибернетический сборник. Новая серия. М.: Мир, 1973, вып. 10, с. 39—50.
  146. Berlekamp E. R., Justesen J. Some long cyclic linear binary codes are not so bad. — IEEE Trans. Inform. Theory, 1974, May, vol. IT-20, p. 351—356.
  147. Burton H. O., Weldon E. J. Cyclic product codes. — IEEE Trans. Inform. Theory, 1965, July, vol. IT-31, p. 433—439.
  148. Chang S. H., Weng L. T. Error-locating codes. — IEEE Intern. Convent. Rec., 1965, pt 7, p. 252—258.
  149. Cohn D. L., Levesque A. H., Meyn J. H., Pierce A. W. Performance of Selected block and convolutional codes on a fading HF channel. — IEEE Trans. Inform. Theory, 1968, Nov., vol. 14, p. 627—640.
  150. Dorsh B. G. A decoding algorithm for binary block codes and J-ary output channel. — IEEE Trans. Inform. Theory, 1974, May, vol. IT-20, p. 391—394.
  151. Gelfand S. I., Dobrushin R. L., Pinsker M. S. On the complexity of coding. — In.: 2nd Intern. Symp. Inform. Theory. Tsahkadsor USSR. Akad. Kiadó, 1973, p. 177—184.
  152. Goethals J. M. Cyclic error-locating codes. — Inform. and Control, 1967, vol. 10, N 4, p. 378—385.  
Forney G. D. Coding and its application in space communication. — IEEE Spectrum, 1970, N 7, p. 47—58.
  153. Kasahara M., Suqiyama Y., Hirasawa S., Namekawa T. New classes of binary codes constructed on the basis of concatenated codes and product codes. — IEEE Trans. Inform. Theory, 1976, July, vol. IT-22.
  154. Kasami T. An upper bound on  $k/n$  for affine-invariant codes with fixed  $d/n$ . — IEEE Trans. Inform. Theory, 1969, vol. IT-15, N 1, pt 1, p. 174—176.
  155. Kolesnik V. D. Block codes: the algebraic theory. — In: Proc. of the 1975 IEEE—USSR Joint Workshop on Information Theory, 1976, p. 111—121.
  156. Lin S., Weldon E. J. Further results on cyclic product codes. — IEEE Trans. Inform. Theory, 1970, vol. IT-16, p. 445—451.

157. *Massey J. S.* Step-by-step decoding of the Bose—Chaudhuri—Hocquenghem codes. — IEEE Trans. Inform. Theory, 1965, vol. 11, N 4, p. 580—585.
158. *McElreath P. J., Rodemich E. R., Rumsey H., Jr., Welch L. D.* New upper bounds on the rate of a code via Delsarte—Mac Williams inequalities. — IEEE Trans. Inform. Theory, 1977, vol. 23, N 2, p. 157—166.
159. *Ramsey J.* Cascaded tree codes. — In: Techn. Rept 478, MIT, Research Laboratory of Electronics. Cambridge (Mass.), 1970.
160. *Savage J. E.* The complexity of decoders — pt I: classes of decoding rules. — IEEE Trans. Inform. Theory, 1969, Nov., vol. IT-15, p. 689—695.
161. *Savage J. E.* A note on the performance of concatenated codes. — IEEE Trans. Inform. Theory, 1970, vol. IT-16, p. 512—513.
162. *Savage J. E.* The complexity of decoders — pt II: computational work and decoding time. — IEEE Trans. Inform. Theory, 1971, Jan., vol. IT-17, p. 77—85.
163. *Savage J. E.* The complexity of decoder. — In: CISM, Courses and Lectures N 216 «Coding and Complexity». Wien; New York: Springer-Verl., 1975, p. 163—205.
164. *Sugiyama Y., Kasahara M., Hirasawa S., Namekawa T.* A modification of the constructive asymptotically good codes of Justesen for low rates. — Inform. and Control, 1974, Aug., vol. 25, p. 341—350.
165. *Sugiyama Y., Kasahara M., Hirasawa S., Namekawa T.* A new class of asymptotically — good codes beyond the Zyablov bound. — IEEE Trans. Inform. Theory, 1978, vol. IT-24, March.
166. *Viterby A. J.* Error bounds for convolutional codes and an asymptotically optimum decoding algorithm. — IEEE Trans. Inform. Theory, 1967, Apr., vol. IT-13, p. 260—269.
167. *Weldon E. J.* Decoding binary block codes on Q-ary Output Channels. — IEEE Trans. Inform. Theory, 1971, Nov., vol. IT-17, p. 713—718.
168. *Weldon E. J.* Justesen's construction — the low rate case. — IEEE Trans. Inform. Theory, 1973, Sept., vol. IT-19, p. 711—713.
169. *Weldon E. J.* Some result on the problem of constructing asymptotically good error-correcting codes. — IEEE Trans. Inform. Theory, 1975, July, vol. IT-21, p. 412—417.
170. *Wolf J. K., Elspas B.* Error-locating codes — a new concept in error control. — IEEE Trans. Inform. Theory, 1963, vol. IT-9, N 2, p. 113—117.
171. *Wolf J. K.* On an extended class of error-locating codes. — Inform. and Control, 1965, vol. 8, N 2, p. 163—168.
172. *Zyablov V. V.* Decoding complexity and concatenated codes. — In: CISM, Courses and Lectures N 216 «Coding and Complexity». Wien; New York: Springer-Verl., 1975, p. 131—162.
173. *Ziv J.* Further results on the asymptotic complexity of an iterative coding scheme. — IEEE Trans. Inform. Theory, 1966, Apr., vol. IT-12, p. 168—191.
174. *Ziv J.* Asymptotic performance and complexity of a coding scheme for memoryless channels. — IEEE Trans. Inform. Theory, 1967, July, vol. IT-13, p. 356—359.

# ОГЛАВЛЕНИЕ

Предисловие . . . . .	3
Глава 1. Цель и проблемы каскадного кодирования . . . . .	4
1.1. Блочное помехоустойчивое кодирование . . . . .	4
1.1.1. Задачи помехоустойчивого кодирования . . . . .	4
1.1.2. Потенциальные корректирующие свойства блочных кодов . . . . .	6
1.1.3. Обменные соотношения для вероятностей ошибки и стирания . . . . .	8
1.2. Реализация помехоустойчивого кодирования . . . . .	11
1.2.1. Проблемы реализации помехоустойчивого кодирования . . . . .	11
1.2.2. Сложность реализации помехоустойчивого кодирования . . . . .	13
1.3. Блочное каскадное кодирование . . . . .	14
1.3.1. Эвристическое описание каскадного кодирования . . . . .	14
1.3.2. Функциональное описание каскадного кодирования . . . . .	16
1.3.3. Геометрическая интерпретация линейных каскадных кодов . . . . .	18
1.4. Заключение . . . . .	21
1.4.1. Замечания о проблемах помехоустойчивого кодирования . . . . .	21
1.4.2. Основные направления исследования каскадных методов кодирования . . . . .	22
Глава 2. Кодирование и весовая структура каскадных кодов . . . . .	24
2.1. Кодирование каскадных кодов . . . . .	24
2.1.1. Линейные каскадные коды . . . . .	24
2.1.2. Несистематическое кодирование . . . . .	30
2.1.3. Систематическое кодирование . . . . .	32
2.2. Весовая структура каскадных кодов . . . . .	35
2.2.1. Анализ весовой структуры каскадных кодов . . . . .	35
2.2.2. Требования к внешним и внутренним кодам . . . . .	37
2.3. Внутренние коды . . . . .	39
2.3.1. Система вложенных кодов БЧХ . . . . .	39
2.3.2. Система вложенных кодов на базе произвольной невырожденной матрицы . . . . .	40
2.3.3. Система сложенных кодов на базе треугольной невырожденной матрицы . . . . .	41
2.3.4. Система вложенных кодов на базе ненулевого элемента поля $GF(2^m)$ . . . . .	42
2.4. Внешние коды . . . . .	45
2.4.1. Выбор основания внешних кодов . . . . .	45
2.4.2. Коды РС в качестве внешних кодов . . . . .	46
Глава 3. Комбинаторные оценки минимальных расстояний . . . . .	47
3.1. Нижние оценки минимальных расстояний . . . . .	47
3.1.1. Равная защита символов . . . . .	47
3.1.2. Неравная защита символов . . . . .	49
3.1.3. Влияние порядка каскадного кода на нижнюю оценку кодового расстояния . . . . .	51
3.2. Верхние оценки кодового расстояния . . . . .	51
3.2.1. Верхние оценки для произвольных каскадных кодов . . . . .	51
3.2.2. Верхние оценки для каскадных кодов структуры А . . . . .	53
3.2.3. Верхние оценки для систематических каскадных кодов . . . . .	54

3.3. Анализ оценок кодового расстояния каскадных кодов структуры $A$ . . . . .	56
3.3.1. Коды первого порядка . . . . .	56
3.3.2. Каскадные коды второго порядка . . . . .	60
3.3.3. Коды произвольного порядка . . . . .	63
3.4. Каскадные коды бесконечного порядка . . . . .	65
3.4.1. Основные ограничения и структура каскадных кодов бесконечного порядка . . . . .	65
3.4.2. Нижние и верхние оценки кодового расстояния каскадных кодов бесконечного порядка . . . . .	67
3.4.3. Коды структуры $A$ . . . . .	68
3.4.4. Коды структуры $B$ . . . . .	70
3.4.5. Коды структуры $C$ . . . . .	71
3.5. Анализ уровней защиты каскадных кодов $H_3$ . . . . .	73
3.5.1. Каскадные коды $H_3$ второго порядка . . . . .	73
3.5.2. Каскадные коды $H_3$ произвольного порядка . . . . .	77
3.5.3. Каскадные коды $H_3$ бесконечного порядка структуры $2A$ . . . . .	78
<b>Глава 4. Каскадное декодирование . . . . .</b>	<b>80</b>
4.1. Описание каскадного декодирования . . . . .	80
4.1.1. Общий принцип каскадного декодирования . . . . .	80
4.1.2. Составной алгоритм каскадного декодирования по расстоянию . . . . .	84
4.1.3. Составной алгоритм каскадного декодирования по вероятности . . . . .	86
4.2. Возможности каскадного декодирования по расстоянию . . . . .	88
4.2.1. Ошибки, исправляемые при каскадном декодировании по расстоянию . . . . .	88
4.2.2. Простой и полный алгоритмы каскадного декодирования . . . . .	91
4.2.3. Эффективное декодирование при сложном характере ошибок . . . . .	93
4.3. Возможности каскадного декодирования по вероятности . . . . .	97
4.3.1. Оценка вероятности неправильного декодирования . . . . .	97
4.3.2. Анализ реализуемой экспоненты вероятности неправильного декодирования . . . . .	100
<b>Глава 5. Случайные каскадные коды . . . . .</b>	<b>103</b>
5.1. Ансамбли каскадных кодов . . . . .	104
5.1.1. Случайные линейные блочные коды . . . . .	104
5.1.2. Оценки кодового расстояния и спектра весов случайных кодов . . . . .	105
5.1.3. Ансамбли каскадных кодов заданной структуры . . . . .	106
5.2. Ансамбли внутренних кодов . . . . .	109
5.2.1. Ансамбль невырожденных матриц . . . . .	109
5.2.2. Ансамбль невырожденных треугольных матриц . . . . .	111
5.2.3. Ансамбль элементов поля $GF(2^a)$ . . . . .	111
5.2.4. Неслучайные внутренние коды . . . . .	112
5.3. Ансамбли внешних кодов . . . . .	113
5.3.1. Ансамбль внешних кодов, определяемый канонической проверочной матрицей . . . . .	113
5.3.2. Ансамбль кодов $PC$ . . . . .	113
5.3.3. Неслучайный код $PC$ . . . . .	114
5.4. Производящие функции среднего спектра весов случайных каскадных кодов . . . . .	115
5.4.1. Вероятность принадлежности произвольного слова случайному каскадному коду . . . . .	115
5.4.2. Производящие функции среднего спектра весов случайных каскадных кодов . . . . .	117
5.5. Оценка кодового расстояния случайных каскадных кодов . . . . .	118
5.5.1. Оценка кодового расстояния случайных каскадных кодов из ансамблей типа $I$ . . . . .	118
5.5.2. Условия достижимости границы $VG$ . . . . .	121

5.5.3. Оценка кодового расстояния и условия достижимости границы ВГ для случайных каскадных кодов из других ансамблей . . .	122
5.6. Оценка потенциальных корректирующих свойств каскадных кодов различного порядка . . . . .	124
5.6.1. Каскадные коды первого порядка . . . . .	124
5.6.2. Каскадные коды второго порядка . . . . .	125
5.6.3. Каскадные коды порядка $m > 2$ . . . . .	128
5.6.4. Каскадные коды бесконечного порядка . . . . .	131
5.6.5. Оценка экспоненты вероятности ошибочного декодирования	134
5.7. Сравнение потенциальных и реализуемых корректирующих свойств каскадных кодов . . . . .	135
5.7.1. Принципы сравнения потенциальных и реализуемых характеристик . . . . .	135
5.7.2. Каскадные коды первого порядка . . . . .	136
5.7.3. Каскадные коды бесконечного порядка . . . . .	137
<b>Глава 6. Проблемы сложности в теории корректирующих кодов . . .</b>	<b>140</b>
6.1. Коды фиксированной длины . . . . .	141
6.1.1. Кодирование и декодирование . . . . .	141
6.1.2. Сложность кодирования и декодирования . . . . .	142
6.1.3. Система вложенных кодов . . . . .	143
6.2. Последовательность кодов с асимптотически «хорошим» кодовым расстоянием . . . . .	145
6.2.1. Задание последовательности . . . . .	145
6.2.2. Задание последовательности кодов с кодированием . . . . .	148
6.2.3. Задание последовательности кодов с декодированием . . . . .	152
6.3. Последовательность кодов с асимптотически «хорошей» экспонентой . . . . .	154
6.3.1. Система вложенных кодов . . . . .	154
6.3.2. Каскадные кодовые множества . . . . .	155
6.4. Заключение . . . . .	157
<b>Приложение П.1 . . . . .</b>	<b>159</b>
<b>Приложение П.2 . . . . .</b>	<b>167</b>
<b>Приложение П.3 . . . . .</b>	<b>179</b>
<b>Приложение П.4 . . . . .</b>	<b>186</b>
<b>Приложение П.5 . . . . .</b>	<b>200</b>
<b>Приложение П.6 . . . . .</b>	<b>211</b>
<b>Литература . . . . .</b>	<b>219</b>

Эфроим Леонтьевич Блох,  
Виктор Васильевич Зяблов

**ЛИНЕЙНЫЕ  
КАСКАДНЫЕ КОДЫ**

Утверждено к печати  
Институтом проблем  
передачи информации

Редактор издательства Н. А. Ермолаева  
Художник С. А. Смирнова  
Художественный редактор Н. Н. Власик  
Технический редактор Ф. М. Хенох  
Корректоры Р. З. Землянская, Н. И. Каварина

ИБ № 24483

Сдано в набор 06.07.81  
Подписано к печати 15.02.82.  
Т-00519. Формат 60×90<sup>1</sup>/<sub>16</sub>.  
Бумага типографская № 2.  
Гарнитура обыкновенная новая  
Печать высокая  
Усл. печ. л. 14,5. Уч.-изд. л. 14,8.  
Усл. кр.-отт. 14,7. Тираж 1800 экз. Тип, зак 738.  
Цена 2 р. 30 к.

Издательство «Наука»  
117864 ГСП-7, Москва, В-485, Профсоюзная ул., 90  
Ордена Трудового Красного Знамени  
Первая типография издательства «Наука»  
199034, Ленинград, В-34, 9 линия, 12

**2 р. 30 к.**