

© 2020 г. Д.С. ОСИПОВ, канд. техн. наук (d_osipov@iitp.ru)
(Институт проблем передачи информации им. А.А. Харкевича РАН, Москва;
Национальный исследовательский университет
“Высшая школа экономики”, Москва)

ВЕРХНЯЯ ГРАНИЦА ВЕРОЯТНОСТИ ОШИБКИ В СИСТЕМАХ СВЯЗИ, ИСПОЛЬЗУЮЩИХ ОДНОПОЛЬЗОВАТЕЛЬСКИЙ ПРИЕМ НА ОСНОВЕ ПОРЯДКОВЫХ СТАТИСТИК¹

Рассматривается модель канала, описывающая передачу информации в системах связи, использующих однопользовательский приемник на основе порядковых статистик. Рассматривается передача информации по такому каналу с использованием линейного блочного кода. Целью работы является отыскание верхней границы вероятности ошибки для случая, когда для декодирования используется алгоритм, основанный на полном переборе множества кодовых слов и заданном критерии декодирования.

Ключевые слова: верхняя граница, вероятность ошибки, порядковые статистики, однопользовательский прием, непересекающиеся подканалы, недвоичные линейные коды.

DOI: 10.31857/S0005231020010092

1. Введение

В современных системах связи и управления применяются техники приема и методы теории помехоустойчивого кодирования, позволяющие обеспечить выполнение требований к качеству (т.е. надежности) и скорости связи для весьма широкого круга приложений, в которых возникает необходимость в использовании таких систем. Вместе с тем в ряде случаев традиционные методы приема (например, “жесткий” посимвольный прием или традиционные методы “мягкого” приема, т.е. вычисления оценок надежности для каждого из символов) оказываются неэффективными (например, если передача происходит в условиях воздействия аддитивной помехи, мощность которой существенно выше, чем мощность полезного сигнала, или если параметры канала не известны приемнику или оценки этих параметров существенно отличаются от истинных значений). Для такого рода случаев необходимы специализированные методы приема, устойчивые к искажениям принятого сигнала и ошибкам в определении параметров распределений решающих статистик. Примерами таких методов являются методы приема, основанные на использовании порядковых статистик [1–3]. Настоящая работа является результатом исследования, первые результаты которого были доложены автором в рамках международного симпозиума по проблеме избыточности в информационных

¹ Исследование выполнено в ИППИ РАН за счет гранта Российского научного фонда (проект № 14-50-00150).

системах в Санкт-Петербурге. Ниже будет рассмотрен метод приема, являющийся обобщением метода, предложенного автором в [1]. Для описания систем связи, использующих такой метод, в [4] была предложена модель канала. Эта модель будет описана в разделе 2, где будет описана и схема системы связи, соответствующей такой модели канала, и связь этой модели с моделями каналов, рассмотренными другими авторами. В разделе 3 будут описаны схема кодирования и правило декодирования. В разделе 4 получен вывод верхней границы на вероятность ошибки (на кодовое слово) для случая, в котором для передачи по каналу рассматриваемого типа используется линейный код с известным спектром и для декодирования используется правило декодирования, введенное в разделе 3. Наконец, в разделе 5 приведены результаты имитационного моделирования, свидетельствующие об эффективности используемого подхода и корректности полученных результатов.

2. Описание модели канала

Пусть q и α — натуральные числа такие, что $\alpha \geq 2$, $q > \alpha$. Введем следующие обозначения:

$$(1) \quad \mathbb{B}_q^x = \{\mathbf{b} = (b_1, \dots, b_q)^T : \forall i \in \{1 : q\} b_i \in \{0, 1\}, w_H(\mathbf{b}) = x\}$$

— множество всех двоичных векторов-столбцов веса x (здесь $w_H(\mathbf{z})$ — вес Хэмминга вектора \mathbf{z}).

Кроме того, для любого вектора-столбца \mathbf{z} такого, что $w_H(\mathbf{z}) < \alpha$, определим множества

$$(2) \quad \begin{aligned} \mathbb{S}^1(\mathbf{z}, \alpha) &= \{\mathbf{s} : \mathbf{s} \in \mathbb{B}_q^\alpha, \mathbf{s} \wedge \mathbf{z} = \mathbf{z}\}, \\ \mathbb{S}^0(\mathbf{z}, \alpha) &= \{\mathbf{s} : \mathbf{s} \in \mathbb{B}_q^\alpha, \mathbf{s} \wedge \mathbf{z} \neq \mathbf{z}\} \end{aligned}$$

— множество двоичных векторов-столбцов веса α , покрывающих вектор-столбец \mathbf{z} , и множество двоичных векторов-столбцов веса α , не покрывающих вектор-столбец \mathbf{z} (здесь \wedge — символ поэлементной конъюнкции). Рассмотрим векторный канал, входом которого является вектор-столбец \mathbf{x} , а выходом вектор-столбец \mathbf{y} . Канал задается условиями

$$(3) \quad \begin{aligned} \forall \alpha \geq 2; \quad q > \alpha; \quad \mathbf{x} \in \mathbb{B}_q^1, \quad \mathbf{y} \in \mathbb{B}_q^\alpha, \quad \frac{1}{2} < p < 1, \\ p(\mathbf{x}) \triangleq \sum_{\mathbf{y} \in \mathbb{S}^1(\mathbf{x}, \alpha)} p(\mathbf{y} | \mathbf{x}) = p, \end{aligned}$$

т.е. входом канала всегда является двоичный вектор веса 1, а выходом двоичный вектор веса α ($\alpha \geq 2$), и каким бы ни был входной вектор, вектор на выходе покрывает его с вероятностью p ($\frac{1}{2} < p < 1$). Кроме того, потребуем выполнения дополнительных условий

$$(4) \quad \begin{aligned} \forall \mathbf{x} \in \mathbb{B}_q^1, \mathbf{y}_a \in \mathbb{S}^1(\mathbf{x}, \alpha), \mathbf{y}_b \in \mathbb{S}^1(\mathbf{x}, \alpha), a \neq b : p(\mathbf{y}_a | \mathbf{x}) = p(\mathbf{y}_b | \mathbf{x}) = p_1, \\ \forall \mathbf{x} \in \mathbb{B}_q^1, \mathbf{y}_n \in \mathbb{S}^0(\mathbf{x}, \alpha), \mathbf{y}_l \in \mathbb{S}^0(\mathbf{x}, \alpha), n \neq l : p(\mathbf{y}_n | \mathbf{x}) = p(\mathbf{y}_l | \mathbf{x}) = p_0. \end{aligned}$$

Выражения (3) могут быть интерпретированы следующим образом. Представим себе систему связи, использующую канал, состоящий из q непересекающихся подканалов. Будем считать, что однократное использование канала соответствует передаче одного q -ичного символа, причем каждому символу взаимно однозначно ставится в соответствие некоторый вектор веса 1 и длины q (такое отображение рассматривалось во многих работах, в частности, в [5]) и передача ведется по подканалу, соответствующему позиции ненулевого элемента в векторе, т.е. используется позиционная модуляция. Кроме полезного сигнала, на выходы подканалов могут влиять сигналы и аддитивные помехи различного рода (сигналы от других пользователей, преднамеренные помехи, фоновые шумы и т.п.). Приемник измеряет значения некоторого заранее определенного параметра (например, мощности) сигнала на выходе каждого из подканалов (будем называть такие величины “решающими статистиками”) и выбирает α номеров подканалов, которым соответствуют “лучшие” (в смысле некоторого критерия) значения решающих статистик (например, α подканалов, у которых мощность сигнала на выходе максимальна). Вероятность p в этом случае интерпретируется как вероятность того, что подканал, по которому передавался полезный сигнал, попал в список на выходе приемника. Условия (4) выполняются в случае, если аддитивные помехи передаются по тем или иным подканалам случайно и равновероятно. Для обеспечения выполнения этого условия достаточно использовать псевдослучайную перестановку на входе при передаче каждого символа (при этом перестановка должна выбираться равновероятно из всего множества возможных перестановок, заново при передаче каждого символа) и обратную перестановку на выходе.

Как уже было сказано, рассмотренная выше модель канала описывает широкий класс реальных систем связи, использующих позиционную модуляцию и передачу по физически разнесенным каналам, в частности многопользовательские каналы с однопользовательским приемом и каналы с аддитивными помехами различного рода. Заметим, что описанная выше модель отличается от дизъюнктивных векторных моделей, описывающих многопользовательские каналы [6] и каналы с аддитивными помехами [7], и модифицированной модели канала, предложенной в [8], так как вес вектора на выходе канала канала описываемого типа фиксирован. С другой стороны, как видно из (3) и (4), исследуемый канал принадлежит к классу дискретных симметричных (в смысле определения [9]) каналов без памяти. Переходные вероятности, характеризующие этот канал, равны

$$(5) \quad p_1 = \frac{p}{\sigma_1}, \quad p_0 = \frac{1-p}{\sigma_0},$$

где

$$(6) \quad \sigma_1 = |\mathbb{S}^1(\mathbf{x}, \alpha)| = \binom{q-1}{\alpha-1}, \quad \sigma_0 = |\mathbb{S}^0(\mathbf{x}, \alpha)| = \binom{q-1}{\alpha}.$$

Отличие модели канала рассматриваемого типа от обычных моделей дискретных симметричных каналов без памяти состоит в том, что в рассмотренной модели никакой символ на выходе нельзя однозначно отождествить

с каким-либо символом на входе, т.е. не существует понятия “ошибочного” (и, соответственно, “правильного”) приема одиночного символа. Сказанное, в частности, означает, что для рассматриваемого случая невозможно использовать классические границы, такие как [10, 11].

3. Кодирование и декодирование

Опишем теперь схему кодирования и декодирования для канала рассматриваемого типа. Будем считать, что информация кодируется линейным кодом $C(N, K, d)$ над полем $GF(q)$. Кроме того, будем считать, что известен спектр кода, т.е. для любого веса w ($d \leq w \leq N$) известно A_w — число слов данного веса в коде C :

$$\forall w : d \leq w \leq N \quad A_w = |\mathbf{v} \in C : w_H(\mathbf{v}) = w|.$$

Передача t -го символа v_t^m кодового слова \mathbf{v}^m сводится к передаче по каналу соответствующего этому символу двоичного вектора \mathbf{x}_t^m . Таким образом, передача кодового слова $\mathbf{v}^m = [v_1^m, \dots, v_N^m]$ в рассматриваемом случае сводится к передаче соответствующей этому кодовому слову матрицы $X^m = [\mathbf{x}_1^m, \dots, \mathbf{x}_N^m]$. Поэтому в дальнейшем будем говорить о “передаче кодового слова” и “передаче матрицы, соответствующей кодовому слову”, подразумевая, что эти выражения синонимичны.

Так как выход канала всегда представляет собой вектор веса α , каждой матрице $X^m = [\mathbf{x}_1^m, \dots, \mathbf{x}_N^m]$ (и, соответственно, каждому кодовому слову \mathbf{v}^m) на входе канала на выходе соответствует матрица $Y^j = [\mathbf{y}_1^j, \dots, \mathbf{y}_N^j]$, такая что $Y^j \in \mathbb{Y}$, где

$$(7) \quad \mathbb{Y} = \left\{ Y : Y = [\mathbf{y}_1, \dots, \mathbf{y}_N], \forall t : t = 1, \dots, N \quad \mathbf{y}_t \in \mathbb{B}_q^\alpha \right\}$$

— множество всех матриц, которые могут возникнуть на выходе канала. Пусть определена $\Theta(Y^j | X^l)$ — функция достоверности гипотезы о том, что в результате передачи матрицы X^l была принята матрица Y^j . Тогда декодирование сводится к поиску кодового слова \mathbf{v}^t , соответствующего матрице X^t такой, что выполняется

$$(8) \quad \forall l = 1, \dots, M \quad l \neq t \quad \Theta(Y^j | X^t) \geq \Theta(Y^j | X^l),$$

поэтому ниже для краткости будем именовать эту функцию функцией декодирования. Декодирование, таким образом, сводится к поиску матрицы, для которой выполняется (8). То, что неравенство в (8) нестрогое, означает, что при определенном выборе функции декодирования максимальное значение функции может достигаться на различных матрицах X^l . В дальнейшем будем считать, что в таких случаях матрица, соответствующая декодированному слову, выбирается случайно из всего множества матриц, для которых выполняется (8).

Так как канал, задаваемый (3), (4), является каналом без памяти и для передачи используется блочный код, в данной работе ограничимся рассмотрением случая, в котором функция декодирования имеет вид

$$(9) \quad \Theta(Y^j|X^l) = \prod_{t=1}^N \theta(y_t^j, \mathbf{x}_t^l),$$

где $X^l = [\mathbf{x}_1^l, \dots, \mathbf{x}_N^l]$ и $Y^j = [y_1^j, \dots, y_N^j]$. Выберем

$$(10) \quad \theta(\mathbf{x}, \mathbf{y}) = \begin{cases} \eta\theta & \mathbf{y} \in \mathbb{S}^1(\mathbf{x}, \alpha), \\ \theta & \mathbf{y} \in \mathbb{S}^0(\mathbf{x}, \alpha), \end{cases}$$

где $\eta > 1, \theta > 0$.

Такой выбор функции декодирования может быть интерпретирован следующим образом: считается, что гипотеза о том, что вектор-столбец, соответствующий переданному символу, покрывается соответствующим вектором-столбцом в принятой матрице (т.е. подканал, по которому передавался сигнал, попал в список α “лучших”), имеет в η раз более высокую достоверность, чем конкурирующая гипотеза. Заметим, что при выборе параметров функции декодирования в форме $\theta = p_0 = \frac{1-p}{\sigma_0}$, $\eta = \frac{p_1}{p_0} = \frac{p}{1-p} \frac{\sigma_0}{\sigma_1}$ описанный выше декодер эквивалентен декодеру по максимуму правдоподобия. В реальных системах связи вероятность p не может быть точно оценена приемником, поэтому важно отметить, что в настоящей работе будет получена граница для произвольного $\eta > 1$. Ниже будет показано, что при использовании описанного метода приема вероятность ошибки практически не зависит от величины параметра η .

4. Верхняя граница вероятности ошибки декодирования

Целью является получение верхней границы на вероятность ошибочного декодирования для рассматриваемого случая, а именно для случая, в котором для передачи по каналу, заданному (3), (4), используется линейный код с известным спектром и для декодирования используется описанное выше правило. Задача отыскания границ для кодированной передачи с использованием недвоичного кода с известным спектром изучена относительно плохо (по сравнению, например, с двоичным случаем, случаем случайных кодов и кодов с известной композицией) и, как правило, требует исследования свойств конкретного канала, причем зачастую полученные границы определяются не для конкретных кодов, а для ансамблей кодов и справедливы лишь для каналов, удовлетворяющих специфическим дополнительным условиям [12, 13]. Ниже будет приведен вывод верхней границы для канала, заданного (3), (4) и использующего конкретный недвоичный код с известным спектром, а также описанный в настоящем разделе критерий декодирования. Для вывода будут использованы классические подходы, предложенные Галлагером [11] и Фано [14], и граница Думана–Салехи [15], что позволит аналитически решить задачу оптимизации предлагаемой границы для канала рассмотренного типа.

Для того чтобы получить верхнюю границу на вероятность ошибочного декодирования, воспользуемся техникой, восходящей к работам Галлагера [11] и Фано [14]: разобьем все множество матриц, которые могут быть приняты из канала, на два непересекающихся подмножества. Первое подмножество, которое будем условно именовать “плохим” (и обозначать как \mathbb{Y}_B), будет включать принятые матрицы, для которых вероятность ошибки декодера велика; второе, условно именуемое “хорошим” (и обозначаемое как \mathbb{Y}_G), состоит из всех остальных матриц, которые могут появиться на выходе канала. Пусть передана матрица X^m . Тогда, учитывая, что $\mathbb{Y}_B \cap \mathbb{Y}_G = \emptyset$, можно утверждать, что

$$(11) \quad p(\text{err} | X^m) = p(\text{err}, Y \in \mathbb{Y}_B | X^m) + p(\text{err}, Y \in \mathbb{Y}_G | X^m),$$

где $p(\text{err} | X^m)$ – условная вероятность ошибки декодера, $p(\text{err}, Y \in \mathbb{Y}_B | X^m)$ – условная вероятность того, что на выходе канала матрица из “плохого” подмножества и произошла ошибка, $p(\text{err}, Y \in \mathbb{Y}_G | X^m)$ – условная вероятность того, что на выходе канала матрица из “хорошего” подмножества и произошла ошибка. Предполагается, что вероятность ошибки для матриц из “плохого” подмножества высока, можно записать

$$(12) \quad p(\text{err} | X^m) \leq p(Y \in \mathbb{Y}_b | X^m) + p(\text{err}, Y \in \mathbb{Y}_G | X^m).$$

Оценим первое слагаемое в правой части (12). Рассмотрим матрицы $X^0 = [\mathbf{x}_1^0, \dots, \mathbf{x}_N^0]$ (соответствующую переданному кодовому слову, которое без ограничения общности будем считать нулевым) и $Y = [\mathbf{y}_1, \dots, \mathbf{y}_N]$ (соответствующую принятой последовательности). Кроме того, рассмотрим множество

$$(13) \quad \mathbb{I}_c(Y, X^0) \triangleq \left\{ t : t \in \{1, \dots, N\}, \mathbf{y}_t \in \mathbb{S}^1(\mathbf{x}_t^0, \alpha) \right\}$$

– множество номеров столбцов матрицы Y , которые покрывают соответствующие столбцы матрицы X^0 (здесь $\mathbb{S}^1(\mathbf{x}_t^0, \alpha)$ – множество векторов-столбцов веса α , покрывающих t -й вектор-столбец матрицы X^0). Введем обозначение

$$(14) \quad i = |\mathbb{I}_c(Y, X^0)|.$$

Заметим, что, так как функция декодирования задана в форме (9), (10), вероятность ошибочного декодирования убывает с ростом i . Определим множество \mathbb{Y}_B следующим образом:

$$(15) \quad \mathbb{Y}_B = \left\{ Y : Y \in \mathbb{Y}, |\mathbb{I}_c(Y, X^0)| < T \right\},$$

где T – параметр, зависящий от p и удовлетворяющий условиям

$$(16) \quad T \in \mathbb{N}, \quad 1 \leq T \leq N - K.$$

При таком определении первое из двух слагаемых в правой части (12) может быть вычислено по формуле

$$(17) \quad p(Y \in \mathbb{Y}_b | X^m) = \sum_{i=0}^{T-1} \binom{N}{i} p^i (1-p)^{N-i}.$$

Для оценки второго слагаемого используется классический подход, который применялся во многих работах (в частности, в [11, 15]). Суть этого подхода в следующем: без ограничения общности будем считать, что по каналу было передано нулевое кодовое слово (или, точнее, матрица, соответствующая нулевому кодовому слову). Разобьем используемый код на подкоды, каждый из которых будет включать нулевое кодовое слово и все слова некоторого веса w . Обозначим множество матриц, соответствующих кодовым словам такого подкода, через \mathbb{S}_w , а все множество матриц, соответствующих различным кодовым словам кода C , через \mathbb{S}_C . В силу границы объединения верна оценка

$$(18) \quad \begin{aligned} & p(\text{err}, Y \in \mathbb{Y}_G | X^m) = \\ & = P\left(X^l = \arg \max_{t: X^t \in \mathbb{S}_C} (\Theta(Y | X^t)) \neq X^0, Y \in \mathbb{Y}_G | X^0\right) \leq \\ & \leq \sum_{w=d}^N P\left(X^l = \arg \max_{t: X^t \in \mathbb{S}_w} (\Theta(Y | X^t)) \neq X^0, Y \in \mathbb{Y}_G | X^0\right). \end{aligned}$$

Для получения аналитического выражения используем границу Думана – Салехи [15]. Для каждого из слагаемых в правой части (18) получим

$$(19) \quad \begin{aligned} & P\left(X^l = \arg \max_{t: X^t \in \mathbb{S}_w} (\Theta(Y | X^t)) \neq X^0, Y \in \mathbb{Y}_G | X^0\right) \leq \\ & \leq \left(\sum_{\substack{l \in \mathbb{S}_w \\ l \neq 0}} \sum_{Y \in \mathbb{Y}_G} (p_N(Y | X^0))^{\frac{1}{\rho}} (\psi_N^0(Y))^{1-\frac{1}{\rho}} \left(\frac{\Theta(Y | X^l)}{\Theta(Y | X^0)} \right)^s \right)^{\rho}, \end{aligned}$$

где ρ и s — параметры, которые будут выбираться с учетом ограничений

$$(20) \quad 1 \geq \rho > 0, \quad s > 0$$

таким образом, чтобы минимизировать оценку (19), а $\psi_N^m(Y)$ — функция перекоса, которая зависит от принятой матрицы Y и (в общем случае) от матрицы X^m , соответствующей переданному слову, и удовлетворяет условиям

$$(21) \quad \forall Y \in \mathbb{Y} \quad \psi_N^m(Y) > 0, \quad \sum_{Y \in \mathbb{Y}_G} \psi_N^m(Y) = 1.$$

Параметры ρ и s имеют тот же смысл, что и соответствующие параметры в границе Галлагера [11], и потому также должны выбираться таким образом, чтобы минимизировать правую часть (19). Функция перекоса также должна выбираться таким образом, чтобы минимизировать правую часть (19).

Остальная часть этого раздела будет посвящена именно оптимальному выбору функции перекоса, учитывающему специфику модели канала (3), (4).

В силу требований, предъявляемых к функции $\psi_N^0(Y)$, эта функция должна зависеть только от Y и, возможно, от X^0 , поэтому естественно потребовать, чтобы значение этой функции для каждой матрицы Y зависело от числа столбцов в матрице X^0 , которые покрывает матрица Y^j . В дальнейшем будем полагать, что функция $\psi_N^0(Y)$ имеет вид

$$(22) \quad \forall Y = [\mathbf{y}_1, \dots, \mathbf{y}_N] : i = |\{t : \mathbf{y}_t \in \mathbb{S}^1(\mathbf{x}_t^0, \alpha)\}| \quad \psi_N^0(Y) = \Psi_i,$$

где Ψ_i — переменные, оптимальные значения которых будут найдены ниже. Введем обозначение

$$(23) \quad \Omega(Y, X^0, X^l) = \left(\frac{\Theta(Y|X^l)}{\Theta(Y^j|X^0)} \right) = \prod_{j=1}^N \omega(\mathbf{x}_j^0, \mathbf{x}_j^l, \mathbf{y}_j),$$

где $\omega(\mathbf{x}_j^0, \mathbf{x}_j^l, \mathbf{y}_j)$ имеет вид

$$(24) \quad \omega(\mathbf{x}_j^0, \mathbf{x}_j^l, \mathbf{y}_j) = \frac{\theta(\mathbf{x}_j^l, \mathbf{y}_j)}{\theta(\mathbf{x}_j^0, \mathbf{y}_j)}.$$

Заметим, что в силу (10) каждый из сомножителей $\omega(\mathbf{x}_j^0, \mathbf{x}_j^l, \mathbf{y}_j)$ в правой части (23) отличен от единицы в том и только том случае, если j -й столбец матрицы Y покрывает соответствующий столбец одной из матриц (X^0 или X^l) и не покрывает соответствующий столбец другой матрицы. Введем следующие обозначения: k — число столбцов матрицы Y таких, что эти столбцы Y покрывают соответствующие столбцы матрицы X^l и не покрывают соответствующие столбцы матрицы X^0 ; g — число столбцов матрицы Y таких, что эти столбцы Y покрывают соответствующие столбцы матрицы X^0 и не покрывают соответствующие столбцы матрицы X^l .

Тогда функция $\Omega(Y, X^0, X^l)$ принимает значение

$$(25) \quad \Omega(Y, X^0, X^l) = \eta^{k-g}.$$

Пусть матрицы X^0 и X^l отличаются в w столбцах. Обозначим переменной h число столбцов таких, что матрицы X^0 и X^l различаются в этих столбцах, а матрица Y покрывает в этих столбцах матрицу X^0 . Заметим, что верно неравенство $\max(i + w - n, 0) \leq h \leq \min(i, w)$. Для каждого набора значений четверки параметров i, h, g и k число матриц Y , для которых эти параметры имеют соответствующие значения, равно

$$(26) \quad \begin{aligned} & \mathbb{H}(N, w, i, h, g, k) = \\ & = \binom{N-w}{i-h} \sigma_1^{i-h} \sigma_0^{N-w-i+h} \binom{w}{h-g, g, k} v_{\langle 1,1 \rangle}^{h-g} v_{\langle 1,0 \rangle}^g v_{\langle 0,1 \rangle}^k v_{\langle 0,0 \rangle}^{w-h-k}, \end{aligned}$$

где σ_1 и σ_0 задаются (6), а $v_{\langle 1,1 \rangle}$, $v_{\langle 1,0 \rangle}$, $v_{\langle 0,1 \rangle}$ и $v_{\langle 0,0 \rangle}$ задаются выражениями

$$(27) \quad v_{\langle 1,1 \rangle} = \binom{q-2}{\alpha-2}, \quad v_{\langle 1,0 \rangle} = \binom{q-2}{\alpha-1}, \quad v_{\langle 0,1 \rangle} = \binom{q-2}{\alpha-1}, \quad v_{\langle 0,0 \rangle} = \binom{q-2}{\alpha}.$$

Заметим также, что вероятность появления каждой из матриц на выходе канала зависит только от i (количества столбцов X^0 , которые покрывает Y) и равна

$$(28) \quad p(Y | X^0) = p_1^i p_0^{N-i} = \left(\frac{p}{\sigma_1}\right)^i \left(\frac{1-p}{\sigma_0}\right)^{N-i}.$$

Заметим, что

- а) значения $\Omega(Y, X^0, X^l)$ пробегает одни и те же значения для любых пар X^0 и X^l , зависят от числа столбцов, в которых X^0 и X^l различаются (это число фиксировано для конкретного подкода, из которого выбираются кодовые слова, соответствующие X^l), и не зависят от конкретной матрицы X^l ;
- б) для любых X^l число матриц на выходе канала Y , которым для тройки X^0, X^l, Y соответствуют конкретные значения g и k , пробегает одни и те же значения $H(N, w, i, h, g, k)$ и не зависит от конкретной матрицы X^l .

Таким образом, ни один из сомножителей в правой части (19) не зависит от номеров кодовых слов подкода, по которым ведется суммирование. С учетом полученных выше соотношений (26), (28), (25), (22) выражение (19) можно записать в виде

$$(29) \quad p(\text{err}, Y \in \mathbb{Y}_G | X^m) \leq \left(\sum_{\substack{X^l \in \mathbb{S}_w \\ l \neq 0}} \sum_{i=T}^N \beta_i(s, \rho) \Psi_i \left(1 - \frac{1}{\rho}\right) \right)^\rho,$$

где $\beta_i(s, \rho)$ имеет вид

$$(30) \quad \beta_i(s, \rho) = \sum_{h=h_l}^{h_u} \sum_{g=0}^h \sum_{k=0}^{w-h} \left(H(N, w, i, h, g, k) p_1^{\binom{i}{\rho}} p_0^{\binom{N-i}{\rho}} \eta^{s(k-g)} \right).$$

Подчеркнем, что ни коэффициенты $\beta_i(s, \rho)$, ни значения функции перекоса Ψ_i не зависят от номера кодового слова l (при условии, что все кодовые слова находятся на расстоянии w от переданного кодового слова). Следовательно, выражение (29) может быть записано в следующем виде:

$$(31) \quad p(\text{err}, Y \in \mathbb{Y}_G | X^m) \leq (A_w)^\rho \left(\sum_{i=T}^N \beta_i(s, \rho) \Psi_i \left(1 - \frac{1}{\rho}\right) \right)^\rho.$$

Отметим, что A_w не зависит от s и ρ (и вообще от каких-либо параметров системы, кроме выбора кода C и величины веса w), а функция вида $z(\xi) = \xi^\rho$

является монотонно возрастающей функцией ξ при $0 > \rho \geq 1$. Поэтому для того, чтобы минимизировать правую часть (31) при любых фиксированных значениях w , s и ρ , удовлетворяющих исходным условиям ($1 \geq \rho > 0$, $s > 0$), достаточно выбрать вектор $\Psi = [\Psi_0, \Psi_1, \dots, \Psi_N]$ значений функции $\psi_N^0(Y)$ таким образом, чтобы минимизировать функцию

$$(32) \quad f_0(w, \psi_N^0(Y)) = \sum_{i=T}^N \beta_i(s, \rho) \Psi_i^{\left(1-\frac{1}{\rho}\right)}.$$

С учетом (22) и ограничений (21) эта оптимизационная задача может быть записана в следующем виде

$$(33a) \quad \sum_{i=T}^N \beta_i(s, \rho) \Psi_i^{\left(1-\frac{1}{\rho}\right)} \xrightarrow{\Psi} \min,$$

$$(33b) \quad \forall i = T, \dots, N \quad \Psi_i > 0 \quad \sum_{Y \in \mathbb{Y}_G} \psi_N^0(Y) = \sum_{i=T}^N \gamma_i \Psi_i = 1,$$

где

$$(34) \quad \gamma_i = \binom{N}{i} \sigma_1^i \sigma_0^{N-i}.$$

Записав условия Каруша – Куна – Таккера для этой задачи, можно показать, что единственным решением является точка

$$(35) \quad \forall i = T, \dots, N \quad \Psi_i = \left(\sum_{i=0}^N \gamma_i^{1-\rho} \beta_i^\rho \right)^{-1} \left(\frac{\beta_i}{\gamma_i} \right)^\rho.$$

Найденное аналитическое выражение (35) для функции перекоса (22) минимизирует правую часть (31) (для канала рассматриваемого типа) при любых фиксированных ρ и s (удовлетворяющих (20)). Подставляя (35) в (31) и учитывая (12) и (17), получим границу:

$$(36) \quad P_e \leq \sum_{i=0}^{T-1} \binom{N}{i} p^i (1-p)^{N-i} + \sum_{w=d}^N A_w^\rho \left(\sum_{i=T}^N (\beta_i(s, \rho, w))^\rho \gamma_i^{1-\rho} \right).$$

Параметры ρ , s и T находятся численной оптимизацией для каждого конкретного значения p (с учетом ограничений (20), (16)), как это традиционно делается для границы Галлагера и других границ, полученных с использованием техник из [11, 14]. В следующем параграфе будут приведены результаты имитационного моделирования.

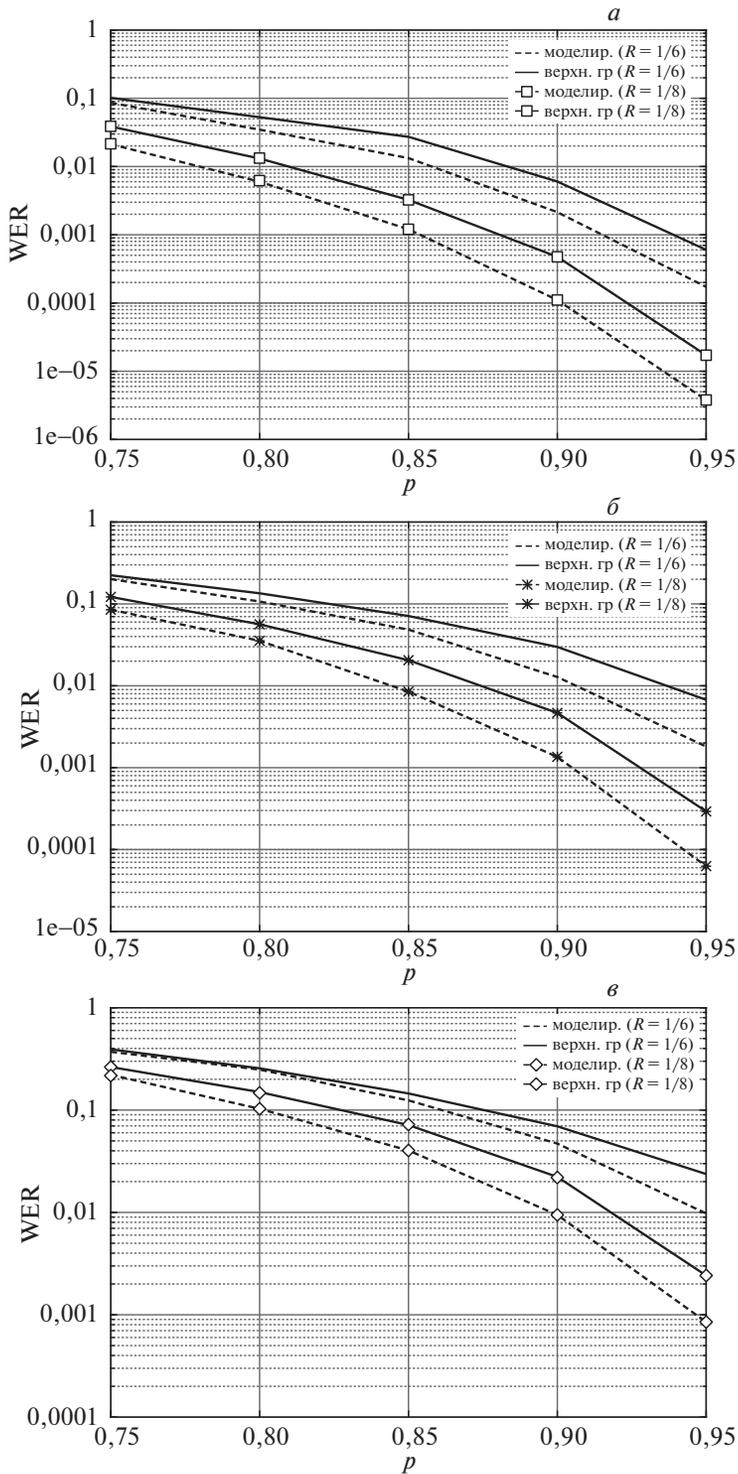


Рис. 1. Зависимость вероятности ошибки WER от вероятности p для $\eta = 12$ и различных α ($a - \alpha = 3$, $б - \alpha = 4$, $в - \alpha = 5$).

5. Моделирование

Для проверки эффективности используемого метода и корректности результатов было проведено имитационное моделирование. При моделировании использовались МДР коды со скоростями $R = 1/6$, $R = 1/7$ и $R = 1/8$ над $GF(2^4)$, полученные из кода Рида – Соломона (15,2,14) выкалыванием проверочных символов (для скоростей $R = 1/6$ и $R = 1/7$) или, напротив, добавлением общей проверки на четность (для скорости $R = 1/8$). В качестве примера на рис. 1 приведено сравнение кривых вероятности ошибки (на кодовое слово) WER в зависимости от вероятности p для скоростей $R = 1/6$ и $R = 1/8$ для различных значений α ($\alpha = 3$, $\alpha = 4$ и $\alpha = 5$).

Как видно из приведенных графиков, предложенное выше выражение действительно позволяет оценить вероятность ошибки сверху, причем точность оценки падает с ростом вероятности p . На рис. 2 приведено сравнение кривых вероятности ошибки (на кодовое слово) WER в зависимости от вероятности p для скорости $R = 1/7$ для $\alpha = 4$ и различных значений параметра η .

Анализируя приведенные графики, можно заметить, что экспериментально полученные кривые вероятности ошибки практически не отличаются для различных величин параметра η . Это подтверждает, что рассматриваемый метод приема (и декодирования) устойчив к изменениям параметра η и, следовательно, не требует информации о распределении решающих статистик и о параметрах таких распределений. Та же особенность присуща и вычисленным с использованием (36) оценкам вероятности.

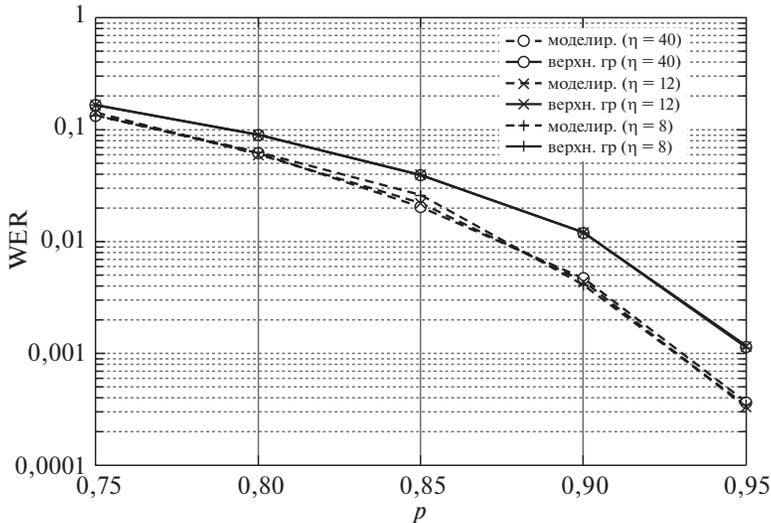


Рис. 2. Зависимость вероятности ошибки WER от вероятности p для $\alpha = 4$, $R = 1/7$.

6. Заключение

В работе рассмотрена модель канала без памяти, описывающего однопользовательский прием на основе порядковых статистик в многопользовательских каналах и каналах с аддитивными помехами. Для передачи по такому

каналу предложено использовать конструкцию Каутса-Синглтона. Предложен метод декодирования, не требующий информации о характеристиках канала и характере аддитивных помех, и получена верхняя граница вероятности ошибки декодирования (на кодовое слово). Состоятельность предложенной верхней границы и устойчивость предлагаемой стратегии приема и декодирования к выбору параметра η подтверждены результатами имитационного моделирования.

СПИСОК ЛИТЕРАТУРЫ

1. *Osipov D.* Reduced-Complexity Robust Detector in a DHA FH OFDMA System under Mixed Interference Multiple Access Communications // MACOM – 7th Int. Work. on Mult. Acc. Comm., Halmstad, Sweden, John Wiley & Sons, 2014. P. 29–34.
2. *Viswanathan R., Gupta S.*, Nonparametric Receiver for FH-MFSK Mobile Radio // IEEE Trans. Commun. 1985. V. 33. No. 2. P. 178–184.
3. *Kreshchuk A., Potapov V.* On applying one-sample goodness-of-fit statistics to coded FSK decoding // REDUNDANCY 2016 – XV Int. Symp. Probl. Redund. Inf. Contr. Syst., St. Petersburg, Russia, IEEE, 2016. P. 66–70.
4. *Osipov D.* An upper bound on the error probability of a communication system with nonparametric detection // REDUNDANCY 2016 – XV Int. Symp. Probl. Redund. Inf. Contr. Syst., St. Petersburg, Russia, IEEE, 2016. P. 100–104.
5. *Kautz W.H., Singleton R.C.* Nonrandom Binary Superimposed Codes // IEEE Transact. Inform. Theory. 1964. No. 4. P. 363–377.
6. *Chang S.C., Wolf J.K.* On the T-User M-Frequency Noiseless Multiple-Access Channels with and without Intensity Information // IEEE Trans. Inform. Theory 1981. V. 27. No. 1. P. 41–48.
7. *Зигангиров К.Ш., Попов С.А., Чепыжов В.В.* Недвоичное сверточное кодирование в канале с преднамеренными помехами // ППИ. 1995. Т. 31. № 2. С. 84–101.
8. *Осипов Д.С., Фролов А.А., Зяблов В.В.* О пропускной способности для пользователя системы множественного доступа в векторном дизъюнктивном канале при наличии ошибок // ППИ. 2013. Т. 49. № 4. С. 13–27.
9. *Cover T.M., Thomas J.A.* Elements of Information Theory. N.Y.: Wiley, 2006.
10. *Herzberg H., Poltyrev G.* Techniques of bounding the probability of decoding error for block coded modulation structures // IEEE Trans. Inform. Theory. 1994. V. 40. No. 3. P. 903–911.
11. *Gallager R.G.* A simple derivation of the coding theorem and some applications // IEEE Trans. Inform. Theory. 1965. V. 11. No. 1. P. 3–18.
12. *Bennatan A., Burshtein D.* On the application of LDPC codes to arbitrary discrete-memoryless channels // IEEE Trans. Inform. Theory. 2004. V. 50. No. 3. P. 417–438.
13. *Erez U., Miller G.* The ML decoding performance of LDPC ensembles over \mathbb{Z}_q // IEEE Trans. Inform. Theory. 2005. V. 51. No. 5. P. 1871–1879.
14. *Fano R.M.* Transmission of Information. M.I.T Press and John Wiley & Sons, 1961.
15. *Duman T.M., Salehi M.* New performance bounds for turbo codes // IEEE Trans. Commun. 1998. V. 46. No. 6. P. 717–723.

Статья представлена к публикации членом редколлегии В.М. Вишневым.

Поступила в редакцию 10.12.2018

После доработки 26.06.2019

Принята к публикации 18.07.2019