Math-Net.Ru
All Russian mathematical portal

V. A. Ivanov, On artificial noising of data transmission channels,
Tr. Diskr. Mat., 2004, Volume 8, 99–115

https://www.mathnet.ru/eng/tdm123

Use of the all-Russian mathematical portal Math-Net.Ru implies that you have read and agreed to these terms of use
https://www.mathnet.ru/eng/agreement

Download details:
IP: 18.97.14.83
December 10, 2025, 11:53:42

Труды по дискретной математике
Том 8, с. 99–115
М.: ФИЗМАТЛИТ, 2004

ОБ ИСКУССТВЕННОМ ЗАШУМЛЕНИИ КАНАЛОВ ПЕРЕДАЧИ ДАННЫХ

В. А. ИВАНОВ

Изучается применение случайных кодов для повышения защиты информации от утечки в каналах передачи данных.

§ 1. ВВЕДЕНИЕ

В работе [1] исследовались алгоритмы случайного кодирования, предназначаемые для защиты информации от утечки в побочных каналах связи. При этом в рассмотренных случаях асимптотические оценки минимальных объемов выборки, необходимых для различения любых двух сигналов на фоне достаточно интенсивного шума, совпадали между собой. Однако такая ситуация не является типичной для общего случая. Асимптотические оценки минимальных объемов выборки для различения некоторых пар сигналов могут существенно отличаться друг от друга. Рассмотрению одного из таких случаев посвящена настоящая работа. В ней исследуются вероятностные характеристики алгоритма кодового зашумления, основанного на случайной перестановке координат сообщения, представленного в виде двоичного вектора.

§ 2. ОПИСАНИЕ СПОСОБА СЛУЧАЙНОЙ ПЕРЕСТАНОВКИ КООРДИНАТ СООБЩЕНИЯ

Рассмотрим конечное пространство элементарных исходов $\Omega = \{\omega\}$, на котором задана вероятностная мера $\mu(\omega)$ и множество сообщений $S = \{s\}$, подлежащих передаче по каналу связи. Далее будем считать, что $s = (s_1, \dots, s_k) \in \mathbf{S} = \mathbf{B}^k$, $s_j \in \mathbf{B} = \{0, 1\}$, $j \in \mathbf{K} = \{1, \dots, k\}$, $k = 2^\nu$, $\nu = 1, 2, \dots$, и что каждому натуральному числу $j \in \mathbf{K}$ сопоставлен вектор

© В. А. Иванов, 2004

$\mathbf{j} = \mathbf{j}(j) = (j_1, \dots, j_\nu)$, а каждому вектору $\mathbf{j} = (j_1, \dots, j_\nu) \in \mathbf{B}^\nu$ сопоставлено такое натуральное число $j = j(\mathbf{j})$, что выполняется равенство

$$j = j(\mathbf{j}) = 1 + j_1 + 2j_2 + \dots + 2^{\nu-1} j_\nu.$$

Вектор $\mathbf{j} = (j_1, \dots, j_\nu) \in \mathbf{B}^\nu$ далее будем отождествлять с числом $j = 1 + j_1 + 2j_2 + \dots + 2^{\nu-1} j_\nu$ и обозначать одним и тем же символом j, понимая под этим в зависимости от контекста число j или вектор $\mathbf{j}$.

Заметим, что по каждому вектору $s \in \mathbf{B}^k$, $k = 2^\nu$, можно однозначно определить булеву функцию $s(j)$ от ν аргументов, если положить $s(j) = s_j$, $j \in \mathbf{B}^\nu$, а по булевой функции $s(j)$ можно однозначно восстановить вектор $s \in \mathbf{B}^k$, если значения функции $s(j)$ записать в порядке возрастания аргументов $j = 1, \dots, 2^\nu$.

Под случайным кодированием будем понимать случайное преобразование вектора $s \in \mathbf{B}^k$ длины k в вектор $\xi(s) = \psi(s, \omega) \in \mathbf{B}^m$ длины m, $m \geqslant k$, с помощью функции ψ, отображающей множество $\mathbf{B}^k \times \Omega$ в множество $\mathbf{B}^m$, для которой выполняются соотношения $\psi_s(\Omega) \cap \psi_g(\Omega) = \varnothing$ при $s \neq g$, где $\psi_s(\Omega) = \{\psi(s, \omega),\ \omega \in \Omega\}$. Эти условия позволяют однозначно определить сообщение s по любой реализации $\xi(s) = \psi(s, \omega)$ и, тем самым, обеспечить достоверное декодирование сигналов на выходе абсолютно надежного канала связи.

Далее будем изучать модель, в которой сообщение s в моменты времени $t = 1, 2, \dots, n$ передается одновременно по двум каналам связи, один из которых работает без ошибок и называется основным, а второй работает как двоичный симметричный канал связи (ДСК) с заданным уровнем ошибок и называется дополнительным или побочным каналом утечки информации. Дополнительный канал связи характеризуется наложением на передаваемый в момент времени t сигнал $\xi_t(s) = \psi(s, \omega_t)$ независимой аддитивной помехи в виде вектора $\varkappa_1 = (\varkappa_{t1}, \dots, \varkappa_{tm})$ с независимыми координатами, распределенными по закону

$$\mathbf{P}(\varkappa_{ti} = \pi) = \frac{1}{2}(1 + (-1)^\pi \delta), \qquad \pi \in \mathbf{B}, \qquad 0 \leqslant \delta \leqslant 1,$$

$i = 1, \dots, m$, $t = 1, 2, \dots$ Таким образом, на выходе дополнительного канала наблюдается сигнал $Z_t = Z_t(s) = \xi_t(s) \oplus \varkappa_t \in \mathbf{B}^m$, где символом $\oplus$ обозначена операция покомпонентного сложения векторов по модулю два.

Рассмотрим в качестве пространства элементарных исходов $\Omega = \{\omega\}$ группу всех подстановок, заданных на множестве $\mathbf{K} = \mathbf{B}^\nu$. Произвольную подстановку ω можно задать с помощью перестановки координат $\omega = (\omega(1), \dots, \omega(k))$, $\omega(i) \neq \omega(j)$, $i \neq j$, $\omega(i), \omega(j), i, j \in \mathbf{K}$, вектора $\omega^* = (1, \dots, k)$, полагая, что координата $j \in \mathbf{K}$ заменяется на координату $\omega(j) \in \mathbf{K}$ множества $\mathbf{K}$:

$$\omega = \begin{pmatrix} 1 & \dots & k \\ \omega(1) & \dots & \omega(k) \end{pmatrix}.$$

Образ вектора $j = (j_1, \dots, j_\nu)$ при применении подстановки ω и соответствующую ему координату в перестановке ω будем обозначать одним и тем же символом $\omega(j)$.

Рассмотрим способ кодового зашумления, состоящий в последовательной передаче по одному и тому же каналу связи случайно выбранных координат сообщения и их номеров. Заметим, что в этом случае для практической реализации метода не потребуется дополнительной памяти, поскольку для этого можно использовать уже имеющуюся память, а считывание координат сообщения на передающем устройстве и их запись на приемном устройстве производить в случайном порядке в соответствии с последовательностью, вырабатываемой генератором случайных подстановок. Таким образом, для передачи сообщения s используется случайный вектор $\psi(s, \omega) = (\omega s, \omega)$, где $\omega = (\omega(1), \dots, \omega(k)) \in \mathbf{B}^{k\nu}$ и $\omega s = (s(\omega(1)), \dots, s(\omega(k))) \in \mathbf{B}^k$. Здесь координаты $(\omega s)_j = s(\omega(j))$ вектора ωs записаны через значения функции $s(j) = s_j$.

Изучим ситуацию, в которой одно и то же сообщение, выбранное из множества $\mathbf{B}^k$ мощности $M = 2^k$, $k = 2^\nu$, многократно передается по каналу связи. Пусть сообщение s перед подачей на вход канала связи в моменты времени $t = 1, 2, \dots, N$ преобразуется в сигналы $\psi(s, \omega_t) = (\omega_t s, \omega_t) \in \mathbf{B}^m$, $m = (\nu + 1)2^\nu$, случайно выбираемые из множества $\mathbf{B}^m$ мощности 2^m. Необходимое для однозначного декодирования на выходе основного канала связи условие $\psi_s(\Omega) \cap \psi_g(\Omega) = \varnothing$ выполняется, поскольку для любого ω и любых s и g из множества сообщений $\mathbf{S}$, $s \neq g$, имеет место неравенство $\omega(s) \neq \omega(g)$. Далее будем предполагать, что значения искусственных помех ω_t, вырабатываемых генератором случайных подстановок при $t = 1, 2, \dots, N$, и значения естественных помех $\varkappa_t$, возникающих в реальном канале связи, независимы в совокупности. Для оптимального декодирования сигналов на выходе побочного канала связи необходимо построить оптимальный критерий различения $M = 2^k$, $k = 2^\nu$, гипотез $H_{\delta s}$, $s \in \mathbf{B}^k$, определяемых распределениями вероятностей случайного вектора

$$Z_t = Z_t(s) = \psi(s, \omega_t) \oplus \varkappa_t, \tag{1}$$

где

$$Z_t(s) \in \mathbf{B}^m, \qquad s = (s_1, \dots, s_k) \in \mathbf{B}^k,$$

$$\omega_t = (\omega_t(1), \dots, \omega_t(k)) \in \mathbf{B}^{k\nu}, \qquad \omega_t(j) = (\omega_{t1}(j), \dots, \omega_{t\nu}(j)) \in \mathbf{B}^\nu, \qquad j \in \mathbf{K},$$

$$\varkappa_t = (\varkappa_{t0}, \varkappa_{t1}, \dots, \varkappa_{tk}) \in \mathbf{B}^{k(\nu+1)}, \qquad \varkappa_{t0} = (\varkappa_{t01}, \dots, \varkappa_{t0k}) \in \mathbf{B}^k,$$

$$\varkappa_{tj} = (\varkappa_{tj1}, \dots, \varkappa_{tj\nu}) \in \mathbf{B}^\nu, \qquad j \in \mathbf{K}, \qquad t = 1, 2, \dots,$$

$$Z_t(s) = (Z_{t0}(s), Z_{t1}, \dots, Z_{tk}), \qquad Z_{t0}(s) = ((\omega_t s)_1 \oplus \varkappa_{t01}, \dots, (\omega_t s)_k \oplus \varkappa_{t0k}),$$

$$Z_{tj} = (\omega_{t0}(j) \oplus \varkappa_{tj0}, \dots, \omega_{t\nu}(j) \oplus \varkappa_{tj\nu}), \qquad j \in \mathbf{K}.$$

§ 3. АСИМПТОТИЧЕСКОЕ РАЗЛОЖЕНИЕ ПЛОТНОСТИ РАСПРЕДЕЛЕНИЯ ВЕРОЯТНОСТЕЙ

Построим асимптотически оптимальный критерий декодирования сигналов на выходе канала с высоким уровнем шума ($\delta \to 0$). Для этого исследуем асимптотическое поведение плотности распределения вероятностей случайного вектора

$$Z_t = Z_t(s) = \psi(s, \omega_t) \oplus \varkappa_t,$$

где $s = (s_1, \dots, s_k)$ — передаваемый сигнал, $\omega_t = (\omega_{t1}, \dots, \omega_{t\nu})$ — искусственный шум, $\varkappa_t = (\varkappa_{t1}, \dots, \varkappa_{tm})$ — естественный шум, характеризующий уровень искажений сигналов на выходе побочного канала связи,

$$\psi(s, \omega_t) = (\omega_t s, \omega_t), \qquad t = 1, 2, \dots$$

Пусть $p_{s\delta}(Z) = \mathbf{P}_\delta(Z_t(s) = z)$, где $z = (z_0, z_1, \dots, z_k) \in \mathbf{B}^{(\nu+1)k}$, $z_0 = (z_{01}, \dots, z_{0k}) \in \mathbf{B}^k$, $z_j = (z_{j1}, \dots, z_{j\nu}) \in \mathbf{B}^\nu$, $j \in \mathbf{K}$, — плотность распределения вероятностей вектора $Z_t(s)$ при гипотезе $H_{s\delta}$, состоящей в том, что сообщение s было передано по ДСК с уровнем канальных ошибок, задаваемым параметром δ, а случайная подстановка ω_t равномерно распределена на множестве Ω. Заметим, что при $\delta \to 0$ плотность распределения вероятностей $p_{s\delta}(z)$ раскладывается в ряд по малому параметру δ:

$$p_{s\delta}(z) = p(z)\left(1 + \sum_{j=1}^{m} \delta^j h_{sj}(z)\right). \tag{2}$$

Найдем значения коэффициентов $h_{sj}(z)$ в разложении (2). Предварительно получим несколько формул, которые нам понадобятся в дальнейшем. Иногда при написании символов ω_t и $\varkappa_t$ в зависимости от контекста индекс t будем опускать, полагая, что $\omega_t(j) = \omega(j) \in \mathbf{B}^\nu$, $\omega_{ti}(j) = \omega_i(j) \in \mathbf{B}$, $i = 1, \dots, \nu$, $\omega s = (s(\omega(1)), \dots, s(\omega(k)))$ и $\varkappa_t = \varkappa$.

Обозначим через $\mathbf{E}$ символ математического ожидания по равновероятной на множестве Ω мере, $I(A)$ — индикатор события A, оператор,

принимающий значение 1, если утверждение A справедливо, и значение 0 в противном случае,

$$p^s = \frac{\|s\|}{k} = \frac{1}{2}(1-\Delta^s) = s\hat{}(0), \qquad \Delta^s = 1-2p^s,$$

$$p^{z_0} = \frac{\|z_0\|}{k}, \qquad \Delta^{z_0} = 1-2p^{z_0} = k^{-1}\sum_{j=1}^{k}(-1)^{z_{0j}},$$

$s\hat{}(l) = 2^{-\nu}\sum_x s(x)(-1)^{(l,x)}$ — преобразование Фурье–Адамара булевой функции $s(x)$, $x \in \mathbf{B}^\nu$, в точке $l = (l_1, \dots, l_\nu) \in \mathbf{B}^\nu$, $(l, x) = l(x) = l_1x_1 \oplus \dots \oplus l_\nu x_\nu$, $l^i = (l_1^i, \dots, l_\nu^i)$, $l_1^i = 1$, $l_j^i = 0$ при $i \neq j$, $s\hat{}(l^i) = s\hat{}_i$, $i = 1, \dots, \nu$, — коэффициенты Фурье–Адамара первого ранга.

Лемма 1. *Пусть $\omega(j) = (\omega_1(j), \dots, \omega_\nu(j))$ — случайная подстановка, равномерно распределенная на группе всех подстановок множества $\mathbf{B}^\nu$. Тогда справедливы следующие соотношения:*

$$\mathbf{E}(-1)^{\omega_q(j)} = 0, \qquad \mathbf{E}(-1)^{\omega_q(j)\oplus\omega_r(i)} = I(i=j,\ q=r),$$
$$\mathbf{E}(-1)^{s(\omega(j))} = \Delta^s, \qquad \mathbf{E}(-1)^{s(\omega(j))\oplus l(\omega(j))} = I(l=0) - 2s\hat{}(l), \tag{3}$$

$$\sum_{j=1}^{k}(-1)^{z_{0j}}\mathbf{E}(-1)^{s(\omega(j))} = (2p^s-1)(2\|z_0\|-k) = k\Delta^s\Delta^{z_0}, \tag{4}$$

$$\mathbf{E}(-1)^{s(\omega(i))\oplus s(\omega(j))} = 1 + I(i\neq j)[(k-1)^{-1}(k(\Delta^s)^2-1)-1], \tag{5}$$

$$\mathbf{E}(-1)^{s(\omega(j))\oplus l(\omega(i))} = \\ = 2I(l\neq 0)\,s\hat{}(l)[I(i\neq j)\,k(k-1)^{-1}-1] + I(l=0)\,\Delta^s, \tag{6}$$

$$\sum_{i=1}^{k}\sum_{\substack{j=1\\(i,r)\neq(j,q)}}^{k}\sum_{r=1}^{\nu}\sum_{q=1}^{\nu}(-1)^{z_{ir}\oplus z_{jq}}\mathbf{E}(-1)^{\omega_q(j)\oplus\omega_r(i)} = \\ = k(k-1)^{-1}\left[\nu - k\sum_{q=1}^{\nu}\left(\Delta^{z_{\cdot q}}\right)^2\right], \quad z_{\cdot q} = (z_{1q}, \dots, z_{kq}), \quad q = 1, \dots, \nu. \tag{7}$$

Сообщения $s \in \mathbf{B}^k$ и $g \in \mathbf{B}^k$ будем называть d-эквивалентными и обозначать $s \overset{d}{\sim} g$, если $h_{sj}(z) = h_{gj}(z)$ для $j = 1, 2, \dots, d$, и строго d-эквивалентными и обозначать $s \overset{d}{\approx} g$, если $s \overset{d}{\sim} g$ и не выполняется условие $s \overset{d+1}{\sim} g$. Очевидно, что отношение «$\sim$» является отношением эквивалентности, а отношение «$\approx$» не является таковым, поскольку для него не выполняется условие транзитивности.

Таким образом, соотношение $s \overset{d}{\approx} g$ означает, что коэффициенты в разложении (2) удовлетворяют условиям $h_{sj}(z) = h_{gj}(z) = h_j(z)$ при $j = 1, \ldots, d$ и $h_{s,d+1}(z) \neq h_{g,d+1}(z)$, или, другими словами, сообщения s и g лежат в одном и том же классе d-эквивалентности, но в разных классах $(d+1)$-эквивалентности. Пусть $d(s, g)$ — такое натуральное d, для которого выполняется свойство $s \overset{d-1}{\approx} g$.

Теорема 1. *Коэффициенты $h_{s1}(z)$ и $h_{s2}(z)$ разложения плотности распределения вероятностей* (2) *случайного вектора* (1) *имеют вид*

$$h_{s1}(z) = k\Delta^s \Delta^{z_0}, \tag{8}$$

$$h_{s2}(z) = \frac{k}{k-1}[k(\Delta^s)^2 - 1][k(\Delta^{z_0})^2 - 1] - 2(k-1)^{-1} \sum_{q-1}^{\nu} s\hat{}(l^q)\, \tau_q(z) + \\ + k(k-1)^{-1}\left[\nu - k\sum_{q=1}^{\nu}(\Delta^{z_{\cdot q}})^2\right], \tag{9}$$

где

$$\tau_q(z) = (k - 2\|z_0\|)(k - 2\|z^q\|) - k(k - 2\|z_0 \oplus z^q\|) = \\ = k^2[\Delta^{z_0}\Delta^{z_{\cdot q}} - \Delta^{z_0 \oplus z_{\cdot q}}],$$

$$p^s = \frac{\|s\|}{k} = \frac{1}{2}(1 - \Delta^s), \qquad p^{z_0} = \frac{\|z_0\|}{k} = \frac{1}{2}(1 - \Delta^{z_0}),$$

$$\Delta^{z_{\cdot q}} = 1 - \frac{2\|z_{\cdot q}\|}{k}, \qquad z_{\cdot q} = (z_{1q}, \ldots, z_{kq}), \qquad q = 1, \ldots, \nu.$$

Доказательство. Из выражения

$$p_{s\delta}(z) = \mathbf{P}(\psi(s, \omega) \oplus \varkappa = z) = \\ = p(z)\mathbf{E}\prod_{j=1}^{k}(1 + (-1)^{s(\omega(j)) \oplus z_{0j}}\delta) \prod_{j=1}^{k}\prod_{r=1}^{\nu}(1 + (-1)^{\omega_r(j) \oplus z_{jr}}\delta) = \\ = p(z)\left(1 + \sum_{j=1}^{\nu} h_{sj}(z)\,\delta^j\right) \tag{10}$$

следует соотношение

$$h_{sj}(z) = \sum_{\|l_0\| + \ldots + \|l_k\| = j} (-1)^{(l,z)}\mathbf{E}(-1)^{(l_0, \omega_t s) \oplus (l_1, \omega_t(1)) \oplus \ldots \oplus (l_k, \omega_t(k))}, \tag{11}$$

где $l = (l_0, \ldots, l_k) \in \mathbf{B}^m$, $l_0(l_{01}, \ldots, l_{0k}) \in \mathbf{B}^k$, $l_j = (l_{j1}, \ldots, l_{j\nu}) \in \mathbf{B}^\nu$, $j = 1, \ldots, k$. С учетом (4) и (8) находим, что коэффициент $h_{s1}(z)$ при δ в разложении (2) равен

$$h_{s1}(z) = \sum_{j=1}^{k} (-1)^{z_{0j}} \mathbf{E}(-1)^{s(\omega(j))} + \sum_{r=1}^{\nu} \sum_{j=1}^{k} (-1)^{z_{jr}} \mathbf{E}(-1)^{\omega_r(j)} =$$

$$= 4\left(p^s - \frac{1}{2}\right)\left(\|z_0\| - \frac{k}{2}\right) = k\Delta^s \Delta^{z_0}. \quad (12)$$

Отсюда видно, что коэффициент $h_{s1}(z)$ зависит лишь от веса функции $s(x)$, или, другими словами, от вероятности p^s того, что значение функции при равновероятном распределении аргументов равно единице, которая, в свою очередь, равна значению $s\hat{}(0)$ преобразования Фурье–Адамара в точке нуль. Поэтому условием 1-эквивалентности функций s и g является выполнение одного из равносильных соотношений $p^s = p^g$, $s\hat{}(0) = g\hat{}(0)$ или $\|s\| = \|g\|$.

Как видно из представления (11), коэффициент $h_{s2}(z)$ можно записать в виде суммы четырех слагаемых $h_{s2}(z) = A_1 + A_2 + A_3 + A_4$, где

$$A_1 = \sum_{i \neq j} \mathbf{E}(-1)^{s(\omega(i)) \oplus s(\omega(j)) \oplus z_{0i} \oplus z_{0j}}, \quad (13)$$

$$A_2 = \sum_{j=1}^{k} \sum_{r=1}^{\nu} \mathbf{E}(-1)^{s(\omega(j)) \oplus \omega_r(j)} (-1)^{z_{0j} \oplus z_{jr}}, \quad (14)$$

$$A_3 = \sum_{\substack{i,j=1 \\ i \neq j}}^{k} \sum_{r=1}^{\nu} \mathbf{E}(-1)^{s(\omega(i)) \oplus \omega_r(j)} (-1)^{z_{0i} \oplus z_{jr}}, \quad (15)$$

$$A_4 = \sum_{\substack{i,j=1 \\ (i,q) \neq (j,r)}}^{k} \sum_{q,r=1}^{\nu} \mathbf{E}(-1)^{\omega_q(i) \oplus \omega_r(j)} (-1)^{z_{iq} \oplus z_{jr}}. \quad (16)$$

Из (16) видно, что A_4 не зависит от вида функции s.

Для определения A_1 воспользуемся равенством (5). Получим

$$A_1 = k(k-1)^{-1}(k(\Delta^s)^2 - 1)(k(\Delta^{z_0})^2 - 1), \qquad \Delta^{z_0} = 1 - \frac{2\|z_0\|}{k}. \quad (17)$$

Коэффициент A_2 равен:

$$A_2 = \sum_{i=1}^{k} \sum_{r=1}^{\nu} \mathbf{E}(-1)^{s(\omega(i)) \oplus \omega_r(i)} (-1)^{z_{0i} \oplus z_{ir}} = -2 \sum_{r=1}^{\nu} s\hat{}(l^r)\, A(z_0 \oplus z^i) =$$

$$= -2 \sum_{r=1}^{\nu} s\hat{}(l^r)(k - 2\|z_0 \oplus z_{\cdot r}\|), \quad z_{\cdot r} = (z_{1r}, \ldots, z_{kr}). \quad (18)$$

Далее из (6) получаем:

$$A_3 = \sum_{i\neq j}^{k}\sum_{r=1}^{\nu} \mathbf{E}(-1)^{s(\omega(i))\oplus\omega_r(j)}(-1)^{z_{0i}\oplus z_{jr}} =$$

$$= 2(k-1)^{-1}\sum_{r=1}^{\nu} s^{\frown}(l^r)\sum_{i\neq j}^{k}(-1)^{z_{0j}\oplus z_{jr}} =$$

$$= 2(k-1)^{-1}\sum_{r=1}^{\nu} s^{\frown}(l^r)[(k-2\|z_0\|)(k-2\|z_{\cdot r}\|)+2\|z_0\oplus z_{\cdot r}\|-k] =$$

$$= \frac{2}{k-1}\sum_{r=1}^{\nu} s^{\frown}(l^r)\left[k^2\Delta^{z_0}\Delta^{z_{\cdot r}} - k\Delta^{z_0\oplus z_{\cdot r}}\right]. \qquad (19)$$

Для определения A_4 заметим, что в слагаемых суммы (16) при $i=j$, $q\neq r$ выполняется равенство

$$\mathbf{E}(-1)^{\omega_q(i)\oplus\omega_r(i)} = 0;$$

при $i\neq j$, $q\neq r$ справедливы соотношения

$$\mathbf{E}(-1)^{\omega_q(i)\oplus\omega_r(j)} = \frac{1}{k(k-1)}\sum_{u\neq w}(-1)^{u_q\oplus w_r} =$$

$$= \frac{1}{k(k-1)}\left[\sum_{u,w}(-1)^{u_q\oplus w_r} - \sum_{u}(-1)^{u_q\oplus u_r}\right] = 0,$$

где

$$u = (u_1,\dots,u_k)\in\mathbf{B}^k, \qquad w = (w_1,\dots,w_k)\in\mathbf{B}^k;$$

при $i\neq j$, $q=r$ получаем:

$$\mathbf{E}(-1)^{\omega_q(i)\oplus\omega_q(j)} = \frac{1}{k(k-1)}\sum_{u\neq w}(-1)^{u_q\oplus w_q} =$$

$$= \frac{1}{k(k-1)}\left[\sum_{u,w}(-1)^{u_q\oplus w_q} - \sum_{u}(-1)^{u_q\oplus u_q}\right] = -(k-1)^{-1}.$$

Поэтому

$$A_4 = -(k-1)^{-1}\sum_{i\neq j,\, q=r}(-1)^{z_{iq}\oplus z_{jr}} =$$

$$= -(k-1)^{-1}\sum_{q=1}^{\nu}\left[\sum_{i,j=1}^{k}(-1)^{z_{iq}\oplus z_{jq}} - \sum_{i=1}^{k}(-1)^{z_{iq}\oplus z_{iq}}\right] =$$

$$= -(k-1)^{-1}\sum_{q=1}^{\nu}\left[\left(\sum_{i=1}^{k}(-1)^{z_{iq}}\right)^2 - k\right] = k(k-1)^{-1}\left[\nu - k\sum_{q=1}^{\nu}(\Delta_{z_{\cdot q}})^2\right], \qquad (20)$$

так как

$$\sum_{i=1}^{k}(-1)^{z_{iq}} = k\Delta_{z\cdot q}, \qquad \Delta_{z\cdot q} = 1 - \frac{2\|z_{\cdot q}\|}{k},$$

$$z_{\cdot q} = (z_{1q}, \dots, z_{kq}), \qquad q = 1, \dots, \nu.$$

Обозначая

$$\tau_r(z) = 2(1-k)^{-1}\left[\left(\sum_{j=1}^{k}(-1)^{z_{0j}}\right)\left(\sum_{j=1}^{k}(-1)^{z_{rj}}\right) - \sum_{j=1}^{k}(-1)^{z_{0j}\oplus z_{jr}}\right] =$$

$$= \frac{2}{1-k}\left[k^2\Delta^{z_0}\Delta^{z\cdot r} - k\Delta^{z_0\oplus z\cdot r}\right],$$

с учетом (17)–(20) получаем формулу (9).

Найдем все математические ожидания, которые встречаются в представлении (11) коэффициента $h_{s3}(z)$.

Лемма 2. *Пусть* $k^{(n)} = \dfrac{k!}{(k-n)!}$, $l(j) = (l, j)$, $L(j) = (L, j)$ — *скалярные произведения векторов* $j, l, L \in \mathbf{B}^\nu$, $l \neq 0$, $L \neq 0$. *Тогда имеют место следующие соотношения: при* $\|l_0\| = 3$

$$\mathbf{E}(-1)^{s(\omega(1))\oplus s(\omega(2))\oplus s(\omega(3))} = \frac{[k^2\Delta_s^3 - (3k-2)\Delta_s]}{(k-1)^{(2)}}; \tag{21}$$

при $\|l_0\| = 2$, $\|l\| = 1$

$$\mathbf{E}(-1)^{s(\omega(1))\oplus s(\omega(2))\oplus l(\omega(1))} = -2\frac{k}{k-1}s\hat{}(l)\Delta_s, \tag{22}$$

$$\mathbf{E}(-1)^{s(\omega(1))\oplus s(\omega(2))\oplus l(\omega(3))} = \frac{4ks\hat{}(l)\Delta_s}{(k-1)^{(2)}}; \tag{23}$$

при $\|l_0\| = 1$, $\|L\| = 2$, $\|l\| = \|l'\| = 1$

$$\mathbf{E}(-1)^{s(\omega(1))\oplus L(\omega(1))} = -2s\hat{}(L), \tag{24}$$

$$\mathbf{E}(-1)^{s(\omega(1))\oplus l(\omega(1))\oplus l'(\omega(2))} = \frac{2s\hat{}(l\oplus l')}{k-1}, \tag{25}$$

$$\mathbf{E}(-1)^{s(\omega(1))\oplus l(\omega(2))\oplus l'(\omega(3))} = \frac{-4s\hat{}(l\oplus l') + k\Delta_s I(l=l')}{(k-1)^{(2)}}. \tag{26}$$

Доказательство формул (21)–(26) проводится непосредственным вычислением математических ожиданий. Следует еще обратить внимание на то, что в вычислениях для случая $\|l_0\| = 0$ функции $s(\omega(j))$ не встречаются.

Из леммы видно, что коэффициенты $h_{s1}(z) - h_{s3}(z)$ в разложении (2) однозначно определяются преобразованиями Фурье $s\hat{}(l)$ на наборах l

веса $\|l\| \leqslant 2$. Аналогичное утверждение имеет место и для общего случая.

Теорема 2. *Коэффициенты $h_{sR}(z)$ в разложении (2) однозначно определяются значениями преобразований Фурье–Адамара $s\hat{}(\sigma)$ на наборах $\sigma \in \mathbf{B}^\nu$ веса $\|\sigma\| \leqslant R-1$.*

Доказательство. Пусть $\|l\| \leqslant R$,

$$f_j(s,\omega,l) = f_j(s,\omega(j),l) = (-1)^{l_{0j}s(\omega(j))\oplus(l_j,\omega(j))}$$

и $j(1),\dots,j(Q)$ — индексы, для которых вектор $(l_{0j},\ l_j) \neq 0,\ j=1,\dots,k$. Параметр Q зависит от конкретного значения, которое принимает вектор l, причем $Q = Q(l) \leqslant R$. Таким образом,

$$\mathbf{E}(-1)^{(l_0,\omega_t s)\oplus(l_1,\omega_t(1))\oplus\ldots\oplus(l_k,\omega_t(k))} = f(s,\omega,l) = \mathbf{E}\prod_{i=1}^{Q} f_{j(i)}(s,\omega(j(i)),l)$$

и, без ограничения общности, можно считать, что коэффициент при $(-1)^{(l,z)}$ в выражении (11) для $h_{sj}(z)$ представим в виде

$$f(s,\omega,l) = \mathbf{E}\prod_{j=1}^{Q} f_j(s,\omega(j),l). \tag{27}$$

Пусть $\mathbf{K}_0$ — подмножество векторов мощности $k^{(Q)} = k(k-1)\ldots(k-Q+1)$ из множества

$$\mathbf{K}^Q = \{u = (u_1,\dots,u_Q),\ u_j \in \mathbf{K},\ j=1,\dots,Q\},$$

координаты которых попарно различны, $\mathbf{K}_0^c = \mathbf{K}^Q \backslash \mathbf{K}_0$ — дополнение множества $\mathbf{K}_0$ в множестве $\mathbf{K}^Q$, $\mathbf{K}_{ij}$, $i<j$, — множество всех векторов u из $\mathbf{K}^Q$, у которых $u_i = u_j$. Расположим все $d = Q(Q-1)/2$ подмножеств $\mathbf{K}_{ij}$, $1 \leqslant i \leqslant j \leqslant Q$, множества $\mathbf{K}^Q$ в произвольном порядке и обозначим их $\mathbf{K}_1,\dots,\mathbf{K}_d$. Тогда если $\|l_0\| + \ldots + \|l_k\| = R$ и число ненулевых векторов (l_{0j}, l_j), $j=1,\dots,k$, равно $Q \leqslant R$, то, учитывая (27) и соотношение

$$\mathbf{K}_0^c = \bigcup_{v=1}^{d} \mathbf{K}_v,$$

получаем:

$$\mathbf{E}f(s,\omega,l) = (k^{(Q)})^{-1}\sum_{u\in\mathbf{K}_0}\prod_{j=1}^{Q} f_j(s,u_j,l) =$$

$$= (k^{(Q)})^{-1}\left[\sum_{u\in\mathbf{K}^Q}\prod_{j=1}^{Q} f_j(s,u_j,l) - \sum_{u\in\mathbf{K}_0^c}\prod_{j=1}^{Q} f_j(s,u_j,l)\right]. \tag{28}$$

Для вычисления первой суммы в (28) достаточно заметить, что

$$k^{-Q}\sum_{u\in\mathbf{K}^Q}\prod_{j=1}^{Q} f_j(s,u_j,l)=\mathbf{E}\prod_{j=1}^{Q}(-1)^{l_{0j}s(\omega(j))\oplus(l_j,\omega(j))}=$$

$$=\prod_{j=1}^{Q}\mathbf{E}(-1)^{l_{0j}s(\omega(j))\oplus(l_j,\omega(j))}=\prod_{j=1}^{Q}\mathbf{E}(1-2l_{0j}s(\omega(j)))(-1)^{(l_j,\omega(j))}=$$

$$=\prod_{j=1}^{Q}[I(l_j=0)-2l_{0j}s\hat{}(l_j)],\qquad(29)$$

поскольку здесь усреднение ведется по равновероятной мере на множестве $\mathbf{K}^Q$. Второе слагаемое в (28) представим в виде

$$\sum_{u\in\mathbf{K}_0}\prod_{j=1}^{Q} f_j(s,u_j,l)=\sum_{u\in\bigcup\limits_j\mathbf{K}_j} f(s,u,l)=$$

$$=\sum_{v=1}^{d}\sum_{u\in\mathbf{K}_v} f(s,u,l)-\sum_{1\leqslant v(1)<v(2)\leqslant d}\ \sum_{u\in\mathbf{K}_{v(1)}\mathbf{K}_{v(2)}} f(s,u,l)+\ldots$$

$$\ldots+(-1)^{d-1}\sum_{u\in\mathbf{K}_1\ldots\mathbf{K}_d} f(s,u,l).\qquad(30)$$

Действительно, если аргумент u входит в множества $\mathbf{K}_{j(1)},\ldots,\mathbf{K}_{j(q)}$ и не входит в $\mathbf{K}_j$, $j=\{1,\ldots,d\}\backslash\{j(1),\ldots,j(q)\}$, то значение функции f на аргументе u войдет в сумму (30) ровно $C_q^1-C_q^2+\ldots+(-1)^{q-1}C_q^q=1$ раз.

Пересечения множеств $\mathbf{K}_{v(1)}\ldots\mathbf{K}_{v(q)}$ для различных индексов

$$1\leqslant v(1)<v(2)<\ldots<v(q)\leqslant Q$$

представляют собой полные наборы переменных $u_1,\ldots,u_q$, оставшихся в результате отождествления некоторых групп аргументов. Поэтому каждая сумма в (30) аналогична сумме (29) с меньшим числом аргументов, поскольку при отождествлении переменных вид функции не меняется, а преобразуются лишь коэффициент l_{0j} при функции $s(\omega(j))$ и вектор l_j в скалярном произведении $(l_j,\omega(j))$ выражений в (29). Заметим, что вес вектора l_j не превосходит $Q-1$, если для данного j коэффициент $l_{0j}=1$. Следовательно, при вычислении математических ожиданий в формуле (29) могут появиться лишь образы Фурье–Адамара $s\hat{}(\sigma)$ на векторах σ веса

$$\|\sigma\|\leqslant\min(\nu,Q-1).$$

§ 4. ОПТИМАЛЬНЫЙ КРИТЕРИЙ РАЗЛИЧЕНИЯ ГИПОТЕЗ

Пусть гипотеза $H_{s\delta}$ задается плотностью распределения $p_{s\delta}(z)$ случайной величины

$$Z_t = X_t \oplus \varkappa_t = (Z_{t0}, Z_{t1}, \dots, Z_{tk}),$$

где

$$Z_{t0} = (Z_{t01}, \dots, Z_{t0k}) \in \mathbf{B}^k, \qquad Z_{tj} = (Z_{tj1}, \dots, Z_{tj\nu}) \in \mathbf{B}^\nu,$$

на множестве векторов

$$z = (z_0, z_1, \dots, z_k) \in \mathbf{B}^m, \qquad m = (\nu+1)2^\nu,$$

$$z_0 = (z_{01}, \dots, z_{0k}) \in \mathbf{B}^k, \qquad z_j = (z_{j1}, \dots, z_{j\nu}) \in \mathbf{B}^\nu, \qquad j = 1, \dots, k,$$

$$X_t = (\omega_t s, \omega_t(1), \dots, \omega_t(k)).$$

Гипотеза H_{s0} задается плотностью $p_{s0}(z) = p(z) = 2^{-m}$ и не зависит от передаваемого сообщения s. Поэтому гипотезу H_{s0} будем обозначать просто H_0.

В дальнейших рассмотрениях мы будем принимать во внимание тот факт, что для всех значений z при достаточно малых значениях параметра δ выполняется неравенство $p_{s\delta}(z) > 0$ и что коэффициенты $h_{sj}(z) \leqslant C$ для любого $z \in \mathbf{B}^m$ и некоторой абсолютной константы C.

Предположим, что при $\delta \to 0$ плотность распределения $p_{s\delta}(z) = \mathbf{P}_\delta(Z_t(s) = z)$ допускает представление

$$p_{s\delta}(z) = p(z)\left(1 + \sum_{j=1}^{m} \delta^j h_{sj}(z)\right).$$

Оценим минимальный объем $n = \mathcal{N}_{sg}(\alpha, \beta)$ выборки Z_t, $t = 1, \dots, n$, необходимый для различения гипотез $H_{s\delta}$ и $H_{g\delta}$ с заданными вероятностями ошибок первого и второго рода $\alpha < 1/2$ и $\beta < 1/2$ при $\delta \to 0$. В этих целях исследуем вероятностные характеристики статистики отношения правдоподобия

$$L_{sg}(Z^{(n)}) = \sum_{t=1}^{n} l_{sg}(Z_t),$$

$$l_{sg}(z) = l_{sg\delta}(z) = \ln\frac{p_{g\delta}(z)}{p_{s\delta}(z)} = l_{g\delta}(z) - l_{s\delta}(z), \qquad l_{s\delta}(z) = \ln\frac{p_{s\delta}(z)}{p(z)}.$$

При $H_{g0} = H_0$ получаем

$$L_s(Z^{(n)}) = \sum_{t=1}^{n} l_{s\delta}(Z_t),$$

где $l_{s\delta}(z)$ — логарифм отношения правдоподобия в задаче различения гипотез, задаваемых распределением $p_{s\delta}(z)$ и равномерным распределением $p(z)$.

Следует отметить, что в [1] и [3] при изучении вероятностных характеристик статистики логарифма отношения правдоподобия оптимального критерия проверки гипотезы H_0 $(\delta = 0)$, состоящей в том, что реализация случайной последовательности представляет собой белый шум $(\delta = 0)$, против гипотезы $H_{s\delta}$, состоящей в том, что реализация случайной последовательности представляет собой сумму по модулю два сигнала s и шума, близкого по вероятностным характеристикам к белому $(\delta > 0,\ \delta \to 0)$, имеют дело со схемой нарастающих сумм при условии, что справедлива гипотеза H_0, и со схемой серий при условии, что справедлива гипотеза $H_{s\delta}$. В нашем случае, который можно трактовать как задачу различения малых сигналов на фоне шума, сближающегося с белым как при основной гипотезе $H_{s\delta}$, так и при альтернативной гипотезе $H_{g\delta}$, $s \neq g$, приходится иметь дело с двумя схемами серий. Кроме того, в нашем случае гипотезы могут сближаться с более высокой скоростью, чем в ранее описанном случае, что приводит к увеличению объема выборки, необходимого для различения гипотез с заданной надежностью.

Таким образом, распределения вероятностей для гипотез, задаваемых распределениями $p_{s\delta}(z)$ и $p_{g\delta}(z)$, при $\delta \to 0$ зависят от параметра δ, определяющего схему серий последовательностей случайных величин. Из асимптотического разложения для плотности распределения вероятностей

$$p_{s\delta}(z) = \mathbf{P}_\delta(Z_t(s) = z) = p(z)\left(1 + \sum_{j=1}^{m} \delta^j h_{sj}(z)\right)$$

следует асимптотическое разложение для логарифма отношения правдоподобия

$$l_{s\delta}(z) = \ln \frac{p_{s\delta}(z)}{p(z)} = \sum_{d=1}^{\infty} \delta^d R_{sd}(z), \tag{31}$$

где

$$R_{sd}(z) = \sum_{k=1}^{d} \frac{(-1)^{k-1}}{k} \sum_{j_1+\ldots+j_k=d} h_{sj_1}(z)\ldots h_{sj_k}(z) =$$

$$= h_{sd}(z) + \Omega(h_{s1}, \ldots, h_{s,d-1}), \quad 1 \leqslant j_1, \ldots, j_k \leqslant m. \tag{32}$$

В частности, разложение $l_{s\delta}(z)$ с точностью до $O(\delta^5)$ принимает вид

$$l_{s\delta}(z) = \ln \frac{p_{s\delta}(z)}{p(z)} = \delta R_{s1}(z) + \delta^2 R_{s2}(z) + \delta^3 R_{s3}(z) + \delta^4 R_{s4}(z) + O(\delta^5),$$

где

$$R_{s1}(z) = h_{s1}(z), \qquad R_{s2}(z) = h_{s2}(z) - \frac{h_{s1}(z)^2}{2},$$

$$R_{s3}(z) = h_{s3}(z) - h_{s1}(z)\,h_{s2}(z) + \frac{1}{3}\,h_{s1}^3(z),$$

$$R_{s4}(z) = h_{s4}(z) - h_{s1}(z)\,h_{s3}(z) - \frac{1}{2}\,h_{s2}^2(z) + h_{s1}^2(z)\,h_{s2}(z) - \frac{1}{4}\,h_{s1}^4(z).$$

Лемма 3. *Пусть*

$$l_w(z) = \sum_{k=1}^{\infty} (-1)^{k-1} k^{-1} (\delta A + \delta^d B_w)^k,$$

где $w = s, g$,

$$A = A(z) = h_1(z) + h_2(z)\,\delta + \ldots + h_{d-1}(z)\,\delta^{d-2},$$

$$B_w = B_w(z) = h_{wd}(z) + h_{w,d+1}(z)\,\delta + \ldots + h_{wm}(z)\,\delta^{m-d},$$

$$l_{sg}(z) = l_g(z) - l_s(z), \qquad B_{sg}(z) = B_g(z) - B_s(z).$$

Тогда

$$l_{sg}(z)\,p_{s\delta}(z)\,p^{-1}(z) = \delta^d B_{sg}(z) - \frac{1}{2}\,\delta^{2d} B_{sg}^2(z) + O(\delta^{2d+1}), \tag{33}$$

$$l_{sg}(z)\,p_{s\delta}(z)\,p^{-1}(z) = \delta^d B_{sg}(z) + \frac{1}{2}\,\delta^{2d} B_{sg}^2(z) + O(\delta^{2d+1}). \tag{34}$$

Доказательство. Из представления $l_{sg}(z)$ в виде

$$l_{sg}(z) = \sum_{k=1}^{\infty} (-1)^{k-1} k^{-1} [(\delta A + \delta^d B_g)^k - (\delta A + \delta^d B_s)^k]$$

получаем

$$l_{sg}(z) = \delta^d B_{sg} \sum_{k=1}^{\infty} (-1)^{k-1} \Pi_{k\delta}(A, B_s, B_g),$$

где

$$\Pi_{k\delta} = \Pi_{k\delta}(A, B_s, B_g) = k^{-1} \sum_{j=1}^{k} (\delta A + \delta^d B_s)^{k-j} (\delta A + \delta^d B_g)^{j-1},$$

$$\Pi_1 = 1, \qquad \Pi_2 = \delta A + \frac{1}{2}\,\delta^d (B_s + B_g),$$

$$\Pi_3 = \delta^2 A^2 + O(\delta^{d+1}), \qquad \Pi_4 = \delta^3 A^3 + O(\delta^{d+2}),$$

$$\Pi_{k\delta} = \delta^{k-1} A^{k-1} + O(\delta^{d+k-2}), \qquad k = 2, 3, \ldots$$

Поэтому

$$l_{sg}(z)p_s(z)p^{-1}(z) = \delta^d B_{sg}\left(1-\delta A-\frac{1}{2}\delta^d(B_s+B_g)\right)+$$

$$+\sum_{k=3}^{\infty}\left[(-1)^{k-1}\delta^{k-1}A^{k-1}+O(\delta^{d+k-2})\right]\left[1+\delta A+\delta^d B_s\right] =$$

$$= \delta^d B_{sg}\left[1-\frac{1}{2}\delta^d(B_s+B_g)+\delta^d B_s+O(\delta^{d+1})\right] = \delta^d B_{sg}-\delta^{2d}B_{sg}^2+O(\delta^{2d+1}).$$

Тем самым соотношение (33) доказано. Разложение (34) доказывается аналогично. Полученные формулы позволяют найти вероятностные характеристики случайной величины $l_{sg}(z_t)$ при гипотезах $H_{s\delta}$ и $H_{g\delta}$.

Оценим теперь объем материала, необходимый для различения гипотез $H_{s\delta}$ и $H_{g\delta}$ при $\delta \to 0$.

Теорема 3. *Пусть сообщения s и g строго $(d-1)$-эквивалентны. Тогда минимальный объем материала $\mathcal{N}_{sg}(\alpha,\beta)$ для различения гипотез $H_{s\delta}$ и $H_{g\delta}$ с вероятностями ошибок первого и второго рода α и β соответственно, $\alpha,\beta<1/2$, при $\delta\to 0$ асимптотически равен*

$$\mathcal{N}_{sg}(\alpha,\beta) \sim \frac{(u_\alpha+u_\beta)^2}{b_{sg}\delta^{2d}}, \tag{35}$$

где $b_{sg} = \mathbf{E}_0[h_{gd}(Z_t)-h_{sd}(Z_t)]^2$, $d=d(s,g)$, $\mathbf{E}_0$ — усреднение по равновероятной мере на множестве значений случайного вектора Z_t, u_δ — δ-квантиль стандартного нормального распределения.

Доказательство. Заметим, что если $s \overset{d-1}{\approx} g$, то справедливы выражения

$$p_{g\delta}(z)-p_{s\delta}(z) = p(z)\,\delta^d(h_{gd}(z)-h_{sd}(z)) = O(\delta^{d+1})$$

и

$$l_{sg\delta}(z) = l_{g\delta}(z)-l_{s\delta}(z) = \ln\frac{p_{g\delta}(z)}{p_{s\delta}(z)} = \delta^d(h_{gd}(z)-h_{sd}(z))+O(\delta^{d+1}),$$

откуда следует, что

$$\mathbf{E}_g l_{sg\delta}(Z_t)-\mathbf{E}_s l_{sg\delta}(Z_t) =$$

$$= \delta^{2d}\mathbf{E}_0[h_{gd}(Z_t)-h_{sd}(Z_t)]^2+O(\delta^{2d+1}) = \delta^{2d}b_{sg}+O(\delta^{2d+1}),$$

$$\mathbf{D}_s l_{sg\delta}(Z_t) \sim \mathbf{D}_g l_{sg\delta}(Z_t) \sim \delta^{2d}\mathbf{E}_0[h_{gd}(Z_t)-h_{sd}(Z_t)]^2 \sim \delta^{2d}b_{sg}.$$

Учитывая, что статистика отношения правдоподобия

$$L_{sg}(Z^{(n)}) = \sum_{t=1}^{n} l_{sg}(Z_t)$$

имеет асимптотически нормальное распределение с параметрами

$$\mathbf{E}_g L_{sg}(Z^{(n)}) - \mathbf{E}_s L_{sg}(Z^{(n)}) =$$

$$= n(\mathbf{E}_g l_{sg}(Z_t) - \mathbf{E}_s l_{sg}(Z_t)) = n\delta^{2d} b_{sg} + o(\delta^{2d}),$$

$$\mathbf{D}_s L_{sg}(Z^{(n)}) \sim \mathbf{D}_g L_{sg}(Z^{(n)}) \sim n\delta^{2d} b_{sg}, \qquad b_{sg} = \mathbf{E}_0(h_{gd}(Z_t) - h_{sd}(Z_t))^2,$$

получаем формулу (35). В целях обоснования асимптотической нормальности статистики критерия отношения правдоподобия заметим, что при гипотезе H_0 статистика $L_{sg}(Z^{(n)})$ асимптотически нормальна, так как в этом случае реализуется модель нарастающих сумм. Далее, по первой лемме Ле Кама (см. [3]) распределения, соответствующие гипотезам H_0 и $H_{s\delta}$ ($H_{g\delta}$), контигуальны при $\delta \to 0$. Поэтому по третьей лемме Ле Кама (см. [3]) распределения статистики $L_{sg}(Z^{(n)})$, соответствующие гипотезам $H_{s\delta}$ и $H_{g\delta}$, асимптотически нормальны.

Учитывая вышесказанное, можно сделать вывод о том, что основными параметрами асимптотической оценки минимального объема материала (35) для различения гипотез $H_{s\delta}$ и $H_{g\delta}$ являются порядок асимптотической оценки минимального объема выборки $d = d(s, g)$ и константа $b_{sg} = \mathbf{E}_0(h_{gd}(Z_t) - h_{sd}(Z_t))^2$.

Теорема 4. *Минимальный объем выборки для различения гипотез $H_{s\delta}$ и $H_{g\delta}$ с вероятностями ошибок первого и второго рода α и β соответственно, $\alpha, \beta < 1/2$, в случае $s \overset{0}{\approx} g$, что равносильно выполнению условий $d(s, g) = 1$ или $\rho_{sg}(0) = s\hat{}(0) - g\hat{}(0) \neq 0$, асимптотически равен*

$$\mathcal{N}_{sg}(\alpha, \beta) \sim \frac{(u_\alpha + u_\beta)^2}{4k\rho_{sg}^2(0)\,\delta^2}; \tag{36}$$

в случае $s \overset{1}{\approx} g$, что равносильно выполнению условий $d(s, g) = 2$ или $s\hat{}(0) = g\hat{}(0)$ и

$$c_{sg}^2 = \sum_{i=1}^{\nu} \rho_{sg}^2(i) > 0, \qquad \rho_{sg}(i) = s\hat{}(l^i) - g\hat{}(l^i),$$

$l^i = (l_1^i, \dots, l_\nu^i)$, $l_i^i = 1$, $l_q^i = 0$ при $q \neq i$, асимптотически равен

$$\mathcal{N}_{sg}(\alpha, \beta) \sim \frac{(k-1)(u_\alpha + u_\beta)^2}{4k^2\delta^4 c_{sg}^2}. \tag{37}$$

Доказательство. Формулы (36) и (37) непосредственно следуют из формулы (35) и соотношений (8), (9).

В заключение заметим, что аналогичным образом исследуется ситуация, когда координаты s_j сообщения $s = (s_1, \dots, s_k)$ представляют собой слова $s_j = (s_{j1}, \dots, s_{j\mu})$ длины μ, которые считываются по случайной подстановке ω перед направлением их в канал связи.

СПИСОК ЛИТЕРАТУРЫ

1. *Иванов В. А.* Статистические методы оценки эффективности кодового зашумления. — В сб.: Труды по дискретной математике. Т. 6. — М.: ФИЗМАТЛИТ, 2003, с. 48–63.
2. *Сачков В. Н.* Введение в комбинаторные методы дискретной математики. — М.: Наука, 1982.
3. *Гаек Я.*, *Шидак З.* Теория ранговых критериев. — М.: Наука, 1971.