ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 58 **2022** **Вып. 3**

УДК 621.391 : 519.724

 М.В. Бурнашев

О ФУНКЦИИ НАДЕЖНОСТИ ДСК С БЕСШУМНОЙ ОБРАТНОЙ СВЯЗЬЮ ПРИ НУЛЕВОЙ СКОРОСТИ[1]

Рассматривается передача неэкспоненциального числа сообщений по двоичному симметричному каналу с бесшумной обратной связью. Получена оценка сверху для наилучшей экспоненты вероятности ошибки декодирования. Вместе с известной подобной оценкой снизу это позволяет найти функцию надежности такого канала при нулевой скорости.

Ключевые слова: функция надежности, бесшумная обратная связь.

DOI: 10.31857/S0555292322030019, **EDN:** DZTOVB

§ 1. Введение и основные результаты

Рассматривается двоичный симметричный канал ДСК(p) с переходной вероятностью $0 < p < 1/2$, $q = 1-p$, и бесшумной обратной связью. Задано общее время передачи n, а также $M_n = 2^{Rn}$, $0 < R < 1$, равновероятных сообщений $\{\theta_1, \theta_2, \ldots, \theta_{M_n}\}$. После момента времени n приемник принимает решение $\widehat{\theta}$, какое из сообщений является истинным сообщением θ_{true}.

Определим минимально возможную вероятность ошибки декодирования

$$P_{\text{e}}(M_n, n, p) = \min \frac{1}{M_n} \sum_{i=1}^{M_n} P(\text{e} \,|\, \theta_i), \tag{1}$$

где $P(\text{e} \,|\, \theta_i)$ – вероятность ошибки декодирования для используемого метода передачи при условии, что θ_i является истинным сообщением θ_{true}, а минимум берется по всем методам передачи длины n.

Обозначим через $F(R,p)$, $0 < R < 1$, наилучшую экспоненту вероятности ошибки декодирования для $M_n = e^{Rn}$ кодовых слов по каналу ДСК(p) с бесшумной обратной связью, т.е.

$$F(R,p) = \limsup_{n\to\infty} \frac{1}{n} \ln \frac{1}{P_{\text{e}}(M_n, n, p)}, \quad M_n = e^{Rn}, \tag{2}$$

где $P_{\text{e}}(M_n, n, p)$ определено в (1). Ясно, что функция $F(R,p)$ не возрастает по R.

Введем также предельную величину $F(0,p)$

$$F(0,p) = \lim_{R\to 0} F(R,p), \quad 0 < p < 1/2. \tag{3}$$

Предел в (3) существует, так как функция $F(R,p)$ ограничена и не возрастает по R.

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

Эквивалентным образом функция $F(0,p)$ определяется соотношением (2), если число сообщений M_n таково, что $M_n \to \infty$, но $\log M_n = o(n)$ при $n \to \infty$.

Аналогично определим величину $F_K(p)$, $K = 2, 3, \ldots$, как наилучшую экспоненту вероятности ошибки декодирования для K кодовых слов в канале ДСК(p) с бесшумной обратной связью, т.е.

$$F_K(p) = \limsup_{n\to\infty} \frac{1}{n} \ln \frac{1}{P_{\mathrm{e}}(K,n,p)}, \tag{4}$$

где $P_{\mathrm{e}}(K,n,p)$ – минимально возможная вероятность ошибки декодирования (для всех методов передачи длины n). В работе [1] было показано, что

$$F_3(p) = F_4(p) = \ldots = F(0,p), \tag{5}$$

и поэтому для исследования величины $F(0,p)$ достаточно изучить величину $F_3(p)$.

Обозначим через $E_k(p)$, $k \geqslant 2$, наилучшую экспоненту вероятности ошибки декодирования для k кодовых слов по каналу ДСК(p) без обратной связи. Ясно, что

$$E_2(p) = F_2(p) = \frac{1}{2} \ln \frac{1}{4pq}.$$

Также понятно, что $E_3(p)$ определяется n-симплексным кодом $(\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{x}_3)$ (т.е. кодом, в котором $d(\boldsymbol{x}_i, \boldsymbol{x}_j) \approx 2n/3$ для всех $i \neq j$), и поэтому

$$E_3(p) = \frac{1}{3} \ln \frac{1}{4pq}.$$

Ясно, что $E_3(p) \leqslant F_3(p) \leqslant E_2(p)$.

В работе [1] было доказано

Предложение. *Для $P_{\mathrm{e}}(3,n,p)$ справедлива оценка сверху (см. (4), (5))*

$$P_{\mathrm{e}}(3,n,p) \leqslant \left(\frac{q}{p}\right)^{1/3} \bigl(p^{1/3}q^{2/3} + p^{2/3}q^{1/3}\bigr)^n. \tag{6}$$

Из (3), (5) и (6) следует

$$F_3(p) \geqslant F_{\mathrm{fb}}(p), \tag{7}$$

где

$$F_{\mathrm{fb}}(p) = -\ln\bigl(p^{1/3}q^{2/3} + p^{2/3}q^{1/3}\bigr) = -\ln\bigl[p^{1/3}q^{2/3}(1 + z^{1/3})\bigr] \geqslant 0 \tag{8}$$

и

$$p + q = 1, \quad z = z(p) = p/q.$$

Из последующих работ [2, 3] (где другими методами исследовалась вся функция надежности $F(R)$) также, в частности, следовала формула (7).

При этом в работе [1] утверждалось, что в формуле (7) выполняется также противоположное неравенство

$$F_3(p) \leqslant F_{\mathrm{fb}}(p), \tag{9}$$

и тогда в случае справедливости формулы (9) из (7) следовало бы равенство

$$F_3(p) = F_{\mathrm{fb}}(p). \tag{10}$$

Однако строгое доказательство формулы (9) в [1] отсутствовало. Позже в работе [4] была сделана еще одна попытка доказать формулу (9) (используя общее уравнение Беллмана), однако позже выяснилось, что доказательство также неверно.

Далее в статье доказывается формула (9), и поэтому справедлива формула (10).

Опишем возможные методы передачи одного из трех сообщений по каналу ДСК с бесшумной обратной связью. Заметим, что любая разумная стратегия передачи имеет следующий вид. В каждый момент k, $k = 1, \ldots, n$, основываясь на полученных на выходе канала сигналах $\boldsymbol{y}^{k-1}$, приемник выделяет некоторое сообщение θ_{i_0} и задает передатчику вопрос, является ли θ_{i_0} истинным сообщением $\theta_{\rm true}$. Здесь важно наличие бесшумной обратной связи! Если истинное сообщение $\theta_{\rm true}$ совпадает с θ_{i_0}, т.е. $\theta_{\rm true} = \theta_{i_0}$, то передается сигнал $x_k = 0$. Если $\theta_{\rm true} \neq \theta_{i_0}$, то передается сигнал $x_k = 1$. После момента n принимается решение в пользу наиболее вероятного сообщения θ_i.

Стратегия передачи, использованная в работах [1–3], вполне естественна: в каждый момент времени k в качестве $\theta_{i_0}(k)$ выбирается наиболее вероятное из сообщений θ_i при условии $\boldsymbol{y}^{k-1}$. Кажется, что такая стратегия передачи дает наилучшую экспоненту вероятности ошибки декодирования $F_3(p)$ (однако это необходимо доказать, что не было сделано в [1–3]).

Основной результат статьи представляет

Теорема 1. *Для $P_{\rm e}(3,n,p)$ справедлива оценка снизу*

$$P_{\rm e}(3,n,p) \geqslant \frac{1}{2}\bigl(p^{1/3}q^{2/3} + p^{2/3}q^{1/3}\bigr)^n = \frac{1}{2}\bigl[p^{1/3}q^{2/3}(1+z^{1/3})\bigr]^n, \quad z = p/q, \tag{11}$$

и поэтому для $F_3(p)$ имеет место формула (*см.* (8))

$$F_3(p) = F(0,p) = F_{\rm fb}(p). \tag{12}$$

Заметим, что

$$E_2(p) = F_2(p) > F_3(p) > E_3(p), \quad 0 < p < 1/2. \tag{13}$$

Выход ДСК будем обозначать через $\boldsymbol{y}^k = y_1^k = (y_1, \ldots, y_k)$, $k = 1, \ldots, n$, где $y_k \in \{0, 1\}$.

Замечание 1. Поясним, почему при трех сообщениях бесшумная обратная связь в принципе может помочь уменьшить вероятность ошибки декодирования. Действительно, предположим, что в момент времени i выполнено

$$p(\boldsymbol{y}^i \,|\, \boldsymbol{x}_1) \approx p(\boldsymbol{y}^i \,|\, \boldsymbol{x}_2) \gg p(\boldsymbol{y}^i \,|\, \boldsymbol{x}_3),$$

т.е. сообщение θ_3 значительно менее вероятно, чем сообщения θ_1, θ_2 (и в силу имеющейся бесшумной обратной связи об этом известно на передающем конце канала!). Тогда для моментов времени $t > i$ можно в основном проверять только оставшиеся сообщения θ_1 и θ_2 (например, используя для этого противоположные кодовые слова, как при двух сообщениях). Так как $E_2(p) > E_3(p)$ (см. (13)), то такое кодирование позволило бы уменьшить вероятность ошибки декодирования.

Замечание 2. Правая часть формулы (8) имеет следующую полезную интерпретацию (не отмечавшуюся ранее). Пусть $(\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{x}_3)$ – n-симплексный код (т.е. код, в котором $d(\boldsymbol{x}_i, \boldsymbol{x}_j) \approx 2n/3$ для всех $i \neq j$). Тогда справедлива формула (доказательство см. в Приложении)

$$\mathbf{P}\{\mathcal{E}_n\} \sim e^{-F_{\rm fb}(p)n}, \tag{14}$$

где

$$\mathcal{E}_n = \bigl\{\boldsymbol{y}^n : \, p(\boldsymbol{y}^n \,|\, \theta_1) \approx p(\boldsymbol{y}^n \,|\, \theta_2) \approx p(\boldsymbol{y}^n \,|\, \theta_3)\bigr\}. \tag{15}$$

Иными словами, событие $\mathcal{E}_n$ определяет экспоненту вероятности ошибки декодирования.

Замечание 3. С точки зрения поведения функций надежности канал ДСК(p) и гауссовский канал $G(A)$ с ограничением на среднюю мощность A во многом похожи друг на друга [5–7]. Однако эти же каналы с бесшумной обратной связью показывают и существенную разницу. В частности, для ДСК(p) имеем $F_3(p) < E_2(p)$ (см. (13)), в то время как для гауссовского канала $G(A)$ справедливо $F_3(A) = E_2(A)$ (см. [7]). Эта разница обусловлена тем, что для гауссовского канала $G(A)$ в некоторые моменты можно передавать очень мощные сигналы, в то время как для канала ДСК(p) это невозможно.

Следующий результат описывает оптимальный метод передачи в случае трех сообщений.

Теорема 2. *В каждый момент k, $k = 1, \ldots, n$, наилучшее разбиение сообщений $\{\theta_1, \theta_2, \theta_3\}$ (минимизирующее вероятность ошибки декодирования $\mathbf{P}_{\mathrm{e}}(n)$) имеет следующий вид: наиболее вероятное сообщение (при условии выхода $\boldsymbol{y}^{k-1}$) против двух оставшихся сообщений.*

Статья организована следующим образом. В § 2 для полноты приводится короткое и очень изящное доказательство формулы (6) из [1] (по-видимому, это доказательство имеется только в диссертации [1] и не публиковалось в более доступных источниках). В § 3 доказывается теорема 2. В § 4 вводится и описывается марковская диаграмма декодера для оптимальной стратегии передачи. В § 5 с помощью этой диаграммы доказывается теорема 1.

§ 2. Доказательство предложения 1

Через $d(\boldsymbol{y}, \boldsymbol{x})$ будем обозначать расстояние Хэмминга между векторами $\boldsymbol{y}$ и $\boldsymbol{x}$. Для каждого момента k, $k = 1, \ldots, n$, через $\theta^{(1)}(k), \theta^{(2)}(k), \theta^{(3)}(k)$ будем обозначать упорядочение сообщений $\theta_1, \theta_2, \theta_3$ при условии $\boldsymbol{y}^k$, такое что

$$p\bigl(\boldsymbol{y}^k \,|\, \theta^{(1)}(k)\bigr) \geqslant p\bigl(\boldsymbol{y}^k \,|\, \theta^{(2)}(k)\bigr) \geqslant p\bigl(\boldsymbol{y}^k \,|\, \theta^{(3)}(k)\bigr). \tag{16}$$

Через $\boldsymbol{x}^{(1)}(k), \boldsymbol{x}^{(2)}(k), \boldsymbol{x}^{(3)}(k)$ будем обозначать соответствующее упорядочение использованных кодовых блоков. Тогда (16) эквивалентно упорядочению

$$d\bigl(\boldsymbol{y}^k, \boldsymbol{x}^{(1)}(k)\bigr) \leqslant d\bigl(\boldsymbol{y}^k, \boldsymbol{x}^{(2)}(k)\bigr) \leqslant d\bigl(\boldsymbol{y}^k, \boldsymbol{x}^{(3)}(k)\bigr).$$

Будем называть $d^{(i)}(k) = d(\boldsymbol{y}^k, \boldsymbol{x}^{(i)}(k))$ числом “отрицательных голосов” против $\theta^{(i)}(k)$ за время k. Обозначим также $d_i = d_i(n)$.

Обозначим через $d_{1,3}(k)$, $k = 1, \ldots, n$, среднее число “отрицательных голосов” против всех сообщений за время k, т.е.

$$d_{1,3}(k) = \frac{1}{3} \sum_{i=1}^{3} d^{(i)}(k). \tag{17}$$

Используем стратегию, в которой в каждый момент времени k выделяется наиболее вероятное сообщение $\theta^{(1)}(k)$ и передатчик отвечает на вопрос, является ли $\theta^{(1)}(k)$ истинным сообщением θ_{true}. Если $\theta_{\mathrm{true}} = \theta^{(1)}(k)$, то передатчик передает сигнал $x_k = 0$, а если $\theta_{\mathrm{true}} \neq \theta^{(1)}(k)$, то передается сигнал $x_k = 1$.

Тогда если выходной сигнал – это $y_k = 1$, то сообщение $\theta^{(1)}(k)$ получает дополнительно один отрицательный голос, а оставшиеся два сообщения $\{\theta^{(2)}(k), \theta^{(3)}(k)\}$ отрицательных голосов не получают. Если же выходной сигнал – это $y_k = 0$, то сообщение $\theta^{(1)}(k)$ дополнительных отрицательных голосов не получает, а каждое из оставшихся сообщений $\theta^{(2)}(k)$ и $\theta^{(3)}(k)$ получает дополнительно по одному отрицательному голосу. В результате, если $y_k = 1$, то величина $d_{1,3}$ из (17) увеличивается на 1/3. Если же $y_k = 0$, то величина $d_{1,3}$ увеличивается на 2/3. Если за все время n было получено на выходе m нулей и $n - m$ единиц, то $d_{1,3}(n) = (n + m)/3$. Всего имеется $\binom{n}{m}$ возможностей разместить m нулей на n позициях.

Для любого момента k справедливы неравенства

$$d^{(1)}(k) \leqslant d^{(2)}(k) \leqslant d^{(3)}(k) \leqslant d^{(2)}(k) + 1. \tag{18}$$

В (18) следует пояснить только последнее неравенство. Действительно, оно выполняется при $k = 1$ (т.е. после получения выхода y_1). Далее при $k \geqslant 2$ для используемой стратегии сообщения $\theta^{(2)}(k)$ и $\theta^{(3)}(k)$ всегда попадают в одну группу, и поэтому условие $d^{(3)}(k) \leqslant d^{(2)}(k)+1$ сохраняется (хотя сами сообщения $\theta^{(2)}(k)$ и $\theta^{(3)}(k)$ могут меняться).

Из (17) и (18) следует неравенство

$$d^{(2)}(k) \geqslant d_{1,3}(k) - 1/3. \tag{19}$$

Заметим, что каждая реализация выхода $\boldsymbol{y}^n$ с e ошибками имеет вероятность $p^e q^{n-e}$. Так как истинное сообщение получает e отрицательных голосов, то для ошибки декодирования необходимо иметь $d^{(2)}(n) = e$ или $d^{(3)}(n) = e$. В любом случае в силу (19) требуется $e \geqslant d_{1,3}(n) - 1/3$, и поэтому необходимо

$$p^e q^{n-e} \leqslant \left(\frac{q}{p}\right)^{1/3} p^{d_{1,3}(n)} q^{n-d_{1,3}(n)}. \tag{20}$$

Условие (20) ограничивает вероятность любой ошибочной траектории через величину $d_{1,3}(n)$. Заметим, что если m – число нулей, полученных на выходе за все время n, то каждой ошибочной траектории соответствует величина $d_{1,3}(n) = (n+m)/3$, $m = 0, 1, \ldots, n$. Так как всего имеется $\binom{n}{m}$ возможностей разместить m нулей на n позициях, то в силу (20) получаем

$$P_{\mathrm{e}}(3, n, p) \leqslant \left(\frac{q}{p}\right)^{1/3} \sum_{m=0}^{n} \binom{n}{m} p^{(n+m)/3} q^{(2n-m)/3} = \left(\frac{q}{p}\right)^{1/3} \left(p^{1/3}q^{2/3} + p^{2/3}q^{1/3}\right)^n,$$

откуда следует (6). ▲

§ 3. Доказательство теоремы 2

Рассмотрим передачу трех равновероятных сообщений $\{\theta_1, \theta_2, \theta_3\}$. После каждого момента k будем находить апостериорные вероятности сообщений $\pi_i(k)$, $i = 1, 2, 3$, используя принятый блок $\boldsymbol{y}^k = y_1^k = (y_1, \ldots, y_k)$, $k = 1, \ldots, n$. Передача в момент $k + 1$ зависит только от этих апостериорных вероятностей $\{\pi_i(k)\}$ (так как они составляют достаточную статистику). Можно считать, что в момент $k+1$ мы начинаем передачу, но используя априорные вероятности $\{\pi_i(k)\}$.

Обозначим через $d_i(k) = d_i(\boldsymbol{y}^k) = d(\boldsymbol{y}^k, \boldsymbol{x}_i(k))$ общее число “отрицательных голосов” против θ_i за время $[1, k]$. Обозначим также $d_i = d_i(n)$.

Всю информацию, которую имеет декодер в момент k, $k = 1, \ldots, n$, после получения сигнала на выходе $\boldsymbol{y}^k$, составляют апостериорные вероятности $\pi_i(\boldsymbol{y}^k)$ сообщений θ_i, $i = 1, 2, 3$ (или, эквивалентным образом, набор расстояний $d_i(\boldsymbol{y}^k)$, $i = 1, 2, 3$). Обозначим через $i_0(\boldsymbol{y}^k) \in \{1, 2, 3\}$ номер, при котором достигается максимальное значение величины $\pi_i(\boldsymbol{y}^k)$ (или, эквивалентным образом, минимальное значение величины $d_i(\boldsymbol{y}^k)$), т.е.

$$\pi_{i_0(\boldsymbol{y}^k)}(\boldsymbol{y}^k) = \max_i \pi_i(\boldsymbol{y}^k), \quad d_{i_0(\boldsymbol{y}^k)}(\boldsymbol{y}^k) = \min_i d_i(\boldsymbol{y}^k), \quad k = 1, \ldots, n. \tag{21}$$

С точки зрения декодера величина $\pi_i(\boldsymbol{y}^n)$ есть апостериорная вероятность события $\{\theta_i = \theta_{\rm true}\}$. Поэтому наилучшим (с точки зрения вероятности ошибки декодирования) является принятие решения в пользу сообщения $\theta_{i_0(\boldsymbol{y}^n)}$ с максимальной апостериорной вероятностью $\pi_{i_0(\boldsymbol{y}^n)}(\boldsymbol{y}^n)$. Поэтому в силу (21) имеем

$$P_{\rm e}(n) = \mathbf{P}\{\theta_{i_0(\boldsymbol{y}^n)} \neq \theta_{\rm true}\} = 1 - \mathbf{E}\, I_{\{\theta_{i_0(\boldsymbol{y}^n)} = \theta_{\rm true}\}} = 1 - \mathbf{E}\, \pi_{i_0(\boldsymbol{y}^n)}. \tag{22}$$

Через $\mathcal{A}_k \in \{\theta_1, \theta_2, \theta_3\}$, $k = 1, \ldots, n$, будем обозначать сообщение, выделяемое приемником в момент k, относительно которого он задает передатчику вопрос, является ли $\mathcal{A}_k$ истинным сообщением $\theta_{\rm true}$.

Рассмотрим изменение величины $\pi_{i_0(\boldsymbol{y}^k)}$ из (21), (22) в зависимости от выбора сообщения $\mathcal{A}_{k+1}$. Для этого достаточно рассмотреть изменение величины

$$\sum_{j \neq i_0} z^{d_j(k) - d_{i_0}(k)},$$

где $z = p/q$, т.е. изменение величины $1/\pi_{i_0(\boldsymbol{y}^k)}$ (см. формулы (37), (38)).

Возможны два случая:

1) Существует единственный номер $i_0(\boldsymbol{y}^k)$, такой что $d_j(\boldsymbol{y}^k) - d_{i_0(\boldsymbol{y}^k)}(\boldsymbol{y}^k) \geqslant 1$ для всех $j \neq i_0(\boldsymbol{y}^k)$. Тогда $i_0(\boldsymbol{y}^{k+1}) = i_0(\boldsymbol{y}^k)$ для всех y_{k+1}. В этом случае наиболее вероятное сообщение $\theta_{i_0(\boldsymbol{y}^k)}$ в момент k остается наиболее вероятным и в момент $k+1$ для любого выхода y_{k+1}.
2) Есть два различных номера $i_0(\boldsymbol{y}^k)$ и $i_1(\boldsymbol{y}^k)$, таких что $d_{i_0(\boldsymbol{y}^k)}(\boldsymbol{y}^k) = d_{i_1(\boldsymbol{y}^k)}(\boldsymbol{y}^k)$ и $d_j(\boldsymbol{y}^k) - d_{i_0(\boldsymbol{y}^k)}(\boldsymbol{y}^k) \geqslant 1$ для третьего номера.

Ясно, что в третьем возможном случае (когда все расстояния $d_j(\boldsymbol{y}^k)$, $j = 1, 2, 3$, равны) в силу симметрии любой выбор сообщения $\mathcal{A}_{k+1}$ (т.е. любое разбиение сообщений) дает одинаковый результат.

Рассмотрим сначала случай 1). Обозначим для краткости (где $z = p/q$)

$$\begin{aligned}
&a_j = a_j(\boldsymbol{y}^k) = z^{d_j(\boldsymbol{y}^k) - d_{i_0(\boldsymbol{y}^k)}(\boldsymbol{y}^k)},\\
&\delta_j = \delta_j(y_{k+1}) = d_j(y_{k+1}) - d_{i_0(\boldsymbol{y}^k)}(y_{k+1}),\\
&B(k, \boldsymbol{y}^k) = \sum_{j \neq i_0} z^{d_j(\boldsymbol{y}^k) - d_{i_0(\boldsymbol{y}^k)}(\boldsymbol{y}^k)} = \sum_{j \neq i_0} a_j,\\
&B(k+1) = \sum_{j \neq i_0} z^{d_j(\boldsymbol{y}^{k+1}) - d_{i_0(\boldsymbol{y}^{k+1})}(\boldsymbol{y}^{k+1})} = \sum_{j \neq i_0} z^{d_j(\boldsymbol{y}^{k+1}) - d_{i_0(\boldsymbol{y}^k)}(\boldsymbol{y}^{k+1})} =\\
&\ = \sum_{j \neq i_0} a_j z^{\delta_j(y_{k+1})}.
\end{aligned} \tag{23}$$

Обозначим также

$$B_j(k+1) = B(k+1), \quad \text{если } \mathcal{A}_{k+1} = \theta_j, \quad j = 1, 2, 3. \tag{24}$$

Заметим, что величины δ_j, $j = 1, 2, 3$, принимают только значения 0, 1 и -1. Без потери общности можно считать, что $i_0(\boldsymbol{y}^k) = 1$, и поэтому $i_0(\boldsymbol{y}^{k+1}) = 1$. Тогда имеем $\delta_1(y_{k+1}) = 0$ и

$$\begin{aligned} &B(k) = a_2 + a_3, \quad B(k+1) = a_2 z^{\delta_2(y_{k+1})} + a_3 z^{\delta_3(y_{k+1})}, \\ &\pi_1(k) = \frac{1}{1+B(k)}, \quad \pi_1(k+1) = \frac{1}{1+B(k+1)}. \end{aligned} \tag{25}$$

Рассмотрим распределения случайных величин $B_j(k+1)$, $j = 1, 2, 3$, при условии $i_0(\boldsymbol{y}^k) = 1$. Для $j = 1$, т.е. если $\mathcal{A}_{k+1} = \theta_1$, имеем

$$\delta_2 = \delta_3 = \begin{cases} 1 & \text{с вероятностью } \pi_1(k)q + (1-\pi_1(k))p = p + (q-p)\pi_1(k), \\ -1 & \text{с вероятностью } q - (q-p)\pi_1(k), \end{cases} \tag{26}$$

и тогда

$$B_1(k+1) = \begin{cases} (a_2 + a_3)z = B(k)z & \text{с вероятностью } p + (q-p)\pi_1(k), \\ (a_2 + a_3)/z = B(k)/z & \text{с вероятностью } q - (q-p)\pi_1(k). \end{cases} \tag{27}$$

Для $j = 2$, т.е. если $\mathcal{A}_{k+1} = \theta_2$, имеем

$$\delta_3 = 0, \quad \delta_2 = \begin{cases} 1 & \text{с вероятностью } \pi_1(k)q + (1-\pi_1(k))p = p + (q-p)\pi_1(k), \\ -1 & \text{с вероятностью } q - (q-p)\pi_1(k), \end{cases} \tag{28}$$

и поэтому

$$B_2(k+1) = \begin{cases} a_2 z + a_3 & \text{с вероятностью } p + (q-p)\pi_1(k), \\ a_2/z + a_3 & \text{с вероятностью } q - (q-p)\pi_1(k). \end{cases} \tag{29}$$

Аналогично для $j = 3$, т.е. если $\mathcal{A}_{k+1} = \theta_3$, имеем

$$\delta_2 = 0, \quad \delta_3 = \begin{cases} 1 & \text{с вероятностью } p + (q-p)\pi_1(k), \\ -1 & \text{с вероятностью } q - (q-p)\pi_1(k), \end{cases} \tag{30}$$

и поэтому

$$B_3(k+1) = \begin{cases} a_3 z + a_2 & \text{с вероятностью } p + (q-p)\pi_1(k), \\ a_3/z + a_2 & \text{с вероятностью } q - (q-p)\pi_1(k). \end{cases} \tag{31}$$

В результате при $i_0(\boldsymbol{y}^k) = 1$ имеем

$$\begin{aligned} E_1 &= \mathbf{E}\big[\pi_{i_0}(k+1) \,|\, \boldsymbol{y}^k, \mathcal{A}_{k+1} = \theta_1\big] = \mathbf{E}\left[\frac{1}{1+B_1(k+1)} \;\Big|\; \boldsymbol{y}^k, \mathcal{A}_{k+1} = \theta_1\right] = \\ &= \frac{p + (q-p)\pi_1(k)}{1 + (a_2+a_3)z} + \frac{q - (q-p)\pi_1(k)}{1 + (a_2+a_3)/z}. \end{aligned} \tag{32}$$

Аналогично имеем

$$\begin{aligned} E_2 &= \mathbf{E}\big[\pi_{i_0}(k+1) \,|\, \boldsymbol{y}^k, \mathcal{A}_{k+1} = \theta_2\big] = \mathbf{E}\left[\frac{1}{1+B_2(k+1)} \;\Big|\; \boldsymbol{y}^k, \mathcal{A}_{k+1} = \theta_2\right] = \\ &= \frac{p + (q-p)\pi_1(k)}{1 + a_2 z + a_3} + \frac{q - (q-p)\pi_1(k)}{1 + a_2/z + a_3} \end{aligned} \tag{33}$$

и

$$E_3 = \mathbf{E}\big[\pi_{i_0}(k+1) \,|\, \boldsymbol{y}^k, \mathcal{A}_{k+1} = \theta_3\big] = \mathbf{E}\left[\frac{1}{1+B_3(k+1)} \,\Big|\, \boldsymbol{y}^k, \mathcal{A}_{k+1} = \theta_3\right] =$$
$$= \frac{p+(q-p)\pi_1(k)}{1+a_2+a_3z} + \frac{q-(q-p)\pi_1(k)}{1+a_2+a_3/z}. \tag{34}$$

Покажем, что $E_1 \geqslant \max\{E_2, E_3\}$, т.е. что наилучшим является использование $\mathcal{A}_{k+1} = \theta_1 = \theta_{i_0(\boldsymbol{y}^k)}$. В силу симметрии достаточно показать, что $E_1 \geqslant E_2$. Действительно, в силу (32) и (33) имеем

$$E_1 - E_2 = [p+(q-p)\pi_1(k)]\left[\frac{1}{1+(a_2+a_3)z} - \frac{1}{1+a_2z+a_3}\right] +$$
$$+ [q-(q-p)\pi_1(k)]\left[\frac{1}{1+(a_2+a_3)/z} - \frac{1}{1+a_2/z+a_3}\right] =$$
$$= \frac{[p+(q-p)\pi_1(k)]a_3(1-z)}{[1+(a_2+a_3)z][1+a_2z+a_3]} + \frac{[q-(q-p)\pi_1(k)]a_3(1-1/z)}{[1+(a_2+a_3)/z][1+a_2/z+a_3]} =$$
$$= a_3(1-z)\left\{\frac{p+(q-p)\pi_1(k)}{[1+(a_2+a_3)z][1+a_2z+a_3]} - \right.$$
$$\left. - \frac{q-(q-p)\pi_1(k)}{z[1+(a_2+a_3)/z][1+a_2/z+a_3]}\right\} = qa_3(1-z) \times$$
$$\times \left\{\frac{z+(1-z)\pi_1(k)}{[1+(a_2+a_3)z](1+a_2z+a_3)} - \frac{1-(1-z)\pi_1(k)}{(z+a_2+a_3)(1+a_2/z+a_3)}\right\}. \tag{35}$$

Достаточно показать, что

$$\frac{z+(1-z)\pi_1(k)}{[1+(a_2+a_3)z](1+a_2z+a_3)} - \frac{1-(1-z)\pi_1(k)}{(z+a_2+a_3)(1+a_2/z+a_3)} \geqslant 0,$$

или, эквивалентным образом (после стандартных преобразований с использованием формулы $\pi_1(k) = 1/(1+a_2+a_3)$),

$$a_2(1-z) \geqslant 0. \tag{36}$$

Формула (36) справедлива, если $z \leqslant 1$ (т.е. если $p \leqslant 1/2$). В силу (35) и (36) получаем $E_1 \geqslant E_2$. Аналогично получаем $E_1 \geqslant E_3$. Поэтому $E_1 \geqslant \max\{E_2, E_3\}$, а это значит, что наилучшим является использование $\mathcal{A}_{k+1} = \theta_1 = \theta_{i_0(\boldsymbol{y}^k)}$. Это завершает рассмотрение случая 1).

Рассмотрим теперь случай 2), когда есть два различных номера $i_0(\boldsymbol{y}^k)$ и $i_1(\boldsymbol{y}^k)$, таких что $d_{i_0(\boldsymbol{y}^k)}(\boldsymbol{y}^k) = d_{i_1(\boldsymbol{y}^k)}(\boldsymbol{y}^k)$ и $d_j(\boldsymbol{y}^k) - d_{i_0(\boldsymbol{y}^k)}(\boldsymbol{y}^k) \geqslant 1$ для третьего номера. Без ограничения общности можно считать, что $i_0(\boldsymbol{y}^k) = 1$ и $i_1(\boldsymbol{y}^k) = 3$. Тогда $E_1 = E_3$, и остается показать, что $E_1 \geqslant E_2$, и тогда наилучшим является использование $\mathcal{A}_{k+1} = \theta_1 = \theta_{i_0(\boldsymbol{y}^k)}$ (или $\mathcal{A}_{k+1} = \theta_3 = \theta_{i_1(\boldsymbol{y}^k)}$). Заметим, что для любого y_{k+1} одно из расстояний $d_{i_0(\boldsymbol{y}^{k+1})}(\boldsymbol{y}^{k+1})$ или $d_{i_1(\boldsymbol{y}^{k+1})}(\boldsymbol{y}^{k+1})$ остается таким же, как и ранее в момент k. Оставшиеся вычисления по существу совпадают с (23)–(36) (в действительности они даже проще), и мы их опускаем. Это завершает доказательство теоремы 2. ▲

§ 4. Марковская диаграмма декодера для оптимальной стратегии

Введем марковскую диаграмму, описывающую эволюцию декодера во времени. Обозначим через $d_i(k) = d(\boldsymbol{y}^k, \boldsymbol{x}_i(k))$ общее число “отрицательных голосов” против θ_i

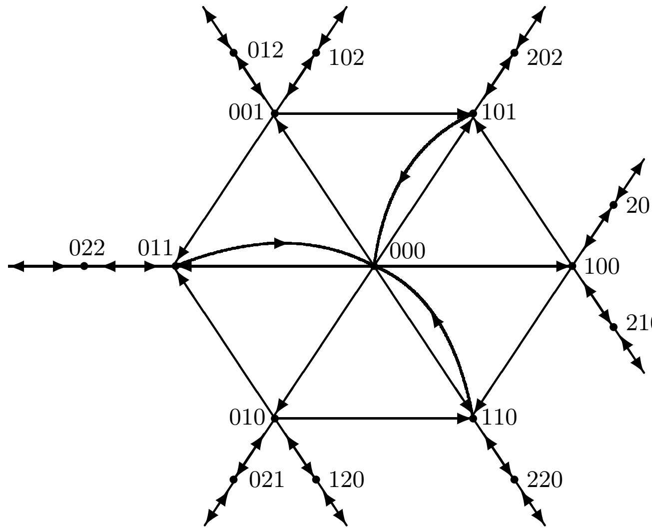

Рис. 1. Марковская диаграмма декодера

за время $[1, k]$. Обозначим также $d_i = d_i(n)$. Тогда ($z = p/q < 1$)

$$\pi_i(k) = \frac{z^{d_i(k)}}{\sum\limits_{j=1}^{3} z^{d_j(k)}} = \frac{1}{1 + \sum\limits_{j \neq i} z^{d_j(k) - d_i(k)}}, \quad \pi_i(n) = \frac{1}{1 + \sum\limits_{j \neq i} z^{d_j(n) - d_i(n)}}. \tag{37}$$

Заметим, что

$$\frac{\pi_i(k)}{1 - \pi_i(k)} = \frac{z^{d_i(k)}}{\sum\limits_{j \neq i} z^{d_j(k)}} = \frac{1}{\sum\limits_{j \neq i} z^{d_j(k) - d_i(k)}}. \tag{38}$$

Для каждого момента k и каждого сигнала на выходе $\boldsymbol{y}^k$ определим для сообщения θ_i метрику $m_i(k, \boldsymbol{y}^k)$ следующим образом:

$$m_i(k, \boldsymbol{y}^k) = d\big(\boldsymbol{y}^k, \boldsymbol{x}_i(k)\big) - \min_j d\big(\boldsymbol{y}^k, \boldsymbol{x}_j(k)\big) = d_i(k) - \min_j d_j(k), \quad i = 1, 2, 3. \tag{39}$$

Ясно, что $m_i(k, \boldsymbol{y}^k) \geqslant 0$ и $\min\limits_i m_i(k, \boldsymbol{y}^k) = 0$. Набор $\{m_i(k, \boldsymbol{y}^k)\}$ является достаточной статистикой, поскольку он определяет апостериорные вероятности $\{\pi_i(k)\}$ (см. (37)–(39)).

Обозначим через $S_{ij\ell} = S_{ijl}(k) = S_{ijl}(k, \boldsymbol{y}^k)$ состояние диаграммы с $i = m_1(k, \boldsymbol{y}^k)$, $j = m_2(k, \boldsymbol{y}^k)$, $\ell = m_3(k, \boldsymbol{y}^k)$.

В результате вся диаграмма выглядит как "осьминог" с девятью "щупальцами" (см. рис. 1). Например, одним из этих "щупалец" является $(S_{011}, S_{022}, S_{033}, \ldots)$.

Будем называть S_{000} *главным* состоянием, а шесть состояний $\{S_{011}, S_{100}, S_{101}, S_{010}, S_{110}, S_{001}\}$ – *основными* состояниями. Оставшиеся состояния расположены на "щупальцах".

Тогда для вероятности ошибки декодирования $P_{\mathrm{e}}(n)$ имеем

$$P_{\mathrm{e}}(n) \geqslant \frac{2}{3} P_0(n), \tag{40}$$

где

$$P_0(n) = P\{S_{000}(0) \Rightarrow S_{000}(n)\}. \tag{41}$$

Опишем переходы между состояниями для оптимальной стратегии. Без ограничения общности можно считать, что $\theta_{\text{true}} = \theta_1$.

Если в момент k декодер находится в состоянии $S_{000}(k)$, то в этом случае множество $\mathcal{A}(k+1)$ выбирается равновероятно между тремя возможными вариантами. В результате для следующего возможного состояния $S(k+1)$ получаем

$$S_{000}(k) \to \begin{cases} S_{011}(k+1) & \text{с вероятностью } q/3, \\ S_{100}(k+1) & \text{с вероятностью } p/3, \\ S_{101}(k+1) & \text{с вероятностью } p/3, \\ S_{010}(k+1) & \text{с вероятностью } q/3, \\ S_{110}(k+1) & \text{с вероятностью } p/3, \\ S_{001}(k+1) & \text{с вероятностью } q/3. \end{cases} \tag{42}$$

Действительно, в момент k каждое сообщение θ_i имеет вероятность $\pi_i(k) = 1/3$, $i = 1, 2, 3$. Поэтому с вероятностью $1/3$ имеем $\mathcal{A}(k+1) = \theta_1$. Так как мы предположили, что $\theta_{\text{true}} = \theta_1$, то с вероятностью $q/3$ получаем $S(k+1) = S_{011}(k+1)$, а с вероятностью $p/3$ получаем $S(k+1) = S_{100}(k+1)$. Аналогично получаются остальные строки в (42).

Проще всего описываются переходы из тех состояний, для которых множество $\mathcal{A}(k+1)$ определяется однозначно, без рандомизации (т.е. когда есть только одно наиболее вероятное сообщение). Это состояния $S_{011}(k), S_{101}(k), S_{110}(k), \ldots$ Для таких состояний получаем

$$S_{011}(k) \to \begin{cases} S_{000}(k+1) & \text{с вероятностью } p, \\ S_{022}(k+1) & \text{с вероятностью } q, \end{cases} \tag{43}$$

$$S_{101}(k) \to \begin{cases} S_{000}(k+1) & \text{с вероятностью } q, \\ S_{202}(k+1) & \text{с вероятностью } p \end{cases} \tag{44}$$

$$S_{110}(k) \to \begin{cases} S_{000}(k+1) & \text{с вероятностью } q, \\ S_{220}(k+1) & \text{с вероятностью } p. \end{cases} \tag{45}$$

Аналогично описываются переходы из подобных же состояний $S_{022}(k), S_{202}(k), S_{220}(k), \ldots$ Переходы из оставшихся состояний $S_{100}(k), S_{010}(k), S_{001}(k)$ описываются аналогично (42):

$$S_{100}(k) \to \begin{cases} S_{101}(k+1) & \text{с вероятностью } q/2, \\ S_{210}(k+1) & \text{с вероятностью } p/2, \\ S_{110}(k+1) & \text{с вероятностью } q/2, \\ S_{201}(k+1) & \text{с вероятностью } p/2, \end{cases} \tag{46}$$

$$S_{010}(k) \to \begin{cases} S_{021}(k+1) & \text{с вероятностью } q/2, \\ S_{110}(k+1) & \text{с вероятностью } p/2, \\ S_{120}(k+1) & \text{с вероятностью } p/2, \\ S_{011}(k+1) & \text{с вероятностью } q/2, \end{cases} \tag{47}$$

$$S_{001}(k) \to \begin{cases} S_{012}(k+1) & \text{с вероятностью } q/2, \\ S_{101}(k+1) & \text{с вероятностью } p/2, \\ S_{102}(k+1) & \text{с вероятностью } p/2, \\ S_{011}(k+1) & \text{с вероятностью } q/2. \end{cases} \tag{48}$$

§ 5. Доказательство теоремы 1

В силу (40), (41) достаточно оценить величину $P_0(n) = P\{S_{000}(0) \Rightarrow S_{000}(n)\}$ снизу. Ясно, что

$$P_0(n) = \sum_{t_n} \mathbf{P}\{t_n\}, \tag{49}$$

где сумма берется по всем путям t_n длины n вида $S_{000}(0) \Rightarrow S_{000}(n)$.

Будем называть 3-путем любой путь длины 3 вида $S_{000}(k) \Rightarrow S_{000}(k+3)$. Будем также называть 2-путем любой путь длины 2 вида $S_{000}(k) \Rightarrow S_{000}(k+2)$.

Ограничимся сначала в сумме в правой части (49) путями t_n, проходящими только через главное и основные состояния (т.е. не выходящие на щупальца). Тогда нетрудно видеть, что любой такой путь t_n состоит из 3-путей и 2-путей.

Всего имеется шесть 3-путей:

$$\begin{aligned}
&S_{000} \to S_{100} \to S_{101} \to S_{000} \quad \text{с вероятностью } pq^2/6, \\
&S_{000} \to S_{100} \to S_{110} \to S_{000} \quad \text{с вероятностью } pq^2/6, \\
&S_{000} \to S_{010} \to S_{011} \to S_{000} \quad \text{с вероятностью } pq^2/6, \\
&S_{000} \to S_{010} \to S_{110} \to S_{000} \quad \text{с вероятностью } pq^2/6, \\
&S_{000} \to S_{001} \to S_{101} \to S_{000} \quad \text{с вероятностью } pq^2/6, \\
&S_{000} \to S_{001} \to S_{011} \to S_{000} \quad \text{с вероятностью } pq^2/6.
\end{aligned}$$

Поэтому

$$P\{S_{000}(k) \to S_{000}(k+3)\} = pq^2. \tag{50}$$

Всего имеется три 2-пути:

$$\begin{aligned}
&S_{000} \to S_{011} \to S_{000} \quad \text{с вероятностью } qp/3, \\
&S_{000} \to S_{101} \to S_{000} \quad \text{с вероятностью } qp/3, \\
&S_{000} \to S_{110} \to S_{000} \quad \text{с вероятностью } qp/3.
\end{aligned} \tag{51}$$

Поэтому

$$P\{S_{000}(k) \to S_{000}(k+2)\} = pq. \tag{52}$$

Оценим теперь величину $P_0(n)$ из (49), используя (50)–(52). Любой путь t_n, ограниченный основными состояниями, состоит из некоторого числа 2-путей n_2 и некоторого числа 3-путей n_3. При этом $2n_2 + 3n_3 = n$, $0 \leqslant n_2 \leqslant n/2$, а общее число путей равно

$$m = n_2 + n_3 = \frac{n + n_2}{3}.$$

Имеется $\binom{m}{n_2}$ способов разместить n_2 2-путей. Оставшиеся $m-n_2$ мест занимают n_3 3-путей. Поэтому имеем ($z = p/q$)

$$P_0(n) = \sum_{n_2=0}^{n/2} \binom{(n+n_2)/3}{n_2} (pq)^{n_2} (pq^2)^{n_3} =$$

$$= \sum_{n_2=0}^{n/2} \binom{(n+n_2)/3}{n_2} (pq)^{n_2} (pq^2)^{(n-2n_2)/3} = (pq^2)^{n/3} \sum_{n_2=0}^{n/2} \binom{(n+n_2)/3}{n_2} z^{n_2/3}. \quad (53)$$

Оценим снизу сумму в правой части (53). Максимум величины $\binom{(n+n_2)/3}{n_2} z^{n_2/3}$ по n_2 достигается при $n_2 = a_0 n$, где величина a_0 будет найдена далее. Тогда

$$\sum_{n_2=0}^{n/2} \binom{(n+n_2)/3}{n_2} z^{n_2/3} \geqslant \binom{n(1+a_0)/3}{a_0 n} z^{a_0 n/3} \geqslant$$

$$\geqslant \frac{1}{n} \sum_{n_2=0}^{n(1+a_0)/3} \binom{n(1+a_0)/3}{n_2} z^{n_2/3} = \frac{1}{n}(1+z^{1/3})^{n(1+a_0)/3}. \quad (54)$$

Для аккуратности оценим также сверху сумму в правой части (53). Имеем

$$\sum_{n_2=0}^{n} \binom{(n+n_2)/3}{n_2} z^{n_2/3} \leqslant n \binom{n(1+a_0)/3}{a_0 n} z^{a_0 n/3} \leqslant$$

$$\leqslant n \sum_{n_2=0}^{n(1+a_0)/3} \binom{n(1+a_0)/3}{n_2} z^{n_2/3} = n(1+z^{1/3})^{n(1+a_0)/3}.$$

В результате из (53) и (54) получаем

$$P_0(n) \geqslant \frac{1}{n}(pq^2)^{n/3}(1+z^{1/3})^{n(1+a_0)/3}. \quad (55)$$

Найдем теперь величину a_0 в (54), (55). Так как

$$\ln \binom{(n+n_2)/3}{n_2} \approx \frac{(n+n_2)}{3} h\left(\frac{3n_2}{n+n_2}\right),$$

то обозначая $n_2 = an$, $0 \leqslant a \leqslant 1/2$, введем функцию

$$f_1(p,a) = (1+a)h\left(\frac{3a}{1+a}\right) - a\ln(q/p), \quad 0 \leqslant a \leqslant 1/2.$$

Величина a_0 максимизирует функцию $f_1(p,a)$ по $0 \leqslant a \leqslant 1/2$. Заметим, что

$$f_1(p,a) = (1+a)\ln(1+a) - 3a\ln(3a) - (1-2a)\ln(1-2a) - a\ln(q/p),$$

$$(f_1(p,a))'_a = \ln\frac{p(1+a)(1-2a)^2}{27qa^3}, \quad (f_1(p,a))''_{aa} < 0,$$

$$(f_1(p,a))'_{a=0} = \infty, \quad (f_1(p,a))'_{a=1/2} = -\infty.$$

Поэтому $a_0(p)$ является единственным корнем уравнения

$$27qa^3 - p(1+a)(1-2a)^2 = 0 = (27-31p)a^3 + 3pa - p.$$

Для этого корня имеем [8, п. 1.8-3]

$$a_0(p) = \left[\frac{p}{2(27-31p)}\right]^{1/3} \left\{ \left[1 + \sqrt{\frac{27(1-p)}{27-31p}}\right]^{1/3} + \left[1 - \sqrt{\frac{27(1-p)}{27-31p}}\right]^{1/3} \right\}.$$

При малых p имеем $3a_0(p) \approx p^{1/3}$. Так как $a_0 < 2$, то оценка (55) уступает оценке сверху (6)–(8) для $P_{\mathrm{e}}(3,n,p)$. Однако оценка (55) показывает, что при исследовании величины $P_0(n)$ нельзя ограничиваться только основными состояниями, а следует учитывать также и состояния на щупальцах.

Усилим теперь оценку (55), принимая во внимание также и состояния на щупальцах. Будем называть 2-петлей любой путь длины 2 с одинаковыми начальным и конечным состояниями (не обязательно состояниями S_{000}). Помимо 2-путей из (51) примерами 2-петель являются также

$$\begin{aligned}
&S_{011} \to S_{022} \to S_{011} && \text{с вероятностью } qp,\\
&S_{100} \to S_{201} \to S_{100} && \text{с вероятностью } qp/2,\\
&S_{100} \to S_{210} \to S_{100} && \text{с вероятностью } qp/2,\\
&S_{101} \to S_{202} \to S_{101} && \text{с вероятностью } qp, \quad \ldots
\end{aligned}$$

Такие 2-петли выходят на щупальца.

Рассмотрим пути t_n, состоящие из некоторого числа 3-путей n_3 и некоторого числа 2-петель k_2. Пусть мы разместили n_3 3-путей на $[1,n]$. После этого вставим k_2 2-петель в любые различные k_2 моментов на $[1,n]$. Если такая 2-петля попадает на начальное состояние 3-пути, то этот 3-путь просто полностью сдвигается вправо на два шага. Если такая 2-петля попадает на внутреннее состояние 3-пути, то часть этого 3-пути сдвигается вправо на два шага, чтобы вместить эту 2-петлю. Аналогичным образом 2-петли можно также вставлять в другие 2-петли.

Так как необходимо, чтобы $n = 3n_3 + 2k_2$, то

$$P_0(n) \geqslant \sum_{k_2=0}^{n/2} \binom{n}{k_2} (pq)^{k_2} (pq^2)^{n_3} = \sum_{k_2=0}^{n/2} \binom{n}{k_2} (pq)^{k_2} (pq^2)^{(n-2k_2)/3} =$$
$$= (pq^2)^{n/3} \sum_{k_2=0}^{n/2} \binom{n}{k_2} z^{k_2/3}. \tag{56}$$

Заметим, что

$$\binom{n}{k_2} z^{k_2/3} + \binom{n}{n-k_2} z^{(n-k_2)/3} \leqslant 2\binom{n}{k_2} z^{k_2/3}, \quad k_2 \leqslant n/2, \quad z < 1.$$

Тогда (56) можно продолжить следующим образом:

$$P_0(n) \geqslant \frac{1}{2}(pq^2)^{n/3} \sum_{k_2=0}^{n} \binom{n}{k_2} z^{k_2/3} = \frac{1}{2}(pq^2)^{n/3}(1+z^{1/3})^n. \tag{57}$$

Поэтому из (57), (40) и (41) получаем

$$P_{\mathrm{e}}(n) \geqslant \frac{2}{3} P_0(n) \geqslant \frac{1}{3}(pq^2)^{n/3}(1+z^{1/3})^n. \tag{58}$$

Из (58) следует (8) и теорема 1 (формулы (11), (12)). ▲

Доказательство формулы (14). Рассмотрим n-симплексный код вида $(\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{x}_3)$, где $\boldsymbol{x}_1$ имеет вначале $n/3$ единиц и затем $2n/3$ нулей, $\boldsymbol{x}_2$ имеет вначале $n/3$ нулей, затем $n/3$ единиц и потом $n/3$ нулей, а $\boldsymbol{x}_3$ имеет вначале $2n/3$ нулей и затем $n/3$ единиц. Тогда $w(\boldsymbol{x}_1) = w(\boldsymbol{x}_2) = w(\boldsymbol{x}_3) = n/3$ и $d_{12} = d_{13} = d_{23} = 2n/3$.

Пусть выход $\boldsymbol{y}$ имеет $u_1 n/3$ единиц на первых $n/3$ позициях, $u_2 n/3$ единиц на следующих $n/3$ позициях и $u_3 n/3$ единиц на последних $n/3$ позициях. Тогда

$$\begin{aligned}
&d(\boldsymbol{x}_1, \boldsymbol{y})/n = (1 - u_1 + u_2 + u_3)/3,\\
&d(\boldsymbol{x}_2, \boldsymbol{y})/n = (1 + u_1 - u_2 + u_3)/3,\\
&d(\boldsymbol{x}_3, \boldsymbol{y})/n = (1 + u_1 + u_2 - u_3)/3.
\end{aligned}$$

Так как $d(\boldsymbol{x}_1, \boldsymbol{y}) = d(\boldsymbol{x}_2, \boldsymbol{y}) = d(\boldsymbol{x}_3, \boldsymbol{y})$, то получаем $u_1 = u_2 = u_3$ и

$$p(\boldsymbol{y}^n \,|\, \boldsymbol{x}_1) = p^{d(\boldsymbol{x}_1, \boldsymbol{y})} q^{n - d(\boldsymbol{x}_1, \boldsymbol{y})} = q^n z^{d(\boldsymbol{x}_1, \boldsymbol{y})} = q^n z^{(1+u)n/3}, \quad z = p/q < 1.$$

Поэтому

$$\begin{aligned}
&\mathbf{P}\bigl\{p(\boldsymbol{y}^n \,|\, \boldsymbol{x}_1) \approx p(\boldsymbol{y}^n \,|\, \boldsymbol{x}_2) \approx p(\boldsymbol{y}^n \,|\, \boldsymbol{x}_3)\bigr\} \sim \max_{0 \leqslant u \leqslant 1} \mathbf{P}\bigl\{p(\boldsymbol{y}^n \,|\, \boldsymbol{x}_1) \approx q^n z^{(1+u)n/3}\bigr\} \sim \\
&\sim \max_{0 \leqslant u \leqslant 1} \left\{ \binom{n}{un} p^{(1+u)n/3} q^{(2-u)n/3} \right\} \sim q^n \max_{0 \leqslant u \leqslant 1} \left\{ \binom{n}{un} z^{(1+u)n/3} \right\},
\end{aligned}$$

и

$$\frac{1}{n} \max_{0 \leqslant u \leqslant 1} \ln \mathbf{P}\{p(\boldsymbol{y}^n \,|\, \boldsymbol{x}_1)\} = \ln q + \max_{0 \leqslant u \leqslant 1} g(u), \tag{59}$$

где

$$g(u) = h(u) + (1+u)\ln(z^{1/3}), \quad g'(u) = \ln\frac{1-u}{u} + \ln(z^{1/3}), \quad g''(u) < 0.$$

Для максимизирующего u_0 получаем

$$u_0 = \frac{1}{1 + z^{-1/3}} = \frac{p^{1/3}}{p^{1/3} + q^{1/3}},$$

и после несложных преобразований

$$\ln q + g(u_0) = \ln\bigl(p^{1/3} q^{2/3} + p^{2/3} q^{1/3}\bigr). \tag{60}$$

Из (59) и (60) следуют формулы (14) и (15). ▲

Автор благодарит Л.А. Бассалыго и Г.А. Кабатянского за полезные обсуждения и конструктивные критические замечания, улучшившие статью.

СПИСОК ЛИТЕРАТУРЫ

1. *Berlekamp E.R.* Block Coding with Noiseless Feedback. PhD Thesis. MIT, Cambridge, USA, 1964. Available at `http://hdl.handle.net/1721.1/14783`.
2. *Зигангиров К.Ш.* Верхние оценки вероятности ошибки для каналов с обратной связью // Пробл. передачи информ. 1970. Т. 6. № 2. С. 87–92. `http://mi.mathnet.ru/ppi1740`
3. *Бурнашев М.В.* О функции надежности двоичного симметричного канала с обратной связью // Пробл. передачи информ. 1988. Т. 24. № 1. С. 3–10. `http://mi.mathnet.ru/ppi681`

4. *Зигангиров К.Ш.* Оптимальная передача сообщений по двоичному симетричному каналу с обратной связью при нулевой скорости // Probl. Control Inform. Theory. 1978. V. 7. № 3. P. 183–198.
5. *Shannon C.E.* Probability of Error for Optimal Codes in a Gaussian Channel // Bell Syst. Tech. J. 1959. V. 38. № 3. P. 611–656. https://doi.org/10.1002/j.1538-7305.1959.tb03905.x
6. *Галлагер Р.* Теория информации и надежная связь. М.: Сов. радио, 1974.
7. *Пинскер М.С.* Вероятность ошибки при блоковой передаче по гауссовскому каналу без памяти с обратной связью // Пробл. передачи информ. 1968. Т. 4. № 4. С. 3–19. http://mi.mathnet.ru/ppi1868
8. *Корн Г., Корн Т.* Справочник по математике для научных работников и инженеров. М.: Наука, 1974.

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

Поступила в редакцию
07.05.2022
После доработки
14.06.2022
Принята к публикации
21.06.2022