ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 55 **2019** **Вып. 4**

УДК 621.391.1 : 519.2

© 2019 г. **М.В. Бурнашев**

О ГРАНИЦАХ СНИЗУ ДЛЯ СПЕКТРА ДВОИЧНОГО КОДА[1]

Уточняется оценка снизу для спектра двоичного кода. Дается простой вывод известной границы для вероятности необнаружения ошибки двоичного кода.

Ключевые слова: спектр двоичного кода, код постоянного веса, вероятность необнаружения ошибки.

DOI: 10.1134/S055529231904003X

§ 1. Введение

Рассмотрим двоичное пространство $E^n = \{0,1\}^n$ векторов $\{\boldsymbol{x}\}$ с расстоянием Хэмминга $d(\boldsymbol{x},\boldsymbol{u}) = \|\boldsymbol{x}-\boldsymbol{u}\|$. Для заданного параметра R, $0 < R < 1$, выберем множество $\mathcal{X}_M = \{\boldsymbol{x}_1,\ldots,\boldsymbol{x}_M\} \subset E^n$ из $M = 2^{Rn}$ *различных* векторов $\{\boldsymbol{x}_i\}$, и будем называть его (M,n)-кодом $\mathcal{C}$. Для (M,n)-кодов $\mathcal{C}$ введем величины

$$d(\mathcal{C}) = \min_{\boldsymbol{x},\boldsymbol{y}\in\mathcal{C}} d(\boldsymbol{x},\boldsymbol{y}), \quad d(M,n) = \max_{\mathcal{C}\subseteq E^n,\,|\mathcal{C}|=M} d(\mathcal{C}). \tag{1}$$

Мощность множества A обозначаем через $|A|$. *Спектр* кода (*распределение расстояний*) $B(\mathcal{C}) = (B_0, B_1, \ldots, B_n)$ – это $(n+1)$-вектор с компонентами

$$B_i = |\mathcal{C}|^{-1}|\{(\boldsymbol{x},\boldsymbol{y}) :\, \boldsymbol{x},\boldsymbol{y}\in\mathcal{C},\, d(\boldsymbol{x},\boldsymbol{y}) = i\}|, \quad i = 0,1,\ldots,n. \tag{2}$$

Введем шары и сферы в E^n

$$\mathbf{B}_{\boldsymbol{x}}(r) = \{\boldsymbol{u} :\, d(\boldsymbol{x},\boldsymbol{u}) \leqslant r\}, \quad \mathbf{S}_{\boldsymbol{x}}(r) = \{\boldsymbol{u} :\, d(\boldsymbol{x},\boldsymbol{u}) = r\}, \quad \boldsymbol{x},\boldsymbol{u}\in E^n. \tag{3}$$

Всюду далее $\log z = \log_2 z$, $h(z) = h_2(z) = -z\log_2 z - (1-z)\log_2(1-z)$.

§ 2. Граница снизу для спектра кода

Введем функцию [1] ($0 \leqslant \tau \leqslant \alpha \leqslant 1/2$)

$$G(\alpha,\tau) = 2\frac{\alpha(1-\alpha)-\tau(1-\tau)}{1+2\sqrt{\tau(1-\tau)}} \geqslant 0. \tag{4}$$

Для α,τ, таких что $0 \leqslant \tau \leqslant \alpha \leqslant 1/2$ и $h_2(\alpha) - h_2(\tau) = 1-R$, введем функцию [2]

$$\mu(R,\alpha,\omega) = h_2(\alpha) - 2\int\limits_0^{\omega/2} \log\frac{P+\sqrt{P^2-4Qy^2}}{Q}\,dy - (1-\omega)h_2\left(\frac{\alpha-\omega/2}{1-\omega}\right), \tag{5}$$

$$P = \alpha(1-\alpha) - \tau(1-\tau) - y(1-2y), \quad Q = (\alpha-y)(1-\alpha-y).$$

[1] Работа выполнена при частичной финансовой поддержке Российского фонда фундаментальных исследований (номер проекта 19-01-00364).

Определим функцию $\delta_{\mathrm{GV}}(R) \leqslant 1/2$ (границу Варшамова – Гилберта) как

$$1 - R = h_2(\delta_{\mathrm{GV}}(R)), \quad 0 \leqslant R \leqslant 1. \tag{6}$$

Важность функции $\mu(R, \alpha, \omega)$ и ее связь со спектром кода $\{B_i\}$ определяет следующий вариант теоремы 5 из [2] (см. также доказательство теоремы 2 в [3]).

Теорема 1. *Для любого (R, n)-кода и любого $\alpha \in [\delta_{\mathrm{GV}}(R), 1/2]$ существует ω, $0 \leqslant \omega \leqslant G(\alpha, \tau)$, где $h_2(\tau) = h_2(\alpha) - 1 + R$, а $G(\alpha, \tau)$ определено в* (4), *такое что*

$$n^{-1} \log B_{\omega n} \geqslant \mu(R, \alpha, \omega) + o(1), \quad n \to \infty, \tag{7}$$

где функция $\mu(R, \alpha, \omega) > 0$, определенная в (5), *имеет также представление* (13).

Отметим, что параметр α определяет код постоянного веса αn, которым заменяется исходный код (с помощью леммы Элайеса – Бассалыго) [1–3].

Введем величину R_0 формулой [4, 5]

$$R_0 = h_2(\tau_0) \approx 0{,}30524, \tag{8}$$

где $\tau_0 \approx 0{,}054507$ – единственный корень уравнения

$$(1 - 2\tau)\left[1 + \frac{1}{2\sqrt{\tau(1-\tau)}}\right] - \ln\frac{1-\tau}{\tau} = 0. \tag{9}$$

Для $0 \leqslant R \leqslant R_0$ наилучшей в теореме 1 является величина $\alpha = 1/2$ [5, замечание 4], так как такое α одновременно минимизирует $G(\alpha, \tau)$ и максимизирует $\mu(R, \alpha, \omega)$ для всех ω. При $\alpha = 1/2$ имеем [6, формула (33)]

$$\begin{aligned}\mu(R, 1/2, \omega) = {} & -2(1-\omega)\log(1-\omega) - \log\tau - 2(1-\tau)\log(1-\tau) + \\ & + (1-2\tau)\log(\tau - \omega + g) + \log[1 - \omega - (1-2\tau)g] - 2\omega\log g - 2,\end{aligned} \tag{10}$$

где

$$\tau = \tau(R) = h_2^{-1}(R), \quad g = g(\tau, \omega) = \frac{1 - 2\tau + \sqrt{(1-2\tau)^2 - 4\omega(1-\omega)}}{2}.$$

Из (10) также следует полезное выражение [3, формула (16)]

$$\mu(h_2(\tau), 1/2, G(1/2, \tau)) = h_2(\tau) + h_2(G(1/2, \tau)) - 1, \quad \tau \geqslant 0. \tag{11}$$

Введем функцию $T(A, B, \omega)$, $0 < A \leqslant B$:

$$\begin{aligned}T(A, B, \omega) = {} & \omega\log(v-1) - (1-\omega)\log\frac{v^2 - A^2}{v^2 - B^2} + B\log\frac{v+B}{v-B} - A\log\frac{v+A}{v-A} - \\ & - \frac{(v-1)(B^2 - A^2)}{(v^2 - B^2)\ln 2}, \quad v = \frac{\sqrt{B^2\omega^2 - 2a_1\omega + a_1^2} + a_1}{\omega}, \quad a_1 = \frac{B^2 - A^2}{2}.\end{aligned} \tag{12}$$

Предложение 1 [6, предложение 3]. *Для функции $\mu(R, \alpha, \omega)$ имеет место представление*

$$\mu(R, \alpha, \omega) = (1-\omega)h_2\Big(\frac{\alpha - \omega/2}{1-\omega}\Big) - h_2(\alpha) + 2h_2(\omega) + \omega\log\frac{2\omega}{e} - T(A, B, \omega), \tag{13}$$

где

$$h_2(\alpha) - h_2(\tau) = 1 - R, \quad A = 1 - 2\alpha, \quad B = 1 - 2\tau, \quad 0 \leqslant \tau \leqslant \alpha \leqslant 1/2. \tag{14}$$

§ 3. Граница снизу для спектра кода постоянного веса

Следующий результат является естественным аналогом теоремы 1 для кодов постоянного веса. Его доказательство можно извлечь из доказательства теоремы 1.

Для $w \leqslant n/2$ рассмотрим код $\mathcal{C}^{(w)} = \mathcal{C}(n, w)$ длины n и постоянного веса w, состоящий из различных кодовых векторов $\{\boldsymbol{x}\}$. Обозначим через $B_i^{(w)}$ его спектральные величины, определенные в (2).

Теорема 2. *Для любого (R, n)-кода постоянного веса αn, $\alpha \leqslant 1/2$, и любого $\tau \leqslant \alpha$ существует ω, $0 \leqslant \omega \leqslant G(\alpha, \tau)$, такое что*

$$n^{-1} \log B_{\omega n}^{(\alpha n)} \geqslant \mu(R, \alpha, \tau, \omega) + o(1), \quad n \to \infty, \tag{15}$$

где (см. (12))

$$\mu(R, \alpha, \tau, \omega) = R + h_2(\tau) - 2q_0(\alpha, \tau, \omega/2), \quad q_0(\alpha, \tau, \omega/2) =$$
$$= h_2(\tau) - \alpha h_2\Big(\frac{\omega}{2\alpha}\Big) - (1-\alpha) h_2\Big(\frac{\omega}{2(1-\alpha)}\Big) - \frac{\omega}{2}\log\frac{\omega}{e} + \frac{1}{2}T(A, B, \omega), \tag{16}$$
$$A = 1 - 2\alpha, \quad B = 1 - 2\tau.$$

Замечание 1. Для небольших w имеет смысл сначала заменить $\mathcal{C}^{(w)}$ на код $\mathcal{C}^{(w_1)}$ с $w_1 < w$ (как это делается в доказательстве теоремы 1 [2, 3]), а затем исследовать код $\mathcal{C}^{(w_1)}$. Мы не делаем этого, чтобы не усложнять формулы.

§ 4. Уточнение границы снизу для спектра кода

Граница снизу (7) из теоремы 1 с $\omega \in [0, G(\alpha, \tau)]$ была ориентирована на анализ функции надежности $E(R, p)$ канала ДСК(p) [2, 3, 5, 6]. При этом можно было пренебречь малыми величинами ω (важной являлась только максимальная величина $G(\alpha, \tau)$). Однако в некоторых других применениях теоремы 1 (например, в проверке гипотез с информационными ограничениями [7, 8]) нельзя пренебрегать малыми величинами ω. Поэтому там требуется результат, аналогичный теореме 1, но для ω, достаточно отделенных от 0. Следующий результат – один из возможных (см. доказательство в Приложении).

Теорема 3. *Для любого (R, n)-кода постоянного веса αn, $\alpha \leqslant 1/2$, любых $\tau \leqslant \alpha$ и $r_1 < G(\alpha, \tau)/2$, таких что*

$$\max_{0 \leqslant v \leqslant r_1} \{2q_0(\alpha, \tau, v) + h_2(2v)\} - h_2(\tau) \leqslant R, \tag{17}$$

или, если выполнено более простое условие

$$h_2(2r_1) + h_2(\tau) \leqslant R, \tag{18}$$

существует ω, $2r_1 \leqslant \omega \leqslant G(\alpha, \tau)$, такое что выполняется неравенство (15).

При $r_1 = 0$ теорема 3 переходит в теорему 2.

§ 5. Об одной полезной формуле

В [6, лемма 4] было показано, что для любых α, τ, таких что $h_2(\alpha) - h_2(\tau) = 1 - R$, справедлива формула

$$\mu(R, \alpha, G(\alpha, \tau)) = L(G(\alpha, \tau)) + R - 1, \tag{19}$$

где

$$L(\omega) = 2h_2[t_1(\omega)] - \omega - (1-\omega) h_2\left[\frac{2t_1(\omega) - \omega}{2(1-\omega)}\right], \quad t_1(\omega) = \frac{1 - \sqrt{1 - 2\omega}}{2}. \tag{20}$$

На самом деле, для $L(\omega)$ из (20) имеется простая формула (22), из которой следует

Лемма 1. *Для любых* α, τ, *таких что* $h_2(\alpha) - h_2(\tau) = 1 - R$, *верна формула*

$$\mu(R, \alpha, G(\alpha, \tau)) = h_2(G(\alpha, \tau)) + R - 1. \tag{21}$$

Доказательство. После замены в (20) переменной $1 - 2\omega = u^2$ имеем

$$L(\omega) = L\left(\frac{1-u^2}{2}\right) = 2h_2\left(\frac{1-u}{2}\right) - \frac{1-u^2}{2} - \frac{(1+u^2)}{2} h_2\left[\frac{(1-u)^2}{2(1+u^2)}\right].$$

После некоторых преобразований получаем для $L(\omega)$ формулу

$$L(\omega) = h_2(\omega). \tag{22}$$

Из (19) и (22) следует формула (21). ▲

Формула (22) обобщает формулу (11) на случай $\alpha < 1/2$.

Замечание 2. Формула (21) весьма упростила бы некоторые вычисления в [6].

§ 6. Еще одна граница снизу для спектра кода

Еще одна граница снизу для спектра кода принадлежит Левенштейну и менее известна, так как она содержится внутри доказательства теоремы из [4]. Приятной особенностью этой простой границы является ее очень короткое и изящное доказательство. При этом она может быть полезной в некоторых применениях. Например, с ее помощью Левенштейн получил (упрощенный) аналог границы (35). Представляется полезным привести эту границу. Для этого введем функцию (см. (2))

$$T_i(\mathcal{C}) = \sum_{j=0}^{i} B_j(\mathcal{C}) = |\mathcal{C}|^{-1} |\{(\boldsymbol{x}, \boldsymbol{y}) : \boldsymbol{x}, \boldsymbol{y} \in \mathcal{C},\ d(\boldsymbol{x}, \boldsymbol{y}) \leqslant i\}|, \quad i = 0, 1, \ldots, n. \tag{23}$$

Иными словами, $T_i(\mathcal{C})$ – среднее число кодовых слов $\boldsymbol{y}$ на расстоянии не более чем i от кодового слова $\boldsymbol{x}$.

Следующий результат является частью доказательства теоремы из [4].

Предложение 2. *Для любого* (M, n)*-кода* $\mathcal{C}$ *и любого натурального* K, $2 \leqslant K \leqslant M$, *справедливо неравенство* (*см.* (1))

$$T_{d(K,n)}(\mathcal{C}) \geqslant \frac{M - K + 1}{2(K-1)}. \tag{24}$$

Доказательство. Рассмотрим код $\mathcal{C}$ как граф G с M вершинами $\boldsymbol{x} \in \mathcal{C}$. Каждую пару $\boldsymbol{x}, \boldsymbol{y} \in G$ соединим ребром, если $d(\boldsymbol{x}, \boldsymbol{y}) \leqslant d(K, n)$. Тогда из определения (1) величины $d(K, n)$ следует, что не существует подмножество $A \subseteq E^n$, такое что $|A| = K$ и все расстояния между вершинами A больше $d(K, n)$. Это означает, что максимальное независимое подмножество графа G содержит менее K вершин.

Тогда по теореме Турана [9, теорема 13.4.1] граф G содержит не менее $(M - K + r + 1)(M - r)/[2(K-1)]$ ребер, где r – остаток от деления $M - 1$ на $K - 1$. Так как $0 \leqslant r < K - 1$, то эта оценка снизу достигает минимума при $r = 0$, откуда следует формула (24). ▲

Известно, что если $d(K, n) = \delta n$ и $K = 2^{\gamma n}$, то [1, формула (1.5)]

$$\gamma \leqslant h\Big[\frac{1}{2} - \sqrt{\delta(1-\delta)}\Big], \quad 0 \leqslant \delta \leqslant 1/2. \tag{25}$$

Граница сверху (25) – наилучшая известная для $0{,}273 \leqslant \delta \leqslant 1/2$. При $\delta < 0{,}273$ известна оценка лучше (см. [1]).

Если $d(K,n)=\delta n$, $M=2^{Rn}$ и $K=2^{\gamma n-1}$, $\gamma\leqslant R$, то из (24) и (25) получаем

$$\lim_{n\to\infty}\frac{1}{n}\log T_{\delta n}(\mathcal{C})\geqslant R-\gamma\geqslant R-h\Big[\frac{1}{2}-\sqrt{\delta(1-\delta)}\Big],\quad 0\leqslant\delta\leqslant 1/2. \tag{26}$$

Из определений (2) и (23) следует

$$\lim_{n\to\infty}\frac{1}{n}\log T_{\delta n}(\mathcal{C})=\max_{0\leqslant\omega\leqslant\delta}\lim_{n\to\infty}\frac{1}{n}\log B_{\omega n}(\mathcal{C}). \tag{27}$$

Поэтому из (26) и (27) получаем

Предложение 3. *Для любого (M,n)-кода $\mathcal{C}$ и любого $0\leqslant\delta\leqslant 1/2$, такого что $h\big[1/2-\sqrt{\delta(1-\delta)}\,\big]\leqslant R$, существует ω, $0\leqslant\omega\leqslant\delta$, такое что*

$$\lim_{n\to\infty}\frac{1}{n}\log B_{\omega n}(\mathcal{C})\geqslant R-h\Big[\frac{1}{2}-\sqrt{\delta(1-\delta)}\Big]. \tag{28}$$

Аналогичный результат можно получить и для кодов постоянного веса. Также при $\delta<0{,}273$, используя вместо (25) лучшую оценку из [1], можно несколько усилить границу (28).

Замечание 3. Можно проверить, что граница снизу (7) (даже при $\alpha=1/2$) сильнее, чем (28), при всех $R>0$.

§ 7. Вероятность необнаружения ошибки

Вероятность необнаружения ошибки $P_{\mathrm{ue}}(C,n)$ для (n,R)-кода $\mathcal{C}$ в канале ДСК(p) возникает в системах передачи с обратной связью и переспросом [2,4,10,11]. В таких системах, если приемник получает сигнал, отличный от кодового слова, он требует повторной передачи сигнала. Вероятность $P_{\mathrm{ue}}(C,n)$ связана со спектром $\{B_i\}$ кода (см. (2)) формулой

$$P_{\mathrm{ue}}(C,n)=\sum_{i=1}^{n}B_ip^i(1-p)^{n-i}. \tag{29}$$

При заданной скорости передачи R нас будет интересовать функция надежности $E_{\mathrm{ue}}(R,p)$, связанная с $P_{\mathrm{ue}}(C,n)$

$$E_{\mathrm{ue}}(R,p)=\limsup_{n\to\infty}\frac{1}{n}\log\frac{1}{P_{\mathrm{ue}}(R,n,p)}, \tag{30}$$

где $P_{\mathrm{ue}}(R,n,p)$ – минимально возможная при заданной скорости R вероятность необнаружения ошибки $P_{\mathrm{ue}}(C,n)$. Тогда с помощью оценки (7) имеем

$$\begin{aligned}E_{\mathrm{ue}}(R,p)&=\lim_{n\to\infty}\frac{1}{n}\log\frac{1}{\max\limits_i\left[B_ip^i(1-p)^{n-i}\right]}=-\log q-\\&-\lim_{n\to\infty}\frac{1}{n}\max_i\left\{\log B_i-i\log z\right\}\leqslant-\log q-\max_{\alpha\leqslant 1/2}\min_{\omega\leqslant G(\alpha,\tau)}V(R,\alpha,\omega,p),\end{aligned} \tag{31}$$

где

$$V(R,\alpha,\omega,p)=\mu(R,\alpha,\omega)-\omega\log z,\quad z=q/p,\quad q=1-p, \tag{32}$$

и (см. (4))

$$0\leqslant\tau\leqslant\alpha\leqslant 1/2,\quad h(\alpha)-h(\tau)=1-R.$$

Для функции $\mu(R,\alpha,\omega)$ также имеем [5, предложение 1]

$$\begin{aligned}
&\mu'_\omega(R,\alpha,\omega)=\log\frac{(1-\omega)\sqrt{(2\alpha-\omega)(2-2\alpha-\omega)}}{a_1-\omega(1-\omega)+\sqrt{(1-2\tau)^2\omega^2-2a_1\omega+a_1^2}},\\
&\mu'_\omega(R,\alpha,\omega)\big|_{\omega=G}=\log\frac{1-G}{G},\quad \mu''_{\omega\omega}(R,\alpha,\omega)<0,\\
&G=G(\alpha,\tau),\quad a_1=2[\alpha(1-\alpha)-\tau(1-\tau)],\\
&\frac{d\mu(R,\alpha,\omega)}{d\alpha}=\frac{dV(R,\alpha,\omega,p)}{d\alpha}>0,\quad \alpha_0(R)=h_2^{-1}(1-R)\leqslant\alpha<1/2,\quad \omega>0,
\end{aligned}\tag{33}$$

и тогда

$$V'_\omega(R,\alpha,\omega,p)\big|_{\omega=G}=\log\frac{(1-G)p}{Gq},\quad V''_{\omega\omega}(R,\alpha,\omega,p)<0.\tag{34}$$

Так как функция $V(R,\alpha,\omega,p)$ вогнута по ω (см. (34)), то в силу формулы (21) оптимизация в правой части (31) становится, по существу, технической задачей. Естественно ожидать, что минимум по ω в (31) достигается при $\omega=G(\alpha,\tau)$, и тогда останется только максимизация по $\alpha\leqslant 1/2$. В результате мы должны получить

Предложение 4. *Для функции $E_{\rm ue}(R,p)$ справедлива оценка сверху*

$$E_{\rm ue}(R,p)\leqslant\begin{cases}1-R-\log q-h(G_0(R))+G_0(R)\log z, & p\leqslant G_0(R),\\ 1-R, & p\geqslant G_0(R),\end{cases}\tag{35}$$

где

$$\begin{aligned}
&G_0(R)=\min_{(\alpha,\tau)\in\mathcal{A}(R)}G(\alpha,\tau),\quad z=q/p,\\
&\mathcal{A}(R)=\{(\alpha,\tau):\ 0\leqslant\tau\leqslant\alpha\leqslant 1/2,\ h(\alpha)-h(\tau)=1-R\}.
\end{aligned}\tag{36}$$

Замечание 4. Граница сверху (35) усиливает границу из [4]. Она появлялась уже в [2, теорема 1], однако ее доказательство (без аналитических свойств (33) функции $\mu(R,\alpha,\omega)$ и формулы (21)) довольно запутано и вызывает некоторые вопросы. Нашей целью является только простой вывод границы (35) из этих свойств.

Доказательство. Для $R\in(0,1)$ и $\alpha\in[\delta_{\rm GV}(R),1/2]$ введем величину

$$\tau_R(\alpha)=h_2^{-1}\left(h_2(\alpha)-1+R\right)\leqslant\alpha.\tag{37}$$

Так как $V''_{\omega\omega}<0$, то минимум по ω в (31) достигается в граничной точке $\omega=0$ или в граничной точке $\omega_0=G(\alpha,\tau_R(\alpha))$. Так как $\mu(R,\alpha,0)=V(R,\alpha,0,p)=0$, то из (31) имеем

$$\min_{\omega\leqslant G(\alpha,\tau)}V(R,\alpha,\omega,p)=\min\left\{0,V(R,\alpha,G(\alpha,\tau),p)\right\},\quad h_2(\alpha)-h_2(\tau)=1-R.$$

Поэтому в силу формулы (21)

$$\begin{aligned}
&E_{\rm ue}(R,p)\leqslant-\log q-\min\left\{0,\max_{(\alpha,\tau)\in\mathcal{A}(R)}V(R,\alpha,G(\alpha,\tau),p)\right\}=\\
&=-\log q-\min\left\{0,R-1+\max_{(\alpha,\tau)\in\mathcal{A}(R)}\{h(G(\alpha,\tau))-G(\alpha,\tau)\log z\}\right\}\leqslant\\
&\leqslant-\log q-\min\left\{0,R-1+\max_{\omega\geqslant G_0(R)}f(\omega,p)\right\},
\end{aligned}\tag{38}$$

где

$$f(\omega, p) = h(\omega) - \omega \log z.$$

Имеем $f''_{\omega\omega} < 0$ для $\omega \in [0, 1/2)$. Уравнение $f'_\omega(\omega, p) = 0$ имеет единственный корень $\omega = p$, причем $f(p, p) = -\log q$. Поэтому наилучшим $\omega = \omega_1(R, p)$ в (38) является

$$\omega_1(R, p) = \max\{p, G_0(R)\}.$$

Тогда (38) принимает вид

$$E_{\mathrm{ue}}(R, p) \leqslant -\log q - \min\{0, R - 1 + h(\omega_1(R, p)) - \omega_1(R, p) \log z\}. \tag{39}$$

Заметим, что если $p \geqslant G_0(R)$ и $R-1+h(p)-p\log z \leqslant 0$ (т.е. если $R \leqslant 1+\log(1-p)$), то из (39) получаем

$$E_{\mathrm{ue}}(R, p) \leqslant 1 - R, \quad \text{если} \quad G_0(R) \leqslant p \leqslant 1 - 2^{R-1}. \tag{40}$$

Так как функция $E_{\mathrm{ue}}(R, p)$ монотонно убывает по p, то неравенство (40) остается верным для всех $p \geqslant G_0(R)$. Аналогично (но проще) рассматривается случай $p \leqslant$ $\leqslant G_0(R)$. В результате получаем формулу (35). ▲

ПРИЛОЖЕНИЕ

Доказательство теоремы 3. Для того чтобы объяснить, откуда возникает условие (17), нам придется повторить часть доказательства теоремы 1 из [3, теорема 2]. Для $w \leqslant n/2$ рассмотрим код $\mathcal{C}^{(w)} = \mathcal{C}(n, w)$ постоянного веса w, состоящий из различных кодовых слов $\{\boldsymbol{x}\}$. Используя *многочлены Хана* $Q_j(i) = Q_j^{(n,w)}(i)$, введем многочлен

$$f(x) = \sum_{j=0}^{w} f_j Q_j(x), \tag{41}$$

где $f_0 > 0$ и $f_i \geqslant 0$, $i = 1, \ldots, w$. Введем целое $r \geqslant 1$. Тогда (см. (3))

$$\sum_{\boldsymbol{x}, \boldsymbol{y} \in \mathcal{C}^{(w)}} f\left(\frac{d(\boldsymbol{x}, \boldsymbol{y})}{2}\right) \leqslant \sum_{\substack{\boldsymbol{x}, \boldsymbol{y} \in \mathcal{C}^{(w)} \\ d(\boldsymbol{x}, \boldsymbol{y}) \geqslant 2r}} f\left(\frac{d(\boldsymbol{x}, \boldsymbol{y})}{2}\right) + 2r\big|\mathcal{C}^{(w)}\big| \max_{0 \leqslant j < 2r} \big\{|\mathbf{S_0}(j)| f(j/2)\big\}. \tag{42}$$

Замечание 5. Так как рассматривается код постоянного веса $\mathcal{C}^{(w)}$, то величину $|\mathbf{S_0}(j)|$ в правой части формулы (42) можно было бы заменить более точным выражением. Мы не стали этого делать, так как формулировка теоремы 3 излишне бы усложнилась.

Для кода $\mathcal{C}^{(w)}$ справедливо неравенство ([11, формула (1.7) и § 6.4])

$$\sum_{\boldsymbol{x}, \boldsymbol{y} \in \mathcal{C}^{(w)}} f\left(\frac{d(\boldsymbol{x}, \boldsymbol{y})}{2}\right) \geqslant \big|\mathcal{C}^{(w)}\big|^2 f_0. \tag{43}$$

Из (42) и (43) получаем

$$\sum_{\substack{\boldsymbol{x}, \boldsymbol{y} \in \mathcal{C}^{(w)} \\ d(\boldsymbol{x}, \boldsymbol{y}) \geqslant 2r}} f\left(\frac{d(\boldsymbol{x}, \boldsymbol{y})}{2}\right) \geqslant \big|\mathcal{C}^{(w)}\big|^2 f_0 - 2r\big|\mathcal{C}^{(w)}\big| \max_{0 \leqslant j < 2r} \big\{|\mathbf{S_0}(j)| f(j/2)\big\}. \tag{44}$$

Для $f(x)$ из (41) и $r \geqslant 1$ введем множество

$$I(r) = \{i \in \{r, \ldots, w\} : \ f(i) > 0\}. \tag{45}$$

Обозначим через $B_i^{(w)}$ спектральные величины кода $\mathcal{C}^{(w)}$, определенные в (2). Тогда из (44) и (45) имеем

$$\sum_{\substack{\boldsymbol{x},\boldsymbol{y}\in\mathcal{C}^{(w)}\\ d(\boldsymbol{x},\boldsymbol{y})/2\in I(r)}} f\left(\frac{d(\boldsymbol{x},\boldsymbol{y})}{2}\right) \geqslant \left|\mathcal{C}^{(w)}\right|^2 f_0 - 2r\left|\mathcal{C}^{(w)}\right| \max_{0\leqslant j<2r}\left\{|\mathbf{S_0}(j)|f(j/2)\right\}. \tag{46}$$

Так как $d(\boldsymbol{x},\boldsymbol{y})$ принимает только четные значения, то из (46) следует

Лемма 2. *Если* $|I(r)| > 0$, *то существует* $i \in I(r)$, *такое что*

$$B_{2i}^{(w)} \geqslant \frac{f_0|\mathcal{C}^{(w)}| - 2r \max\limits_{0\leqslant j<2r}\left\{|\mathbf{S_0}(j)|f(j/2)\right\}}{|I(r)|f(i)}. \tag{47}$$

Пусть x_t^w – минимальный корень многочлена $Q_t^{(n,w)}(x)$. Тогда $x_{t+1}^w < x_t^w$. Используем в (47) тот же многочлен $f(x)$, что и в [1, формулы (4.4) и (4.6)]:

$$f(x) = \frac{1}{(a-x)} Q_t^2(a)\left[Q_t(x) + Q_{t+1}(x)\right]^2, \tag{48}$$

где величина $t \leqslant w$ будет выбрана позже, а параметр $a \in (x_{t+1}^w, x_t^w)$ выбран так, что $Q_t(a) = -Q_{t+1}(a)$. Тогда $f(a) = 0$ и $f(x) \leqslant 0$, $a < x \leqslant w$. Коэффициенты разложения $f(x)$ в базисе многочленов $\{Q_j\}$ неотрицательны. Тогда имеем [1]

$$\begin{aligned} f_0 &= \left(\binom{n}{t} - \binom{n}{t-1}\right) \frac{(n-2t)(n-2t-1)}{(t+1)(w-t)(n-w-t)} Q_t^2(a), \\ f(0) &= \frac{1}{a}\left(\binom{n}{t+1} - \binom{n}{t-1}\right)^2 Q_t^2(a). \end{aligned} \tag{49}$$

Выберем t, так что

$$2r \max_{0\leqslant j<2r}\left\{|\mathbf{S_0}(j)|f(j/2)\right\} \leqslant f_0|\mathcal{C}^{(w)}|/2. \tag{50}$$

Возможность выбора такого t обеспечивается условием (17) и показывается далее.

Если выполнено (50), то (см. (47))

$$f_0|\mathcal{C}^{(w)}| - 2r \max_{0\leqslant j<2r}\left\{|\mathbf{S_0}(j)|f(j/2)\right\} \geqslant f_0|\mathcal{C}^{(w)}|/2.$$

В силу (42) для $r \leqslant a-1$ множество $I(r)$ имеет вид

$$I(r) = \{i \in \{r, \ldots, w\} : \ f(i) > 0\} = \{r, \ldots, a-1\},$$

и тогда в силу (47) и (50) для некоторого $i \in [r, a-1]$ имеем

$$B_{2i}^{(w)} \geqslant \frac{f_0|\mathcal{C}^{(w)}|}{2|I|f(i)} \geqslant \frac{f_0|\mathcal{C}^{(w)}|}{2x_t^w f(i)}. \tag{51}$$

Оценим величины $f_0, f(i), x_t^w$ в правой части (51). Из (48) и (49) имеем

$$\frac{f_0}{f(i)} = \binom{n}{t} \frac{(n-2t+1)(n-2t)(n-2t-1)(a-i)}{(n-t+1)(t+1)(w-t)(n-w-t)\left[Q_t(i) + Q_{t+1}(i)\right]^2}. \tag{52}$$

Рассмотрим асимптотический случай, когда $w = \alpha n,\ i = \xi n,\ t = \tau n$, где $\tau \leqslant \alpha \leqslant h_2^{-1}(R)$, $n \to \infty$. Известно [1, формула (B.21); 11], что

$$\frac{x_{\tau n}^{\alpha n}}{n} = \frac{G(\alpha,\tau)}{2} + o(1) \quad \text{для всех } \tau \leqslant \alpha \leqslant 1/2. \tag{53}$$

Обозначим

$$q(\alpha,\tau,\xi) = \lim_{n\to\infty} \frac{1}{n} \log Q_{\tau n}^{(n,\alpha n)}(\xi n). \tag{54}$$

Тогда из (52) следует

$$\lim_{n\to\infty} \frac{1}{n} \log \frac{f_0}{f(i)} = h_2(\tau) - 2q(\alpha,\tau,\xi). \tag{55}$$

Для функции $q(\alpha,\tau,\xi)$ из (54) справедлива оценка сверху [2; 3, лемма 4]

$$q(\alpha,\tau,\xi) \leqslant q_0(\alpha,\tau,\xi), \quad \xi < \frac{G(\alpha,\tau)}{2}, \tag{56}$$

где $q_0(\alpha,\tau,\xi)$ определено в (16) и (12).

Замечание 6. Возможно, в формуле (56) выполняется равенство, но это требует дополнительного исследования (см. [3, замечание 5]).

Из (50), (55) и (56) для $w = \alpha n$, $j = \eta n$, $t = \tau n$ имеем

$$\lim_{n\to\infty} \frac{1}{n} \log \frac{f_0}{f(j/2)} \geqslant h_2(\tau) - 2q_0(\alpha,\tau,\eta/2), \quad \eta < G(\alpha,\tau). \tag{57}$$

Так как $a \in (x_{t+1}^w, x_t^w)$ и $i \in [r, a-1]$, то при $r = r_1 n$ в силу (53) достаточно иметь

$$r_1 \leqslant \frac{a-1}{n} = \frac{x_{\tau n}^{\alpha n}}{n} + o(1) = \frac{G(\alpha,\tau)}{2} + o(1), \quad \tau \leqslant \alpha \leqslant 1/2. \tag{58}$$

Заметим, что $|\mathbf{S_0}(\eta n)| = 2^{h(\eta)n[1+o(1)]}$, $n \to \infty$. Поэтому, используя (57) при $j = \eta n$, $t = \tau n$, получаем, что для того чтобы можно было выбрать t (т.е. τ), такое что справедливо (50), достаточно чтобы при $n \to \infty$ выполнялось условие (17). Тогда в силу (51) для любых $\tau \leqslant \alpha$ и $r_1 < G(\alpha,\tau)/2$, таких что выполняется условие (17), для некоторого $\xi \in [r_1, G(\alpha,\tau)/2]$ имеем

$$\lim_{n\to\infty} \frac{1}{n} \log B_{2\xi n}^{(\alpha n)} \geqslant R + h_2(\tau) - 2q_0(\alpha,\tau,\xi). \tag{59}$$

Из (59) следует теорема 3, если выполняется условие (17).

Остается показать, что условие (17) выполнено, если справедливо (18). Заметим, что для левой части условия (17) имеем (так как $2r_1 < G(\alpha,\tau) \leqslant 1/2$)

$$\max_{0<v\leqslant r_1} \{2q_0(\alpha,\tau,v) + h_2(2v)\} - h_2(\tau) \leqslant 2 \max_{0<v\leqslant r_1} \{q_0(\alpha,\tau,v)\} + h_2(2r_1) - h_2(\tau). \tag{60}$$

Для функции $q_0(\alpha,\tau,u)$ в (60) выполняется следующий результат.

Лемма 3. *Имеем*

$$\begin{aligned} &[q_0(\alpha,\tau,u)]'_u \leqslant 0, \quad \textit{если} \ \ u \leqslant \alpha; \\ &[q_0(\alpha,\tau,u)]'_u \geqslant 0, \quad \textit{если} \ \ u \geqslant \alpha, \end{aligned} \tag{61}$$

и поэтому

$$\max_{u\leqslant\alpha} q_0(\alpha,\tau,u) = q_0(\alpha,\tau,0) = h_2(\tau). \tag{62}$$

Доказательство. Представление (16) функции $q_0(\alpha,\tau,u)$ идет из ее первоначального вида [2; 3, лемма 4] (см. обозначения в (12))

$$q_0(\alpha,\tau,u) = h_2(\tau) - \alpha h_2\Big(\frac{u}{\alpha}\Big) - (1-\alpha)h_2\Big(\frac{u}{1-\alpha}\Big) - 2u\log\frac{2u}{e} + I_1,$$
$$I_1 = \frac{1}{2}\int\limits_0^{2u} \log f_1(y)dy, \quad f_1(y) = y^2 - y + a_1 + \sqrt{B^2y^2 - 2a_1y + a_1^2}. \tag{63}$$

Тогда из (63) имеем

$$[q_0(\alpha,\tau,u)]'_u = -\log[y^2 - 2y + 1 - A^2] + \log\Big[y^2 - y + a_1 + \sqrt{B^2y^2 - 2a_1y + a_1^2}\Big],$$

где $y = 2u$. После стандартного анализа получаем (61) и (62). ▲

Заметим, что $G(\alpha,\tau)/2 \leqslant 2\alpha$ для любых α,τ. Поэтому в силу (62) для любого $r_1 < G(\alpha,\tau)/2$ формула (60) принимает вид

$$\max_{0<v\leqslant r_1}\{2q_0(\alpha,\tau,v) + h_2(2v)\} - h_2(\tau) \leqslant h_2(2r_1) + h_2(\tau). \tag{64}$$

Это завершает доказательство теоремы 3. ▲

Автор благодарит рецензента за конструктивные критические замечания, улучшившие статью.

СПИСОК ЛИТЕРАТУРЫ

1. *McEliece R.J., Rodemich E.R., Rumsey H., Jr., Welch L.R.* New Upper Bounds on the Rate of a Code via the Delsarte–MacWilliams Inequalities // IEEE Trans. Inform. Theory. 1977. V. 23. № 2. P. 157–166.
2. *Litsyn S.* New Upper Bounds on Error Exponents // IEEE Trans. Inform. Theory. 1999. V. 45. № 2. P. 385–398.
3. *Бурнашев М.В.* Спектр кода и функция надежности: двоичный симметричный канал // Пробл. передачи информ. 2006. Т. 42. № 4. С. 3–22.
4. *Левенштейн В.И.* О прямолинейной границе для экспоненты вероятности необнаруженной ошибки // Пробл. передачи информ. 1989. Т. 25. № 1. С. 33–37.
5. *Бурнашев М.В.* Усиление оценки сверху для функции надежности двоичного симметричного канала // Пробл. передачи информ. 2005. Т. 41. № 4. С. 3–22.
6. *Бурнашев М.В.* О функции надежности ДСК: расширение области, где она известна в точности // Пробл. передачи информ. 2015. Т. 51. № 4. С. 3–22.
7. *Бурнашев М.В., Амари Ш., Хан Т.С.* О некоторых задачах проверки гипотез с информационными ограничениями // Теория вероятностей и ее применения. 2000. Т. 45. № 4. С. 625–638.
8. *Shimokawa H., Han T.S., Amari S.* Error Bounds of Hypothesis Testing with Data Compression // Proc. 1994 IEEE Int. Sympos. on Information Theory (ISIT'94). Trondheim, Norway. June 27 – July 1, 1994. P. 114.
9. *Оре О.* Теория графов. М.: Наука, 1980.
10. *Левенштейн В.И.* О границах вероятности необнаружения ошибки // Пробл. передачи информ. 1977. Т. 13. № 1. С. 3–18.
11. *Левенштейн В.И.* Границы для упаковок метрических пространств и некоторые их приложения // Проблемы кибернетики. Вып. 40. М.: Наука, 1983. С. 43–110.

Бурнашев Марат Валиевич
Институт проблем передачи информации
им. А.А. Харкевича РАН
burn@iitp.ru

Поступила в редакцию
11.09.2019
После доработки
05.11.2019
Принята к публикации
12.11.2019