V. I. Levenshtein, Bounds on the Probability of Undetected Error,
*Probl. Peredachi Inf.*, 1977, Volume 13, Issue 1, 3–18

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том XIII 1977 Вып. 1

УДК 621.391.15:519.2

# О ГРАНИЦАХ ВЕРОЯТНОСТИ НЕОБНАРУЖЕНИЯ ОШИБКИ

*В. И. Левенштейн*

Получены новые верхние и нижние границы вероятности необнаружения ошибки для блочных кодов в двоичном симметричном канале (ДСК). Эти границы в экспоненциально растущее с ростом длины блока $n$ число раз улучшают известные границы при условии, что скорость передачи фиксирована и не превышает пропускной способности ДСК. Полученные границы используются для выбора параметров близкого к оптимальному кода для передачи по ДСК с мгновенной и бесшумной обратной связью.

## § 1. Введение

Пусть $B^n$ — $n$-мерное векторное пространство над полем из двух элементов 0 и 1 с метрикой Хэмминга $d(U, V)$, равной числу несовпадающих координат векторов $U$, $V \in B^n$. Ниже используются также следующие обозначения: $\|U\|$ — число единичных координат (норма) вектора $U \in B^n$, $|K|$ — число элементов множества $K \subseteq B^n$, $\ln x$ — натуральный логарифм числа $x$, $\log x$ — двоичный логарифм числа $x$, $[x]$ — целая часть числа $x$, $]x[$ — наименьшее целое, не меньшее числа $x$. Произвольное подмножество (код) $K \subseteq B^n$ будем характеризовать *минимальным расстоянием*

$$d(K) = \min_{U, V \in K;\ U \neq V} d(U, V),$$

*мощностью* $m(K) = |K|$ и *скоростью* $R(K) = n^{-1} \log |K|$. Если код образует линейное подпространство пространства $B^n$ размерности $k$, то будем называть его $(n, k)$-*кодом*, или линейным кодом; скорость $(n, k)$-кода равна $k/n$. Для любого числа (скорости) $R$, $0 \leqslant R \leqslant 1$, удобно ввести параметр $\rho(R)$, который однозначно определяется условиями

$$R = 1 - H(\rho(R)), \quad 0 \leqslant \rho(R) \leqslant 1/2,$$

где $H(x) = -x \log x - (1-x) \log (1-x)$. Пусть $d(n, m) = \max d(K)$, где максимум берется по всем кодам $K \subseteq B^n$ мощности $m$, и $\tilde{d}(n, k) = \max d(K)$, где максимум берется по всем $(n, k)$-кодам $K$. Заметим, что с помощью параметра $\rho(R)$ известную (см., например, [1]) границу Варшамова — Гилберта можно записать в следующем простом виде:

$$d(n, m) \geqslant n\rho(R), \quad \text{где } R = n^{-1} \log m, \tag{1}$$

$$\tilde{d}(n, k) \geqslant n\rho(R) + 1, \quad \text{где } R = k/n. \tag{2}$$

Настоящая работа посвящена исследованию величины

$$P(K, p) = \frac{1}{m(K)} \sum_{U, V \in K;\ U \neq V} p^{d(U,V)} (1-p)^{n - d(U,V)}, \tag{3}$$

характеризующей среднюю вероятность необнаружения ошибки при использовании кода $K \subseteq B^n$ в двоичном симметричном канале (ДСК) с вероятностью ошибки $p$ $(0 < p \leqslant 1/2)$. Эта величина играет существенную роль в системах передачи с обратной связью. Заметим, что величина (3) по своей

природе существенно отличается от известной величины (см., например, [2]), характеризующей вероятность ошибки декодирования при использовании кода $K$ в ДСК. В частности, величина (3), вообще говоря, не является возрастающей * функцией параметра $p$. Оптимальные возможности произвольных и линейных кодов обнаруживать ошибки будем характеризовать величинами

$$P(n, m, p) = \min P(K, p),$$

где минимум берется по всем кодам $K \subseteq B^n$ мощности $m$, и

$$\tilde{P}(n, k, p) = \min P(K, p),$$

где минимум берется по всем $(n, k)$-кодам $K$.

Легко видеть, что в любом коде $K \subseteq B^n$ мощности $m$ существует ** подмножество $K' \subseteq K$ произвольной мощности $m'$ $(m' \leqslant m)$ такое, что $P(K', p) \leqslant P(K, p)$. Отсюда немедленно следует, что функции $P(n, m, p)$ и $\tilde{P}(n, k, p)$ не убывают по второму аргументу при фиксации двух других и что

$$P(n, m, p) \leqslant \tilde{P}(n, \lceil \log m \rceil, p). \tag{4}$$

В силу неравенства (4) при исследовании величин $P(n, m, p)$ и $\tilde{P}(n, k, p)$ представляется разумным оценивать $P(n, m, p)$ снизу, а $\tilde{P}(n, k, p)$ сверху.

Приведем известные результаты. В. И. Коржик [3] установил, что

$$P(n, m, p) \geqslant (m-1) p^{\bar{d}(n, m)} (1-p)^{n-\bar{d}(n, m)}, \tag{5}$$

где

$$\bar{d}(n, m) = \frac{mn}{2(m-1)}.$$

Границу (5) естественно назвать границей среднего расстояния, так как она получается, если к (3) применить неравенство Иенсена и воспользоваться тем, что среднее расстояние между различными векторами любого кода $K \subseteq B^n$ мощности $m$ не превышает $\bar{d}(n, m)$. Верхние границы, установленные в [3], имеют вид

$$\tilde{P}(n, k, p) \leqslant (2^k-1) p^{\tilde{d}(n, k)} (1-p)^{n-\tilde{d}(n, k)}, \tag{6}$$

$$\tilde{P}(n, k, p) \leqslant \frac{2^k-1}{2^n-1} (1-(1-p)^n) < 2^{k-n}, \tag{7}$$

причем первая из них непосредственно следует из определения величины $\tilde{d}(n, k)$, а вторая получена методом случайного выбора $(n, k)$-кода. Отметим, что при $m = 2^k = n+1$ имеет место $\tilde{d}(n, k) = \bar{d}(n, m)$ и

$$P(n, m, p) = \tilde{P}(n, k, p) = (m-1) p^{\frac{mn}{2(m-1)}} (1-p)^{n - \frac{mn}{2(m-1)}},$$

так что неравенства (4)–(6) могут достигаться одновременно, когда скорость кода близка к нулю $(R = n^{-1} \log(n+1))$. С другой стороны, В. К. Леонтьев [4] установил, использовав тождество Мак-Вильямс, что

$$\tilde{P}(n, k, p) > 2^{k-n} - (1-p)^n, \tag{8}$$

* Заметим, что

$$\frac{dP(K, p)}{dp} = \frac{1}{m(K)} \sum_{U \neq V} (d(U, V) - np) p^{d(U,V)-1} (1-p)^{n-d(U,V)-1}.$$

Поэтому, если $d(K) \geqslant n\rho(R)$, где $R = R(K)$, то $P(K, p)$ является возрастающей функцией параметра $p$ в области $p \leqslant \rho(R)$, т. е. когда $R \leqslant C(p) = 1 - H(p)$.

** В качестве $K'$ достаточно взять подмножество, состоящее из $m'$ векторов, для которых вероятности перехода в другие векторы кода $K$ минимальны.

и получил в качестве следствия из (7) и (8) асимптотику

(9) $\quad \tilde{P}(n, k, p) \sim 2^{k-n}$ при условии, что $k - n \log 2(1-p) \to \infty$.

Заметим, что неравенство (8) является нетривиальным, а асимптотика (9) — доказанной лишь при условии, что скорость кода $R = k/n$ больше критической скорости

(10) $\quad R(p) = \log 2(1-p)$.

При этом следует отметить, что критическая скорость (10) при любом $p$ $(0 < p \leqslant 1/2)$ больше пропускной способности $C(p) = 1 - H(p)$ ДСК и что в реальных случаях, когда $p$ имеет порядок $10^{-2}$—$10^{-4}$, критическая скорость $R(p)$ (и пропускная способность $C(p)$) весьма близка к единице. Вопрос об улучшении границ (5)—(7) для скоростей $R$, $0 < R < R(p)$, оставался открытым.

В настоящей работе получены новые границы для величин $P(n, m, p)$ и $\tilde{P}(n, k, p)$ и проведено асимптотическое исследование этих границ при условии, что скорость кода ($n^{-1} \log m$ или $k/n$) не меньше некоторого фиксированного числа $R$, $0 < R \leqslant 1$, а $n \to \infty$. В § 2 с помощью некоторой модификации метода случайного выбора получена граница

(11) $\quad \tilde{P}(n, k, p) < p^{n\rho(R)}(1-p)^{n(1-\rho(R))}$, если $0 < R = k/n \leqslant C(p)$.

Заметим, что если в неравенство (6) вместо $\tilde{d}(n, k)$ подставить (как это делалось в [3]) границу Варшамова — Гилберта (2) как наилучшую из известных нижних границ этой величины, то полученная верхняя граница для $\tilde{P}(n, k, p)$ будет почти в $2^k$ раз хуже границы (11). Из дальнейшего ясно, что и граница (7) в указанном асимптотическом процессе при $0 < R < C(p)$ также в экспоненциально растущее с ростом $n$ число раз хуже границы (11). В § 3 двумя различными способами выведен следующий естественный аналог границы (8) для произвольных кодов:

(12) $\quad P(n, m, p) \geqslant m2^{-n} - (1-p)^n$.

С помощью неравенства (12) и одного соотношения установлена так называемая продолженная граница, согласно которой при $n^{-1} < R = n^{-1} \log m \leqslant R(p) + n^{-1}$

(13) $\quad P(n, m, p) \geqslant mp^{n\alpha(n, R)}(1-p)^{n(1-\alpha(n, R))}$,

где

$$\alpha(n, R) = \frac{R}{-\log(2^{1-R+n^{-1}} - 1)}.$$

Граница (13) в указанном асимптотическом процессе улучшает в экспоненциально растущее с ростом $n$ число раз границу (5), так как $-R/\log(2^{1-R} - 1) < 1/2$ при любом $R > 0$. В § 4 получена другая нижняя граница для $P(n, m, p)$, названная границей минимального расстояния, которая основана на использовании верхней границы для $d(n, m)$. Если в качестве верхней границы для $d(n, m)$ взять новую верхнюю границу этой величины, вытекающую из работ В. М. Сидельникова [5] и автора [6] и улучшающую известную границу Элайса (см., например, [1]), то полученная нижняя граница для $P(n, m, p)$ при любом $p$ $(0 < p < 1/2)$ будет лучше границы (13) для малых скоростей. Более того, если справедливо весьма правдоподобное предположение о том, что граница Варшамова — Гилберта (1) является асимптотически точной, то граница минимального расстояния для $P(n, m, p)$ при $0 \leqslant R \leqslant C(p)$ будет иметь ту же асимптотику логарифма, что и верхняя граница (11). В § 5 проведено асимптотическое ис-

следование полученных границ и их сопоставление. Последний параграф посвящен использованию полученных границ для выбора параметров близкого к оптимальному кода для передачи по ДСК с мгновенной и бесшумной обратной связью.

Результаты настоящей работы доложены на IV Международном симпозиуме по теории информации (Репино, июнь 1976 г.).

## § 2. Граница случайного выбора

Ниже фактически используются рассуждения метода случайного выбора кода из некоторого ансамбля с последующим выбрасыванием «плохих» векторов [2]. Однако при получении верхней границы для $\tilde{P}(n, k, p)$ эти рассуждения удается провести без выбрасывания векторов. Числа $n$ и $k$ предполагаются целыми и такими, что $1 \leqslant k \leqslant n$, а число $p$ таким, что $0 < p \leqslant \leqslant 1/2$.

Теорема 1. *При любых* $t$ $(0 < t \leqslant 1)$, $p$, $n$ и $k$ *существует* $(n, k)$*-код* $K$, *для которого*

$$P(K, p) \leqslant \left( \frac{2^k - 1}{2^n - 1} \left( (p^t + (1-p)^t)^n - (1-p)^{nt} \right) \right)^{1/t}. \tag{14}$$

Доказательство. Пусть $L = \{U_0, U_1, \ldots, U_{2^k-1}\}$ — произвольный $(n, k)$-код и $U_0$ — нулевой вектор. Отождествим векторы из $B^n$ с соответствующими элементами поля $GF(2^n)$. Для любого ненулевого $g \in GF(2^n)$ обозначим через $gL$ $(n, k)$-код $\{gU_0, gU_1, \ldots, gU_{2^k-1}\}$ и рассмотрим величину

$$\xi(g) = \begin{cases} 1, & \text{если } P(gL, p) > J, \\ 0, & \text{если } P(gL, p) \leqslant J, \end{cases}$$

где число $J = J(t, p, n, k)$ по определению равно правой части (14). Отметим, что

$$P(gL, p) = \sum_{i=1}^{2^k-1} p^{\|gU_i\|} (1-p)^{n-\|gU_i\|}$$

и убедимся в том, что

$$\xi(g) < \sum_{i=1}^{2^k-1} \left( J^{-1} p^{\|gU_i\|} (1-p)^{n-\|gU_i\|} \right)^t. \tag{15}$$

Действительно, если $\xi(g) = 0$ или $\xi(g) = 1$ и $p^{\|gU_i\|}(1-p)^{n-\|gU_i\|} > J$ при некотором $i$, то неравенство (15) очевидно. Если же $\xi(g) = 1$ и $p^{\|gU_i\|}(1-p)^{n-\|gU_i\|} \leqslant J$ при всех $i = 1, \ldots, 2^k - 1$, то

$$\xi(g) = 1 < \frac{P(gL, p)}{J} = \sum_{i=1}^{2^k-1} J^{-1} p^{\|gU_i\|} (1-p)^{n-\|gU_i\|} \leqslant$$

$$\leqslant \sum_{i=1}^{2^k-1} \left( J^{-1} p^{\|gU_i\|} (1-p)^{n-\|gU_i\|} \right)^t,$$

и неравенство (15) также выполняется.

Обозначим через $g_j$, $j = 1, \ldots, 2^n - 1$, ненулевые элементы поля $GF(2^n)$. Используя неравенство (15), тот факт, что при любом ненулевом $U \in GF(2^n)$ элементы $g_j U$, $j = 1, \ldots, 2^n - 1$, пробегают все ненулевые элементы поля

$GF(2^n)$, и определение числа $J$, получаем

$$\sum_{j=1}^{2^n-1}\xi(g_j)<\frac{1}{J^t}\sum_{j=1}^{2^n-1}\sum_{i=1}^{2^k-1}p^{\|g_jU_i\|t}(1-p)^{(n-\|g_jU_i\|)t}=$$

$$=\frac{(1-p)^{nt}}{J^t}\sum_{i=1}^{2^k-1}\sum_{j=1}^{2^n-1}\left(\frac{p}{1-p}\right)^{\|g_jU_i\|t}=\frac{(2^k-1)(1-p)^{nt}}{J^t}\sum_{l=1}^{n}C_n^{\,l}\left(\frac{p}{1-p}\right)^{lt}=2^n-1.$$

Поэтому в классе из $2^n-1$ кодов $g_1L,\ldots,g_{2^n-1}L$ существует $(n, k)$-код $gL$ такой, что $\xi(g)=0$ и, следовательно, $P(gL, p)\leqslant J$, что и доказывает теорему.

Несколько огрубляя границу, получаем

Следствие 1. *При любых $t$ $(0<t\leqslant 1)$, $p$, $n$ и $k$ существует $(n, k)$-код $K$, для которого*

$$P(K, p)<(2^{k-n}(p^t+(1-p)^t)^n)^{1/t}. \tag{16}$$

Следствие 2. *При любых $p$, $n$ и $k$ таких, что $R=k/n\leqslant C(p)$ (или, что то же самое $\rho(R)\geqslant p$) существует $(n, k)$-код $K$, для которого*

$$P(K, p)<p^{n\rho(R)}(1-p)^{n(1-\rho(R))}. \tag{17}$$

*Любой $(n, k)$-код $K$, для которого при некотором $p$ выполнено неравенство* (17) *с $R=k/n$, обладает следующими свойствами:* 1) $d(K)>n\rho(R)$ *и* 2) *функция $P(K, p)$ возрастает по $p$ на отрезке* $[0, \rho(R)]$.

Для получения следствия 2 достаточно использовать следствие 1 при значении

$$t=\left(\log\frac{1-\rho(R)}{\rho(R)}\right)\Big/\left(\log\frac{1-p}{p}\right),$$

которое минимизирует правую часть (16) при условии $R=k/n\leqslant C(p)$ и преобразует (16) в (17), сопоставить (17) с очевидным неравенством $P(K, p)\geqslant p^{d(K)}(1-p)^{n-d(K)}$ и воспользоваться сноской на странице 4.

Использование следствия 1 при значении $t=1$, которое минимизирует правую часть (16) при условии $R=k/n\geqslant C(p)$, приводит к следующему хорошо известному [3] результату, который для рассмотренного в теореме 1 ансамбля $(n, k)$-кодов был доказан в [7].

Следствие 3. *При любых $p$, $n$ и $k$ существует $(n, k)$-код $K$, для которого*

$$P(K, p)<2^{k-n}. \tag{18}$$

Из следствия 2 (при $p=\rho(R)$, где $R=k/n$) вытекает, что для любых $n$ и $k$ существует $(n, k)$-код $K$, для которого неравенство (18) справедливо для всех $p$ из отрезка $[0, \rho(R)]$. Однако вопрос о существовании для любых $n$ и $k$ $(n, k)$-кода $K$, для которого неравенство (18) справедливо для всех $p$ из отрезка $[0, 1/2]$, остается открытым.

Следствие 4 (граница случайного выбора).

$$\bar{P}(n, k, p)<\begin{cases}p^{n\rho(R)}(1-p)^{n(1-\rho(R))}, & \text{если } 0<R=k/n\leqslant C(p),\\ 2^{-(1-R)n}, & \text{если } C(p)\leqslant R=k/n\leqslant 1.\end{cases}$$

Заметим, что в силу неравенства (4) следствие 4 при $k=]\log m[$ дает верхнюю границу для величины $P(n, m, p)$.

## § 3. Продолженная граница

Убедимся сначала, что граница (8) может быть распространена на случай произвольных кодов. С этой целью воспользуемся нелинейной версией тождества Мак-Вильямс. В двоичном случае преобразованием Мак-Вильямс произвольного вектора $A=(a_0, a_1, \ldots, a_n)$ над полем действительных чисел называют вектор $A'=(a_0', a_1', \ldots, a_n')$ такой, что $a_j'=\sum_{i=0}^{n} a_i P_j(i)$, $0\leqslant j\leqslant n$, где $P_j(x)=\sum_{l=0} (-1)^l C_x^l C_{n-x}^{j-l}$ и $C_x^l=\dfrac{x(x-1)\ldots(x-l+1)}{l!}$. Из этого определения следует тождество

$$\sum_{i=0}^{n} a_i (1-y)^i (1+y)^{n-i} = \sum_{j=0}^{n} a_j' y^j,$$

которое при $y=1-2p$ принимает вид

$$\sum_{i=0}^{n} a_i p^i (1-p)^{n-i} = 2^{-n} \sum_{j=0}^{n} a_j' (1-2p)^j. \tag{19}$$

Лемма 1 (Делзарт [8]). *Пусть $K=\{U_1, \ldots, U_m\}$ — произвольный код в $B^n$ и вектор $A=(a_0, a_1, \ldots, a_n)$ такой, что $a_i$ — деленное на $m$ число упорядоченных пар векторов кода $K$, находящихся на хэмминговом расстоянии $i$ друг от друга. Тогда все компоненты вектора $A'=(a_0', a_1', \ldots, a_n')$ неотрицательны.*

Если воспользоваться леммой 1 и тем, что $a_0' = \sum_{i=0}^{n} a_i = m$, то из (19) вытекает

Следствие. *Для любого кода $K=\{U_1, \ldots, U_m\}\subseteq B^n$*

$$\frac{1}{m} \sum_{i,j} p^{d(U_i, U_j)} (1-p)^{n-d(U_i, U_j)} \geqslant m 2^{-n} \tag{20}$$

*и, значит,*

$$P(K, p) \geqslant m 2^{-n} - (1-p)^n. \tag{21}$$

*Замечание.* Возможно также другое доказательство неравенства (21), основанное на оценке * В. М. Сидельникова [9]

$$\frac{1}{m^2} \sum_{i,j} \left(1 - \frac{2d(U_i, U_j)}{n}\right)^h \geqslant \frac{1}{2^n} \sum_{d=0} C_n^d \left(1 - \frac{2d}{n}\right)^h, \tag{22}$$

справедливой при любом $h=0, 1, 2, \ldots$. Если при некотором $\sigma>0$ умножить левую и правую части неравенства (22) на $\sigma^h / h!$ и просуммировать по $h$, то получится неравенство

$$\frac{1}{m^2} \sum_{i,j} \exp\left\{\left(1 - \frac{2d(U_i, U_j)}{n}\right)\sigma\right\} \geqslant \frac{1}{2^n} \sum_{a=0} C_n^d \exp\left\{\left(1 - \frac{2d}{n}\right)\sigma\right\} = \left(\operatorname{ch}\frac{\sigma}{n}\right)^n,$$

* Эта оценка была повторена в работе [10], вышедшей через три года после [9].

которое при $\sigma=(n/2)\ln((1-p)/p)$ переходит в неравенство (20).

Граница (21) является нетривиальной лишь при скоростях $R(K)>R(p)=\log 2(1-p)$. Чтобы продолжить ее на область скоростей, не превышающих $R(p)$, нам понадобится одно соотношение, к формулировке которого мы приступаем. Пусть $t$ и $p_0$ — произвольные числа такие, что $0\leqslant t\leqslant 1$, $p\leqslant p_0\leqslant 1/2$, и пусть

$$p_t=\frac{p^t p_0^{1-t}}{p^t p_0^{1-t}+(1-p)^t(1-p_0)^{1-t}}. \tag{23}$$

Легко проверить, что $p_t$ при возрастании $t$ от 0 до 1 монотонно убывает от $p_0$ до $p_1=p$.

Лемма 2. *Пусть* $P(p)=\sum_{i=0}^{n} c_i p^i (1-p)^{n-i}$, *где коэффициенты* $c_i$ $(i=0, 1, \ldots, n)$ *неотрицательны. Тогда*

$$\left(\frac{P(p)}{(1-p)^n}\right)^t\left(\frac{P(p_0)}{(1-p_0)^n}\right)^{1-t}\geqslant\frac{P(p_t)}{(1-p_t)^n}. \tag{24}$$

Доказательство. Для неотрицательных чисел $\alpha_i$, $\beta_i$ $(i=0, 1, \ldots, n)$ справедливо неравенство Гельдера

$$\sum_{i=0}^{n}\alpha_i^t\beta_i^{1-t}\leqslant\left(\sum_{i=0}^{n}\alpha_i\right)^t\left(\sum_{i=0}^{n}\beta_i\right)^{1-t}.$$

Поэтому

$$\frac{P(p_t)}{(1-p_t)^n}=\sum_{i=0}^{n}c_i\left(\frac{p_t}{1-p_t}\right)^i=\sum_{i=0}^{n}c_i\left(\left(\frac{p}{1-p}\right)^t\left(\frac{p_0}{1-p_0}\right)^{1-t}\right)^i=$$

$$=\sum_{i=0}^{n}\left(c_i\left(\frac{p}{1-p}\right)^i\right)^t\left(c_i\left(\frac{p_0}{1-p_0}\right)^i\right)^{1-t}\leqslant\left(\frac{P(p)}{(1-p)^n}\right)^t\left(\frac{P(p_0)}{(1-p_0)^n}\right)^{1-t}.$$

Полагая в (24) $p_0=1/2$ и замечая, что для любого кода $K\subseteq B^n$ $P(K, 1/2)=(m(K)-1)2^{-n}$, получаем

Следствие. *Для любого кода* $K\subseteq B^n$ *мощности* $m$ *и любого числа* $t$ $(0<t\leqslant 1)$

$$P(K,p)\geqslant(m-1)^{1-1/t}(p^t+(1-p)^t)^{n/t}\left(P\left(K,\frac{p^t}{p^t+(1-p)^t}\right)\right)^{1/t}.$$

Теорема 2. *Для любого кода* $K\subseteq B^n$ *мощности* $m$ *и любого числа* $x$ *такого, что* $\max(R-R(p), 0)\leqslant x/n<R$, *где* $R=n^{-1}\log m$,

$$P(K,p)\geqslant(m-1)(1-p)^n\exp\left\{\frac{\ln(p/(1-p))}{\ln(2^{1-R+x/n}-1)}\ln\frac{2^x-1}{m-1}\right\}. \tag{25}$$

Доказательство. Рассмотрим число

$$t=(\ln(2^{1-R+x/n}-1))/\ln(p/(1-p)).$$

Из условий $(R-R(p))n\leqslant x<Rn$ следует, что $p<1/2$ и $0<t\leqslant 1$, а из определения числа $t$, что

$$\frac{m}{2^n}=2^x\left(\frac{(1-p)^t}{p^t+(1-p)^t}\right)^n.$$

Поэтому из следствий лемм 1 и 2 и условия $x\geqslant 0$ вытекает

$$P(K,p)\geqslant(m-1)^{1-1/t}(p^t+(1-p)^t)^{n/t}\left(\frac{m}{2^n}-\left(\frac{(1-p)^t}{p^t+(1-p)^t}\right)^n\right)^{1/t}=$$

$$=(m-1)(1-p)^n\left(\frac{2^x-1}{m-1}\right)^{1/t},$$

что приводит к утверждению теоремы.

Интересно отметить, что при $x\to Rn$ из (25) предельным переходом получается граница (5), а при $x=(R-R(p))n\geqslant 0$ из (25) получается граница (21). При условии $m>n+1$ правая часть (25) как функция от $x$ на отрезке $[0, Rn]$ сначала возрастает, а затем убывает, достигая максимума при значении $x^*=x^*(n, R)$, являющимся единственным (не считая $Rn$) корнем уравнения

$$\frac{1}{n}\frac{2^{1-R+x/n}}{2^{1-R+x/n}-1}\ln\frac{2^x-1}{m-1}-\frac{2^x}{2^x-1}\ln(2^{1-R+x/n}-1)=0.$$

Поэтому в случае $m>n+1$ при подстановке значения $x^*$ в (25) получается граница, которая сильнее границы (5) (а также сильнее границы (21), если $R<R(p)+x^*/n$).

Из теоремы 2 при $x=1$ вытекает

Следствие (продолженная граница). *Если* $n^{-1}<R=n^{-1}\log m\leqslant R(p)+n^{-1}$, *то*

$$P(n, m, p)\geqslant mp^{n\alpha(n, R)}(1-p)^{n(1-\alpha(n, R))},$$

*где*

$$\alpha(n,R)=\frac{R}{-\log(2^{1-R+1/n}-1)}.$$

## § 4. Граница минимального расстояния

В настоящем параграфе приводится другая нижняя граница для величины $P(n, m, p)$, которая, как ясно из дальнейшего, лучше продолженной границы при скоростях, близких к нулю. При получении этой границы используется то обстоятельство [2], что в любом коде заданной мощности имеется достаточно много пар векторов, расстояния между которыми достаточно малы. В частности, каждый вектор произвольного $(n, k)$-кода должен находиться на расстоянии не более $\tilde{d}(n, k)$ от некоторого другого вектора этого кода и, следовательно, $\tilde{P}(n, k, p)\geqslant p^{\tilde{d}(n, k)}(1-p)^{n-\tilde{d}(n, k)}$. Несколько более слабое неравенство можно получить и в случае произвольных кодов.

Лемма 3 (граница минимального расстояния).

$$P(n, m, p)>1/2\,p^{d(n, \,]m/2[)}(1-p)^{n-d(n, \,]m/2[)}. \tag{26}$$

Доказательство. Пусть $K$ — произвольное подмножество $B^n$ мощности $m$ и $K'$ — множество всех векторов кода $K$, для каждого из которых существует некоторый другой вектор из $K$, находящийся от него на расстоянии не более $d(n, ]m/2[)$. Из определения множества $K'$ следует, что все векторы множества $K\setminus K'$ находятся на расстояниях более

$d(n, ]m/2[)$ друг от друга. Следовательно, $|K \setminus K'| \leqslant ]m/2[ - 1$ и $|K'| \geqslant m + 1 - ]m/2[ > m/2$. Поэтому $P(K, p) > {}^1/_2 p^{d(n, ]m/2[)} (1-p)^{n-d(n, ]m/2[)}$, что доказывает лемму.

Чтобы применить лемму 3 для получения нижней границы величины $P(n, m, p)$, нужно использовать верхнюю границу величины $d(n, m)$. Ниже приводится верхняя граница для $d(n, m)$, которая получается методами работ [5, 6] и, в частности, усиливает известную [1] границу Элайса.

Теорема 3. *Для любых целых положительных $w$ и $s$*

$$d(n, m) \leqslant \tag{27}$$

$$\leqslant \frac{2w(n-w)}{n}\left(1 - \left(\frac{m\sum_{i=0}^{w} C_w^i C_n^{i-w}\left(1 - \frac{in}{w(n-w)}\right)^{2s-1} - 2^n}{mC_n^w - 2^n}\right)^{\frac{1}{2s-1}}\right),$$

*если* $mC_n^w > 2^n$.

Доказательство. Пусть $K = \{U_1, \ldots, U_m\}$ — произвольное подмножество $B^n$ с минимальным расстоянием $d$ и $B_w^n$ — множество всех векторов $B^n$, имеющих норму $w$. Используя известное рассуждение, можно показать, что существует * код $K' \subseteq B_w^n$, имеющий мощность

$$m' \geqslant mC_n^w 2^{-n} \tag{28}$$

и минимальное расстояние не менее $d$. Каждому вектору $U = (u_1, \ldots, u_n) \in B_w^n$ поставим в соответствие вектор $\mathfrak{A}(U) = \gamma(u_1), \ldots, \gamma(u_n))$, где $\gamma(0) = \sqrt{w/(n(n-w))}$ и $\gamma(1) = -\sqrt{(n-w)/(nw)}$. Легко проверить, что каждый вектор $\mathfrak{A}(U)$, где $U \in B_w^n$, принадлежит единичной сфере $n$-мерного евклидова пространства. Из следствия 1 леммы 1 работы В. М. Сидельникова [5] вытекает, что при любом целом положительном $s$

$$\sum_{U, V \in K'} (\mathfrak{A}(U), \mathfrak{A}(V))^{2s-1} \geqslant \frac{(m')^2}{C_n^w} \sum_{i=0}^{w} C_w^i C_{n-w}^i \left(1 - \frac{in}{w(n-w)}\right)^{2s-1}, \tag{29}$$

где $(X, Y)$ — скалярное произведение векторов $X$ и $Y$ евклидова пространства. С другой стороны, так как для любых $U, V \in B_w^n$ имеет место $(\mathfrak{A}(U), \mathfrak{A}(V)) = 1 - d(U, V) n/(2w(n-w))$ и код $K'$ обладает минимальным расстоянием не менее $d$, то

$$\sum_{U, V \in K'} (\mathfrak{A}(U), \mathfrak{A}(V))^{2s-1} \leqslant m' + m'(m'-1)\left(1 - \frac{dn}{2w(n-w)}\right)^{2s-1}. \tag{30}$$

Утверждение теоремы следует из (29), (30) и (28).

При $s = 1$ получается

Следствие (граница Элайса). *Если* $mC_n^w > 2^n$, *то*

$$d(n, m) \leqslant \frac{2w(n-w)}{n} \cdot \frac{mC_n^w}{mC_n^w - 2^n}. \tag{31}$$

Асимптотическое поведение нижних границ для $P(n, m, p)$, полученных на основании (26), (27) и (31) при оптимальном выборе параметров $w$ и $s$, рассматривается в следующем параграфе.

---

* Действительно, рассмотрим $m$ множеств $K_i = \{U_i + B_w^n\}$, $i = 1, \ldots, m$, содержащих по $C_n^w$ векторов, и обозначим через $W$ вектор (или любой из векторов, если их несколько), принадлежащий максимальному числу этих множеств. Обозначим множества, которым принадлежит $W$, через $K_{i_j}$, $j = 1, \ldots, m'$. Ясно, что $m' \geqslant mC_n^w 2^{-n}$ и что код $K' = \{U_{i_j} + W, j = 1, \ldots, m'\}$ принадлежит $B_w^n$ и имеет минимальное расстояние не менее $d$.

## § 5. Асимптотические результаты

Рассматривается асимптотическое поведение границ для величины $P(n, m, p)$ (а также для вспомогательной в данном случае величины $d(n, m)$) при условии, что вероятность ошибки $p$ $(0<p<1/2)$ фиксирована, скорость кода $n^{-1}\log m$ не меньше некоторого фиксированного числа $R$ $(0<R\leqslant 1)$ и $n\to\infty$. В этом асимптотическом процессе величина $P(n, m, p)$ экспоненциально убывает, причем показатель экспоненты убывает линейно с ростом $n$, а величина $d(n, m)$ растет линейно с ростом $n$. В связи с этим при $0<R\leqslant 1$ исследуется функция надежности

$$E(R, p)=\overline{\lim_{n\to\infty}}-\frac{1}{n}\log P(n, ]2^{Rn}[, p)$$

и функция

$$\delta(R)=\overline{\lim_{n\to\infty}}\frac{1}{n}d(n, ]2^{Rn}[\,).$$

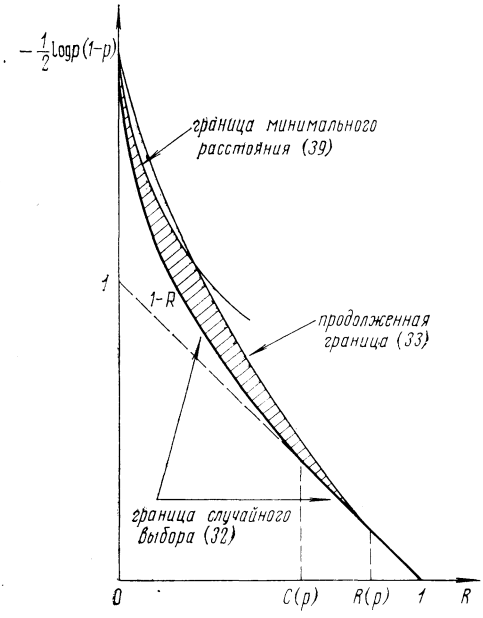
Чтобы определить эти функции при $R=0$ так, чтобы они не имели разрыва в этой точке, достаточно рассмотреть последовательности пар $(n, m_n)$ такие, что $R_n=n^{-1}\log m_n\to 0$ и $m_n\to\infty$ при $n\to\infty$, и положить

$$E(0, p)=\sup\overline{\lim_{n\to\infty}}-$$

$$-\frac{1}{n}\log P(n, m_n, p),$$

$$\delta(0)=\sup\overline{\lim_{n\to\infty}}\frac{1}{n}d(n, m_n),$$

где верхние грани берутся по всем последовательностям пар указанного вида. Тогда, как следует из (5), (6) и (2), $E(0, p)=-1/2\log p(1-p)$ и, как следует из границы Варшамова — Гилберта (1) и границы Плоткина $d(n, m)\leqslant\bar{d}(n, m)$ (см. (5)), $\delta(0)=1/2$. Заметим, что если числа $m_n$ не возрастают, то закономерности будут иными *. Таким образом, при рассмотрении асимптотических закономерностей мы пренебрегаем теми случаями, когда скорость кодов стремится к нулю, но мощность кодов не стремится к $\infty$.




Границы для функции надежности $E(R, p)$ при фиксированном $p(0<p<1/2)$ $C(p)=1-H(p)$, $R(p)=1+\log(1-p)$

Ниже полученные результаты трактуются как границы для функции надежности $E(R, p)$ при фиксированном $p$, $0<p<1/2$ (см. рисунок). Из следствия 4 теоремы 1 и неравенства (4) вытекает граница случайного выбора

(32) $$E(R, p)\geqslant E_1(R, p),$$

* Легко показать, что при фиксированном четном $m$ и $n\to\infty$ $d(n, m)\sim d(n, m-1)\sim(nm)/(2(m-1))$ и, следовательно,

$$-\frac{1}{n}\log P(n, m, p)\sim-\frac{1}{n}\log P(n, m-1, p)\sim-1/2\log p(1-p)+\frac{1}{2(m-1)}\log\frac{1-p}{p}.$$

где

$$E_1(R,p)=\begin{cases}-\rho(R)\log p-(1-\rho(R))\log(1-p), & \text{если } 0<R\leqslant C(p),\\ 1-R, & \text{если } C(p)\leqslant R\leqslant 1.\end{cases}$$

Из следствия теоремы 2 и неравенства (21) вытекает граница

$$E(R,p)\leqslant E_2(R,p), \tag{33}$$

где

$$E_2(R,p)=$$

$$=\begin{cases}\dfrac{R}{\log(2^{1-R}-1)}\log p-\left(1+\dfrac{R}{\log(2^{1-R}-1)}\right)\log(1-p)-R, & \text{если } 0<R\leqslant R(p),\\ 1-R, & \text{если } R(p)\leqslant R\leqslant 1.\end{cases}$$

Легко проверить, что функции $E_1(R,p)$ и $E_2(R,p)$ при $R\to 0$ стремятся к $-\frac{1}{2}\log p(1-p)=E(0,p)$. Кроме того, эти функции совпадают при $R(p)\leqslant R\leqslant 1$ и, следовательно,

$$E(R,p)=1-R, \text{ если } R(p)\leqslant R\leqslant 1. \tag{34}$$

Отметим также, что производная функции $E_1(R,p)$ по $R$ равна $-\infty$ в точке $R=0$, а производная функции $E_2(R,p)$ по $R$ равна $-1-\frac{1}{4}\ln((1-p)/p)$ в точке $R=0$ и имеет разрыв * в точке $R=R(p)$.

Из леммы 3 следует граница минимального расстояния

$$E(R,p)\leqslant -\delta(R-\varepsilon)\log p-(1-\delta(R-\varepsilon))\log(1-p), \tag{35}$$

где $\varepsilon$ — сколь угодно малое положительное число **. Заметим, что если выполнено весьма правдоподобное предположение о том, что граница Варшамова — Гилберта (1) является асимптотически точной, т. е. $\delta(R)=\rho(R)$, то из (32) и (35) немедленно следует, что $E(R,p)=-\rho(R)\log p-(1-\rho(R))\log(1-p)$ при $0\leqslant R\leqslant C(p)$. Однако, поскольку это предположение в настоящее время не доказано, то можно подставлять в (35) лишь верхние границы величины $\delta(R)$. Для $\delta(R)$ известна верхняя граница Элайса

$$\delta(R)\leqslant 2\rho(R)(1-\rho(R)), \tag{36}$$

которая получается, например, из (31) оптимизацией параметра $w$. Подстановка этой границы в (35) приводит к границе

$$E(R,p)\leqslant E_3(R,p), \tag{37}$$

где $E_3(R,p)=-2\rho(R)(1-\rho(R))\log p-(1-2\rho(R)(1-\rho(R)))\log(1-p)$. Производная функции $E_3(R,p)$ по $R$ в точке $R=0$ равна $-\ln((1-p)/p)$, и поэтому граница (37) улучшает границу (33) в некоторой окрестности точки $R=0$ лишь когда вероятность $p$ достаточно мала.

Более сильную верхнюю границу для $\delta(R)$ можно получить, если провести асимптотическое исследование границы (27) при фиксированном отношении $w/n=\rho$ и оптимальном выборе параметра $s$ точно так же, как это делалось в работах [5, 6] для верхней границы максимальной мощности кода при заданном минимальном расстоянии. В результате получается граница

$$\delta(R)\leqslant\delta_1(R)=\min_{\rho(R)\leqslant\rho\leqslant 1/2} g(R,\rho), \tag{38}$$

---

* Это объясняется тем, что при получении продолженной границы мы смогли использовать (24) лишь при $p_0=\frac{1}{2}$, а не при значении $p_0$, которое является корнем уравнения $m=2^n(1-p_0)^n$.

** В настоящее время мы не располагаем доказательством того, что функция $\delta(x)$ непрерывна. Однако далее функция $\delta(x)$ при $x=R-\varepsilon$ оценивается сверху непрерывными функциями от $x$, и поэтому в получаемых неравенствах можно положить $\varepsilon=0$.

где

$$g(R,\rho)=2\rho(1-\rho)\left(1-\exp\left\{\frac{1-R-H(\rho)}{(\rho(1-\rho)-z)\log((\rho-z)(1-\rho-z)/z^2)}\right\}\right),$$

а $z=z(R,\rho)$ $(0\leqslant z\leqslant\rho(1-\rho))$ — корень уравнения

$$\rho H\left(\frac{z}{\rho}\right)+(1-\rho)H\left(\frac{z}{1-\rho}\right)+(\rho(1-\rho)-z)\log\frac{(\rho-z)(1-\rho-z)}{z^2}\times$$

$$\times\ln\left(1-\frac{z}{\rho(1-\rho)}\right)=1-R.$$

Можно проверить, что функция $g(R,\rho)$ в точке $\rho=\rho(R)$ равна $2\rho(R)(1-\rho(R))$, а ее производная по $\rho$ в этой точке равна $-\infty$ (при $0<\rho(R)<1/2$) и, следовательно, граница (38) улучшает границу (36) при всех $R$, $0<R<1$. Можно проверить также, что производная функции $g(R,1/2)$ (и, следовательно, функции $-g(R,1/2)\log p-(1-g(R,1/2))\log(1-p)$) по $R$ в точке $R=0$ равна $-\infty$ (как и производная функции $E_1(R,p)$), так что при подстановке границы (38) в (35) получается граница

$$E(R,p)\leqslant-\delta_1(R)\log p-(1-\delta_1(R))\log(1-p), \tag{39}$$

которая при любом $p$ $(0<p<1/2)$ заведомо сильнее границы (33) в некоторой окрестности точки $R=0$.

В заключение отметим, что те же самые асимптотические результаты справедливы и в классе линейных кодов.

## § 6. О выборе параметров кода для передачи по ДСК с мгновенной и бесшумной обратной связью

Полученные границы вероятности необнаружения ошибки позволяют продвинуться в решении задачи выбора оптимального кода для передачи по ДСК с мгновенной и бесшумной обратной связью.

Рассматривается следующая система передачи информации. Имеется источник, который в последовательные моменты времени независимо и с равными вероятностями порождает символы 0 и 1. Сообщения источника кодируются векторами некоторого $(n, k)$-кода * $K$ и посылаются по ДСК, который имеет вероятность ошибки $p$ на символ. Декодирующее устройство определяет относительно каждого полученного блока длины $n$ принадлежит ли он коду $K$ или нет. Если полученный блок совпадает с некоторым кодовым вектором, что соответствующее ему сообщение передается получателю. В противном случае (при обнаружении ошибки) декодирующее устройство стирает этот блок и посылает по обратному каналу (который предполагается мгновенным и бесшумным) сигнал переспроса. При получении сигнала переспроса кодирующее устройство повторяет передачу кодового вектора. Параметрами такой системы с переспросом являются *эффективная скорость передачи*

$$S(K,p)=R(K)(P(K,p)+(1-p)^n), \tag{40}$$

которая учитывает, что с вероятностью $1-P(K,p)-(1-p)^n$ происходит переспрос, и *остаточная вероятность ошибочного приема* (кодового вектора)

$$Q(K,p)=P(K,p)/(P(K,p)+(1-p)^n), \tag{41}$$

* Класс линейных кодов рассматривается для упрощения изложения и потому, что для произвольных кодов более сильных результатов не получено.

которая равна вероятности того, что получателю передается неверное сообщение.

Зафиксируем вероятность ошибки $p$ $(0<p<1/2)$ в ДСК. Будем называть $(n, k)$-код $K$ *$Q$-кодом*, если $Q(K, p)\leqslant Q$. Рассмотрим следующую задачу. Требуется для заданного числа $Q$ (максимально допустимой остаточной вероятности ошибочного приема) найти $Q$-код (и, в частности, указать его параметры $n$ и $k$), который максимизирует эффективную скорость передачи в классе всех $Q$-кодов. Такой $Q$-код будем называть *оптимальным*, а его эффективную скорость передачи обозначать через $S_p(Q)$.

Указанную задачу можно считать разумной, если окажется, что для оптимального $Q$-кода $K$ при любом $p'<p$ имеет место $S(K, p')\geqslant S_p(Q)$ и $Q(K, p')\leqslant Q$ (т. е. если при улучшении ДСК не происходит ухудшения параметров (40) и (41)). Как будет показано, это действительно имеет место, поскольку для любого (не обязательно, линейного) кода $K$ функции $S(K, p)$ и $Q(K, p)$ являются монотонными по $p$, что, вообще говоря, не верно для функции $P(K, p)$.

То, что *для любого кода $K$ функция $S(K, p)$ убывает по $p$*, доказывается следующим образом. В силу леммы 1 и тождества (19) величину $P(K, p)+(1-p)^n$ можно представить в виде $2^{-n}\sum_{j=0}^{n} a_j'(1-2p)^j$, где все числа $a_j'$ неотрицательны, и, следовательно, эта величина, а вместе с ней и $S(K, p)$ убывают* по $p$. То, что *для любого кода $K$ функция $Q(K, p)$ возрастает по $p$*, следует из того, что $Q(K, p)=(1+(P(K, p)(1-p)^{-n})^{-1})^{-1}$, а величину $P(K, p)(1-p)^{-n}$ можно представить в виде $\sum_{i=1}^{n} a_i(p/(1-p))^i$, где все числа $a_i$ неотрицательны, и, следовательно, эта величина, а вместе с ней и $Q(K, p)$ возрастают по $p$.

Отметим, что для любого $(n, k)$-кода $K$

$$(k/n)(1-p)^n\leqslant S(K, p)=(k/n)(1-p)^n/(1-Q(K, p)), \tag{42}$$

$$P(K, p)(1-p)^{-n}=Q(K, p)/(1-Q(K, p)). \tag{43}$$

В силу (43) и неравенства $P(K, p)\geqslant p^{d(K)}(1-p)^{n-d(K)}$ для любого $Q$-кода $K$ справедливо неравенство

$$d(K)\geqslant \frac{\log(Q/(1-Q))}{\log(p/(1-p))}. \tag{44}$$

Из (44) и (42) следует, что при $Q\to 0$ длина оптимального $Q$-кода стремится к бесконечности, а эффективная скорость передачи $S_p(Q)$ стремится к нулю. Однако, как будет ясно из дальнейшего, $S_p(Q)$ стремится к нулю очень медленно, что является основанием для использования указанной системы передачи в практических целях.

Исследуем как, исходя из полученных границ вероятности необнаружения ошибки, следует выбирать параметры $n$ и $k$, чтобы они были наиболее близки к параметрам оптимального $Q$-кода. При этом, будем считать, что $Q\leqslant 0{,}01$, хотя все дальнейшее справедливо и при более слабом ограничении. Согласно следствию 2 теоремы 1 для любых $n$ и $k$ таких, что $R=k/n\leqslant C(p)$, существует $(n, k)$-код $K$, для которого

$$Q(K, p)/(1-Q(K, p))=P(K, p)(1-p)^{-n}\leqslant(p/(1-p))^{n\rho}, \tag{45}$$

* Отсюда также следует, что для любого кода $K$ вероятность переспроса $1-P(K, p)-(1-p)^n$ возрастает по $p$.

где $\rho=\rho(R)$. Предположим, что для такого кода выполнено неравенство

$$Q(K,\ p)/(1-Q(K,\ p))\leqslant(p/(1-p))^{n\rho}\leqslant Q/(1-Q). \tag{46}$$

Из (42) и (46) следует, что

$$S(K,p)\leqslant\frac{1-H(\rho)}{1-Q}\exp\left\{-\frac{\tau(Q,p)}{\rho}\right\},\ \text{где}\ \tau(Q,p)=\frac{\ln(Q/(1-Q))}{\ln(p/(1-p))}\ln\frac{1}{1-p}.$$

Пусть

$$S^*=S^*(Q,p)=\max_{0\leqslant\rho\leqslant 1/2}(1-H(\rho))\exp\{-\tau(Q,p)/\rho\}. \tag{47}$$

Величина $S^*$ равна (с точностью до $Q$) максимальной эффективной скорости передачи, которой может обладать код $K$, удовлетворяющий (46). Можно показать, что максимум достигается при $\rho=\rho^*$, где $\rho^*=\rho^*(Q,\ p)$ — единственный в области $0\leqslant\rho<1/2$ корень уравнения

$$f(\rho)=\tau(Q,\ p)(\ln 2(1-\rho)-\rho\ln((1-\rho)/\rho))-\rho^2\ln((1-\rho)/\rho)=0.$$

Важно отметить, что при любом $p$, $0<p<1/2$, имеет место $\rho^*>p$. Это следует из того, что $Q/(1-Q)\leqslant e^{-4}$ (в силу ограничения $Q\leqslant 0{,}01$), $-\ln(1-p)\geqslant p$ и

$$f(p)\geqslant\frac{p}{\ln((1-p)/p)}\left(4\left(\ln 2(1-p)-p\ln\frac{1-p}{p}\right)-p\ln^2\frac{1-p}{p}\right)>0.$$

Проведенный анализ показывает, что при фиксированных $Q$ и $p$ параметры $n$ и $k$ целесообразно выбирать следующим образом:

$$n=\left]\frac{\ln(Q/(1-Q))}{\rho^*\ln(p/(1-p))}\right[,\quad k=[(1-H(\rho^*))n]. \tag{48}$$

Убедимся в том, что существует $(n,\ k)$-код с параметрами (48), который является $Q$-кодом и, следовательно, в силу (42) величина $S_p(Q)=(k/n)\cdot(1-p)^n$ является нижней границей для $S_p(Q)$. Из (48) и неравенства $\rho^*>p$ следует, что

$$R=k/n\leqslant 1-H(\rho^*)<1-H(p)=C(p) \tag{49}$$

и по следствию 2 теоремы 1 существует $(n,\ k)$-код $K$, для которого справедливо (45). Поскольку в силу (49) $\rho=\rho(R)\geqslant\rho^*$, то из (45) и (48) следует, что $Q(K,\ p)\leqslant Q$. С другой стороны, в силу (42) и (47)

$$S_p(Q)\geqslant\underline{S}_p(Q)=(k/n)(1-p)^n\geqslant S^*(1-p)(1-1/(k+1)). \tag{50}$$

При малых $Q$ и $p$ нижняя граница (50) для $S_p(Q)$ лишь незначительно отличается от $S^*$. В табл. 1 и 2 для ряда значений $Q$ подсчитаны параметры (48), а также величины $R=k/n$ и $\underline{S}_p(Q)=R(1-p)^n$ при $p=0{,}01$ и $p=0{,}001$ соответственно.

На основании весьма правдоподобного предположения о том, что граница Варшамова — Гилберта (2) является асимптотически точной (т. е. $\tilde{d}(n,\ k)\sim n\rho(R)$ при фиксированном $R=k/n$ и $n\to\infty$), можно ожидать, что $Q$-коды с параметрами (48) близки к оптимальным. Во всяком случае, из (42), (44) и (47) следует, что если $(n,\ k)$-код $K$ является $Q$-кодом и $d(K)=(n+c)\rho(R)$, где $R=k/n$, то

$$S(K,\ p)\leqslant S^*(1-Q)^{-1}(1-p)^{-c}. \tag{51}$$

Приведем еще одну верхнюю границу для $S_p(Q)$, полученную на основании результатов § 3. Легко проверить, что в силу определения (41) и

Таблица 1

**Параметры $Q$-кодов, близких к оптимальным при $p=0{,}01$**

| $Q$ | $n$ | $k$ | $R$ | $\underline{S}_p(Q)$ | $\bar{S}_p(Q)$ | $Q$ | $n$ | $k$ | $R$ | $\underline{S}_p(Q)$ | $\bar{S}_p(Q)$ |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $10^{-2}$ | 25 | 18 | 0,720 | 0,560 | 1,000 | $10^{-9}$ | 52 | 29 | 0,558 | 0,331 | 0,649 |
| $10^{-3}$ | 30 | 21 | 0,700 | 0,518 | 0,745 | $10^{-10}$ | 55 | 30 | 0,545 | 0,314 | 0,622 |
| $10^{-4}$ | 35 | 23 | 0,657 | 0,462 | 0,745 | $10^{-11}$ | 58 | 31 | 0,534 | 0,298 | 0,600 |
| $10^{-5}$ | 39 | 25 | 0,641 | 0,433 | 0,745 | $10^{-12}$ | 60 | 31 | 0,517 | 0,283 | 0,589 |
| $10^{-6}$ | 42 | 26 | 0,619 | 0,406 | 0,696 | $10^{-16}$ | 70 | 33 | 0,471 | 0,233 | 0,522 |
| $10^{-7}$ | 46 | 27 | 0,587 | 0,370 | 0,696 | $10^{-20}$ | 79 | 35 | 0,443 | 0,200 | 0,468 |
| $10^{-8}$ | 49 | 28 | 0,571 | 0,349 | 0,656 | | | | | | |

Таблица 2

**Параметры $Q$-кодов, близких к оптимальным при $p=0{,}001$**

| $Q$ | $n$ | $k$ | $R$ | $\underline{S}_p(Q)$ | $\bar{S}_p(Q)$ | $Q$ | $n$ | $k$ | $R$ | $\underline{S}_p(Q)$ | $\bar{S}_p(Q)$ |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $10^{-3}$ | 84 | 76 | 0,905 | 0,832 | 1,000 | $10^{-9}$ | 140 | 119 | 0,850 | 0,739 | 0,913 |
| $10^{-4}$ | 96 | 85 | 0,885 | 0,804 | 0,916 | $10^{-10}$ | 147 | 123 | 0,837 | 0,722 | 0,913 |
| $10^{-5}$ | 107 | 94 | 0,879 | 0,789 | 0,913 | $10^{-11}$ | 154 | 128 | 0,831 | 0,712 | 0,913 |
| $10^{-6}$ | 116 | 101 | 0,871 | 0,775 | 0,913 | $10^{-12}$ | 160 | 132 | 0,825 | 0,703 | 0,913 |
| $10^{-7}$ | 124 | 107 | 0,863 | 0,762 | 0,913 | $10^{-16}$ | 183 | 148 | 0,809 | 0,673 | 0,913 |
| $10^{-8}$ | 132 | 113 | 0,856 | 0,750 | 0,913 | $10^{-20}$ | 203 | 160 | 0,788 | 0,643 | 0,895 |

границы (8) условие $k\leqslant nR(p)-\log(1-Q)$ является необходимым для того, чтобы $(n, k)$-код был $Q$-кодом. Поэтому в силу (42), (43) и теоремы 2 верхней границей для $S_p(Q)$ является величина

$$\bar{S}_p(Q)=(1-Q)^{-1}\max\,(k/n)\,(1-p)^n, \tag{52}$$

где максимум берется по всем параметрам $n$ и $k$ $(k\leqslant nR(p)-\log(1-Q))$ таким, что

$$\max_{-\log(1-Q)\leqslant x<k}(2^k-1)\exp\left\{\frac{\ln(p/(1-p))}{\ln(2^{1-k/n+x/n}-1)}\ln\frac{2^x-1}{2^k-1}\right\}\leqslant\frac{Q}{1-Q}. \tag{53}$$

Граница $\bar{S}_p(Q)$ также подсчитана в табл. 1 и 2 для соответствующих значений $Q$ и $p$. При этом, в случаях $k=n$ и $k=n-1$ условие (53) заменялось более сильными условиями $Q\geqslant 1-(1-p)^n$ и $Q\geqslant(1+(1-2p)^n-2(1-p)^n)/(1+(1-2p)^n)$ соответственно, которые должны выполняться для $Q$-кодов с такими параметрами. Для сокращения перебора использовалось то обстоятельство, что длина оптимального $Q$-кода не превышает $(\ln S(1-Q))/\ln(1-p)$, где $S$ — эффективная скорость передачи любого $Q$-кода.

Отметим, что аналогичным образом можно использовать полученные границы вероятности необнаружения ошибки для выбора параметров $n$ и $k$ в случае более сложных систем передачи с переспросом (см., например, [11]), когда обратная связь не предполагается мгновенной и бесшумной.

Автор выражает глубокую признательность Э. М. Габидулину, Л. М. Финку и Б. С. Цыбакову за полезные замечания, учтенные в окончательном варианте статьи.

ЛИТЕРАТУРА

1. *Берлекэмп Э.* Алгебраическая теория кодирования. М., «Мир», 1971.
2. *Галлагер Р.* Теория информации и надежная связь. М., «Сов. радио», 1974.
3. *Коржик В. И.* Границы по вероятности необнаружения ошибок и оптимальные групповые коды в канале с обратной связью. Радиотехника, 1965, 20, *1*, 27–33.

4. *Леонтьев В. К.* Кодирование с обнаружением ошибок. Проблемы передачи информации, 1972, 8, *2*, 6–14.
5. *Сидельников В. М.* Верхние оценки числа точек двоичного кода с заданным кодовым расстоянием. Проблемы передачи информации, 1974, 10, *2*, 43–51.
6. *Левенштейн В. И.* О минимальной избыточности двоичных кодов, исправляющих ошибки. Проблемы передачи информации, 1974, 10, *2*, 26–42.
7. *Коржик В. И., Осмоловский С. А., Финк Л. М.* Универсальное стохастическое кодирование в системах с решающей обратной связью. Проблемы передачи информации, 1974, 10, *4*, 25–29.
8. *Delsarte P.* Bounds for Unrestricted Codes, by Linear Programming. Philips Res. Rep., 1972, 27, 272–289.
9. *Сидельников В. М.* О взаимной корреляции последовательностей. Сб. «Проблемы кибернетики», *24*. М., «Наука», 1971, 15–42.
10. *Welch L. R., McEliece P. J., Rumsey H., Jr.* A Low Rate Improvement on the Elias Bound. IEEE Trans. Inform. Theory, 1974, 20, *5*, 676–678.
11. *Коржик В. И., Финк Л. М.* Помехоустойчивое кодирование дискретных сообщений в каналах со случайной структурой. М., «Связь», 1975.

Поступила в редакцию
4 ноября 1975 г.