УДК 621.391.019.4

КАЧЕСТВО ПЕРЕДАЧИ ДИСКРЕТНЫХ СООБЩЕНИЙ ПО КАНАЛУ СВЯЗИ С ПОМЕХАМИ

М. В. Литвин *

Нижегородский госуниверситет им. Н. И. Лобачевского, г. Нижний Новгород, Россия

В статье рассмотрена передача дискретных сообщений с использованием кодов на основе теоремы Шеннона, леммы Файнстейна и кодов Хэмминга. При этом оценка качества передачи выполнена с использованием не случайных, а детерминированных связей между сообщениями и сигналами. Показано, что избыточность кодирования, как и условие безошибочной передачи, не являются достаточными для реализации такой передачи. Более точным параметром, определяющим качество передачи, является отношение сигнал/шум. Только при превышении его пороговой величины применение кода Хэмминга для длинных последовательностей сообщений становится эффективным.

ВВЕДЕНИЕ

Условия передачи дискретных сообщений s_* по каналу связи с помехами определяются теоремой Шеннона. Сообщения могут быть переданы со сколь угодно малой вероятностью ошибок $P_{\text{err}} = 2^{-k[C-H(s_*)/T_s]}$, если производительность источника сообщений $H(s_*)/T_s$ (где H — энтропия) не превышает пропускную способность канала связи C, а количество сообщений в передаваемой группе k не ограничено [1, с. 40–41]. Возможность безошибочной передачи в этих условиях обеспечивается системой избыточного кодирования. Полезность избыточности в том, что часть множества искажённых помехой сообщений может быть связана с передаваемыми сообщениями. Поэтому около них можно выделить непересекающиеся группы искажённых сообщений и считать, что искажения при приёме этих групп допустимы. Очевидно, что такое правило принятия решений соответствует принципу максимального правдоподобия или близости между переданным и принятым сигналами [2, с. 423].

Исследование методов кодирования является классической задачей, связанной с передачей информации. В работах [2–5] исследуются различные коды и их свойства, устройства кодирования и декодирования. Большое внимание уделяется кодам с возможностью определения искажённого помехой элемента и восстановления его истинного значения. Реализация этих операций связывается с наличием избыточности кодирования, что позволяет проводить проверки кодов на чётность или использовать для этого синдромы [3, с. 386–387].

Следует заметить, что в работах [2–5] не рассматривается использование различных кодов для передачи сообщений в соответствии с теоремой Шеннона. Однако именно коды с избыточностью представляются наиболее перспективными для передачи сообщений со сколь угодно малыми ошибками. Эффективность их следует из более строгого доказательства теоремы Шеннона [6, 7]. В этом доказательстве исследованы свойства канала связи, подверженного действию помех, и доказано, что количество сообщений в длинной последовательности, переданных без ошибок, определяется пропускной способностью канала связи и равно $N = 2^{kCT_s}$ (лемма Файнстейна) [7]. Поэтому для авторов доказательств, приведённых в работах [6, 7], представляется очевидной возможность использования $N = 2^{kCT_s}$ сообщений для безошибочной передачи сообщений другого источника s_*. При этом необходимо и достаточно, чтобы их количество $N_* = 2^{kH(s_*)}$ не

* mlit.post@yandex.ru

превышало $N = 2^{kCT_s}$, что приводит к условию безошибочной передачи $H(s_*) \le CT_s$ [1, с. 40–41]. При этом в работах [6, 7] нет примеров, из которых было бы видно, каким образом применение вышеуказанных теоремы и леммы позволяет на основе кодов с избыточностью реализовать безошибочную передачу сообщений. В работе [1, с. 43–44] лишь кратко упоминается об избыточности англоязычного текста и об увеличении его длительности, которые оказываются полезными при передаче с помехами, а в работе [5, с. 31–32] говорится о многократном повторении передач.

В связи с этим представляется интересным исследовать возможности применения известных кодов с избыточностью [2, 3] для передачи дискретных сообщений с кодированием на основе методов Файнстейна и Хэмминга. В обоих случаях коды обладают избыточностью, однако способы её формирования различны [5, 6]. Поэтому далее рассматривается влияние этих различий на качество передачи сообщений. Для этого исследуются свойства канала связи, статистика гипотез на выходе канала, формирование областей принятия гипотез и оценки качества передачи. При этом учитываются условия безошибочной передачи сообщений, определяемые теоремой Шеннона.

1. КАНАЛ СВЯЗИ

В работах [1–3, 5–7] не конкретизируются виды сигналов, способы их обработки и используемые коды. Основная идея безошибочной передачи связана с использованием последовательности сигналов (сообщений), количество которых k может неограниченно увеличиваться. В связи с этим, далее рассмотрим источник, создающий M равновероятных сообщений через интервал времени T_s. Для кодирования сообщений и последующей обработки сигналов при приёме удобно нумеровать сообщения двоичными числами с $n_s \approx \log_2 H$ разрядами. Кодирование сообщения заключается в образовании сигнала, структура которого повторяет последовательность разрядов передаваемого сообщения. Для этого можно использовать различные сигналы с амплитудной, частотной и фазовой модуляцией, а также реализации шума [3, с. 147–156].

Известно, что энергетические затраты при передаче минимальны при использовании сигналов с активной паузой и, в частности, сигналов с противоположными значениями сигнальных функций $\pm\tilde{s}(t)$, называемых антиподными [2, с. 202]. Если $M = 2$, то достаточно пары таких сигналов. Оптимальная обработка сигналов в условиях действия белого гауссова шума проводится с использованием согласованного с сигналом $\tilde{s}(t)$ фильтра. Применение критерия максимальной апостериорной вероятности приводит к следующим условным вероятностям гипотез H, определяющих качество передачи отдельных сообщений S_1 и S_2 [3, с. 217]:

$$P_{\mathrm{cor}\,1} = P(H_1 \mid S_1) = P_{\mathrm{cor}\,2} = P(H_2 \mid S_2) = \frac{1 + \Phi(\sqrt{\rho_s})}{2} = P_1,$$
$$P_{\mathrm{err}\,1} = P(H_2 \mid S_1) = P_{\mathrm{err}\,2} = P(H_1 \mid S_2) = P_0 = 1 - P_1. \qquad (1)$$

Здесь $\Phi(x) = (2/\sqrt{2\pi}) \int_0^x \exp(-t^2/2)\,\mathrm{d}t$ — интеграл вероятности, $\rho_s = g_0^{-1} \int_0^{T_s} s^2(t)\,\mathrm{d}t$ — отношение сигнал/шум, g_0 — спектральная плотность мощности шума. Вероятности в выражении (1) удобно представить матрицей 2×2 для сообщений и гипотез, где на главной диагонали расположены вероятности истинных гипотез, а на другой — ложных.

Если передаются два последовательных сообщения (например $k = 2$), то число сообщений возрастает до M^k. В случае двух сообщений возможны их комбинации S_1, S_1; S_1, S_2; S_2, S_1; S_2, S_2, для передачи которых используются прежние сигналы $\pm\tilde{s}(t)$. Поскольку последовательности сигналов коррелированны, то их оптимальная обработка возможна на основе анализа результатов обработки отдельных сообщений. Если учесть, что выборки напряжений на выходе согласованного фильтра некоррелированы, то эти условные вероятности просто определяются через вероятности (1). При этом матрица условных вероятностей имеет размер 4×4. Вероятности истинных и лож-

ных гипотез располагаются указанным выше образом на её диагоналях. Кроме вероятностей истинных гипотез P_1^2, каждая строка содержит вероятности ложных гипотез P_1P_0, P_0P_1, P_0^2.

Таблица 1

	$h=00$	$h=01$	$h=10$	$h=11$
$s=00$	0	1	1	2
$s=01$	1	0	2	1
$s=10$	1	2	0	1
$s=11$	2	1	1	0

Следует отметить, что более интересна матрица искажений, элементы которой определяют условные вероятности гипотез и в то же время позволяют просто определить правила трансформации матрицы при увеличении k. Так, в приведённых выше вероятностях гипотез числа искажений составляют 0; 1; 1; 2 соответственно, т. е. эти искажения связаны с ошибочными решениями в передаваемой последовательности сообщений. Вид матрицы искажений приведён в табл. 1. Двоичные числа представляют структуру передаваемых сообщений s в указанной выше последовательности и соответствующие им гипотезы h, а искажения располагаются на пересечении сообщений и гипотез. Количество искажений определяется как квадрат эвклидова расстояния между точками, отображающими сообщения и гипотезы в пространстве двух измерений, или как расстояние Хэмминга, т. е. логическая сумма двоичных чисел, определяющих сообщение и гипотезу [5, с. 41]. Главная диагональ матрицы содержит нулевые искажения, другая — максимальные. Видим, что матрица искажений содержит четыре матрицы 2×2, из которых вдоль главной диагонали расположены матрицы для случая передачи двух сообщений при $k = 1$. Остальные матрицы отличаются от них на единичную матрицу 2×2.

Нетрудно показать, что это правило справедливо для любого k. Действительно, при переходе от матрицы с размером $2^k \times 2^k$ к матрице с размером $2^{k+1} \times 2^{k+1}$ последняя содержит четыре предшествующих матрицы. При этом разрядность используемого двоичного числа увеличивается на единицу. Поэтому, если матрица с размером $2^k \times 2^k$, расположенная в левом верхнем углу, смещается вправо или вниз, то количество искажений увеличивается на единицу, поскольку двоичные числа, соответствующие сообщениям и гипотезам для этих матриц, различаются на единицу. При смещении по диагонали двоичные числа изменяются на единицу, как для сообщений, так и для гипотез, что оставляет искажения неизменными. Например, при $k = 3$ имеем матрицу с размером 8×8 ($2^k \times 2^k$), в первой строке которой содержатся искажения 0; 1; 1; 2; 1; 2; 2; 3, т. е. при переходе от $k = 1$ к $k = 3$ дважды произошло удвоение размера начальной матрицы с размером 2×2 с соответствующим изменением искажений. Ещё одна особенность таких матриц состоит в том, что они симметричны. Это следует из того, что количество искажений остаётся прежним, если меняются местами сообщения и гипотезы (строки и столбцы).

Число случаев с одинаковыми искажениями i в строке матрицы определяется сочетаниями C_k^i, а условная вероятность гипотезы при приёме с i искажениями с учётом (1) равна

$$P_{s,h,i} = P_1^{k-i} P_0^i. \tag{2}$$

При $i = 0$ имеем условную вероятность истинной гипотезы $P_{s,h,0} = P_{ss} = P_1^k$. Сумма всех вероятностей в строках матрицы, $\Sigma_{i=0}^k C_k^i P_1^{k-i} P_0^i$, равна 1 т. е. вероятности (2) исчерпывают все возможные события при передаче k сообщений.

Если источник создаёт на интервале T_s более двух сообщений, то их число $M = 2^{n_s}$ выражается через энтропию $n_s > 1$. Особенность этого случая состоит в том, что при сохранении при передаче прежней мощности следует уменьшить в n_s раз длительность сигналов $\pm\tilde{s}(t)$ и, соответственно, отношение сигнал/шум при оценке вероятностей (1). Заметим, что матрица искажений $2^{n_s} \times 2^{n_s}$ получается в этом случае в результате рассмотренной выше трансформации матрицы с размером 2×2, соответствующей передаче двух сообщений. Если M сообщений передаются

последовательно k раз, то число сообщений и гипотез увеличивается до 2^{kn_s}. Поэтому имеем матрицу искажений с размером $2^{kn_s} \times 2^{kn_s}$, свойства которой аналогичны матрице из табл. 1. Таким образом, можно полагать, что матрицы для M сообщений располагаются в ряду матриц $2^k \times 2^k$ с интервалом $k_1 = n_s$. Выражения для вероятностей гипотез (2) и количества искажений в строках матрицы, определяемые числом сочетаний $C^i_{kn_s}$, остаются прежними.

Таким образом, для оценки качества передачи сообщений удобно пользоваться матрицами искажений, свойства которых просто связаны с количеством сообщений, создаваемых их источником и содержащихся в передаваемой последовательности. Далее эти свойства будут использованы для оценки качества передачи.

2. ЛЕММА ФАЙНСТЕЙНА И КОДИРОВАНИЕ

Рассмотрим теперь, какое качество передачи сообщений может быть реализовано, если следовать результатам вышеуказанной леммы и использовать коды с избыточностью [2, с. 362]. Прежде всего, надо заметить, что в этой лемме доказывается справедливость определения пропускной способности канала связи [1, с. 38–41]. Действительно, из соотношения для энтропии источника на входе канала связи и количества информации на его выходе $I_{\text{exit}}(s) = H(s) - H(s \mid h) \to CT_s$ следует, что количество сообщений, переданных без ошибок в длинной последовательности с вероятностью P, сколь угодно близкой к единице, равно $N \approx 2^{kCT_s}$. Поэтому группа из N сообщений названа в лемме различимой, т. е. передаваемой без ошибок. В связи с этим предполагается, что использование данных сообщений в качестве сигналов позволит передать другие сообщения s_* тоже без ошибок [7]. Необходимо лишь, чтобы $N \approx 2^{kCT_s}$ было достаточным числом сообщений, т. е. должно выполняться условие теоремы Шеннона $2^{kH(s_*)} \leq 2^{kCT_s}$. Поскольку в канале с помехами $CT_s < H(s)$, то ясно, что при такой передаче сообщений s_* используется код с избыточностью.

Оценим подробнее качество передачи дискретных сообщений, чтобы убедиться в возможности или невозможности реализации вероятности истинной гипотезы с упомянутой выше величиной $P \to 1$. Пусть источник сообщений s создаёт 2^{n_s} равновероятных сообщений на интервале T_s, а источник s_* — $2^{n_{s*}}$ сообщений на том же интервале. В соответствии с леммой для передачи сообщений s_* необходимо использовать 2^{kCT_s} различимых сообщений s. Рассмотрим сначала случай $H(s_*) = n_{s_*} = CT_s$. Ясно, что это условие может быть выполнено с учётом выражения (1) и выражения $CT_s = n_s(1 + P_1 \log_2 P_1 + P_0 \log_2 P_0)$.

Качество передачи просто определить, используя матрицы искажений, аналогичные представленным в табл. 1 . При передаче k последовательных сообщений s матрица искажений имеет размер $2^{kn_s} \times 2^{kn_s}$. Согласно лемме, для передачи сообщений s_* необходимо выбрать $2^{kCT_s} = 2^{kn_{s*}}$ различимых сообщений s. Интервал между ними $\Delta N = 2^{kn_s}/2^{kCT_s}$ определяется ненадёжностью канала $H(s \mid h) = H(s) = CT_s$ [1, с. 37]. Эта ситуация иллюстрируется диаграммой сообщений на рис. 1 [1, с. 42]. Действие помех при использовании для передачи сообщения s_μ приводит к существованию «веера» неопределённости на приёмной стороне, содержащего $2^{kH(h|s)} = 2^{k(n_s - n_{s*})}$ гипотез. Согласно лемме, именно эта неопределённость определяет допустимую близость между используемыми сообщениями s. Очевидно, что допустимое количество сообщений $s_{*\mu}$ определяется условием $\mu \in [1, 2^{kCT_s}]$. При этом выполняется ещё одно условие леммы об отсутствии общих точек у «вееров» неопределённости [7, с. 57].

Матрицу искажений для сообщений s (далее называем её большой) можно считать состоящей из малых матриц с размером $2^{k(n_s - n_{s*})} \times 2^{k(n_s - n_{s*})}$, соответствующих тем сообщениям s, которые используются для передачи сообщений s_*. Заметим, что количество малых матриц в строке (столбце) большой матрицы равно $2^{kn_s}/2^{k(n_s - n_{s*})} = 2^{kn_{s*}}$, т. е. определяется числом передаваемых сообщений s_*. В разделе 1 показано, что матрицы искажений реализуются при расширении

матрицы элементарного сообщения с $n_s = 1$. При этом каждое смещение вправо и вниз увеличивает матрицу на единичную матрицу, а смещение по диагонали происходит без её изменения (2). В результате такого расширения малая матрица содержит $i \in [0, k(n_s - n_{s_*})]$ искажений, среди которых имеется $C^i_{k(n_s-n_{s_*})}$ одинаковых. Аналогичные изменения происходят и в большой матрице. Поэтому в $2^{kn_{s*}}$ малых матрицах первой строки, начиная с первой, количество искажений увеличивается на $\nu \in [0, kn_{s_*}]$. При этом число одинаковых искажений равно $C^\nu_{kn_{s*}}$.

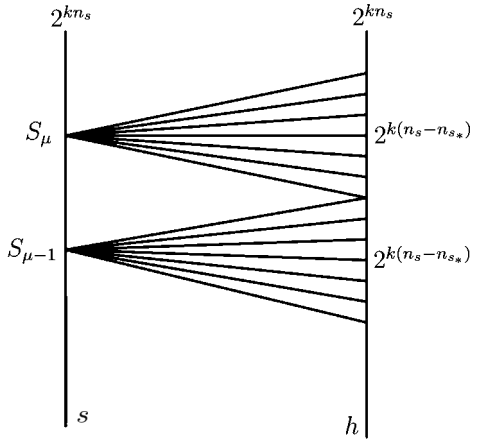

Рис. 1

Условные вероятности гипотез определяются с учётом всех допустимых искажений i, расположенных в пределах малых матриц. Кроме этого, в зависимости от положения матрицы в строке добавляются упомянутые выше ν искажений. Таким образом, получаются вероятности для всех возможных гипотез. Обозначим вероятности гипотез через $P_{\nu,s,k}$. Здесь ν и s соответствуют рассматриваемой гипотезе, которая определяется количеством искажений, и передаваемому сообщению, а k задаётся длиной последовательности сообщений. Если $\nu = 0$, то имеем вероятность истинной гипотезы, при иных ν — вероятности ложных. Если учесть вероятность (2) и свойства матриц искажений, то для условных вероятностей гипотез получаем

$$P_{\nu,s,k} = \sum_{i=0}^{k(n_s-n_{s_*})} C^i_{k(n_s-n_{s_*})} P_1^{kn_s-i-\nu} P_0^{i+\nu} = \\ = P_1^{kn_{s*}-\nu} P_0^\nu \sum_{i=0}^{k(n_s-n_{s_*})} C^i_{k(n_s-n_{s_*})} P^{k(n_s-n_{s_*})-i} P_0^i = P_1^{kn_{s*}-\nu} P_0^\nu. \quad (3)$$

Выше упоминалось, что гипотезы, определяемые вероятностями (3), исчерпывают все возможные события при передаче сообщений s_*. Справедливость этого подтверждается соотношением

$$\sum_{\nu=0}^{kn_{s*}} C^\nu_{kn_{s_*}} P_{\nu,s,k} = \sum_{\nu=0}^{kn_{s*}} C^\nu_{kn_{s_*}} P_1^{kn_{s*}-\nu} P_0^\nu = 1. \quad (4)$$

Как указывалось выше, вероятность истинной гипотезы соответствует $\nu = 0$ в выражении (3). Поэтому справедливо соотношение

$$P_{0,s,k} = P_{ss,k} = P_1^{kn_{s*}} \le P_1. \quad (5)$$

Из полученной формулы следует, что $P_{ss,k} \le P_1$, причём это и неравенство усиливается при увеличении k. Получается, что при кодировании согласно лемме увеличение количества передаваемых сообщений не обеспечивает необходимого изменения $P_{ss,k} \to 1$ и это происходит в условиях увеличения избыточности кодирования. В связи с этим возникает вопрос о эффективности избыточности. Очевидно, что судить об этом можно, сравнивая вероятности истинных гипотез при передаче сообщений s и s_*. При передаче сообщений s число гипотез определяется большой

матрицей искажений с одинаковым числом 2^{kn_s} сообщений и гипотез, т. е. код имеет нулевую избыточностью. С учётом этого из (3) определяем вероятность истинной гипотезы для сообщения s и сравниваем её с вероятностью (5):

$$P_{ss,k}(s) = P_1^{kn_s} \text{ и } P_{ss,k}(s_*) = P_1^{kn_{s_*}}. \tag{6}$$

Поскольку рассматривается случай с $n_s > n_{s_*}$, ясно, что при любых k справедливо соотношение $P_{ss,k}(s_{s_*}) > P_{ss,k}(s)$. Следовательно, избыточность полезна и вероятность истинной гипотезы сообщения s_* увеличивается. Однако такое её увеличение недостаточно, поскольку при этом не может быть превышена вероятность P_1 и передача сообщений s_* без ошибок тоже невозможна (см. (5) и (6)).

Рассмотрим теперь оценку вероятностей гипотез, если равенство $H(S_*) = CT_s$ не выполняется и энтропия передаваемых сообщений $H(s_*) = n_{s_*}$ может принимать все значения из интервала $1 \div n_s$. Вероятность P_1 остаётся при этом неизменной. Пусть, как и ранее, из 2^{kn_s} сообщений s используются $2^{kn_{s*}}$ сообщений, необходимых для передачи сообщений s_*, и, следовательно, малая матрица искажений имеет размер $2^{k(n_s-n_{s_*})} \times 2^{k(n_s-n_{s_*})}$. Очевидно, что оценка вероятностей гипотез из (3) справедлива и в этом случае. Для вероятности истинной гипотезы $P_{ss,k} = P_1^{kn_{s*}}$ и рассматриваемых длительностей n_{s_*} можно получить неравенство $P_1^{kn_s} \le P_{ss,k} \le P_1^k$, из которого следует, что вероятность $P_{ss,k}$ ухудшается при увеличении как числа передаваемых сообщений $2^{n_{s*}}$, так и количества их k в передаваемой группе.

Таким образом, использование согласно лемме известных кодов с избыточностью в части способа кодирования не приводит к успеху. Применение сообщений s в качестве переносчиков сообщений s_* и увеличение количества сообщений k в передаваемой группе не позволяют осуществить безошибочную передачу. Вероятности гипотез определяются вероятностями (1), и только при $P_1 \to 1$ возможна передача сообщений со сколь угодно малой вероятностью ошибок (5), (6). Упомянутая выше сколь угодно близкая к единице вероятность P справедлива лишь для оценки вероятности среднего числа правильно переданных сообщений s, полученного с использованием закона больших чисел [6, с. 51], и не определяет качества передачи (6). Причины этого рассматриваются далее.

3. КОД ХЭММИНГА

Иная возможность передачи дискретных сообщений связана с использованием кода Хэмминга [7]. Особенность этого кода заключается в способе формирования областей принятия решений около передаваемых сообщений. В отличие от кодирования на основе леммы Файнстейна эти области содержат все гипотезы, вероятности которых достаточно близки к вероятностям истинных гипотез. Поскольку вероятности гипотез определяются матрицами искажений (см. (2) и табл. 1), то близость гипотез в каждой из этих областей определяется допустимыми искажениями i_*, количество которых даётся формулой [5, с. 41–43]

$$\sum_{i=0}^{i_*} C_{kn_s}^i \le 2^{k(n_s-n_{s_*})}. \tag{7}$$

Как и ранее, n_{s_*} и n_s в неравенстве (7) отвечают числу разрядов двоичного числа, определяющего количество передаваемых сообщений, и максимальному количеству сообщений, которые могут быть переданы по каналу связи, соответственно, k определяет количество передаваемых сообщений в последовательности. Из (7) очевиден способ формирования областей принятия гипотез. В эту область, кроме истинной гипотезы с $i = 0$, входят гипотезы с искажениями $i \in [1, i_*]$,

количество которых определено сочетаниями $C^i_{kn_s}$. Коды, получаемые из (7) при условии равенства, названы совершенными [3, с. 387]. В случае таких кодов области гипотез с искажениями $i \le i_*$ занимают весь объём 2^{kn_s}-мерного куба в сигнальном пространстве. Как показано в [3], такие коды довольно редки.

С учётом выражений (1) и свойств матрицы искажений условная вероятность истинной гипотезы для находимого из (7) числа искажений i_* равна

$$P_{ss,k} = \sum_{i=0}^{i_*} C^i_{kn_s} P_1^{kn_s - i} P_0^i. \tag{8}$$

Для предельных значений P_1, равных 0,5 и 1,0 (1), вероятности (8) принимают значения $\Sigma_{i=0}^{i_*} C^i_{kn_s}/2^{kn_s}$ и 1 соответственно. Если учесть неравенство (7), то первое значение не превышает $2^{-kn_{s*}}$. В области $P_{ss,k} \approx 1$ близость к единице определяется производной $\mathrm{d}P_{ss,k}/\mathrm{d}P_1 \mid_{P_1=1}$. Несложно показать, что отличие $P_{ss,k}$ от единицы уменьшается с увеличением k и n_s. Учитывая монотонность функций $P_1(\rho_s)$, можно утверждать, что вероятности $P_{ss,k}$, как функции P_1 или ρ_s, имеют точки пересечения при P_{1*}. Следовательно, только при превышении пороговой вероятности P_{1*} или соответствующего ей ρ_{s_*} увеличение количества передаваемых сообщений k полезно. Вероятность правильной гипотезы (9) при этом может сколь угодно мало отличаться от единицы. Оценка порогового отношения сигнал/шум для кодов Хэмминга исследована в работе [8]. Определение вероятности ложных гипотез существенно сложнее. Однако актуальность их в интересующем нас случае невелика, поскольку при $P_1 > P_{1*}$ и $k \to \infty$ вероятность истинной гипотезы $P_{ss,k} \to 1$, а суммарная вероятность ложных гипотез обращается в нуль.

Наряду с оценкой i_*, в работе [5, с. 36–43] исследованы способы определения сообщений, соответствующих коду Хэмминга. Выбор таких сообщений, как и последующий их приём, основан на определении синдромов, получаемых проверками сигналов на чётность [2, с. 362]. Число таких проверок определяется разностью $k(n_s - n_{s_*})$ и растёт с увеличением k. Проверки при приёме позволяют определить местоположение искажений в сообщении и затем исправить их при условии, что количество искажений не превышает i_*.

Однако эти специальные операции могут быть заменены более простыми, которые не требуют проверок на чётность и исправления ошибок, а реализуют выбор $\Sigma_{i=0}^{i_*} C^i_{kn_s}$ гипотез по критерию близости. В качестве примера можно привести случай передачи двух сообщений при максимально возможном их количестве равном восьми, т. е. случай $k = 1$, $n_{s_*} = 1$ и $n_s = 3$ в формулах (8) и (9). При использовании сигналов 000 и 111 и $i_* = 1$ область принятия истинной гипотезы для первого сообщения есть 000; 001; 010; 100, для второго — 111; 110; 101; 011. При этом нет необходимости определения и исправления ошибок, поскольку для допустимых искажений i_* области принятия гипотез оказываются строго определёнными и не имеющими общих точек.

Более сложной оказывается ситуация с несовершенными кодами, когда часть гипотез оказывается вне этих областей. В этих условиях можно увеличить области принятия гипотез с учётом принципа близости их к гипотезам, соответствующим неискажённым сообщениям. Иной вариант заключается в использовании случайного механизма принятия гипотез из этих областей [7]. Однако, как упоминалось выше, при превышении порогового значения отношения сигнал/шум увеличение k позволяет получить $P_{ss,k} \approx 1$ и практически нулевые суммарные вероятности ложных гипотез. В этих условиях можно ограничиться лишь областями принятия истинных гипотез, определяемыми искажениями i_*.

Видно, что использование кода Хэмминга приводит к совершенно иным результатам, чем кодирование согласно лемме Файнстейна. В случае кода Хэмминга существует пороговое значение вероятности P_{1*} или отношения сигнал/шум ρ_{s*} (1), поэтому безошибочная передача сообщений

становится возможной при $P_1 > P_{1*}$, а не при $P_1 \approx 1$.

4. ОБСУЖДЕНИЕ РЕЗУЛЬТАТОВ

Анализ способов кодирования сообщений, проведённый в разделах 2 и 3, показал, что наличие избыточности полезно, но не гарантирует, что вероятность истинной гипотезы $P_{ss,k} \to 1$ при увеличении количества сообщений k в передаваемой группе. Существенное значение для качества передачи имеют способ формирования областей принятия гипотез около передаваемых сообщений и отношение сигнал/шум. Поэтому интересен вопрос о связи условия безошибочной передачи $H(s) \le CT_s$ с её качеством, определяемым вероятностями (3) и (8). Наряду с этим принципиально различаются как вероятности истинных гипотез P, $P_{ss,k}$ см. (разделы 2, 3), так и вероятности ошибок, связанные с условиями передачи. Рассмотрим подробнее эти вопросы.

4.1 Условие передачи без ошибок

В разделах 2 и 3 получены оценки вероятностей гипотез для кодирования согласно лемме Файнстейна [6, 7] и кода Хэмминга [5]. Принципиальное их отличие в том, что в лемме развивается идея Шеннона об использовании сообщений s в качестве переносчика для передачи сообщений s_*, тогда как коды Хэмминга определяются из количества передаваемых сообщений s_* и приемлемой избыточности.

В разделе 2 показано, что при различных соотношениях между $H(s_*)$ и CT_s вероятность истинной гипотезы при кодировании на основе леммы равна $P_1^{kn_{s*}}$ и быстро уменьшается с увеличением kn_{s_*} (5). При этом увеличивается суммарная вероятность ложных гипотез, что, казалось бы, указывает на снижение качества передачи сообщений. Для более точной оценки качества передачи в этих условиях следует определить количество информации $I_{\text{exit}\,k}$ на выходе канала связи. Воспользуемся для этого выражением $I_{\text{exit}\,k} = H_k(h) - H_k(h \mid s)$, где индексы k у энтропии и ненадёжности указывают на количества передаваемых в группе сообщений, для которых получены эти величины.

Энтропию и ненадёжность просто определить с использованием расширенной матрицы искажений. Ранее указывалось, что матрица искажений симметрична, и потому для равновероятных сообщений справедливо $H(h) = H(s_*) = n_{s_*}$. Если учесть вероятности гипотез из формул (4) и (5), то количество информации на выходе канала

$$I_{\text{exit}\,k} = kn_{s_*} + \sum_{\nu=0}^{kn_{s*}} C_{kn_{s_*}}^{\nu} P_1^{kn_{s_*}-\nu} P_0^{\nu} \log_2(P_1^{kn_{s_*}-\nu} P_0^{\nu}). \tag{9}$$

Нетрудно показать, что из (9) следует

$$I_{\text{exit}\,k} = kn_{s_*}(1 + P_1 \log_2 P_1 + P_0 \log_2 P_0) = k\,\frac{n_{s_*}}{n_s}\,CT_s. \tag{10}$$

Здесь учтено, что величина в скобках определяет количество информации, приходящееся на один элемент (букву) сообщения s. Видно, что при простом увеличении количества сообщений k в передаваемой группе количество информации на выходе канала связи, как и следовало ожидать, увеличивается в k раз. При этом качество передачи сообщений не изменяется (см. (15) и (10)), поскольку с увеличением k происходит только изменение количества сообщений в передаваемой группе. Качество передачи в этом случае определено матрицей искажений (табл. 1), расширение

которой при изменении k происходит по одним и тем же правилам и не приводит к новым положительным результатам. Следовательно, выполнение условия леммы $2^{kn_{s*}} \le 2^{kCT_s}$ при $k \to \infty$ не обеспечивает передачу сообщений без ошибок. С таким же качеством передаётся информация источника сообщений s: по аналогии с выражением (10) количество информации на выходе канала $I_{\text{exit}\,k} = kn_s(1 + P_1 \log_2 P_1 + P_0 \log_2 P_0) = kCT_s$, и большее количество информации источника s достигает выхода канала только из-за соотношения их энтропий $n_s > n_{s*}$.

Рассмотрим, как изменяется качество передачи в случае кода Хэмминга при $n_{s*} \in [1, n_s - 1]$ и фиксированном n_s, и как неравенство $n_{s*} \le CT_s$ влияет на качество передачи. Выше упоминалось, что увеличение количества передаваемых сообщений k оказывается полезным и вероятность истинной гипотезы становится сколь угодно близкой к единице, если вероятность P_1 из (1) превышает пороговую величину P_{1*}. Поэтому пропускную способность канала определим для вероятности P_{1*} и $k = 1$. Её оценку можно выполнить, используя результаты работы [8], в соответствии с которыми справедливо уравнение

$$kn_s(1 - P_{1*}) = i_*. \tag{11}$$

Здесь i_* — количество допустимых искажений, определяемых уравнением (7). Рассмотрим сначала случай $n_{s*} = 1$, при этом, чтобы исключить необходимость устранения неоднозначности при принятии гипотез далее рассматриваются нечётные n_s. При $n_{s*} = 1$ и $k = 1$ из (7) следует $i_* = (n_s - 1)/2$. Тогда из уравнения (11) для пороговой вероятности получается выражение

$$P_{1*} = \frac{1}{2} + \frac{1}{2n_s}\,. \tag{12}$$

Опуская промежуточные значения n_{s*}, рассмотрим другой предельный случай максимальной энтропии источника $n_{s*} = n_s - 1$. Из уравнения (7) получаем $i_* = 0$, и тогда из уравнения (11) следует

$$P_{1*} = 1. \tag{13}$$

Заметим, что случай с $n_{s*} = n_s$ не представляет интереса, поскольку соответствует передаче без избыточности. Используя пороговые вероятности (12) или (13), можно определить соответствующие пропускные способности

$$C \approx \frac{1}{n_s T_s \ln 2} \;\text{ и }\; C = \frac{n_s}{T_s}\,. \tag{14}$$

Здесь приближённое равенство справедливо при $n_s > 5$. При $n_{s*} = 1$ пороговая вероятность (12) близка к минимальному значению (1). Следовательно, увеличение числа передаваемых в группе сообщений позволит получить сколь угодно близкие к единице вероятности истинных гипотез (8) при малых отношениях сигнал/шум. В случае малой избыточности при максимальном n_{s*} пороговая вероятность (13) $P_{1*} = 1$ и, следовательно, передача группы из k сообщений не имеет смысла, поскольку это не изменит качества приёма (8) и (10), но усложнит его алгоритмы. Используя уравнение (7), можно получить неравенство $1 + n_s > 2^{\Delta n}$, в котором $\Delta n = n_s - n_{s*}$. Это неравенство определяет значения $n_{s*} \in [n_s - \widehat{\Delta n}, n_s - 2]$, где $\Delta n = \log_2(1 + n_s)$, для которых $i_* = 0$. Поэтому ситуацию с $n_{s*} = n_s - 1$ из выражений (13) и (14) можно распространить на значения с $n_{s*} = n_s - \widehat{\Delta n}$.

Представление об изменении рассмотренных выше величин даёт рис. 2, где приведены зависимости величин CT_s и $5P_{1*}$ от энтропии n_{s*} (кривые *1* и *2* соответственно). К этим зависимостям, полученным из формул (8), (11) и (12) при $n_s = 15$, добавлена энтропия n_{s*} (кривая *3*). Видим, что условие теоремы и леммы $n_{s*} \le CT_s$ выполняется лишь при нескольких (5 из 15) значениях n_{s*} и, казалось бы, безошибочная передача сообщений невозможна. Однако для всех n_{s*} существуют

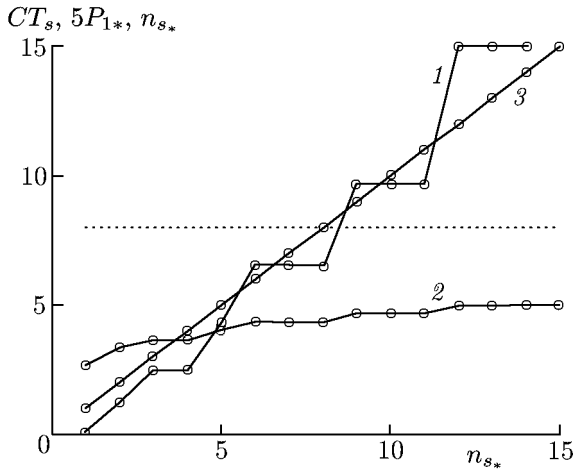

Рис. 2

вероятности P_{1*} и, следовательно, при их превышении за счёт отношения сигнал/шум и передаче с $k \to \infty$ можно реализовать безошибочную передачу сообщений [8]. При этом с увеличением n_{s_*} избыточность и допустимые искажения (7) уменьшаются, а вероятность P_{1*} увеличивается (11), что приводит к росту необходимого отношения сигнал/шум (1).

На рис. 2 отображена ситуация для кодирования согласно лемме Файнстейна. В этом случае пропускная способность канала зависит только от вероятности P_1 (10). Поэтому величина правой части условия безошибочной передачи $n_{s_*} \le CT_s$ с учётом P_1 может принимать значения в интервале $0 \div n_s$. На рис. 2 она представлена пунктирной линией для $P_1 = 0{,}9$. Видно, что для малых n_{s_*} условие выполняется, для больши́х — не выполняется. Однако это никак не влияет на качество передачи сообщений, поскольку количество передаваемой информации зависит лишь от вероятности P_1 или отношения сигнал/шум ((1), (9)).

Таким образом, можно утверждать, что для рассматриваемых здесь кодов неравенство $H(s_*) \le CT_s$ не является критерием безошибочной передачи сообщений.

4.2 Вероятности гипотез

Анализ вероятностей гипотез позволяет ещё раз убедиться в нереализуемости идеи леммы об использовании выбранных априори сообщений s для безошибочной передачи сообщений s_* [7]. Как и выше, полагаем, что сообщения и гипотезы определяются n-разрядными двоичными числами, пропускная способность канала равна C, а сообщения равновероятны. В соответствии с законом больших чисел количество информации на выходе канала связи $\log_2[P(h \mid s)/P(h)]$ при увеличении количества сообщений k в передаваемой группе сходится по вероятности к среднему значению CT_s. Это определяется известным соотношением

$$P\left\{\left|\frac{1}{k}\log_2\left[\frac{P(h \mid s)}{P(h)}\right] - CT_s\right| < \lambda\right\} > 1 - \varepsilon. \tag{15}$$

Здесь λ и ε — положительные сколь угодно малые величины. После несложных преобразований левую часть (15) можно представить иначе:

$$P\left\{2^{-k[H(h|s)+\lambda]} < P(h \mid s) < 2^{-k[H(h|s)-\lambda]}\right\}. \tag{16}$$

Видно, что условная вероятность гипотез (2) определяется ненадёжностью канала $H(h \mid s) = H(h) - CT_s$. Если использовать высоковероятные группы сообщений [7], то вероятность передачи без ошибок запишется как

$$P_{ss,k} = \frac{2^{kCT_s}}{2^{kH(h)}} = 2^{-kH(h|s)}. \tag{17}$$

Таким образом, соотношения (15) и (16) показывают, что в длинной последовательности сообщений вероятность гипотез группируется около вероятности передачи без ошибок, которая определяется пропускной способностью канала связи (17) и может быть меньше единицы.

Возможность реализации безошибочной передачи сообщений по такому каналу связывается с избыточностью, при которой число гипотез превышает число передаваемых сообщений [7]. В этих условиях объединение ряда таких гипотез позволяет увеличить вероятность $P_{ss,k}$. Если иметь в виду неравенство (16), то увеличение вероятности $P_{ss,k}$ происходит за счёт области $\pm\lambda$ около средней вероятности гипотез. Именно в этой области должны располагаться гипотезы, обеспечивающие избыточность кодирования. Тогда, согласно неравенствам (15) и (16), реализуется условие

$$\sum_{\lambda} P(h_\lambda \mid s) > 1-\varepsilon, \tag{18}$$

которое оказывается достаточным для передачи сообщений s_* по каналу с отличной от нуля ненадёжностью практически без ошибок. Однако в разделах 2 и 4.1 показано, что избыточность при таком кодировании не приводит к успеху ((3), (5) и (6)).

Причина этого заключается в свойствах распределения вероятностей гипотез (2). В рассматриваемом случае это полиномиальное распределение, являющееся многомодальным и некомпактным, что хорошо видно из матрицы искажений и её трансформации при изменении k. При увеличении k на единицу её размер удваивается, смещённые вправо и вниз начальные матрицы увеличиваются на единичные матрицы. В результате вторая половина первой строки начинается с единичного искажения. Матрица искажений, полученная расширением матрицы с размером 2×2, имеет единичное искажение в начале второй половины первой строки. Каждое последующее расширение матрицы приводит к такому же результату. При $k=3$ в первой строке получаем ряд искажений 0; 1; 1; 2; 1; 2; 2; 3. В результате имеем группы гипотез с одинаковыми искажениями ν и равными вероятностями (3) и (4). Количество таких гипотез, определяемое сочетаниями $C^{\nu}_{kn_{s*}}$, быстро увеличивается с ростом k, что и приводит к некомпактному многомодальнму распределению. Свойства этого распределения зависят от вероятностей оценки элементов сообщений P_1 и P_0, которые определяются отношением сигнал/шум ρ_s (1).

Следует заметить, что при доказательстве леммы в [6, 7] свойства распределения вероятностей гипотез не рассматриваются и не приведён пример использования результатов леммы при передаче сообщений. Между тем, существенное значение распределения вероятностей гипотез для леммы Файнстейна и для передачи информации в целом следует из известной задачи измерения случайной амплитуды детерминированного сигнала $\alpha s(t)$ [3, с. 219–221]. Если амплитуда и аддитивная помеха гауссовы, то оценка амплитуды $\alpha_{\rm E}$ связана линейной зависимостью с входным напряжением. Априорная $p(\alpha)$ и апостериорная $p(\alpha \mid \alpha_{\rm E})$ плотности вероятностей амплитуды тоже гауссовы с дисперсиями σ^2_α для априорной плотности и $\sigma^2_\alpha/(1+\sigma^2_\alpha\rho_s)$ для апостериорной. Здесь ρ_s — отношение сигнал/шум для сигнала $\tilde{s}(t)$. Видно, что дисперсия апостериорной плотности меньше. Поэтому при $\sigma^2_\alpha \gg 1$ можно выделить j оценок амплитуд $\alpha_{\rm E}$. Около них существуют области, в которых сосредоточена практически вся апостериорная плотность вероятности. Здесь проявляется закон больши́х чисел (15), и выбор соответствующих λ и ε обеспечивает с вероятностью $1-\varepsilon$ различение амплитуд $\alpha_{{\rm E}p}$, $p=1,\ldots,j$. Ясно, что эти амплитуды можно использовать для передачи других случайных амплитуд α_*, количество которых не должно превышать j. По существу, это и есть измерение α_* с использованием избыточности. При этом вероятность ошибки меньше $1-\varepsilon$ и результаты леммы оказываются справедливыми. Однако эта ситуация имеет место при $\sigma^2_\alpha\rho_s \gg 1$. Если это условие не выполняется и $\sigma^2_\alpha\rho_s \approx 1$, то дисперсии априорного и апостериорного распределений амплитуды одного порядка и измерение амплитуды α_* с избыточностью невозможно.

Таким образом, при необходимости передачи с избыточностью, условия $\sigma^2_\alpha\rho_s \gg 1$ в случае измерения амплитуды или $P_1 \gg 0{,}5$ при передаче сообщений (см. (1) и рис. 2) имеют существенное значение, поскольку именно они обеспечивают сколь угодно близкие к единице вероятности

истинных гипотез (18). Поэтому вряд ли можно рассматривать возможность передачи с использованием сообщений-переносчиков согласно лемме Файнстейна, игнорируя статистику вероятностей гипотез.

4.3 Актуальность величины отношения сигнал/шум

В разделах 4.1 и 4.2 показано, что условие безошибочной передачи сообщений $H(s_*) \le CT_s$ [1, 7] не является необходимым (см. (3), (10), (11) и рис. 2). Существенно большее значение в рассмотренных случаях имеет отношение сигнал/шум ρ_s, поскольку оно, как видно из вышеизложенного, определяет необходимый и достаточный критерий качества передачи. Используя свойства матрицы искажений, просто показать, что в случае кодирования согласно лемме Файнстейна именно величина ρ_s определяет распределение вероятностей гипотез и, в конечном счёте, качество передачи.

Как показано в разделе 4.2, это распределение многомодальное и некомпактное. Поэтому для анализа проще определить интегральное распределение вероятностей гипотез $W(m)$. Как и в случае вероятностей (15) и (16), нас интересует такое распределение для случая передачи сообщений s, являющихся переносчиками сообщений s_*. Определим значения распределения $W(m)$ в точках, кратных 2^{kn_s-m}, где $m \in [1, kn_s - 1]$, а n_s и k фиксированы. Поскольку матрицы искажений симметричны, будем рассматривать их первые строки. Ясно, что m делит строку с 2^{kn_s} гипотезами на 2^m частей. Поэтому далее будем определять интегральную вероятность гипотез $W(m,l)$ в $l \in [0, 2^m]$ точках. Для этого следует последовательно суммировать условные вероятности гипотез (2) на этих интервалах с учётом (3). При этом крайние значения $W(m,0) = 0$ и $W(m,2^m) = 1$.

При $m = 1$ имеем две половинки строки и согласно (3) получаем

$$W(1,1) = \sum_{i=0}^{kn_s-1} C^i_{kn_s-1} P_1^{kn_s-i} P_0^i = P_1. \tag{19}$$

Искажения второй половины строки отличаются на единицу. Поэтому

$$W(1,2) = W(1,1) + \sum_{i=0}^{kn_s-1} C^i_{kn_s-1} P_1^{kn_s-i-1} P_0^{i+1} = P_1 + P_0 = 1. \tag{20}$$

Поскольку интервалы 2^{kn_s-m} кратны минимальным, то при изменении m определяются новые значения $W(m,l)$ при сохранении прежних. При этом свойства матриц искажений позволяют просто определять все промежуточные значения $W(m,l)$. При $m = 1$ было учтено, что искажения ν в двух половинках строки отличаются на единицу. При $m = 2$ имеем четыре части строки с искажениями ν, определяющимися $C_2^\nu \to 0;\ 1;\ 1;\ 2$. С учётом этого, в дополнение к $W(2,2) = W(1,1) = P_1$, получаем

$$W(2,1) = \sum_{i=0}^{kn_s-2} C^i_{kn_s-2} P_1^{kn_s-i} P_0^i = P_1^2; \qquad W(2,3) = W(1,1) + P_1P_0. \tag{21}$$

Здесь использовано значение вероятностей гипотез с $\nu = 1$, равное P_1P_0. Величину $W(2,1)$ можно получить аналогично $W(2,3)$ из (21), поскольку искажения с $\nu = 1$ повторяются при $m = 2$ дважды, т. е. $W(2,1) = W(1,1) - P_1P_0$. Если учесть значение вероятности с $\nu = 2$, равное P_0^2, то ясно, что $W(2,4) = 1$.

Таким образом, при переходе от m к $m+1$ количество отсчётов $W(m,l)$ удваивается, а прежние отсчёты не изменяются. Ещё одна характеристика вероятности $W(m,l)$ становится ясной из

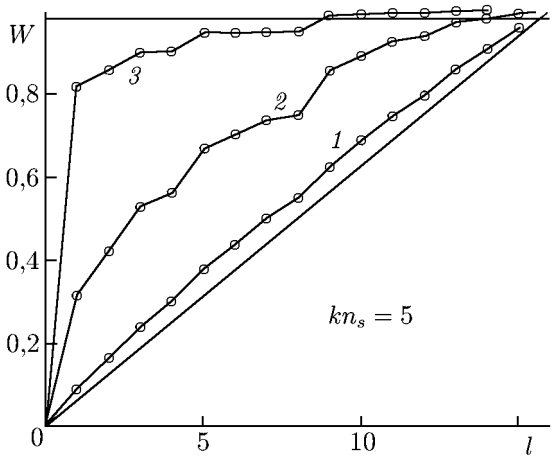

Рис. 3

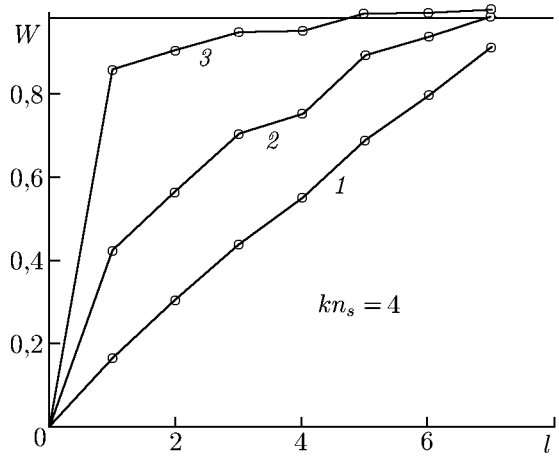

Рис. 4

оценки значения $W(m,1)$, следующего за значением $W(m,0)$. Действуя аналогично (19), можно показать, что $W(m,1) = P_1^m$. На рис. 3 вероятность $W(m,l)$ представлена как функция l при $kn_s = 5$ для $P_1 = 0{,}55$; 0,75 и 0,95 (кривые *1*, *2* и *3* соответственно). На рис. 4 эти же зависимости изображены при $kn_s = 4$. Кроме этого, на рисунках показана вероятность (16) при $1 - \varepsilon = 0{,}98$. Значения $W(m,l)$ определялись в соответствии с рассмотренной выше методикой. Сравнение рис. 3 и 4 показывает, что при увеличении m и kn_s происходит интерполяция распределения $W(m,l)$. При этом свойства $W(m,l)$ существенным образом зависят от отношения сигнал/шум, определяющего вероятность P_1 в выражении (1), и практически не зависят от n_s и k. Существенная особенность вероятности $W(m,l)$ заключается в том, что она располагается над прямой, соединяющей её крайние точки $W(m,0) = 0$ и $W(m,l^m) = 1$. Это следует из того, что $P_1 > 0{,}5$ (1), т. к. тогда ясно, что $W(m,1) = P_1^m > 2^{-m}$.

Распределение $W(m,l)$ вполне характеризует качество передачи сообщений. При передаче двух сообщений ($m = n_{s_*} = 1$) гипотезы с учётом избыточности должны быть разделены на две равные области (см. рис. 1). Поэтому согласно (19)–(21) вероятность истинной гипотезы определяется как $W(n_{s_*}, 2^{n_{s*}-1}) = W(1,1) = P_1$. Для различения этих сообщений, например с вероятностью $P = 0{,}98$, необходимо выполнение условия (18), которое с учётом значения $W(n_{s_*}, 2^{n_{s*}-1})$ приводится к виду $P_1 \geq 0{,}98$. Но из неравенства $P_1 \geq 0{,}98$ следует, что такое же качество реализуется при передаче одиночных сообщений (1), и, следовательно, увеличение количества сообщений в передаваемой группе не улучшает качество передачи. Аналогичная ситуация наблюдается при передаче большего числа сообщений ($n_{s_*} > 1$). Например, при $n_{s*\max} = m_{\max} = kn_s - 1$ имеем $W(kn_s - 1, 1) = P_1^{kn_s - 1}$, и, с учётом вероятности $P = 0{,}98$, для выполнения условия $W(kn_s - 1, 1) > 0{,}98$ необходима вероятность P_1 существенно бóльшая, чем при передаче двух сообщений. Поэтому и в случае источника с несколькими сообщениями передача их объединённых групп их не приводит к улучшению качества. Заметим, что этот вывод согласуется с результатом оценки количества информации на выходе канала (9) и (10).

Следовательно, не условие $H(s_*) \leq CT_s$ при $k \to \infty$, а необходимость превышения некоторого (порогового) отношения сигнал/шум позволяет различать сообщения с требуемой вероятностью (15) и (16) (см. рис. 3). Причины этого связаны с проявлением закона больши́х чисел. В случае передачи дискретных сообщений и в рассмотренном в разделе 4.2 случае измерения амплитуды сигнала избыточность кодирования возможна только, если область гипотез $W(m,l)$, определяемая условиями (17) и (19), существенно меньше общего их количества. Из свойств $W(m,l)$ следует, что это условие выполняется при достаточно больши́х отношениях сигнал/шум (см. (1), (19)–(21)

и рис. 3).

Рассмотрим подробнее влияние отношения ρ_s на качество передачи при использовании кода Хэмминга. В разделе 3 показано, что код Хэмминга предполагает объединение гипотез с допустимыми искажениями i_* около каждой истинной гипотезы [5, с. 41–43]. Именно вероятности с одинаковыми искажениями $i \le i_*$, собранные в одну группу, определяют вероятность истинной гипотезы (7) и (8). Поэтому случайный характер вероятности истинной гипотезы теперь полностью определяется искажениями i, которые, как видно из (8), имеют биномиальное распределение

$$P(i) = C^i_{kn_s} P_1^{kn_s - i} P_0^i. \tag{22}$$

Здесь P_1, P_0 — вероятности из выражения (1), n_s и k — используемые выше параметры сообщений. Таким образом, в отличие от случая кодирования в соответствии с леммой Файнстейна, для вероятностей гипотез получается распределение, которое существенно проще и компактнее распределения (3).

Как показано в работе [8], допустимое число искажений i_* (7) можно аппроксимировать линейной функцией k. Аналогично зависит от k и математическое ожидание числа искажений $E(i) = kn_s(1 - P_1)$ распределения (22). В этих условиях при оценке вероятности истинной гипотезы (8) существенным оказывается равенство между $E(i)$ и $i_*(k)$:

$$kn_s(1 - P_1) = k\,\frac{i(k_{\max})}{k_{\max}}\,. \tag{23}$$

Здесь $k_{\max}$ определяет интервал $k \in [1, k_{\max}]$, который интересует нас при анализе вероятности истинной гипотезы $P_{ss,k}$. Равенство (23) даёт пороговую величину вероятности $P_1 = P_{1*}$, для которой справедлива формула

$$n_s(1 - P_{1*}) = \frac{i(k_{\max})}{k_{\max}}\,. \tag{24}$$

Для вероятности P_{1*} взаимное положение «порога» i_* и распределения $P(i)$ не зависит от k. Поэтому не зависит от k и вероятность $P_{ss,k}$ из (8). В случае невыполнения равенства (24) взаимное положение i_* и $P(i)$ зависит от k. Действительно, если P_1 больше P_{1*}, определяемого из (24), то при увеличении k изменение i_* происходит быстрее, чем $E(i)$ (23). В результате вероятность $P_{ss,k}$ тоже увеличивается. В случае $P_1 < P_{1*}$ «порог» i_* изменяется медленнее и вероятность $P_{ss,k}$ уменьшается при увеличении k. Таким образом, условие (24) и выражение (1) позволяют определить величину порогового отношения ρ_{s_*}, начиная с которого применение кода Хэмминга становится полезным. Из уравнения (7) и условия (24) следует, что увеличение избыточности ($n_s > n_{s_*}$) и энтропии передаваемых сообщений n_{s_*} по-разному влияют на пороговое ρ_{s_*}. С увеличением избыточности отношение ρ_{s_*} уменьшается, тогда как при увеличении энтропии сообщения величина ρ_{s_*} увеличивается (7). Такая ситуация естественна, поскольку избыточность полезна при передаче, тогда как увеличение числа передаваемых сообщений её усложняет.

Таким образом, становится очевидным существенное различие кодирования сообщений в соответствии с леммой Файнстейна и кодом Хэмминга. Причины этого связаны с обработкой последовательности k сообщений. Оптимальный её приём ограничивается согласованной фильтрацией сигналов $\tilde{s}(t)$, а дальнейшая обработка проводится с учётом избыточности и критерия максимальной апостериорной вероятности или близости гипотез. В случае леммы Файнстейна области близких (истинных) гипотез определяются ненадёжностью (см. (3) и рис. 1). В случае кода Хэмминга они максимизируются за счёт выбора допустимых искажений (7). Поэтому для этого кода обработка сигналов оказывается эффективнее, т. к. она распространяется на большее количество гипотез. Иначе говоря, её эффективность обеспечивается за счёт лучшей обработки в наиболее «узком» месте при критерийной обработке.

ВЫВОДЫ

Проведённый анализ передачи дискретных сообщений показывает, что оценка качества передачи упрощается при применении матрицы искажений, элементы которой определяют вероятности гипотез (2). Применение этой матрицы удобно, поскольку её элементы изменяются по очень простым правилам при увеличении числа передаваемых сообщений k. Именно это её свойство позволяет оценить качество передачи при использовании принципиально различных способов кодирования сообщений, объединённых в длинные группы (3) и (8). При этом нет необходимости использовать случайное кодирование сообщений и в результате можно определить вероятности всех возможных гипотез, а не суммарную вероятность ложных гипотез [1].

Оценки качества передачи показали, что код Хэмминга [5] более эффективен, нежели кодирование с использованием сообщений-переносчиков [1, 7]. Однако в обоих случаях применение критерия безошибочной передачи $H(s_*) \le CT_s$ не гарантирует её безошибочности (см. рис. 2). Более простой и точный критерий качества передачи основан на отношении сигнал/шум ((1), (22) и (25)), которое является необходимой характеристикой любой системы передачи информации [3].

Сравнение кода Хэмминга [5] и кодирования с использованием сообщений-переносчиков [1, 7] показывает, что только в случае кода Хэмминга при превышении порогового отношения сигнал/шум может быть реализована безошибочная передача сообщений за счёт увеличения количества объединяемых при передаче сообщений.

Анализ вероятностей гипотез (3) и (17) показал, что использование их для выводов о качестве сообщений может приводить к заблуждениям. Особенно осторожно следует относиться к ним в случае передач длинных последовательностей сообщений (см. разделы 4.2, 4.3). Для получения более точных результатов необходимо рассматривать изменение информации на выходе канала связи или его пропускной способности и его ненадёжности при изменении k, поскольку только соответствующее изменение этих параметров гарантирует реализацию безошибочной передачи сообщений.

Наиболее достоверным критерием качества для рассматриваемых способов кодирования следует считать отношение сигнал/шум (1). Существенно, что его использование при анализе качества передачи позволяет получать достоверные результаты как в случае одиночных, так и длительных последовательностей сообщений.

СПИСОК ЛИТЕРАТУРЫ

1. Шэннон К. // В сб. «Теория передачи электрических сигналов при наличии помех». М.: Изд. иностр. лит-ры, 1953. С. 787.
2. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. М.: Изд. дом «Вильямс», 2003. 1 104 с.
3. Прокис Дж. Цифровая связь. М.: Радио и связь, 2000. 800 с.
4. Гаранин М. В., Журавлёв В. И., Кунегин С. В. Системы и сети передачи информации, М.: Радио и связь, 2001. 325 с.
5. Хэмминг Р. В. Теория кодирования и теория информации. М.: Радио и связь, 1983. 176 с.
6. Файнстейн А. Основы теории информации. М.: Изд. иностр. лит-ры, 1960. 147 с.
7. Хинчин А. Я. // Успехи мат. наук. 1956. Т. 11, вып. 1. С. 17.
8. Литвин М. В. // Изв. вузов. Радиофизика. 2011. Т. 54, № 11. С. 859.

Поступила в редакцию 14 апреля 2015 г.; принята в печать 24 сенятбря 2015 г.

QUALITY OF THE DISCRETE-MESSAGE TRANSMISSION OVER THE COMMUNICATION CHANNEL WITH INTERFERENCE

M. V. Litvin

We consider the problem of the discrete-message transmission using the codes on the basis of the Shannon theorem, the Feinstein lemma, and the Hamming codes. In this case, the transmission quality is estimated using the deterministic rather than random couplings among the messages and signals. It is shown that the coding redundancy, as well as the error-free transmission condition are not sufficient for realizing such a transmission. The signal-to-noise ratio is a more accurate parameter determining the transmission quality. The use of the Hamming code for long message sequences becomes efficient only if the threshold value of the signal-to-noise ratio is exceeded.