ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ им. проф. М. А. БОНЧ-БРУЕВИЧА»
(СПбГУТ)

О. С. Когновицкий, В. М. Охорзин, С. С. Владимиров

ПРАКТИКА ПОМЕХОУСТОЙЧИВОГО КОДИРОВАНИЯ

Часть 1

Системы с обнаружением ошибок и обратной связью

Учебное пособие

СПб ГУТ)))

Санкт-Петербург
2018

УДК 621.391(075.8)
ББК 32.811.4я73
К 57

Рецензенты
профессор кафедры СС и ПД СПбГУТ,
доктор технических наук
А. Е. Кучерявый,
ведущий инженер АО «НПП «ИСТА-Системс»,
кандидат технических наук
А. А. Берёзкин

Утверждено редакционно-издательским советом СПбГУТ
в качестве учебного пособия

Когновицкий, О. С.

К 57 Практика помехоустойчивого кодирования : в 2 ч. : учебное пособие / О. С. Когновицкий, В. М. Охорзин, С. С. Владимиров ; СПбГУТ. — СПб, 2018.

ISBN 978-5-89160-173-4

Часть 1. Системы с обнаружением ошибок и обратной связью / О. С. Когновицкий, В. М. Охорзин, С. С. Владимиров ; СПбГУТ. — СПб, 2018. — 100 с.

ISBN 978-5-89160-174-1

Призвано ознакомить студентов с практическими вопросами теории помехоустойчивого кодирования. Рассмотрены вопросы помехоустойчивого кодирования в системах с обнаружением ошибок и системах с обратной связью.

Предназначено для студентов, обучающихся по направлениям 11.03.02 «Инфокоммуникационные технологии и системы связи» и 09.03.01 «Информатика и вычислительная техника».

УДК 621.391(075.8)
ББК 32.811.4я73

ISBN 978-5-89160-174-1 (Ч. 1)
ISBN 978-5-89160-173-4

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Задачей помехоустойчивого кодирования является повышение качества передачи данных. Одной из качественных характеристик является достоверность поступающей к потребителю информации по каналу с помехами. В реальных практических системах передачи информации такая задача решается по разному в зависимости от требований пользователей. Во многих системах достаточно установить факт наличия в принятом сообщении ошибок и принять соответствующее решение: либо забраковать ошибочное сообщение, не отправляя его к получателю, либо забраковать и послать на передающую сторону запрос на повторную передачу ошибочно принятого сообщения.

Первый случай характерен, как правило, для систем реального времени, допускающих потерю отдельных фрагментов сообщения, например цифровых отсчётов аудио или видео. В таких системах недопустимо создавать задержки сообщения в приёмном оборудовании и поэтому эти системы, как правило, не имеют обратной связи для переспросов ошибочно принятых сообщений или их части.

Второй случай относится к ситуации, когда допускаются задержки в выдаче получателю данных, что позволяет послать запрос на повторную передачу ошибочно принятой информации. Для этого используется канал обратной связи между отправителем и получателем.

В обоих случаях применяют помехоустойчивые коды для обнаружения ошибок, которые в литературе называют *кодами с обнаружением ошибок* (EDC — Error Detection Code). Так как такие коды предназначены только для установления факта наличия ошибок в принятом сообщении, то в кодовые комбинации, передающие сообщения, вносится избыточность, которая обеспечивает повышение достоверности за счёт обнаружения ошибок. В системах же реального времени для обеспечения требуемой достоверности без введения существенных задержек применяют помехоустойчивые *коды с прямой коррекцией ошибок* (ECC — Error Correction Code; FEC — Forward Error Correction). В отечественной литературе их называют кодами с исправлением ошибок, избыточность в которых существенно выше, чем у кодов с обнаружением ошибок. Значение избыточности определятся требуемой кратностью $t_{\text{оо}}$ обнаруживаемых ошибок, в первом случае, и кратностью t исправляемых ошибок – во втором. Корректирующие свойства помехоустойчивого кода напрямую зависят от такой важной характеристики как минимальное кодовое расстояние Хэмминга $d_{\min}$ между кодовыми комбинациями. Так, при известном $d_{\min}$ помехоустойчивый код в режиме обнаружения способен обнаруживать все ошибки с кратностью $t_{\text{оо}} \leq (d_{\min} - 1)$, а в режиме исправления (прямой коррекции) способен исправлять все ошибки кратностью $t \leq \left\lfloor \frac{d_{\min}-1}{2} \right\rfloor$, где $\lfloor x \rfloor$ — наибольшее целое, не превосходящее x.

Напомним, что расстояние $d_{\min}$ в метрике Хэмминга равно наименьшему из возможных расстояний Хэмминга между всеми кодовыми комбинациями определенной длины n. По определению — расстояние Хэмминга между двумя комбинациями одинаковой длины равно количеству не совпадающих по своему значению элементов, расположенных на одноименных позициях (разрядах) сравниваемых комбинаций. В случае групповых кодов, когда среди кодовых комбинаций присутствует нулевая (на всех позициях нули), и комбинации обладают свойством замкнутости, то минимальное кодовое расстояние $d_{\min}$ будет равно минимальному весу $w_{\min}$ ненулевой кодовой комбинации, где под весом понимается число ненулевых элементов в комбинации.

Для оценки эффективности помехоустойчивых кодов часто пользуются следующими вероятностными характеристиками:

- для кода ECC:

– $P_{\text{пд}}$ — вероятность правильного декодирования принятой декодером комбинации;

– $P_{\text{нд}}$ — вероятность неправильного декодирования принятой декодером комбинации;

- для кода EDC:

– $P_{\text{пп}}$ — вероятность правильного приема комбинации;

– $P_{\text{оо}}$ — вероятность приема комбинации с ошибками, обнаруживаемыми декодером;

– $P_{\text{но}}$ — вероятность приема комбинации с ошибками, необнаруживаемыми декодером.

Естественно, что указанные вероятностные характеристики зависят от многих факторов, прежде всего от типа сигналов и помех в канале связи, а также от характеристик и параметров самого помехоустойчивого кода.

Вероятностные характеристики помехоустойчивого кода оцениваются либо аналитически, либо путем моделирования по известной модели канала. При этом модель канала должна соответствовать (быть адекватной) реальному дискретному или непрерывному каналу связи. Для оценки вероятностных характеристик в большинстве случаев должна быть определена вероятность правильного (или ошибочного) приёма отдельного элемента кода. В более редких случаях разрабатывают помехоустойчивые коды, вероятностные характеристики которых определяются по результатам так называемого «приёма в целом». Свою специфику на определение вероятностных характеристик помехоустойчивого кода накладывают также структурные свойства кода, например, основание кода, блочный, каскадный или непрерывный.

Наконец, заканчивая это введение, приведём ещё две характеристики, которые довольно часто используют для оценки эффективности помехоустойчивого кода. Одна из них — это остаточная битовая вероятность ошиб-

ки P_b в комбинации после декодирования. Часто используют и такую другую характеристику как энергетический выигрыш от применения помехоустойчивого кода, который оценивается как разность в дБ между соотношениями сигнал/шум простого (не помехоустойчивого) кода и помехоустойчивого кода, при которых оба кода обеспечивают одинаковую достоверность передачи данных.

Конечно это ещё не полный набор характеристик, с помощью которых оценивают эффективность помехоустойчивого кода. В частности, это могут быть задержки при декодировании, расширение полосы частот, сложность реализации, емкость требуемой памяти при кодировании и декодировании и др.

При рассмотрении конкретных вариантов помехоустойчивых кодов в следующих разделах настоящего учебного пособия в качестве оценочных характеристик эффективности кодов будем использовать, в основном, вероятностные характеристики. При этом будут рассматриваться варианты помехоустойчивых кодов, практически применяемых в реальных системах или протоколах передачи данных.

В первой части учебного пособия рассматриваются двоичные помехоустойчивые коды, предназначенные для обнаружения ошибок, т. е. коды EDC. Учебный материал, представленный в первой части, базируется на ранее прослушанных курсах по теории помехоустойчивых кодов, а также на классических монографиях по теории помехоустойчивого кодирования [1–8] и учебных пособиях [9, 10]. Особенно хотелось бы отметить практическое пособие Е. Г. Власова [8], в котором автор приводит примеры известных помехоустойчивых кодов, применяемых в реальных телекоммуникационных системах.

1. ДИСКРЕТНЫЕ КАНАЛЫ И МОДЕЛИ ОШИБОК

1.1. Общее понятие канала передачи данных

Точное математическое описание любого реального канала передачи данных обычно весьма сложное [11]. Вместо этого используют упрощенные математические модели, которые позволяют выявить важнейшие закономерности реального канала.

В физическом канале сигнал $S(t)$ подвергается воздействию шума $n(t)$ [12]. Схема этого явления показана на рис. 1.1.

Рис. 1.1. Структурная схема физического канала в общем виде

Для количественной оценки степени влияния шума $n(t)$ на сигнал $S(t)$ обычно используют *отношение сигнал/шум* (SNR), определяемое как отношение мощности сигнала к мощности шума, как показано в формуле

$$\mathrm{SNR} = \frac{P_\mathrm{c}}{P_\mathrm{ш}} = \left(\frac{A_\mathrm{c}}{A_\mathrm{ш}}\right)^2, \tag{1.1}$$

где P — средняя мощность, а A — среднеквадратичное значение амплитуды. Параметры сигнала и шума измеряются в полосе пропускания системы передачи данных.

Как правило отношение сигнал/шум выражается в децибелах и рассчитывается по формуле

$$\mathrm{SNR}_\mathrm{dB} = 10\log_{10}\left(\frac{P_\mathrm{c}}{P_\mathrm{ш}}\right) = 20\log_{10}\left(\frac{A_\mathrm{c}}{A_\mathrm{ш}}\right). \tag{1.2}$$

В цифровой связи основным критерием качества канала связи и системы передачи данных является *отношение сигнал/шум, нормированное на ширину полосы пропускания и битовую скорость передачи данных*. Нормированное отношение сигнал/шум обозначается как $\frac{E_b}{N_0}$ и рассчитывается по формуле (1.3). E_b — это энергия бита, которая представляет из себя мощность сигнала P_c, умноженную на время передачи одного бита T_b. N_0 — это спектральная плотность мощности шума, которая выражается как отношение мощности шума $P_\mathrm{ш}$ на ширину полосы пропускания канала W [13]:

$$\frac{E_b}{N_0} = \frac{P_\mathrm{c}T_b}{P_\mathrm{ш}/W} = \frac{P_\mathrm{c}/R}{P_\mathrm{ш}/W} = \frac{P_\mathrm{c}}{P_\mathrm{ш}} \cdot \frac{W}{R} = \mathrm{SNR} \cdot \frac{W}{R}, \tag{1.3}$$

где R — битовая скорость передачи данных.

Выделяют два основных вида моделей каналов передачи данных. Непрерывные (аналоговые) каналы и дискретные (цифровые) каналы.

Непрерывные каналы имеют непрерывный сигнал $S(t)$ на входе и непрерывный сигнал $R(t)$ на выходе. Эти сигналы являются непрерывной функцией от времени.

Дискретные каналы имеют на входе дискретные кодовые символы x_j, а на выходе — дискретные кодовые символы y_i, в общем случае не совпадающие с x_i [14].

Почти во всех реальных линиях связи дискретный канал содержит внутри себя непрерывный канал, на вход которого подаются сигналы $S(t)$, а с выхода снимаются искаженные помехами сигналы $R(t)$ [14]. Свойства этого непрерывного канала наряду с характеристиками модулятора и демодулятора однозначно определяют все параметры дискретного канала. Поэтому иногда дискретный канал называют дискретным отображением непрерывного канала. Однако при математическом исследовании дискретного канала обычно отвлекаются от непрерывного канала и действующих в нем помех и определяют дискретный канал через алфавит источника $\{x_0, x_1, \ldots, x_{q-1}\}$, вероятности появления символов алфавита, скорость передачи символов, алфавит получателя $\{y_0, y_1, \ldots, y_{Q-1}\}$ и значения переходных вероятностей $P(y_i|x_j)$, где $i = 0,1,\ldots,Q$, $j = 0,1,\ldots,q$ [11, 14].

Переходные вероятности $P(y_i|x_j)$ являются вероятностями того, что при отправке в канал символа x_j на выходе будет получен символ y_i.

Как правило, переходные вероятности в канале записывают в виде матрицы переходов, являющейся стохастической матрицей, у которой сумма всех элементов каждой строки равна единице [15]. В общем случае матрица переходов с входным алфавитом из q символов x_j и выходным алфавитом из Q символов y_i, содержит все переходные вероятности и имеет вид

$$P_{X/Y} = \begin{pmatrix} P(y_0|x_0) & P(y_1|x_0) & \cdots & P(y_{Q-1}|x_0) \\ P(y_0|x_1) & P(y_1|x_1) & \cdots & P(y_{Q-1}|x_1) \\ \vdots & \vdots & \ddots & \vdots \\ P(y_0|x_{q-1}) & P(y_1|x_{q-1}) & \cdots & P(y_{Q-1}|x_{q-1}) \end{pmatrix}. \qquad (1.4)$$

Если переходные вероятности для каждой пары i, j остаются постоянными и не зависят от того, какие символы передавались и принимались ранее, то дискретный канал называется постоянным или однородным. Иногда применяют также другие названия: канал без памяти или канал с независимыми ошибками. Если же вероятности перехода зависят от времени или от имевших место ранее переходов, то канал называют неоднородным или каналом с памятью [14].

Помимо дискретных и непрерывных каналов выделяют дискретно-непрерывные каналы, которые имеют дискретный вход и непрерывный выход.

1.2. Поток ошибок в дискретном канале

На входе и выходе дискретного канала информация представлена в виде последовательности посылок постоянного тока i $(i = 1, 2, 3, \ldots)$ длительностью t_0. В простейшем случае двухполярного сигнала амплитуда каждой из посылок может принимать два значения (рис. 1.2, а, б). Каждому значению амплитуды однозначно соответствует «0» или «1», поэтому входную и выходную последовательности дискретного канала можно рассматривать как случайную двоичную последовательность. Пусть $\tilde{A} = (\tilde{a}_1, \tilde{a}_2, \ldots, \tilde{a}_L)$ является L-элементной двоичной последовательностью на выходе дискретного канала, которая отличается от аналогичной последовательности на входе канала $A = (a_1, a_2, \ldots, a_L)$ только наличием ошибок. *Ошибка* это результат неправильного решения регистрирующего устройства о значении принятого единичного элемента в случае, когда величина искажения превышает исправляющую способность. Результат воздействия различного рода помех может быть представлен так называемой последовательностью ошибок ε (рис. 1.2, в) [16]:

$$\varepsilon = \tilde{A} - A = (\tilde{a}_1 - a_1, \tilde{a}_2 - a_2, \ldots, \tilde{a}_L - a_L).$$

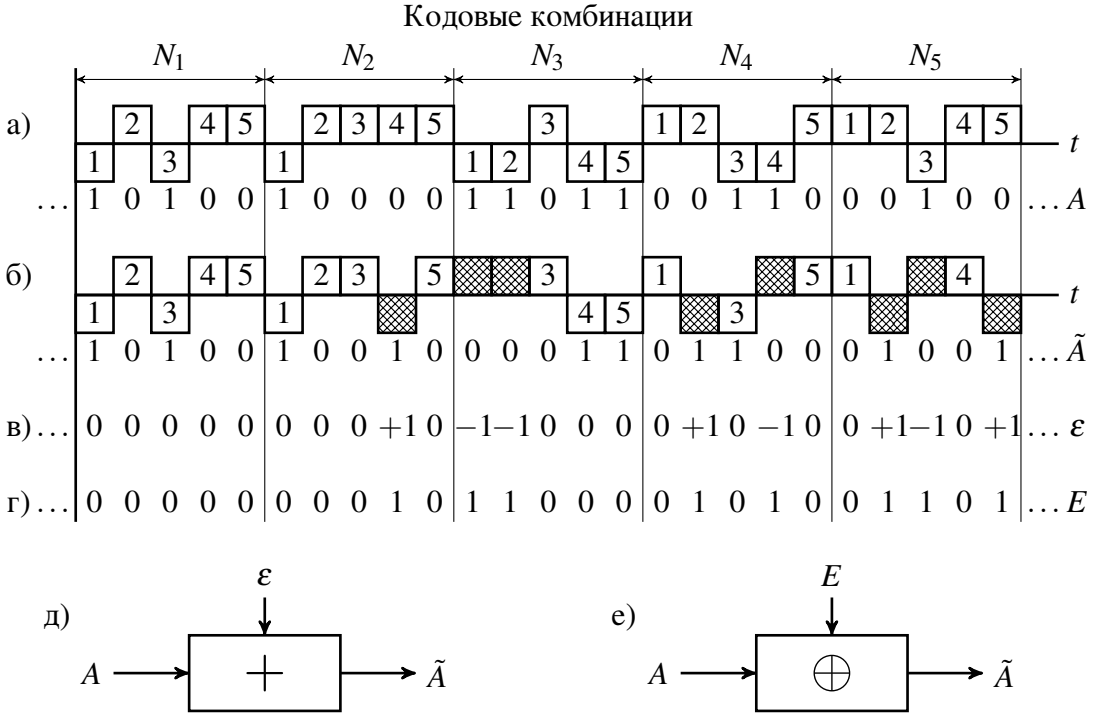


Рис. 1.2. Последовательности ошибок

В последовательности ε элементу $\tilde{a}_i$, принятому правильно, будет соответствовать «0», принятому с ошибкой вида $0 \to 1$ будет соответствовать

«+1» и принятому с ошибкой вида $1 \to 0$ будет соответствовать «−1». Таким образом, воздействие помех в канале можно описать суммированием A с ε:

$$\tilde{A} = A + \varepsilon = (a_1 + \varepsilon_1, a_2 + \varepsilon_2, \ldots, a_L + \varepsilon_L) = (\tilde{a_1}, \tilde{a_2}, \ldots, \tilde{a_L}).$$

Причем по определению ε_i может принимать значение «−1» при $a_i = 1$, «+1» при $a_i = 0$ и нулевое значение при любых a_i. В этом случае дискретный канал может быть отображен моделью, изображенной на рис. 1.2, д.

Если знак ошибки не имеет существенного значения, то суммарный результат воздействия помех можно представить *последовательностью модулей ошибок* E (рис. 1.2, г), в которой «0» соответствует отсутствию ошибок, а «1» — наличию ошибок:

$$E = |\varepsilon| = (|\varepsilon_1|, |\varepsilon_2|, \ldots, |\varepsilon_L|) = (e_1, e_2, \ldots, e_L).$$

Принятая из канала двоичная последовательность $\tilde{A}$ будет равна сумме A и E по mod 2:

$$\tilde{A} = A \oplus E = (a_1 + e_1, a_2 + e_2, \ldots, a_L + e_L) = (\tilde{a_1}, \tilde{a_2}, \ldots, \tilde{a_L}).$$

В этом случае дискретный канал может быть отображен моделью, показанной на рис. 1.2, е.

При блочном кодировании входная и выходная последовательности составлены из подпоследовательностей длины n, т. е. из кодовых n-элементных комбинаций. Подпоследовательность ошибок из n элементов $E_n = (e_1, e_2, \ldots, e_n)$, которая соответствует кодовым комбинациям, называется *комбинацией ошибок*.

Кодовая комбинация, все элементы которой приняты на выходе дискретного канала правильно, называется *неискаженной кодовой комбинацией*. Комбинация ошибок в этом случае состоит из одних нулевых элементов и поэтому ее вес равен нулю.

Кодовая комбинация, у которой один или более элементов приняты неверно, называется *искаженной кодовой комбинацией*. В этом случае комбинация ошибок имеет ненулевые элементы и ее вес равен сумме ее элементов

$$w_{E_n} = \sum_{i=1}^{n} e_i > 0.$$

В частности, в изображенной на рис. 1.2, б последовательности комбинация № 1 — неискаженная ($\sum_{i=1}^{n} e_i = 0$), остальные комбинации искаженные.

Комбинация № 2 содержит одну ошибку ($\sum_{i=1}^{n} e_i = 1$), комбинации № 3 и 4 — по две ошибки ($\sum_{i=1}^{n} e_i = 2$), а комбинация № 5 — три ошибки ($\sum_{i=1}^{n} e_i = 3$).

Число ошибок (кратность ошибок) в кодовых комбинациях определяется весом комбинации модулей ошибок. Если кодовая комбинация содержит m ошибок $(0 \le m \le n)$, то:

$$\sum_{i=1}^{n} e_i = m.$$

Число комбинаций ошибок веса m равно C_n^m. Например, если $n = 5$, то число комбинаций ошибок с однократными ошибками равно $C_5^1 = 5$, с двукратными ошибками — $C_5^2 = 10$ и т. д. Общее число ненулевых комбинаций ошибок равно

$$\sum_{m=1}^{n} C_n^m = 2^n - 1.$$

Если алгебраическая сумма элементов ненулевой комбинации ошибок равна нулю ($\sum_{i=1}^{n} \varepsilon_i = 0$ при $\sum_{i=1}^{n} e_i > 0$), то такие ошибки называются *симметричными*. В этом случае в пределах одной кодовой комбинации число ошибок вида $0 \to 1$ ($\varepsilon_i = +1$) и число ошибок вида $1 \to 0$ ($\varepsilon_i = -1$) одинаково (комбинация № 4, рис. 1.2). Характерная особенность симметричных ошибок состоит в том, что они не изменяют веса кодовой комбинации. Поэтому часто симметричные ошибки называются *транспозицией элементов* или *смещением элементов*.

Если $\sum_{i=1}^{n} \varepsilon_i = |m|$ при $\sum_{i=1}^{n} |\varepsilon_i| = \sum_{i=1}^{n} e_i = m$, то такие ошибки называются *асимметричными*. В этом случае все ошибки в пределах одной кодовой комбинации будут только одного вида: либо $0 \to 1$, либо $1 \to 0$ (комбинация № 3, рис. 1.2).

Если $0 < \left| \sum_{i=1}^{n} \varepsilon_i \right| < m$, при $\sum_{i=1}^{n} |\varepsilon_i| = m$, то такие ошибки называются *частично асимметричными* (комбинация № 5, рис. 1.2).

Важным понятием характеристики потока ошибок является *пачка ошибок*. Существует два определения пачки ошибок: одно — для потока ошибок, а другое — для кодовой комбинации.

Для определения *пачки ошибок на потоке ошибок* используется понятие длительности неискаженного интервала L. При этом *пачкой ошибок* называют *часть последовательности ошибок, ограниченную искаженными элементами и отделенную от ближайших искаженных элементов последовательности ошибок не менее, чем L правильными элементами*. Понятно, что внутри пачки расстояние между ошибками должно быть меньше L.

Пачкой ошибок в кодовой комбинации принято называть *часть ее элементов, ограниченную искаженными элементами*. При этом длина пачки не всегда совпадает с числом ошибок в пачке. Иногда пачка ошибок в кодовой комбинации произвольным образом делится на отдельные подпачки. Тогда говорят о нескольких пачках ошибок в кодовой комбинации.

1.3. Параметры моделей каналов ПД

Одним из параметров, использующихся для оценки и сравнения моделей каналов ПД, является *вероятность безошибочного участка*, определяемая, как вероятность появления последовательности m (или более) безошибочных бит, за которыми следует бит с ошибкой. Она обозначается как $\mathrm{EFR}(m)$[1] [17], либо как $P(0^m|1)$ [18].

По аналогии с вероятностью безошибочного участка вводится и *вероятность пачки ошибок*, определяемая, как вероятность появления последовательности из m (или более) ошибок, за которыми следует безошибочный бит. Обозначается как $P(1^m|0)$ [18].

Для определения вероятности появления ошибок в кодовой комбинации длины n вводится параметр $P(i,n)$, где i — количество ошибок в кодовой комбинации длины n. Как правило рассматривают вероятность появления хотя бы 1 ошибки, т. е. $P(\geq 1,n)$, и вероятность появления m ошибок и более $P(\geq m,n)$.

Важным параметром канала ПД является его *пропускная способность*, т. е. максимальная скорость передачи информации по всем допустимым распределениям вероятностей входных сигналов. Пропускная способность канала обозначается как C [14].

С понятием пропускной способности канала связана основная теорема теории информации — теорема кодирования. Она вперные была сформулирована К. Шенноном [19] и заключается в том, что сообщения всякого дискретного источника могут быть закодированы сигналами канала $x(t)$ и восстановлены по сигналам на выходе канала $y(t)$ с вероятностью ошибки, сколь угодно близкой к нулю, если производительность источника с фиксированной скоростью (либо производительность передающего устройства для источника с управляемой скоростью) $H'(x)$ меньше C. Если же $H'(x) > C$, то такое кодирование невозможно [14].

Для источника с управляемой скоростью эта теорема формулируется иначе: сообщения источника с управляемой скоростью можно закодировать сигналами $x(t)$ и восстановить по сигналам $y(t)$ на выходе канала так, чтобы вероятность ошибки была сколь угодно близка к нулю, а средняя скорость передачи — сколь угодно близка к $\frac{C}{H(x)}$ сообщений в секунду, где $H(x)$ — *эн-*

[1] От англ. Error Free Run

тропия источника, т. е. средняя собственная информация на одно сообщение источника [14, 20].

1.4. Основные закономерности распределения ошибок в реальных каналах связи

1.4.1. Независимое распределение ошибок

В течение длительного времени, когда отсутствовали статистические данные реальных каналов связи, предполагалось, что ошибки в каналах связи появляются независимо. При таком распределении ошибок значение i-го элемента последовательности ошибок E не зависит от того, какое значение принимает любой другой j-й элемент данной последовательности.

При независимых ошибках достаточно знать значение единственного параметра p, вероятности ошибки в канале, чтобы определить распределение любой случайной величины. Для этого достаточно воспользоваться схемой Бернулли. В частности, вероятность появления в n-элементной комбинации ровно i ошибок $P(i,n)$ определяется биномиальным распределением:

$$P(i,n) = C_n^i p^i (1-p)^{n-i}, \qquad (0 \le i \le n).$$

Вероятность приема комбинации без ошибки $P(0,n) = (1-p)^n$. Следовательно, вероятность появления искаженной комбинации, т. е. комбинации, содержащей хотя бы одну ошибку, равна

$$P(\ge 1,n) = 1 - P(0,n) = 1 - (1-p)^n, \quad \text{при } np \ll 1, P(\ge 1,n) \approx np.$$

Вероятность появления m и более ошибок в комбинации длины n равна

$$P(\ge m,n) = \sum_{i=m}^{n} P(i,n) = \sum_{i=m}^{n} C_n^i p^i (1-p)^{n-i}.$$

Иногда (при $m < n/2$) для вычисления $P(\ge m,n)$ удобнее пользоваться формулой, полученной из условия, что $\sum\limits_{i=0}^{n} P(i,n) = 1$. В этом случае

$$P(\ge m,n) = 1 - \sum_{i=0}^{m-1} C_n^i p^i (1-p)^{n-i}.$$

Представленные формулы для расчета различных вероятностей появления ошибок в кодовых комбинациях, основанные на *схеме независимых испытаний Бернулли*, составляют основу *модели двоичного симметричного канала (ДСК)*.

Многочисленные исследования реальных каналов связи не подтвердили гипотезу о независимом характере появления ошибок. Было показано, что ошибки появляются группами (пачками). Частота ошибок во время появления группы ошибок возрастает и становится значительно больше вероятности p. Таким образом, появление ошибок в реальных каналах является зависимым событием, поэтому схема Бернулли неприменима. Расчеты по формулам, полученным на основе данной схемы, приводят к значительным, а во многих важных для практики случаях и недопустимым погрешностям. Групповой характер появления ошибок проявляется во всех статистических характеристиках последовательности ошибок. Поэтому для математического описания этой последовательности недостаточно знать один параметр p, а необходимо определить дополнительные параметры, учитывающие степень зависимости появления ошибок в реальных каналах.

1.4.2. Зависимость вероятности появления искаженной комбинации от длины комбинации

Статистическая вероятность появления искаженной комбинации определяется как отношение числа искаженных комбинаций $B_{\text{ош}}(n)$ к общему числу комбинаций $B_0(n)$:

$$P(\geq 1, n) = \frac{B_{\text{ош}}(n)}{B_0(n)}.$$

Вероятность $P(\geq 1, n)$ является неубывающей функцией n. При $n = 1$ $P(\geq 1, n) = p$, а при $n \to \infty$ вероятность $P(\geq 1, n)$ с ростом n зависит от характера распределения ошибок.

На рис. 1.3 [16] показана функция $P(\geq 1, n)$ в двойном логарифмическом масштабе, т. е. $\log P(\geq 1, n) = \log p + \log n$. Это выражение является уравнением прямой I, пересекающейся с осью y в точке $y = p$ под углом β_1. Так как угловой коэффициент $\operatorname{tg} \beta_1 = 1$, то $\beta_1 = \frac{\pi}{4}$.

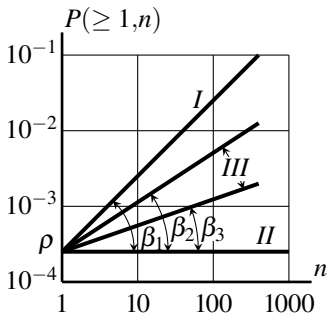


Рис. 1.3. Графическое представление экспериментальной зависимости вероятности искажения кодовой комбинации от ее длины

Исследования большого количества каналов показали, что для реальных каналов зависимости $\log P(\geq 1, n) = f(\log n)$ достаточно хорошо аппроксимируются прямыми линиями при числе элементов в комбинации от 1 до 500. Прямые, соответствующие этим зависимостям, находятся между прямыми I и II и имеют угол наклона $\beta < \beta_1$ (прямые III на рис. 1.3 с углами наклона β_2

и β_3). Такой характер зависимости $P(\geq 1,n) = f(n)$ является следствием группового характера появления ошибок в реальных каналах (п. 1.6.2).

1.4.3. Распределение ошибок в комбинациях различной длины

При оценке эффективности блоковых корректирующих кодов интерес представляет не только вероятность появления n-элементных искаженных комбинаций $P(\geq 1,n)$, но и вероятности появления комбинаций с одной $P(1,n)$, двумя $P(2,n)$ и m ошибками $P(m,n)$.

Под вероятностью появления комбинаций длины n с m ошибками будем понимать

$$P(\geq 1,n) = P\left\{\sum_{i=1}^{n} e_i = m\right\}.$$

Очевидно, что:

$$P(\geq 1,n) = P(1,n) + P(2,n) + \ldots + P(n,n) = \sum_{i=1}^{n} P(i,n).$$

Кроме того, для оценки эффективности некоторых корректирующих кодов необходимо знать суммарную (накопленную) вероятность появления искаженных комбинаций с m и более ошибками:

$$P(\geq m,n) = P(m,n) + P(m+1,n) + \ldots + P(n,n) = \sum_{i=m}^{n} P(i,n).$$

Статистическая вероятность появления n-элементных комбинаций с m и более ошибками определяется как отношение числа комбинаций с m и более ошибками к общему числу комбинаций:

$$P(\geq m,n) = \frac{\sum\limits_{i=m}^{n} B(i,n)}{B_0(n)},$$

где $B(i,n)$ — число n-элементных комбинаций, содержащих i ошибок; $B_0(n) = \sum\limits_{i=0}^{n} B(i,n)$ — общее число переданных n-элементных комбинаций.

На рис. 1.4 в логарифмическом масштабе показаны графики $P(\geq m,n)$ для радиотелеграфного канала с параметрами $p = 1{,}37 \cdot 10^{-2}$ и $\alpha = 0{,}4$. Точками на рис. 1.4 нанесены экспериментальные значения $P(\geq m,n)$, которые на участке $1 \leq m \leq \frac{n}{3}$ достаточно хорошо аппроксимируются прямыми линиями (сплошные линии). Исследования зависимости $P(\geq m,n) = f(m)$ на реальных каналах показали, что на участке $m < \frac{n}{3}$ значения $P(\geq m,n)$ с ростом m убывают медленно, что свидетельствует о наличии искаженных комбинаций с большим числом ошибок и является следствием группового характера появления ошибок в реальных. Скорость убывания вероятности $P(\geq m,n)$ с ростом

m различна для различных каналов и определяется степенью группирования ошибок.

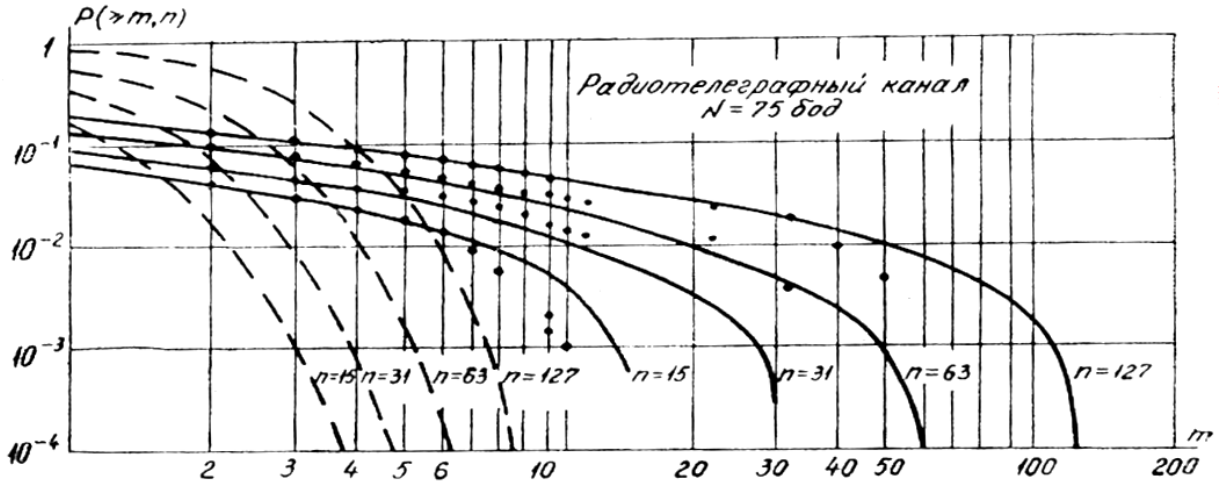


Рис. 1.4. Графическое представление экспериментальной зависимости вероятности искажения кодовой комбинации ошибками кратности m и более

1.5. Двоичные цифровые каналы с независимыми ошибками

1.5.1. Двоичный симметричный канал

Модель двоичного симметричного канала[2] (ДСК) является самой простой моделью дискретного канала [12]. Модель ДСК соответствует случаю использования двоичной модуляции в канале с аддитивным шумом (в котором выходной сигнал $R(t)$ равен сумме входного сигнала $S(t)$ и шума $n(t)$) и жёсткого решения демодулятора. Таким образом, модель ДСК является дискретной двоичной моделью передачи информации по каналу с аддитивным белым гауссовским шумом (АБГШ) [13, 15]. Граф, описывающий модель ДСК, представлен на рис. 1.5.

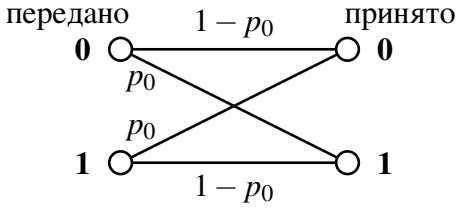


Рис. 1.5. Граф модели двоичного симметричного канала

Входом и выходом данного канала являются наборы $X = \{0,1\}$ и $Y = \{0,1\}$ из двух возможных двоичных символов. Также ДСК характеризуется набором переходных вероятностей $P(Y|X)$, определяющих вероятность приёма из канала символа Y при передаче символа X. Переходные вероятности для ДСК задаются выражениями [15, 21]

$$\begin{aligned} P(0|0) &= P(1|1) = 1 - p_0; \\ P(0|1) &= P(1|0) = p_0, \end{aligned} \tag{1.5}$$

[2] В зарубежной литературе используется англоязычное наименование Binary Symmetric Channel (BSC).

где p_0 — вероятность битовой ошибки в канале.

Для случая использования двух противоположных сигналов $s_0(t) = -s_1(t)$ вероятность битовой ошибки p_0 связана с отношением сигнал/шум выражением [12, 13]

$$p_0 = Q\left(\sqrt{2 \cdot \frac{E_b}{N_0}}\right), \tag{1.6}$$

где $Q(x)$ — функция, определяемая по формуле:

$$Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{-\frac{t^2}{2}} dt. \tag{1.7}$$

Переходные вероятности в канале ДСК не зависят от того, какие символы передавались и принимались ранее, и следовательно канал ДСК является каналом без памяти [11].

Пропускная способность канала ДСК рассчитывается как [11, 22]

$$C_{\text{ДСК}} = 1 + p_0 \log_2 p_0 + (1 - p_0) \log_2 (1 - p_0). \tag{1.8}$$

Из формулы (1.8) видно, что при $p_0 = 0{,}5$ пропускная способность канала C равна нулю. Этот случай называют обрывом канала [11].

Канал ДСК является частным случаем дикретного канала без памяти (ДКБП) [12]. Канал ДКБП имеет на входе набор $\{x_0, x_1, \ldots, x_{q-1}\}$ из q символов, а на выходе — набор $\{y_0, y_1, \ldots, y_{Q-1}\}$ из Q символов, и характеризуется набором из $q \cdot Q$ переходных вероятностей $P(y_i|x_j)$, где $i = 0,1,\ldots,Q$, $j = 0,1,\ldots,q$. Эти переходные вероятности постоянны во времени, и переходы различных символов независимы.

1.5.2. Двоичный симметричный канал со стираниями

Двоичный симметричный канал со стираниями[3] (ДСКС) является важным частным случаем канала ДСК. Как и ДСК, двоичный симметричный канал со стираниями может служить упрощённой моделью передачи данных по каналу АБГШ. Граф модели канала ДСКС представлен на рис. 1.6 [23].

Можно видеть, что по сравнению с моделью ДСК в ДСКС добавляется третье состояние на выходе — «стирание», вероятность которого обозначается p_e. С точки зрения аналогового канала стирание происходит в случае, когда продетектированный аналоговый сигнал V попадает в зону, в которой значения условных функций плотности распределения вероятностей $f(V/0)$

[3] В зарубежной литературе используется англоязычное наименование Binary Erasure Channel (BEC).

и $f(V/1)$ оказываются близки к нулю, т. е., когда демодулятор не может надежно опознать переданный символ. Пример подобной ситуации представлен на рис. 1.7 [23].

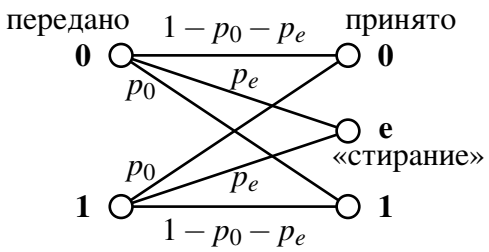


Рис. 1.6. Граф модели двоичного симметричного канала со стираниями

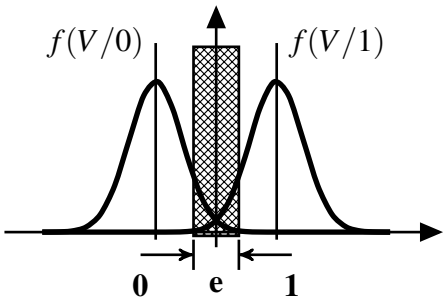


Рис. 1.7. Пример области принятия решений о стирании

Матрица переходных вероятностей канала ДСКС равна [23]

$$P_{\text{ДСКС}} = \begin{pmatrix} 1-p_0-p_e & p_e & p_0 \\ p_0 & p_e & 1-p_0-p_e \end{pmatrix}. \tag{1.9}$$

Пропускная способность канала ДСКС рассчитывается по формуле (1.10) и зависит только от вероятностей p_0 и p_e, т. е., является функцией $C_{\text{ДСКС}} = f(p_0, p_e)$ [23]:

$$C_{\text{ДСКС}} = 1 - p_e + (1-p_0-p_e)\log_2\frac{1-p_0-p_e}{1-p_e} + p_0\log_2\frac{p_0}{1-p_e}. \tag{1.10}$$

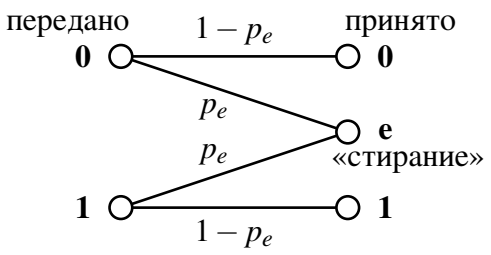


Рис. 1.8. Граф модели канала ДСКС для случая $p_0 = 0$

Важным частным случаем канала ДСКС является канал, содержащий только стирания. В таком канале $p_0 = 0$ — т. е. ошибок либо нет, либо мы ими пренебрегаем. На практике такой канал реализуется оптимальным подбором области стирания, показанной на рис. 1.7. Граф такой модели ДСКС показан на рис. 1.8. Этот вариант канала ДСКС интересен тем, что он позволяет достичь большей пропускной способности, нежели обычный канал ДСК. Пропускная способность такого канала определяется формулой [23]

$$C_{\text{ДСКС}} = 1 - p_e. \tag{1.11}$$

1.6. Двоичные цифровые каналы с группированием ошибок

1.6.1. Модель неоднородного канала

В модели неоднородного канала используется модель канала с независимыми ошибками для описания канала с зависимыми ошибками. В основу этой модели положена гипотеза о том, что дискретный канал может находиться в ρ различных состояниях, в пределах которых ошибки появляются независимо с вероятностью p_i $(i = 1, 2, \ldots, \rho)$. В этом случае знание весовых коэффициентов γ, соответствующих удельным весам различных состояний каналов, дает возможность определять различные характеристики, используя разработанный математический аппарат для независимых событий [24].

Например, вероятность появления искаженной кодовой комбинации определяется как

$$P(\geq 1, n) = \sum_{i=1}^{\rho} \gamma_i (1 - q_i^n),$$

а вероятность появления n-элементной комбинации с m и более ошибками определяется как

$$P(\geq m, n) = \sum_{i=1}^{\rho} \gamma_i P_i(\geq m, n) = \sum_{i=1}^{\rho} \left(\gamma_i \sum_{j=m}^{n} C_n^j p_i^j q_i^{n-j} \right).$$

Несомненным достоинством такого подхода является возможность распространения теоретических результатов, полученных ранее для канала с независимыми ошибками, на неоднородные каналы. Профессор П. А. Котов показал, что для практических расчетов во многих каналах можно ограничиться 2–3 состояниями канала с различными интенсивностями ошибок и с соответствующими весовыми коэффициентами. Данное предположение удобно для использования при группировании ошибок, однако экспериментальное определение весовых коэффициентов и вероятностей ошибочного приема элемента в различных состояниях достаточно сложно [24].

Эта модель получила название модели П. А. Котова.

1.6.2. Двухпараметрическая модель дискретного канала

На основании обобщения результатов проведенных испытаний дискретных каналов группа сотрудников Военной академии связи, возглавляемая доцентом Л. П. Пуртовым, выявив основные закономерности распределения ошибок реальных каналов связи, позволившие описать последовательность ошибок лишь с помощью двух параметров — p и α, где параметр α связан с угловым коэффициентом $\operatorname{tg}\beta$ наклона графика функции $P(\geq 1, n) = f(n)$ (рис. 1.3), предложила на этой основе двухпараметрическую модель дискретного канала — модель (p, α) [16].

Авторы модели доказали, что для описания зависимости $P(\geq 1,n) = f(n)$ достаточно определить экспериментально значение двух параметров: вероятности ошибки p и углового коэффициента $\operatorname{tg}\beta$. Рассуждения авторов двухпараметрической модели (p,α) по определению выражения для расчетной формулы вероятности искажения кодовой комбинации $P(\geq 1,n)$ можно проиллюстрировать решением следующего примера [16].

Пример. В ходе экспериментального исследования некоторого дискретного канала был передан испытательный тест длиной L бит. Информация передавалась в виде кодовых комбинаций длины n. В ходе обработки экспериментальных данных было установлено, что M бит принято ошибочно и ошибки содержались в B кодовых комбинациях. Построенная на основе экспериментальных данных вероятность искажения кодовой комбинации $P(\geq 1,n) = f(n)$ соответствует положению прямых III на рис. 1.3. Требуется найти выражение для вероятности искажения кодовой комбинации $P(\geq 1,n) = f(n,p,\alpha)$.

Для решения поставленной задачи вычислим вероятность битовой ошибки $p = \frac{M}{L}$ и вероятность искажения кодовой комбинации $P(\geq 1,n) = \frac{B}{L/n} = \frac{Bn}{L}$ на основании результатов экспериментального исследования, а также рассмотрим три возможных случая для зависимости $P(\geq 1,n) = f(n,p,\alpha)$.

1 случай. Группирование ошибок отсутствует и ошибки равномерно распределены по ошибочно принятым комбинациям, а в каждой искаженной комбинации содержится только одна ошибка, т. е. $P(\geq 1,n) = \frac{(B=M)n}{L} = np$.

Полученное выражение соответствует графику линии I на рис. 1.3, которая в случае одинакового масштаба десятичных порядков по горизонтальной и вертикальной оси имеет наклон к горизонтальной оси 45 градусов.

2 случай. Группирование максимально возможное — все ошибки сосредоточены в одной комбинации и все символы этой комбинации ошибочны, т. е. $P(\geq 1,n) = \frac{(B=1)(n=M)}{L} = \frac{M}{L} = p$. Полученное выражение соответствует графику линии II на рис. 1.3, т. е. предельно сильному группированию ошибок.

3 случай. Группирование реальное и график $P(\geq 1,n)$ соответствует прямым III на рис. 1.3 с углами наклона в промежутке между β_2 и β_3, т. е. $p \leq P(\geq 1,n) \leq np$.

Обозначим $\operatorname{tg}\beta = 1-\alpha$, тогда $\log P(\geq 1,n) = \log p + (1-\alpha)\log n$ или

$$P(\geq 1,n) = n^{1-\alpha}p. \tag{1.12}$$

Параметр α характеризует степень группирования ошибок и поэтому получил название *показателя группирования ошибок*. Показатель группирования является важным параметром последовательности ошибок [16].

Параметр α определяется по статистическим данным. Из выражения для $\log P(\geq 1, n)$ имеем:

$$\alpha = 1 - \frac{\log P(\geq 1, n) - \log p}{\log n}.$$

Подставив исходные значения $P(\geq 1, n)$, после преобразования получим:

$$\alpha = \frac{\log M_{\text{ош}} - \log B_{\text{ош}}(n)}{\log n}.$$

Для вычисления параметра α по статистическим данным последовательность ошибок разбивают на подпоследовательности длиной n, определяют число искаженных комбинаций $B_{\text{ош}}(n)$ и вычисляют значение α. Однако вычисление параметра α при одном значении n может дать значительную погрешность, так как значения $B_{\text{ош}}(n)$ на конечной выборке могут иметь случайные выбросы. Для более точного вычисления параметра α вычисляют ρ значений α при ρ значениях n. По полученным значениям α_i определяют параметр α как среднее значение α_i, т. е.

$$\alpha = \frac{1}{\rho} \sum_{i=1}^{\rho} \alpha_i.$$

Значения n берутся из интервала, где $np \ll 1$ [16].

При $\rho = 5 \div 10$ погрешность вычисления параметра α становится несущественной.

Значения параметра α для различных каналов связи приведены в табл. 1.1 [16].

Таблица 1.1

Значения параметра α для различных каналов связи

Типы каналов	Значение p		Значение α	
	макс.	мин.	макс.	мин.
Кабельные телефонные	10^{-4}	10^{-6}	0,7	0,5
Радиорелейные телефонные	10^{-3}	10^{-4}	0,5	0,3
КВ радиотелеграфные	10^{-1}	10^{-3}	0,4	0,3

Наибольшее значение α принимает для телефонных кабельных каналов, потому что кратковременные прерывания в различных промежуточных пунктах кабельной магистрали приводят к появлению групп с большой плотностью ошибок.

Меньшее значение α имеет для радиорелейных телефонных каналов, так как в них, наряду с участками большой плотности, наблюдаются участки с редкими ошибками, появляющимися за счет повышения уровня шумов.

В КВ радиотелеграфных каналах вследствие замирания сигнала и воздействия помех обычно наблюдаются не только пачки ошибок, но и одиночные ошибки. Поэтому показатель группирования принимает, как правило, наименьшие значения.

Для каналов тонального телеграфирования обычно параметр α имеет такое же значение, что и для кабельных телефонных каналов, так как причины возникновения ошибок одни и те же.

Достаточно хорошая аппроксимация начальной части зависимости $\log P(\geq m,n) = f(\log m)$ прямыми линиями позволяет получить приближенную формулу для вычисления $P(\geq m,n)$ при $m < \frac{n}{3}$ с использованием параметров p и α:

$$P(\geq m,n) \approx \left(\frac{n}{m}\right)^{1-\alpha} p. \tag{1.13}$$

Представленные выше выражения (1.12) и (1.13) получили название *двухпараметрической модели дискретного канала* (p,α) или модели Л. П. Пуртова [16].

1.6.3. Канал Гилберта–Эллиотта

Канал Гилберта–Эллиотта[4] (GEC) относится к дискретным каналам с памятью, в которых состояние канала зависит от предыдущего состояния [25, 26]. Эта модель предложена в 1963 г. Эллиоттом [27] и является общим случаем модели Гилберта, представленной в 1960 г. [28].

Канал GEC представляет из себя цепь Маркова первого порядка с двумя состояниями — «хорошим» **G** и «плохим» **B**, как показано на рис. 1.9.

Каждое из состояний канала можно описать как канал ДСК с соответствующей вероятностью ошибки [25, 29]. В «хорошем» состоянии вероятность битовой ошибки в канале равна p_G, в «плохом» состоянии — p_B. В любой момент времени канал может перейти из одного состояния в другое. При этом вероятности перехода могут быть отличны друг от друга. Вероятность перехода из «хорошего» состояния в «плохое» обозначим как P_{GB}, а вероятность перехода из «плохого» состояния в «хорошее» обозначим как P_{BG}, что отображено на рис. 1.9. Соответствующая этим вероятностям матрица переходов A имеет вид [25]

[4] В зарубежной и переводной литературе используется англоязычное наименование Gilbert–Elliott Channel (GEC).

$$A = \begin{pmatrix} 1 - P_{GB} & P_{GB} \\ P_{BG} & 1 - P_{BG} \end{pmatrix}. \tag{1.14}$$

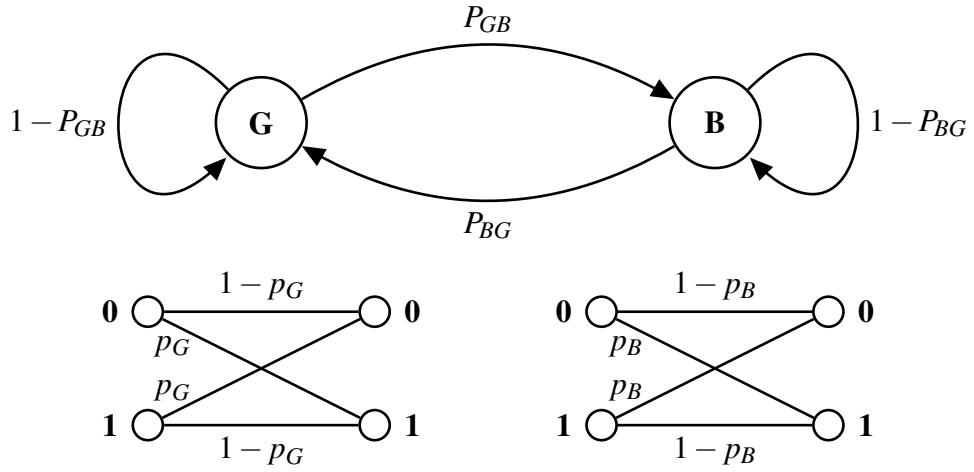


Рис. 1.9. Канал Гилберта–Эллиотта

Из рис. 1.9 следует, что финальные вероятности пребывания канала в состояниях **G** и **B** будут определяться выражениями [26]:

$$\pi_G = \frac{P_{BG}}{P_{GB} + P_{BG}}, \qquad \pi_B = \frac{P_{GB}}{P_{GB} + P_{BG}}. \tag{1.15}$$

Из формул (1.15) следует, что средняя вероятность битовой ошибки в канале может быть вычислена по формуле

$$p_e = p_G \cdot \pi_G + p_B \cdot \pi_B. \tag{1.16}$$

Вероятность того, что в блоке длиной n возникнет m ошибок рассчитывается по формуле

$$P(m,n) = \pi_G \cdot G(m,n) + \pi_B \cdot B(m,n), \tag{1.17}$$

где $G(m,n)$ — вероятность появления m ошибок в блоке длиной n, при условии, что канал во время передачи первого бита находился в состоянии **G**; $B(m,n)$ — вероятность появления m ошибок в блоке длиной n, при условии, что канал во время передачи первого бита находился в состоянии **B**.

Для расчета этих вероятностей Эллиоттом были введены рекуррентные соотношения (1.18), описывающие процесс возникновения ошибок в канале, учитывая, что канал с каждым поступившим новым разрядом может оставаться в прежнем состоянии или переходить в другое [27]:

$$
\begin{aligned}
G(m,n) = \;& G(m,n-1)\cdot(1-P_{GB})\cdot(1-p_G)+ \\
& +B(m,n-1)\cdot P_{BG}\cdot(1-p_G)+ \\
& +G(m-1,n-1)\cdot(1-P_{GB})\cdot p_G+ \\
& +B(m-1,n-1)\cdot P_{BG}\cdot p_G, \\
B(m,n) = \;& G(m,n-1)\cdot P_{GB}\cdot(1-p_B)+ \\
& +B(m,n-1)\cdot(1-P_{BG})\cdot(1-p_B)+ \\
& +G(m-1,n-1)\cdot P_{GB}\cdot p_B+ \\
& +B(m-1,n-1)\cdot(1-P_{BG})\cdot p_B.
\end{aligned}
\tag{1.18}
$$

В формулах (1.19) приведены очевидные начальные значения вероятностей (1.18) при $n = 1$ [27]:

$$
\begin{aligned}
&G(0,1) = (1-p_G), \quad B(0,1) = (1-p_B), \\
&G(1,1) = p_G, \qquad\quad B(1,1) = p_B.
\end{aligned}
\tag{1.19}
$$

Также необходимо учитывать, что:

$$
G(m,n) = B(m,n) = 0, \quad \text{при } m < 0 \text{ или } m > n.
$$

Вероятность безошибочного участка для стационарного канала GEC рассчитывается по формуле [17]:

$$
\mathrm{EFR}_{GEC}(m) = \pi_G p_G (1-p_G)^m + \pi_B p_B (1-p_B)^m. \tag{1.20}
$$

Канал GEC широко используется для описания источников ошибок в системах передачи данных, а также при анализе эффективности алгоритмов декодирования помехоустойчивых кодов [26].

Существуют исследования, показывающие, что канал GEC близок по своим свойствам к преобразованному в двоичную форму (квантованному) двухлучевому Релеевскому каналу с замираниями без поворота фазы [17].

Часто при использовании модели GEC для двоичного канала полагают, что вероятность $p_B = \frac{1}{2}$, т. е. «плохое» состояние рассматривается как полный обрыв связи [11]. Это согласуется с представлением о канале, в котором действуют мультипликативные помехи.

1.6.4. Частный случай модели Гилберта

Рассмотрим дискретный канал связи со следующими свойствами. Известны средние вероятности наличия p и отсутствия q ошибки в передаваемом элементе сообщения x_i в результате воздействия помех. Предположим, что появление ошибки в некотором элементе сообщения x_i повышает вероятность по отношению к среднему значению вероятности ошибки p в следующем x_{i+1} элементе сообщения. Аналогично предположим, что отсутствие

ошибки в элементе сообщения x_i повышает вероятность правильного приема по отношению к среднему значению вероятности отсутствия ошибки q в следующем x_{i+1} элементе сообщения. Другими словами припишем дискретному каналу связи способность некоторое время сохранять то состояние в отношении появления или отсутствия ошибок, в котором он находился в i момент времени. Предположим также, что статистические свойства последовательности ошибок в $i+1$ момент времени и в $j+1$ момент одни и те же, если известно, что в i и в j моменты канал находился в одном и том же состоянии, т. е. процесс появления ошибок в рассматриваемом канале протекает во времени однородно. Предположим также, что если известно состояние канала в i момент времени, то независимо от течения процесса появления или отсутствия ошибок в прошлом вероятностный закон его поведения в будущем таков, как если бы процесс начинался в i момент. При сделанных предположениях процесс появления ошибок в рассматриваемом дискретном канале полностью определяется средними вероятностями наличия p и отсутствия q ошибки в передаваемом элементе сообщения и матрицей

$$\pi = \begin{pmatrix} p_0(0) & p_0(1) \\ p_1(0) & p_1(1) \end{pmatrix} \tag{1.21}$$

условных вероятностей появления в последовательности ошибок 0 и 1 после 0 (первая строка) или появления в последовательности ошибок 0 и 1 после 1 (вторая строка). Для характеристики рассматриваемой модели удобно выразить условные вероятности переходов через вероятности p и q: $p_0(0) = \alpha q$, $p_0(1) = \sigma p$, $p_1(0) = \beta q$ и $p_1(1) = \tau p$. Очевидно, имеют место следующие тождества:

$$p + q = 1, \quad \alpha q + \sigma p = 1, \quad \beta q + \tau p = 1, \tag{1.22}$$

и коэффициенты α, σ, β, τ должны отображать статистическую зависимость ошибок и их тенденцию к группированию. Последовательность событий, воссоздаваемых при помощи такой модели, при условии постоянства ее параметров во времени, является однородной цепью Маркова. В табл. 1.2 приведены параметры рассматриваемой модели канала для некоторых кабельных и радиорелейных каналов, статистические характеристики и условия испытаний которых приводятся в работе [30].

Таблица 1.2

Параметры рассматриваемой модели канала для некоторых кабельных и радиорелейных каналов

p	$\alpha - 1$	$\sigma = \beta$	τ
10^{-2}	$57 \cdot 10^{-4}$	0,439	56,5
$5 \cdot 10^{-3}$	$28 \cdot 10^{-4}$	0.452	110
10^{-3}	$52 \cdot 10^{-5}$	0,480	520

Окончание табл. 1.2

Параметры рассматриваемой модели канала для некоторых кабельных и радиорелейных каналов

p	$\alpha-1$	$\sigma=\beta$	τ
$5\cdot10^{-4}$	$25\cdot10^{-5}$	0,493	1014
10^{-4}	$48\cdot10^{-6}$	0,521	4190
$5\cdot10^{-5}$	$23\cdot10^{-6}$	0,534	9320
10^{-5}	$43\cdot10^{-7}$	0,562	43800
$5\cdot10^{-6}$	$21\cdot10^{-7}$	0,574	85200
10^{-6}	$4\cdot10^{-7}$	0,602	398000

Используя методику, представленную в [31], вычисляем вероятность появления ошибок кратности m в кодовой комбинации длины n в параметрах рассматриваемой модели при $0<m<n$.

$$P(m,n) = p^m q^{n-m} \sum_{j=1}^{m} C_{m-1}^{j-1} C_{n-m-1}^{j-1} \alpha^{n-m-j-1} \beta^{2(j-1)} \tau^{m-j} \times \\ \times \left[\beta\left(\alpha+\beta\frac{n-m-j}{j}\right)+\alpha\left(\beta+\alpha\frac{j-1}{n-m-j+1}\right)\right], \tag{1.23}$$

$$P(0,n)=\alpha^{n-1}q^n, \quad P(n,n)=\tau^{n-1}p^n, \quad P(\geq 1,n)=1-\alpha^{n-1}q^n. \tag{1.24}$$

Учитывая реальные значения параметров модели и пренебрегая слагаемыми по крайней мере в τ раз меньшими, получаем упрощенную формулу, удобную для практических расчетов

$$P(m,n)=np(\tau p)^{m-1}(\alpha q)^{n-m}\beta^2=np^m(\alpha q)^{n-m}\tau^{m-1}\beta^2. \tag{1.25}$$

Для сокращения числа параметров в выражении для $P(m,n)$ выразим условные вероятности переходов матрицы π через коэффициент корреляции между соседними ошибками в последовательности ошибок R_{11}. Известно, что коэффициент корреляции между двумя событиями можно вычислить по формуле:

$$R=\frac{p(AB)-p(A)p(B)}{\sqrt{p(A)[1-p(A)]p(B)[1-p(B)]}}.$$

Коэффициенты корреляции между двумя соседними символами в последовательности ошибок при различном значении этих символов в парамет-

рах рассматриваемой модели имеют вид:

$$R_{00} = \frac{(1-p)p_0(0) - (1-p)^2}{(1-p)p} = \frac{\alpha(1-p) - (1-p)}{p};$$
$$R_{01} = \frac{(1-p)p_0(1) - (1-p)p}{(1-p)p} = \frac{\sigma p - p}{p} = \sigma - 1;$$
$$R_{11} = \frac{pp_1(1) - p^2}{(1-p)p} = \frac{\tau p - p}{1-p};$$
$$R_{10} = \frac{pp_1(0) - p(1-p)}{(1-p)p} = \frac{\beta(1-p) - (1-p)}{1-p} = \beta - 1.$$

Анализ полученных значений R_{ij} позволяет сделать ряд следующих выводов [32].

1. $R_{00} + R_{01} + R_{10} + R_{11} = 0$.
2. $|R_{00}| = |R_{01}| = |R_{10}| = |R_{11}| = R$.
3. Коэффициенты $\sigma = \beta$ являются дополнением коэффициента корреляции R до единицы, т. е. $\sigma = \beta = 1 - R$.
4. Коэффициент $\alpha = \frac{1-p(1-R)}{1-p} \cong 1$.
5. Коэффициент $\tau = \frac{1-(1-p)(1-R)}{p} \cong \frac{R}{p}$.

Окончательно матрица π и формула (1.25) принимают вид:

$$\pi = \begin{pmatrix} 1-p(1-R) & p(1-R) \\ (1-p)(1-R) & 1-(1-p)(1-R) \end{pmatrix};$$

$$P(m,n) \approx np(1-p)^{n-m}R^{m-1}(1-R)^2.$$

1.7. Троичные цифровые каналы

Троичные каналы используются в тех случаях, когда система передачи данных предполагает использование информационных сигналов, принимающих три состояния. Как правило эти состояния обозначаются либо как $\{0,1,2\}$, либо как $\{0,1,-1\}$. По аналогии с обозначением двоичного элемента («бит»), для обозначения единицы информации, принимающей три различных значения, используют термин «трит»[5] [33].

1.7.1. Троичный симметричный канал

Троичный симметричный канал[6] является вариантом q-ичного симметричного канала без памяти при $q = 3$.

Граф, описывающий модель ТСК, представлен на рис. 1.10 [2].

[5] От англ. trit — **tr**inary dig**it**.

[6] В зарубежной литературе используется англоязычное наименование Ternary Symmetric Channel (TSC).

Входом и выходом данного канала являются наборы $X = \{0,1,2\}$ и $Y = \{0,1,2\}$ из трех возможных троичных символов, соответственно. ТСК характеризуется набором переходных вероятностей $P(Y|X)$, определяющих вероятность приёма из канала символа Y при передаче символа X. Переходные вероятности для ТСК задаются выражениями

$$\begin{aligned} &P(0|0) = P(1|1) = P(2|2) = 1-p; \\ &P(1|0) = P(2|0) = P(0|1) = P(2|1) = P(0|2) = P(1|2) = p, \end{aligned} \tag{1.26}$$

где p — вероятность ошибки в канале.

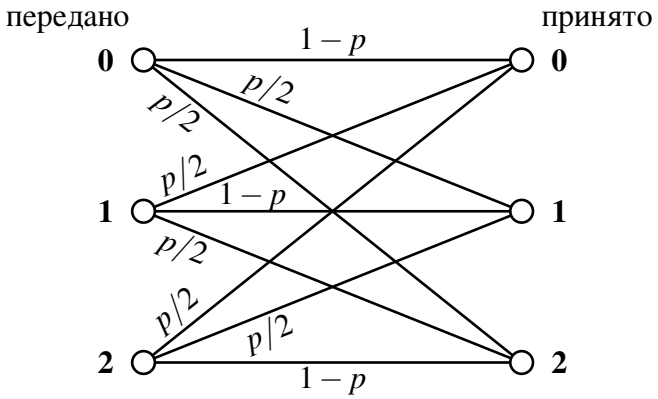


Рис. 1.10. Граф модели троичного симметричного канала

1.7.2. Троичный строго симметричный канал

Троичный строго симметричный канал[7] представляет собой троичный канал, в котором каждый столбец матрицы переходов представляет собой перестановку других столбцов и каждая строка представляет собой перестановку других строк [34].

Граф, описывающий модель ТССК, представлен на рис. 1.11 [34].

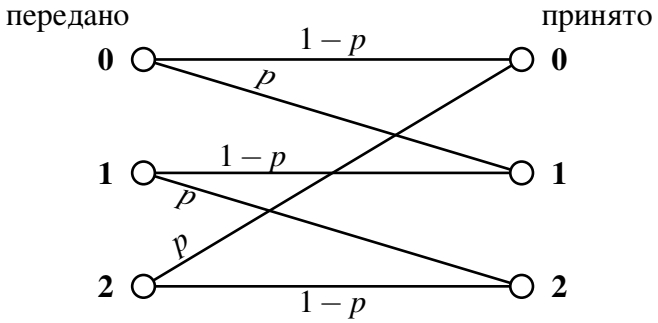


Рис. 1.11. Граф модели троичного строго симметричного канала

[7] В зарубежной литературе используется англоязычное наименование Ternary Strongly Symmetric Channel (TSSC).

Переходные вероятности для ТССК задаются выражениями

$$\begin{aligned} &P(0|0) = P(1|1) = P(2|2) = 1 - p; \\ &P(1|0) = P(2|1) = P(0|2) = p; \\ &P(2|0) = P(0|1) = P(1|2) = 0, \end{aligned} \tag{1.27}$$

где p — вероятность ошибки в канале [34].

1.7.3. Троичный несимметричный канал

Троичный несимметричный канал[8] является вариантом троичного канала без памяти в котором не допускаются переходы $1 \longrightarrow 2$ и $2 \longrightarrow 1$. Во входном и выходном наборах состояний этого канала в некоторых случаях удобно обозначать состояние 2 как -1. То есть входной и выходной наборы будут равны $X = Y = \{0, 1, -1\}$ [35].

Граф, описывающий модель ТНСК, представлен на рис. 1.12 [35].

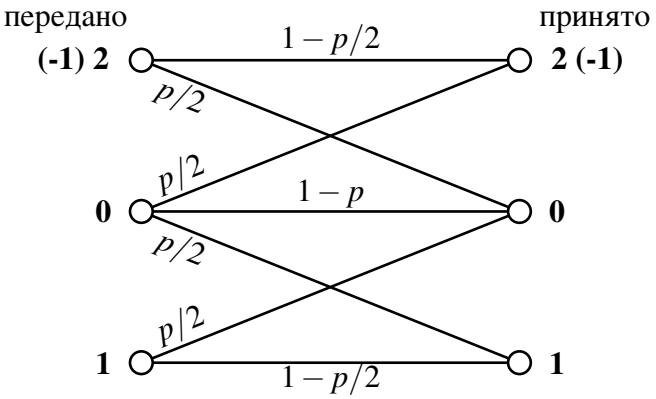


Рис. 1.12. Граф модели троичного несимметричного канала

Переходные вероятности для ТНСК задаются выражениями

$$\begin{aligned} &P(0|0) = 1 - p; \\ &P(1|1) = P(2|2) = 1 - p/2; \\ &P(1|0) = P(2|0) = P(0|1) = P(0|2) = p/2; \\ &P(2|1) = P(1|2) = 0, \end{aligned} \tag{1.28}$$

где p — вероятность ошибки в канале.

Модель ошибок, описываемая графом ТНСК, показанным на рис. 1.12, соответствует физическим особенностям энергонезависимой твердотельной памяти типа EEPROM [35].

[8] В зарубежной литературе используется англоязычное наименование Ternary Non-Symmetric Channel (TNSC).

Контрольные вопросы

1. Приведите основные параметры моделей каналов передачи данных.
2. Каким образом расчитывается распределение ошибок в комбинациях различной длины?
3. Дайте понятие двоичного симметричного канала. Как рассчитывается его пропускная способность?
4. Что такое двоичный симметричный канал со стираниями?
5. Какие принципы лежат в основе двухпараметрической модели дискретного канала?
6. Опишите модель канала Гилберта–Эллиотта.
7. Опишите модель троичного несимметричного канала.
8. Какие положения лежат в основе модели, являющейся частным случаем модели Гилберта?
9. Докажите равенство $R_{00} + R_{01} + R_{10} + R_{11} = 0$.
10. Докажите равенство $|R_{00}| = |R_{01}| = |R_{10}| = |R_{11}|$.
11. Поясните равенство $\sigma = \beta$.

Рекомендуемая литература

1. Шеннон, К. Математическая теория связи / К. Шеннон // Работы по теории информации и кибернетике. — М. : Изд-во иностранной литературы, 1963.

2. Теория и техника передачи данных и телеграфия : учебник / Л. П. Пуртов, А. С. Замрий, А. И. Захаров, Н. И. Иванов, В. М. Охорзин. — СПб. : ВАС, 1973.

3. Прокис, Дж. Цифровая связь / Дж. Прокис ; под ред. Д. Д. Кловского. — М. : «Радио и Связь», 2000.

4. Вернер, М. Основы кодирования : учебник для ВУЗов / М. Вернер. — М. : Техносфера, 2006.

5. Владимиров, С. С. Математические основы теории помехоустойчивого кодирования : учебное пособие / С. С. Владимиров. — СПб. : СПбГУТ, 2016.

2. ИНФОКОММУНИКАЦИОННЫЕ СИСТЕМЫ С ПРИМЕНЕНИЕМ ПОМЕХОУСТОЙЧИВЫХ КОДОВ, ОБНАРУЖИВАЮЩИХ ОШИБКИ

Большинство методов обнаружения ошибок основаны на использовании дополнительных избыточных элементов, передаваемых по каналу в сторону получателя. Передаётся такая избыточная информация в составе каждого блока данных при блочном кодировании либо в составе непрерывной последовательности в непрерывных кодах. Сами избыточные элементы формируются по определенному алгоритму и зависят от передаваемых информационных элементов. Именно вводимая избыточность позволяет судить с определённой вероятностью о наличии ошибок в принятом сообщении.

В настоящем учебном пособии рассматриваются различные блочные помехоустойчивые коды с обнаружением ошибок. Наиболее простым методом обнаружения ошибок, широко применяемым в различных системах и протоколах передачи данных, является контроль на четность. Его достоинством является малая избыточность и простота реализации.

2.1. Коды с проверкой на четность и их характеристика

2.1.1. Краткая характеристика кода

Кодами с проверкой на четность[9] называют семейство двоичных помехоустойчивых кодов, в которых для обнаружения или исправления ошибок используются линейные суммы информационных бит, так называемые биты четности[10] или контрольные биты [13, 36].

Часто под кодом с проверкой на четность понимают блочный систематический (n,k)-код с одним проверочным элементом[11]. Абсолютная избыточность такого кода равна $(n-k)=1$, а относительная — $\eta = \frac{n-k}{n} = \frac{1}{n}$. Относительная кодовая скорость равна

$$R = \frac{k}{n} = \frac{n-1}{n} = 1 - \frac{1}{n} = 1 - \eta.$$

Контрольный бит (бит четности) в таком коде может равняться нулю или единице. Значение этого бита выбирается таким, чтобы сумма всех бит в кодовом слове была четной или нечетной. Если бит четности таков, что сумма всех бит четная, то код называют кодом с положительной четностью[12]; если же добавление бита четности приводит к получению нечетной суммы всех

[9] Parity-check codes (англ.)

[10] Parity bits (англ.)

[11] Single parity-check code, SPC-code (англ.)

[12] Even parity (англ.)

бит, то говорят про код с отрицательной четностью[13]. Как правило используются именно коды с положительной четностью, которые и будут рассматриваться в дальнейшем [13, 36].

Любая разрешенная кодовая комбинация кода с положительной четностью имеет четное число «1», число разрешенных кодовых комбинаций равно $2^k = 2^{n-1}$, т. е. ровно половине от общего числа n-элементных двоичных комбинаций. Тогда относительная избыточность кода по комбинациям, как отношение числа запрещенных комбинаций к общему числу n-элементных комбинаций, будет равна $\frac{1}{2}$.

2.1.2. Кодирование

Кодирующее устройство является довольно простым, алгоритм его работы состоит в нахождении проверочного элемента, равного сумме по mod 2 двоичных информационных элементов.

Пусть k-элементная информационная комбинация, где $k = (n-1)$, имеет общий вид $(a_0, a_1, a_2, \ldots, a_{k-1})$. Проверочный элемент b будет равен:

$$b = \sum_{i=0}^{k-1} a_i \pmod 2. \tag{2.1}$$

Образующая матрица кода с проверкой на четность имеет вид

$$\mathbf{G} = \underbrace{\begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 1 \\ 0 & 1 & 0 & \cdots & 0 & 1 \\ 0 & 0 & 1 & \cdots & 0 & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 1 \end{bmatrix}}_{\mathbf{E}_{k\times k}\qquad\qquad\mathbf{R}_{1\times k}}, \tag{2.2}$$

где $\mathbf{E}_{k\times k}$ — единичная матрица информационных элементов порядка k; $\mathbf{R}_{1\times k}$ — матрица (вектор-столбец) проверочных элементов.

По виду матрицы $\mathbf{G}$ можно сделать вывод, что код с проверкой на четность, во-первых, является линейным, т. е. сумма по mod 2 разрешенных комбинаций порождает также разрешенную комбинацию и, во-вторых, его минимальное кодовое расстояние Хэмминга равно $d_{\min} = 2$. Отсюда следует, что код с проверкой на четность способен обнаружить все однократные ошибки $(t = 1)$, так как $t = d_{\min} - 1$. В действительности код будет обнаруживать все ошибки нечетной кратности, так как поэлементная сумма по mod 2 разрешенной комбинации с четным числом единиц и комбинации ошибок с нечетным

[13] Odd parity (англ.)

числом единиц (ошибок) порождает комбинацию с нечетным числом «1», т. е. запрещённую комбинацию.

Для примера рассмотрим простой код $(4,3)$ положительной четности. Его кодовые слова показаны в табл. 2.1. Видно, что в каждом кодовом слове находится четное число единиц [13].

Таблица 2.1

Пример кода $(4,3)$ *положительной четности*

Информационные элементы $a_0a_1a_2$	Бит четности a_3	Информационные элементы $a_0a_1a_2$	Бит четности a_3
000	0	100	1
001	1	101	0
010	1	110	0
011	0	111	1

2.1.3. Особенности декодирующего устройства

Проверочная матрица $\mathbf{H}$ кода (n,k) с проверкой на четность имеет вид:

$$H = \left[\mathbf{R}^T \quad \mathbf{E}_{(n-k)\times(n-k)}\right] = \left[\mathbf{R}^T \quad \mathbf{E}_{1\times 1}\right], \tag{2.3}$$

где $\mathbf{R}^T$ — транспонированная матрица проверок в порождающей матрице (2.2); $\mathbf{E}_{1\times 1} = 1$ — единичная матрица первого порядка.

Таким образом, проверочная матрица (2.3) будет представлять собой вектор-строку из n единиц и иметь развернутый вид:

$$\mathbf{H} = \underbrace{[1\ 1\ 1\ \ldots\ 1}_{\mathbf{R}^T}\ \underbrace{1]}_{\mathbf{E}_{1\times 1}}.$$

Легко показать, что множество разрешенных комбинаций кода с проверкой на четность является нулевым пространством по отношению к проверочной матрице $\mathbf{H}$, т. е. будет выполняться равенство $\mathbf{G}\cdot\mathbf{H}^T = 0$. Также произведение вектор-строки любой разрешенной комбинации кода с проверкой на четность на $\mathbf{H}^T$ будет равно «0», так как произведение вектор-строки двоичной комбинации с четным числом «1» на $\mathbf{H}^T$ всегда будет равно «0» по mod 2. В общем случае, умножив принятую n-элементную комбинацию на $\mathbf{H}^T$, получим синдром S, который будет равен «0», если в принятой комбинации ошибок нет или они не обнаруживаются кодом, и равен «1», если в принятой комбинации возникло нечетное число ошибок.

Исходя из сказанного, алгоритм декодирования состоит в простом сложении по mod 2 всех элементов принятой комбинации $(c_0, c_1, c_2, \ldots, c_{n-1})$, т. е.

$$S = \sum_{i=0}^{n-1} c_i \pmod 2. \tag{2.4}$$

Как сказано выше, нулевой синдром ($S = 0$) будет иметь место в том случае, когда в принятой комбинации возникнет четное число ошибок. Такая ситуация приводит к необнаруживаемым ошибкам.

Таким образом, исходя из особенностей n-элементного кода с проверкой на четность, вероятностные характеристики кода для канала ДСК с вероятностью ошибки двоичного символа p будут следующие:

- вероятность приема комбинации без ошибок (правильного приема):

$$P_{\text{пп}} = (1-p)^n; \tag{2.5}$$

- вероятность приема комбинации с обнаруживаемыми ошибками:

$$P_{\text{оо}} = \sum_{i=1,3,5,\ldots} C_n^i p^i (1-p)^{n-i} = \frac{1}{2}\left[1-(1-2p)^n\right]; \tag{2.6}$$

- вероятность приема комбинации с необнаруживаемыми ошибками:

$$P_{\text{но}} = \sum_{i=2,4,6,\ldots} C_n^i p^i (1-p)^{n-i} = \frac{1}{2}\left[1+(1-2p)^n\right] - (1-p)^n. \tag{2.7}$$

Среднюю вероятность ошибки на 1 бит P_b в переданных получателю n-элементных комбинациях (с необнаруженными ошибками) найдем как отношение среднего количества ошибочных элементов в n-элементной комбинации к общей её длине [13, 20]:

$$P_{\text{b}} = \frac{1}{n}\sum_{i=2,4,\ldots} iP(i,n) = \frac{1}{n}\sum_{i=2,4,\ldots} iC_n^i p^i (1-p)^{n-i}. \tag{2.8}$$

2.1.4. Примеры реальных систем с применением кодов с проверкой на четность

Приведем теперь примеры конкретного применения кода с проверкой на четность в реальных системах или протоколах.

Коды с проверкой на четность имеют простую реализацию и благодаря этому широко используются там, где быстродействие важнее кратности гарантированно обнаруживаемой ошибки, или в случаях, когда достаточно простого обнаружения одиночных ошибок. Например, простая проверка на четность используется в компьютерных шинах SCSI и PCI для контроля правильности передаваемых данных и широко применялась при записи на магнитные ленты [37]. Проверка на четность применяется в последовательных интерфейсах. К примеру, в RS-232 применяются схемы, где к 7 или 8 информационным битам добавляется бит четности [38].

Наиболее простой пример — международный код для обмена информацией КОИ-7 (ASCII — American Standard Code for Information Interchange), в котором сообщения представляются байтами, состоящими из 7 информационных бит и одного проверочного элемента на четность (хотя возможен и код с проверкой на нечетность). Аналогом кода ASCII является международный код МТК-5, версия МККТТ.

Пример 2.1. Определим вероятностные характеристики кода с проверкой на четность КОИ-7 в соответствии с (2.5)–(2.8) для канала ДСК с вероятностью ошибки $p = 10^{-3}$:

$P_{\text{пп}} = (1-p)^8 = 0{,}999^8 = 0{,}992;$

$P_{\text{оо}} = \frac{1}{2}\left[1-(1-2p)^8\right] = \frac{1}{2}\left[1-0{,}998^8\right] = 7{,}9\cdot 10^{-3};$

$P_{\text{но}} = \frac{1}{2}\left[1+(1-2p)^8\right] - (1-p)^8 = \frac{1}{2}\left[1+0{,}998^8\right] - 0{,}999^8 = 1\cdot 10^{-4};$

$P_{\text{b}} = \frac{1}{8}\sum\limits_{i=2,4,6,8} iP(i,8) = \frac{1}{8}\sum\limits_{i=2,4,6,8} iC_8^i p^i (1-p)^{8-i} \approx \frac{1}{8} 2C_8^2 p^2 (1-p)^6 = 6{,}9\cdot 10^{-6}.$

На рис. 2.1 приведены вероятностные характеристики кода КОИ-7 для канала ДСК, полученные расчетом по формулам (2.5)–(2.8).

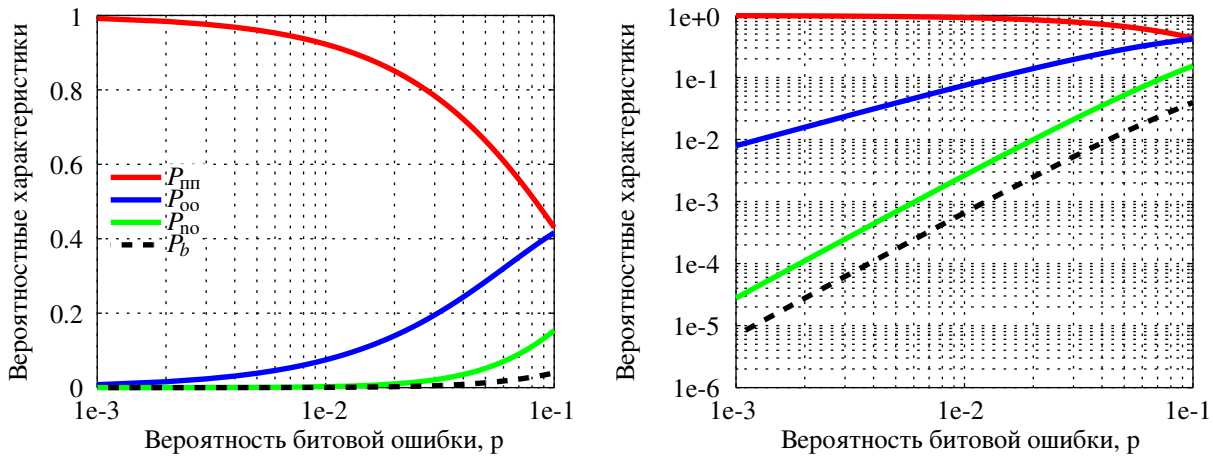


Рис. 2.1. Вероятностные характеристики кода КОИ-7 для канала ДСК

На базе простого метода контроля комбинации на четность в ряде систем реализуют его модификации. Рассмотрим некоторые из них.

Протокол передачи файлов XModem, разработанный для связи между персональными компьютерами, для повышения надёжности использует двухбайтовую нумерацию блоков: первый из двух байт представляет натуральный номер блока, а второй — его двоичное дополнение, другими словами, его двоичная инверсия. Например, первому блоку будет соответствовать двухбайтовый номер $(01\text{FE})_{16}$ в шестнадцатеричной системе счисления. В двоичной системе это будет комбинация $(0000\ 0001\ 1111\ 1110)_2$. Как видно, здесь мы имеем 8 комбинаций простейшего помехоустойчивого кода

$(n,k)=(2,1)$ с проверкой на нечетность, т. е. к одному информационному элементу $(k=1)$ добавлен один проверочный элемент на нечетность $(n-k)=1$. Любая двухэлементная разрешенная комбинация такого простого кода всегда будет иметь нечетное число «1» и, соответственно, вес комбинации также будет равен «1», а минимальное кодовое расстояние равно 2. Поэтому однократные ошибки в двухэлементных комбинациях будут обнаруживаться, а двукратные ошибки обнаруживаться не будут и приведут к неверному определению номера блока.

Характеристики такого двухбайтового кода будут следующие.

Абсолютная избыточность по элементам равна 8, а относительная избыточность — 0,5. Поэтому кодовая скорость будет $R=1/2$.

Вероятностные характеристики для канала ДСК с вероятностью ошибки в двоичном сигнале p будут определяться выражениями:

- вероятность правильного приема номера блока

$$P_{\text{пп}}=(1-p)^{16}; \tag{2.9}$$

- вероятность появления обнаруживаемых ошибок

$$P_{\text{оо}}=\sum_{i=1}^{8}C_8^i\theta^i(1-\theta)^{8-i}, \tag{2.10}$$

где $\theta=2p(1-p)$ — вероятность однократной ошибки в двухэлементной двоичной комбинации;

- вероятность неверного определения номера блока

$$P_{\text{но}}=\sum_{i=1}^{8}C_8^i p^{2i}(1-p)^{16-2i}. \tag{2.11}$$

Расчетные значения вероятностных характеристик данного кода для канала ДСК с вероятностью ошибки $p=10^{-3}$ будут равны

$$P_{\text{пп}}=0{,}9841; \quad P_{\text{оо}}=0{,}01587; \quad P_{\text{но}}=3\cdot 10^{-5}.$$

На рис. 2.2 приведены вычисленные по формулам (2.9)–(2.11) графики вероятностных характеристик двухбайтового кода проверки на четность, использующегося в протоколе Xmodem, для канала ДСК.

В ряде случаев проверка на четность используется для расширения другого помехоустойчивого кода. Например, в расширенном коде Хэмминга дополнительная проверка на четность позволяет в режиме только обнаружения ошибок обнаруживать все однократные, двукратные и трехкратные ошибки, а также ошибки более высокой нечетной кратности [23].

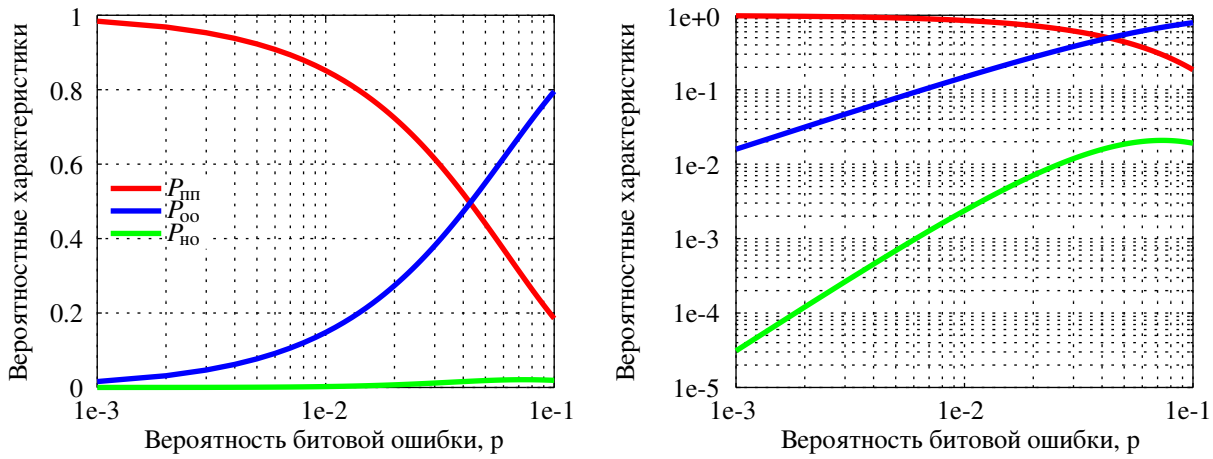


Рис. 2.2. Вероятностные характеристики двухбайтового кода проверки на четность, использующегося в протоколе Xmodem, для канала ДСК

2.2. Методы обнаружения ошибок в блоках данных с использованием контрольной суммы

Контрольная сумма (КС) блока или кадра (FCS — Frame Check Sequnce) вычисляется по определенному алгоритму на передаче и посылается вместе с информацией на приемную сторону. Приемная сторона по принятой информационной части блока повторно вычисляет контрольную сумму по тому же алгоритму и сравнивает с принятой КС. При совпадении контрольных сумм считается, что блок данных принят правильно, хотя в действительности в блоке могут быть ошибки, не обнаруживаемые помехоустойчивым кодом.

Рассмотрим несколько алгоритмов вычисления контрольной суммы.

2.2.1. Метод формирования контрольной суммы блока по mod 255

Для метода характерно, что блок имеет байтовую структуру, а контрольная сумма размером в один байт вычисляется путем сложения десятичных значений всех информационных байтов в коде ASCII и последующим приведением суммы по mod 255. Такой алгоритм реализован в упомянутом ранее протоколе передачи файлов между компьютерами XModem. Протокол XModem с контрольной суммой байтов по mod 255 применяется во многих терминальных программах.

Блок данных в этом протоколе состоит из 128 байт. Ошибки в блоке будут обнаружены, если контрольные суммы, вычисленные на передаче и на приеме, не совпадают.

Необнаруженными ошибки в блоке будут в том случае, когда суммарные десятичные значения ошибочных позиций среди «1» в исходном блоке будут компенсироваться суммарными десятичными значениями ошибочных

позиций среди «0» в исходном блоке, например, $\sum_{n_i} 2^{n_i} = \sum_{m_j} 2^{m_j}$, где n_i — ошибочные позиции среди «1», m_j — ошибочные позиции среди «0» в исходном блоке. Так как блок имеет байтовую структуру, то значения n_i и m_j могут принимать значения от 0 до 7 по всему множеству байтов от 1 до 128. Получение точного аналитического выражения для вероятности появления необнаруживаемых ошибок в блоке представляет собой довольно трудоемкую задачу. Поэтому целесообразно ограничиться приближёнными оценками или оценить вероятность необнаруживаемых ошибок путем моделирования.

Применительно к каналу без памяти ДСК с вероятностью ошибки в двоичном элементе p вероятность правильного приема для рассматриваемого примера будут определяться выражением:

$$P_{\text{пп}} = \left[(1-p)^8\right]^{128}. \tag{2.12}$$

Рассматривая вероятность приема блока с необнаруживаемыми ошибками при малых вероятностях p в двоичном симметричном канале и в предположении равновероятных «0» и «1» в блоке, можно ограничиться двукратными ошибками типа замещения в одной строке: одна ошибка среди единичных элементов строки, а другая — среди нулевых элементов той же строки. Так как «1» и «0» предполагаются равновероятными, то для приближённых расчетов можно принять, что в каждой из 8 строк блока будет в среднем 64 единицы и 64 нуля. Тогда вероятность двукратной необнаруживаемой ошибки в блоке можно приближенно оценить выражением:

$$P_{\text{но}}(t=2) = C_8^1 \left[C_{64}^1 p(1-p)^{63}\right]^2 (1-p)^{128\cdot 7} = 32768 p^2 (1-p)^{1022}. \tag{2.13}$$

Расчетные значения вероятности $P_{\text{но}}(t=2)$ для некоторых p, при условии, что средний вес строки $\bar{w} = 64$, представлены в табл. 2.2.

Для более точной оценки вероятности необнаруживаемых ошибок можно учесть также трёхкратные ошибки, которые код не обнаружит. К таким ошибкам относятся однократная ошибка в i-й байтовой строке, $1 \le i \le 7$, и двукратная ошибка в $(i-1)$-й байтовой строке. Причём, ошибки в i-й строке и в $(i-1)$-й строке должны быть в противоположных символах, например, среди «1» в i-й строке и два «0» в $(i-1)$-й строке или наоборот. При этом нулевой строке $(i=0)$ соответствуют младшие разряды байтов.

При определенных выше условиях вероятность трёхкратных необнаруживаемых ошибок можно определить из выражения:

$$\begin{aligned} P_{\text{но}}(t=3) = 2\cdot 7 \left[C_{64}^1 p(1-p)^{63}(1-p)^{64}\right] \times \\ \times \left[C_{64}^2 p^2 (1-p)^{62}(1-p)^{64}\right] \cdot (1-p)^{128\cdot 6}. \end{aligned} \tag{2.14}$$

В первой квадратной скобке стоит вероятность однократной ошибки в i-й строке, а во второй квадратной скобке — вероятность появления двукратной ошибки типа замещения в $(i-1)$-й строке. Последний множитель — вероятность отсутствия ошибок в остальных строках блока. Коэффициент «2» соответствует двум ситуациям: одна — когда одна ошибка в i-й строке возникает среди «1» и две ошибки в $(i-1)$-й строке возникают среди нулевых символов; вторая — наоборот, когда ошибка в i-й строке возникает среди «0» и две ошибки в $(i-1)$-й строке возникают среди единичных символов.

Расчетные значения вероятности $P_{\text{но}}(t=3)$ для некоторых p и среднем весе строки $\bar{w}=64$ представлены в табл. 2.2.

В табл. 2.2 также приведены расчетные значения суммы $P_{\text{но}}(t=2)$ и $P_{\text{но}}(t=3)$.

Таблица 2.2

Вероятности необнаруженных ошибок при использовании контрольной суммы блока по mod 255

p	10^{-2}	10^{-3}	10^{-4}
$P_{\text{но}}(t=2)$	$1{,}1\cdot10^{-4}$	$1{,}2\cdot10^{-2}$	$2{,}9\cdot10^{-4}$
$P_{\text{но}}(t=3)$	$6{,}3\cdot10^{-5}$	$6{,}44\cdot10^{-4}$	$1{,}61\cdot10^{-6}$
$P_{\text{но}}(t=2)+P_{\text{но}}(t=3)$	$1{,}7\cdot10^{-4}$	$1{,}21\cdot10^{-2}$	$2{,}9\cdot10^{-4}$

На рис. 2.3 приведены полученные расчетом вероятностные характеристики контрольной суммы блока по mod 255, использующейся в протоколе Xmodem, для канала ДСК.

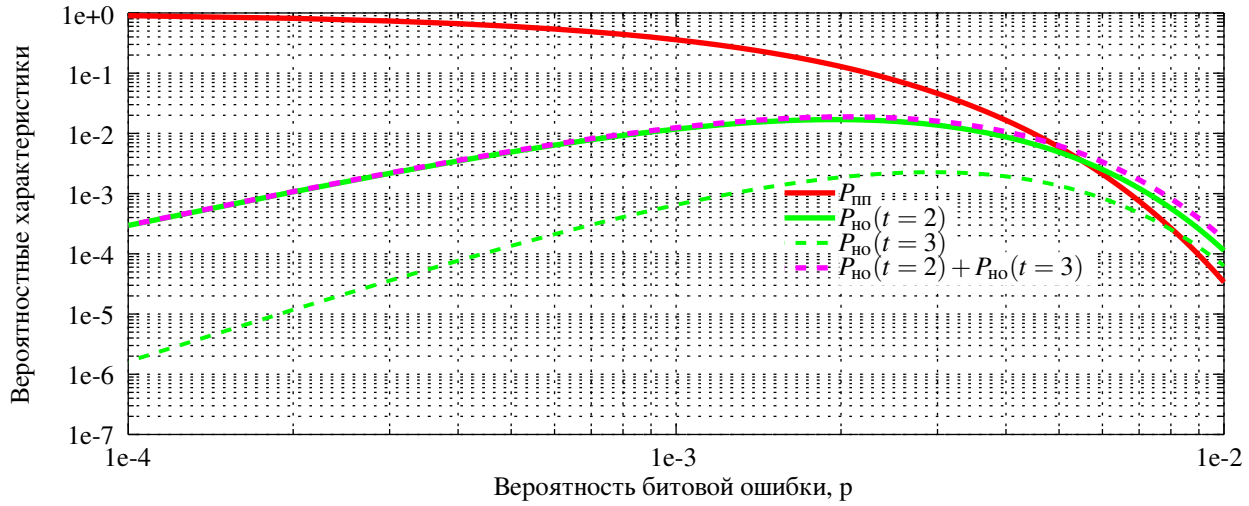


Рис. 2.3. Вероятностные характеристики контрольной суммы блока по mod 255, использующейся в протоколе Xmodem, для канала ДСК

2.2.2. Метод формирования контрольной суммы с проверкой на четность по строкам

Пусть и в этом варианте блоки двоичных данных имеют байтовую структуру, и контрольная сумма равна одному дополнительному байту. В отличие от предыдущего, контрольная сумма вычисляется как поэлементная сумма всех информационных байт по mod 2. Следовательно, каждая из 8 строк является помехоустойчивым кодом с проверкой на четность. Тогда вероятность приема блока с необнаруживаемыми ошибками будет определяться как вероятность того, что в строках появится только четное число ошибок. Для сравнения эффективности такого помехоустойчивого кода с эффективностью предыдущего кода примем, что длина блока данных также состоит из 128 байт, включая контрольный. Тогда вероятность приема блока по каналу ДСК с необнаруживаемыми ошибками будет определяться выражением

$$P_{\text{но}} = \sum_{j=1}^{8} C_8^j \theta^j (1-p)^{128(8-j)}, \tag{2.15}$$

где θ — вероятность появления четного числа ошибок в одной строке, которая для нашего примера определяется выражением:

$$\theta = \sum_{i=2,4,6,\ldots} C_{128}^i p^i (1-p)^{128-i}.$$

Расчетные значения вероятности $P_{\text{но}}$ для некоторых p представлены в табл. 2.3.

Таблица 2.3

Вероятности необнаруженных ошибок при использовании контрольной суммы с проверкой на четность по строкам

p	10^{-2}	10^{-3}	10^{-4}
θ	$2{,}61 \cdot 10^{-1}$	$7{,}2 \cdot 10^{-1}$	$1 \cdot 10^{-4}$
$P_{\text{но}}$	$8{,}76 \cdot 10^{-3}$ $j = 1 \div 8$	$2{,}35 \cdot 10^{-2}$ $j = 1$	$7{,}3 \cdot 10^{-4}$ $j = 1$

На рис. 2.4 приведены расчетные вероятностные характеристики контрольной суммы с проверкой на четность по строкам для канала ДСК.

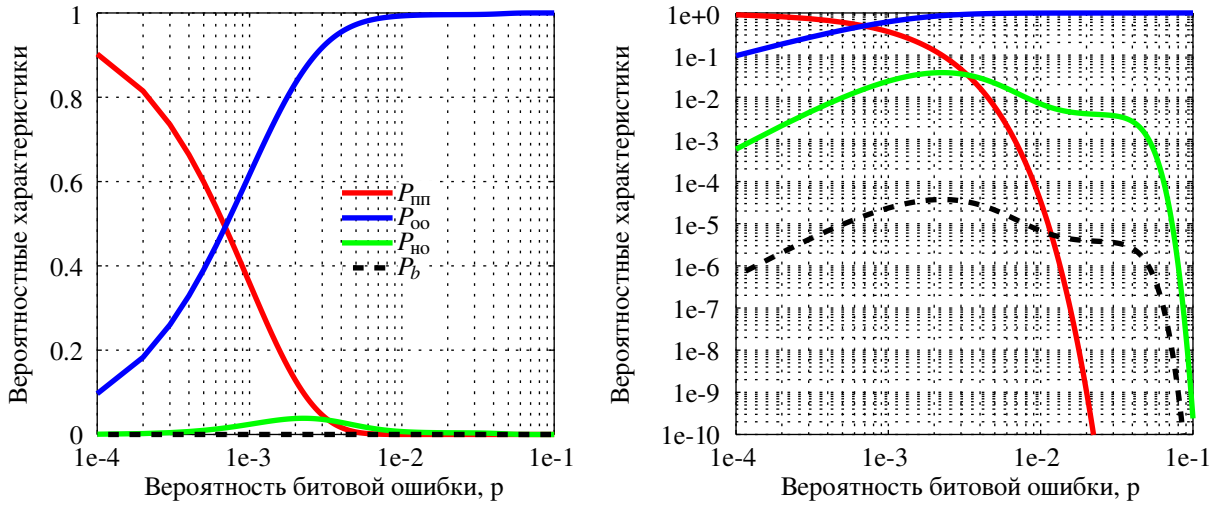


Рис. 2.4. Вероятностные характеристики контрольной суммы с проверкой на четность по строкам для канала ДСК

2.2.3. Метод контроля четности по строкам и столбцам блока

Данный метод является модификацией рассмотренного ранее метода с простой проверкой комбинации на четность. Отличие заключается в том, что кодовое сообщение представляется в виде двоичной прямоугольной матрицы из k строк и n столбцов. Таким образом общее число элементов блока $N = k \cdot n$. Контрольные элементы блока определяются как проверки на четность отдельно для каждой строки и для каждого столбца. Исходя из структуры кодового блока, такие коды называют матричными или кодами с двухмерной схемой проверки на четность. Помимо этого, в литературе их также называют прямоугольными или композиционными [13, 39], а также прямым произведением кодов [2].

Код с проверкой на четность по строкам и столбцам имеет следующую скорость:

$$R = \frac{(k-1)(n-1)}{N}.$$

Абсолютная избыточность кода: $r = N - (k-1)(n-1)$ [13].

Для примера рассмотрим кодовое слово прямоугольного кода $(30,20)$, у которого $k=5$, а $n=6$:

$$\begin{array}{cccccc} 1 & 0 & 0 & 1 & 1 & \mathbf{1} \\ 0 & 1 & 1 & 0 & 0 & \mathbf{0} \\ 1 & 1 & 0 & 0 & 1 & \mathbf{1} \\ 0 & 0 & 1 & 0 & 1 & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{0} \end{array}$$

Жирным шрифтом отмечены биты четности. В каждой строке и каждом столбце получившегося кодового блока находится четное число единиц. Таким образом, это код с положительной четностью.

Код с двухмерной схемой проверки на четность имеет минимальное расстояние Хэмминга $d_{\min}$, равное 4, поэтому он имеет более высокие обнаруживающие способности по сравнению с простой проверкой комбинации на четность. В частности, данный матричный код сохраняет обнаруживающие способности кода с проверкой на четность, т. е. может обнаруживать все ошибки нечетной кратности, но, кроме того, может дополнительно обнаруживать любые двукратные ошибки в блоке. Минимальная кратность необнаруживаемых ошибок равна минимальному кодовому расстоянию, т. е. 4, при этом ошибочные позиции должны располагаться в вершинах условного прямоугольника. Например, ошибки в выделенных рамками позициях в следующем примере обнаружены не будут, так как не изменяют первоначальную четность по строкам и по столбцам:

$$\begin{array}{cccccc} 1 & 0 & 0 & 1 & 1 & \mathbf{1} \\ 0 & \boxed{0} & 1 & \boxed{1} & 0 & \mathbf{0} \\ 1 & 1 & 0 & 0 & 1 & \mathbf{1} \\ 0 & \boxed{1} & 1 & \boxed{1} & 1 & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{0} \end{array}$$

Могут быть необнаруживаемые ошибки и более высокой четной кратности — 6, 8, ...

Пусть имеется блок из k строк и n столбцов. Тогда в канале ДСК с вероятностью ошибки p в одном элементе можно определить вероятность 4-кратной необнаруживаемой ошибки в блоке из выражения:

$$P_{\text{но}}(4,N) = C_n^2 C_k^2 p^4 (1-p)^{N-4}, \tag{2.16}$$

где $N = nk$ — общее число двоичных элементов блока.

Аналогично может быть найдено выражение для 6-кратных необнаруживаемых ошибок, которое в результате проведенного анализа, имеет вид:

$$P_{\text{но}}(6,N) = C_n^2 C_{n-2}^1 C_k^3 p^6 (1-p)^{N-6}. \tag{2.17}$$

Рассмотренный метод контроля за ошибками применяется в байт-ориентированном асинхронном бинарном протоколе канального уровня с использованием кода ASCII (МТК-5). Для сравнительной оценки метода с ранее рассмотренными выберем длину кадра также равную 128 байтам. Тогда блок данных может быть представлен двоичной матрицей, состоящей из $n = 128$ столбцов и $k = 8$ строк. Таким образом, каждый байт является столбцом с одним проверочным элементом на четность, т. е. код $(8,7)$ с проверкой на четность. Также каждая строка матрицы представляет собой код $(128,127)$ с проверкой на четность.

На рис. 2.5 приведены расчетные вероятностные характеристики матричного кода, использующегося в байт-ориентированном асинхронном бинарном протоколе канального уровня с использованием кода ASCII (МТК-5), для канала ДСК при длине блока $n = 128$ байт.

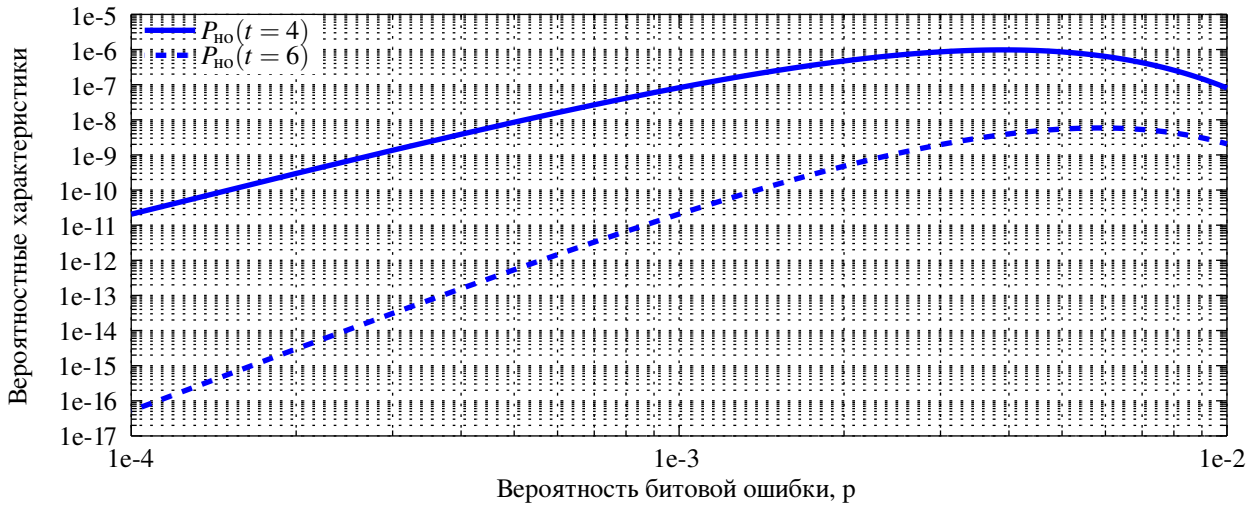


Рис. 2.5. Вероятностные характеристики матричного кода, использующегося в байт-ориентированном асинхронном бинарном протоколе канального уровня с использованием кода ASCII (МТК-5), для канала ДСК

В табл. 2.4 приведены значения вероятностей необнаруживаемых ошибок такого матричного кода с $d_{\min} = 4$, рассчитанные по формулам (2.16) и (2.17), для некоторых значений битовой вероятности ошибки в канале ДСК.

Таблица 2.4

Вероятности необнаруженных ошибок для простого матричного кода с проверкой на четность

p	10^{-2}	10^{-3}	10^{-4}
$P_{но}(t=4)$	$8 \cdot 10^{-8}$	$8{,}2 \cdot 10^{-8}$	$2 \cdot 10^{-11}$
$P_{но}(t=6)$	$2{,}1 \cdot 10^{-9}$	$2{,}1 \cdot 10^{-11}$	$5{,}2 \cdot 10^{-17}$

Как видно из табл. 2.4, данный матричный код по сравнению с ранее рассмотренными имеет существенное преимущество по обеспечению достоверности передачи данных. Это объясняется его конструктивными особенностями, прежде всего каскадной структурой, и существенно большей избыточностью — 135 бит, по сравнению с ранее рассмотренными, где контрольная сумма составляла всего один байт. Кроме того, из данных табл. 2.4 видно, что для оценки эффективности матричного кода можно ограничиться вероятностью 4-кратной битовой ошибки в реальных каналах ДСК с $p = 10^{-2}$.

2.3. Методы обнаружения ошибок помехоустойчивыми кодами CRC

В настоящее время применяют более совершенные методы обнаружения ошибок, основанные на математических алгоритмах высшей алгебры. Наиболее популярными методами обнаружения ошибок в вычислительных сетях и сетях передачи данных являются методы с циклической избыточной суммой CRC (Cyclic Redundancy Check), для вычисления которой используются элементы высшей алгебры — теория групп, теория полей с операциями сложения, умножения и деления по определенным модулям. В большинстве случаев циклическая проверочная сумма, как известно, является остатком от деления одного, скажем, информационного, числа (или многочлена) на другое заданное число (или многочлен). Контроль за ошибками осуществляется сравнением переданной циклической проверочной суммы CRC и суммы, вычисленной на приемной стороне. Несовпадение CRC говорит о наличии (обнаружении) ошибок в принятом сообщении.

В системах передачи данных используются различные алгоритмы формирования циклической проверочной суммы CRC. При этом такие коды можно поделить на два класса:

1) с нулевыми начальными состояниями ячеек регистра деления как в кодере, так и в декодере;

2) с ненулевыми начальными состояниями ячеек регистра деления как в кодере, так и в декодере.

Рассмотрим их более подробно.

2.3.1. Алгоритм с простой CRC

Этот алгоритм, названный «простым», относится к классическим систематическим циклическим (n,k)-кодам с числом избыточных элементов в кодовой комбинации, равным $(n-k)=m$, где m — степень образующего примитивного многочлена $P(x)$.

Рассмотрим, прежде всего, варианты *кодов с простой CRC с нулевыми начальными состояниями ячеек регистров деления* на многочлен $P(x)$.

Напомним, что одним из свойств классического циклического кода является деление без остатка любой разрешенной комбинации кода в виде многочлена $f(x)$ на образующий многочлен $P(x)$.

Общий *алгоритм кодирования* классическим систематическим (n,k)-кодом состоит из следующих последовательных операций:

1) умножение исходного информационного многочлена длины k $\varphi(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_{k-1} x^{k-1}$ на одночлен x^m;

2) деление произведения $x^m \varphi(x)$ на образующий многочлен $P(x)$ степени m и определение остатка от деления $r(x) = r_0 + r_1 x + r_2 x^2 + \ldots + r_{m-1} x^{m-1}$;

3) формирование разрешенной кодовой комбинации длины n $f(x) = r(x) + x^m \varphi(x)$.

Очевидно, что $f(x) = 0 \bmod P(x)$ т. е. разрешенная кодовая комбинация $f(x)$ делится на $P(x)$ без остатка.

Алгоритм декодирования сводится к делению принятой комбинации $h(x)$ на образующий многочлен. Если $h(x)$ делится на $P(x)$ без остатка (нулевой синдром), то считается, что в принятой комбинации ошибки отсутствуют и $h(x) = f(x)$. Напротив, если остаток (синдром) не равен нулю, то это свидетельствует о наличии в принятой комбинации ошибок, которые обнаружены кодом. Другой часто используемый *алгоритм декодирования сводится к вычислению CRC по принятым информационным элементам и сравнению с принятыми проверочными элементами*. Если циклические проверочные элементы CRC совпадают, то считается, что ошибки в комбинации отсутствуют. И наоборот – несовпадение хотя бы в одном разряде сравниваемых контрольных сумм (CRC) будет говорить о наличии в принятой комбинации ошибок.

В литературе циклическую проверку, порожденную многочленом $P(x)$ степени m, часто обозначают CRC-m.

Различают три варианта длин n комбинаций:

- оптимальная полная длина $n = 2^m - 1$;
- укороченный код с длиной комбинации $n < 2^m - 1$;
- удлиненный код с $n > 2^m - 1$.

Рассмотрим особенности кодов CRC-m.

2.3.1.1. Оптимальный полный код CRC

В оптимальном варианте при $n = 2^m - 1$ наиболее полно проявляются свойства циклического кода:

- деление разрешенных комбинаций $f(x)$ на образующий многочлен $P(x)$ без остатка;

• поэлементная сумма по mod 2 двух или более разрешенных комбинаций порождает новую разрешенную комбинацию;

• циклический сдвиг разрешенной комбинации также порождает другую разрешенную комбинацию;

• наиболее оптимальным образом согласуются обнаруживающая способность кода и скорость кода k/n.

Из равенства $n = 2^m - 1$ следует равенство Хэмминга $(n-k) = m = \log_2(n+1)$, доказывающее, что это действительно оптимальный (n,k)-код, имеющий плотную упаковку, минимальное кодовое расстояние Хэмминга $d_{\min} = 3$ и способный в режиме исправления ошибок исправлять однократные ошибки. Такие циклические коды CRC не являются классическими кодами Хэмминга, их часто не совсем корректно называют кодами Хэмминга.

В режиме обнаружения ошибок такой код может гарантированно обнаруживать все однократные и двукратные ошибки. Кроме того, код сможет обнаруживать многие ошибки большей кратности $d_{\min} \le t \le n$ при условии, что комбинации таких ошибок не будут совпадать с разрешенными кодовыми комбинациями.

Вероятность появления необнаруживаемых ошибок в комбинации длины $n = 2^m - 1$ для канала ДСК будет определяться выражением

$$P_{\text{но}} = \sum_{w_i = d_{\min}}^{n} A(w_i) p^{w_i} (1-p)^{n-w_i}, \tag{2.18}$$

где w_i — вес разрешенной комбинации кода; $A(w_i)$ — количество разрешенных комбинаций с весом w_i (эту характеристику называют еще весовым спектром кода); p — вероятность битовой ошибки в канале ДСК.

Для полных двоичных кодов, для которых $n = 2^m - 1$ и $d_{\min} = 3$, весовой спектр находится как коэффициенты при z^{w_i} в разложении по степеням z следующей функции [5]:

$$\nu(z) = \frac{1}{n+1}\left[(1+z)^n + n(1+z)^{\frac{n-1}{2}}(1-z)^{\frac{n+1}{2}}\right].$$

Например, для циклического кода $(n,k) = (15,11)$ с CRC-4 весовой спектр представлен в табл. 2.5.

Таблица 2.5

Весовой спектр циклического кода (15,11)

w_i	0	3	4	5	6	7	8	9	10	11	12	15
$A(w_i)$	1	35	105	168	280	435	435	280	168	105	35	1

Вероятность приема n-элементной комбинации с обнаруживаемыми ошибками будем определять из выражения: $P_{\text{оо}} = 1 - P_{\text{пп}} - P_{\text{но}}$, где $P_{\text{пп}}$ — вероятность правильного приема комбинации, равная $P_{\text{пп}} = (1-p)^n$.

Пример 2.2. Рассчитаем вероятностные характеристики для кода $(n,k) = (15,11)$ с CRC-4 в канале ДСК с битовой вероятностью ошибки $p = 10^{-3}$.

Вероятность правильного приема $P_{\text{пп}} = (1-p)^{15} = (0{,}999)^{15} = 0{,}9851$.

Расчетные вероятности необнаруживаемых ошибок кратности w_i и суммарная вероятность $P_{\text{но}}$ в соответствии с формулой (2.18) представлены в табл. 2.6.

Таблица 2.6

Вероятности необнаруживаемых ошибок для циклического кода $(15,11)$

w_i	3	4	5	6	7	$P_{\text{но сумм.}}$
$P_{\text{но}}(w_i)$	$3{,}46 \cdot 10^{-8}$	$1{,}04 \cdot 10^{-10}$	$1{,}66 \cdot 10^{-13}$	$2{,}77 \cdot 10^{-16}$	$4{,}31 \cdot 10^{-19}$	$\approx 3{,}46 \cdot 10^{-8}$

Как видно из табл. 2.6, при $p = 10^{-3}$ в канале ДСК для оценки вероятности необнаруживаемых ошибок можно ограничиться весом $w_i = 3$.

Учитывая вычисленные значения $P_{\text{пп}}$ и $P_{\text{но}}$, вероятность появления в комбинации обнаруживаемых ошибок будет равна $P_{\text{оо}} = 1{,}5 \cdot 10^{-2}$.

На рис. 2.6 приведены расчетные вероятностные характеристики циклического кода $(n,k) = (15,11)$ с CRC-4 для канала ДСК.

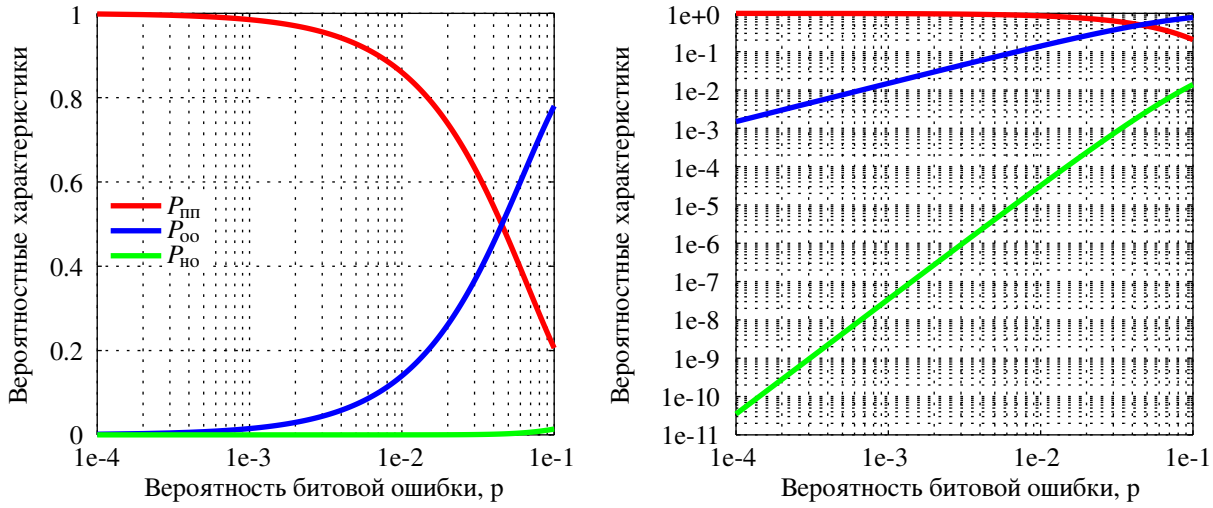


Рис. 2.6. Вероятностные характеристики циклического кода $(n,k) = (15,11)$ *с CRC-4 для канала ДСК*

2.3.1.2. Укороченные CRC-m коды

При $n < 2^m - 1$ получим укороченный код с проверочной контрольной суммой CRC-m и числом информационных элементов $k = n - m$. Такой код имеет меньшую относительную кодовую скорость k/n и, соответственно, большую относительную избыточность. Например, полный код $(n,k) = (15,11)$ имеет скорость $k/n = 0{,}733$ и избыточность $(n-k)/n = 0{,}266$. А укороченный $(9,5)$-код имеет скорость 0,555, а избыточность — 0,444. При этом минимальное кодовое расстояние остается равным $d_{\min} = 3$, чем и определяется обнаруживающая способность укороченного кода. Вместе с тем, при оценке вероятностных характеристик необходимо учесть, что для укороченного кода поменяется весовой спектр, который чаще всего определяется путем моделирования.

В укороченном (n,k)-коде свойства циклических кодов сохраняются не полностью. Так, сохраняются свойство делимости разрешенной комбинации в виде многочлена $f(x)$ на образующий многочлен $P(x)$ без остатка и свойство линейности, но не сохраняется свойство циклических сдвигов, так как примитивный многочлен $P(x)$ степени m не будет делителем двучлена $(x^n + 1)$, если $n < 2^m - 1$.

2.3.1.3. Удлиненные CRC-m коды

В ряде систем применяется код с CRC-m при длине комбинации $n > 2^m - 1$ при том же числе проверочных элементов $m = n - k$. Такой код, по сравнению с оптимальным полным кодом, имеет большую относительную скорость k/n и, соответственно, меньшую относительную избыточность. Например, если взять код $(20,16)$ вместо $(15,11)$, то получим скорость $k/n = 0{,}8$ и избыточность 0,2. Особенностью такого кода является то, что у него, по сравнению с полным кодом, увеличится доля необнаруживаемых ошибок. Поясним, чем это вызвано.

Известно, что образующий многочлен $P(x)$ степени m должен быть делителем двучлена $(x^{2^m-1} + 1)$. А так как в удлиненном коде $n > 2^m - 1$, то в комбинации могут возникнуть такие двукратные ошибки с многочленом $e(x) = x^i(x^{2^m-1} + 1)$, что $i + (2^m - 1) \le n - 1$, а многочлен $e(x)$ будет делиться на двучлен $(x^{2^m-1} + 1)$ и, следовательно, на образующий многочлен $P(x)$ без остатка. То есть такие двукратные ошибки не будут обнаруживаться кодом с CRC-m при длине комбинации $n > 2^m - 1$.

Кодирующее и декодирующее устройства циклического (n,k)-кода с «простой» CRC-m и $d_{\min} = 3$ реализуются на базе регистра сдвига длиной m ячеек, осуществляющего для систематического кода деление на образующий

многочлен $P(x)$ степени m. При этом перед началом процедуры кодирования и декодирования ячейки регистров сдвига должны быть обнулены.

2.3.1.4. Обнаружение ошибок кодами с простой CRC-m

Проанализируем способность циклического кода с простой CRC-m обнаруживать ошибки.

Так как образующий многочлен $P(x)$ степени $m > 1$ для полного кода является примитивным, то он должен иметь нечетное число слагаемых, включая 1 и x^m, т. е. 3, 5, 7 и т. д. Исходя из этого, можно дать оценку обнаруживающей способности такого кода, учитывая, что многочлен обнаруживаемых ошибок $e(x)$ не должен делиться на $P(x)$ без остатка. Начнем с однократной ошибки, многочлен которой будет $e(x) = x^i$, где $0 \le i \le n-1$. Такой многочлен однократной ошибки не может делиться без остатка на другой многочлен, имеющий более одного члена. Значит, однократные ошибки будут гарантированно обнаруживаться.

Двукратную ошибку с многочленом $e(x) = x^i + x^j$, $0 \le i < j \le n-1$, можно представить произведением двух сомножителей $e(x) = x^i(1 + x^{j-i}) = x^i(1 + x^v)$. Такой многочлен двукратных ошибок $e(x)$ не будет делиться на $P(x)$ без остатка в том случае, если ни один из сомножителей не будет делиться на $P(x)$. Одночлен x^i не делится на $P(x)$ без остатка. Второй сомножитель $(1 + x^v)$ также не будет делиться без остатка на $P(x)$ степени m, так как $v \le n-1 = 2^m - 2$, а примитивный многочлен степени m является делителем двучлена $(1 + x^i)$ с наименьшей степенью $i = (2^m - 1)$. Таким образом, двукратные ошибки код с CRC-m также гарантированно обнаруживает.

Кроме того, будут обнаруживаться и ошибки большей кратности, многочлены которых $e(x)$ не делятся без остатка на $P(x)$.

Наоборот, необнаруживаемыми будут те ошибки, многочлены которых $e(x)$ будут кратны многочлену $P(x)$. Общее количество и вес этих комбинаций ошибок определяется весовым спектром кода $A(w_i)$.

2.3.1.5. Варианты кодов с простой CRC-m, применяемых в реальных системах (протоколах)

Напомним, что в этом разделе рассматриваются примеры кодов с простой CRC-m и с нулевыми начальными состояниями ячеек регистра деления как в кодере, так и в декодере.

Наиболее простыми кодами с CRC-m являются коды с малыми значениями $m = 4, 6, 7$, которые нашли применение в цифровых системах передачи PDH и SDH. Такие коды при низкой избыточности и простой реализации

обеспечивают требуемую достоверность в достаточно хороших цифровых каналах.

Так, для контроля за ошибками в цифровом тракте E1 плезиохронной цифровой иерархии PDH, в соответствии с рекомендацией **ITU-T G.704**, используется код **CRC-4** с образующим многочленом $P(x) = 1 + x + x^4$ [40, 41]. Рассмотрим особенности такого кода.

Информационные последовательности кода в системе PDH представляют собой [40, 41] половины сверхциклов, состоящих из 8 циклов E1, т. е. содержат $8 \times 8 \times 32 = 2048$ бит. Выходная разрешенная комбинация $f(x)$ кода CRC-4 образуется как комбинация систематического кода $f(x) = r(x) + x^4\varphi(x)$, где $r(x)$ — остаток от деления $x^4\varphi(x)$ на $P(x)$, т. е. контрольная проверочная последовательность CRC-4. Таким образом, комбинация (n,k)-кода на выходе кодера содержит $n = 2052$ бита. Так как структура цикла цифрового потока E1 стандартизована и состоит из 32 канальных байтов, то контрольная сумма CRC-4 половины сверхцикла (субсверхцикла), т. е. проверочные элементы (r_0, r_1, r_2, r_3), передается на определенных позициях следующего субсверхцикла. Поэтому при декодировании, прежде чем принять решение о наличии ошибок в субсверхцикле, необходимо его сначала принять полностью и вычислить по принятой информации CRC-4 по тому же алгоритму, что и на передаче. Затем, принимая следующий субсверхцикл, выделить из него проверочные элементы (r_0, r_1, r_2, r_3) предшествующего субсверхцикла и сверить их с вычисленной на приемной стороне контрольной суммой CRC-4 в результате декодирования предшествующего субсверхцикла. Если сравниваемые контрольные суммы не совпадают, это говорит о наличии обнаруживаемых ошибок в предшествующем субсверхцикле. Но при этом следует иметь ввиду, что ошибка может иметь место и в самих проверочных элементах (r_0, r_1, r_2, r_3), принятых в следующем субсверхцикле, тогда как в самом предшествующем субсверхцикле ошибок нет. Таким образом, одной из особенностей является задержка на приеме длительностью в один субсверхцикл.

Другая особенность рассматриваемого кода CRC-4 заключается в том, что это удлиненный код, так как длина комбинации $n = 2052$ бит существенно больше $2^m - 1 = 15$. Это, как было сказано выше, ведет к снижению помехоустойчивости кода вследствие появления в комбинации двукратных ошибок, многочлены которых будут делиться на образующий многочлен $P(x)$ без остатка. Действительно, если двукратной ошибке соответствует двучлен $e(x) = x^i + x^j$, $0 \le i < j \le n-1$, который можно представить произведением двух сомножителей $e(x) = x^i(1 + x^{j-i}) = x^i(1 + x^v)$, то при v кратном числу 15 примитивный многочлен $P(x)$ будет делителем двучлена $(1 + x^v)$, т. е. такие ошибки код не обнаружит.

Еще одна особенность кода состоит в том, что при вычислении контрольной суммы субсверхцикла позиции, на которых устанавливают проверочные элементы, как в кодере, так и в декодере, должны считаться нулевыми.

Другими примерами простых кодов с CRC-m являются рекомендованные для цифровых сетей синхронной иерархии SDH код **CRC-6** с образующим многочленом $P(x) = 1 + x + x^6$, рекомендация **ITU-T G.704** и код **CRC-7** с образующим многочленом $P(x) = 1 + x^3 + x^7$, рекомендации **ITU-T G.704** и **G.832** [40].

Но самым простым является код **CRC-3** в схеме управления пропускной способностью канала (LCAS — Link Capacity Adjustment Scheme), применяемый для передачи кадров в сети SDH [8] в соответствии с рекомендацией **ITU-T G.707**. Информационная последовательность, состоящая из 29 бит, кодируется систематическим (n,k)-кодом $(32,29)$ с образующим многочленом $P(x) = 1 + x + x^3$. Очевидно, код является удлиненным, поэтому он гарантированно обнаруживает все однократные и многие двукратные ошибки. В то же время, как было пояснено выше, часть двукратных ошибок он не обнаруживает.

На сегодняшний день, пожалуй, самым сложным является пример кода с **CRC-32** стандарта **IEEE 802.3**, применяемый в кадрах Ethernet на MAC уровне. Образующий многочлен имеет вид:

$$P(x) = 1 + x + x^2 + x^4 + x^5 + x^7 + x^8 + x^{10} + x^{11} + x^{12} + x^{16} + x^{22} + x^{23} + x^{26} + x^{32}.$$

В кодируемую часть кадра входят MAC-адреса передатчика и приемника кадра по 6 байт, поле длины — 2 байта и поле данных длиной от 42 до 1500 байт. Для контрольной суммы CRC-32 отведено 4-байтовое поле в конце кадра. Таким образом, общая кодируемая часть кодовой комбинации имеет переменную длину в пределах от 56 до 1514 байт.

2.3.2. Алгоритмы обнаружения ошибок двоичными (n, k)-кодами с расширенной CRC и нулевыми состояниями ячеек регистров

Название «расширенная CRC» здесь вводится в связи с тем, что образующий многочлен имеет вид: $G(x) = (1 + x)P(x)$, где $P(x)$ — примитивный многочлен степени m. Варианты таких кодов будут, как и ранее, оптимальные (полные или с плотной упаковкой) при $n = 2^m - 1$, укороченные — при $n < 2^m - 1$ и удлиненные — при $n > 2^m - 1$. В таких (n,k)-кодах с расширенной CRC число проверочных элементов равно $(n-k) = m + 1$, а число информационных элементов — $k = n - m - 1$.

Рассмотрим общие свойства (n,k)-кода с расширенной CRC на примере оптимального систематического кода (плотная упаковка) с $n = 2^m - 1$.

Для большей наглядности будем вести построение такого кода с образующим многочленом $G(x) = (1+x)P(x)$ в два этапа. На первом этапе информационная k-элементная комбинация $\varphi(x) = a_0 + a_1x + a_2x^2 + \ldots + a_{k-1}x^{k-1}$ умножается на x^m $(m \geq 3)$ и делится на многочлен $P(x)$. Остаток от деления $r(x) = r_0 + r_1x + \ldots + r_{m-1}x^{m-1}$ добавляется к информационным элементам со стороны младшего разряда. При этом будет получена комбинация из $(n-1)$ элементов:

$$(r_0, r_1, \ldots, r_{m-1}, a_0, a_1, a_2, \ldots, a_{k-1}) \tag{2.19}$$

с минимальным кодовым расстоянием Хэмминга $d_{\min} = 3$.

На втором этапе комбинация (2.19) проверяется на четность и к ней со стороны младшего разряда добавляется еще один проверочный элемент «b».

Таким образом, на выходе кодера будет получена n-элементная разрешенная кодовая комбинация: $(b, r_0, r_1, \ldots, r_{m-1}, a_0, a_1, a_2, \ldots, a_{k-1})$, в которой $b = 0$, если в комбинации (2.19) четное число «1», и $b = 1$ при нечетном числе «1». В данном случае контрольной суммой CRC-$(m+1)$ будет комбинация проверочных элементов $(b, r_0, r_1, \ldots, r_{m-1})$.

Следовательно, разрешенные комбинации кода с расширенной CRC будут иметь только четный вес, начиная с $w_{\min} = 4$ среди ненулевых комбинаций. Отсюда также следует, что минимальное кодовое расстояние кода с расширенной CRC также будет равно $d_{\min} = 4$. Исходя из этого, такой полный код способен гарантированно обнаруживать однократные, двукратные и трехкратные ошибки. Кроме того, код будет обнаруживать также ошибки более высокой кратности, если многочлен ошибок $e(x)$ не будет делиться на $G(x)$ без остатка. Следовательно, код не сможет обнаружить только те ошибки, многочлен которых $e(x)$ кратен образующему многочлену $G(x)$.

Очевидно, что кодер практически проще реализовать в один этап с помощью одного регистра деления $x^{m+1}\varphi(x)$ на многочлен $G(x) = (1+x)P(x)$ с нулевыми начальными состоянием ячеек регистра.

Так как код является систематическим, то в декодере информационные элементы $x^{m+1}\varphi(x)$ делятся на образующий многочлен $G(x)$, в результате чего будет получена контрольная сумма CRC-$(m+1)$, которая, в случае отсутствия ошибок, будет совпадать с принятой, что будет восприниматься как отсутствие ошибок в принятой комбинации. В действительности, на практике чаще вся принятая комбинация $h(x)$ делится на образующий многочлен $G(x)$ и полученный остаток (синдром $S(x)$) проверяется на равенство нулю. Если $S(x) = 0$, то считается, что принятая комбинация не содержит ошибки, в противном случае принимается решение об обнаружении ошибок в комбинации.

Еще одной особенностью кода с расширенной CRC является то, что его образующий многочлен $G(x)$ всегда будет иметь четное число слагаемых. Это связано с тем, что примитивный многочлен $P(x)$ степени $m > 1$ имеет обяза-

тельно нечетное число слагаемых, включая x^m и 1, а умножение $P(x)$ на $(1+x)$ делает его, соответственно, четным.

Например, для кода $(n,k)=(15,10)$ с CRC-5 и примитивным многочленом $P(x)=1+x+x^4$ получим образующий многочлен $G(x)=(1+x)P(x)=1+x^2+x^4+x^5$. Весовой спектр такого кода с $n=2^4-1=15$ будет только четным с числами $A(w_i)$ комбинаций веса w_i, показанным в табл. 2.7.

Таблица 2.7

Весовой спектр кода CRC-5 $(15,10)$

w_i	0	4	6	8	10	12
$A(w_i)$	1	105	280	435	168	35

Исходя из структуры многочлена $G(x)=(1+x)P(x)$, можно провести оценку обнаруживающей способности кода с расширенной CRC. Очевидно, что однократная ошибка всегда обнаружится, так как одночлен ошибки $e(x)=x^i$ не будет делиться без остатка ни на первый, ни на второй сомножитель, имеющий также более одного члена. Многочлен двукратной ошибки $e(x)=x^i+x^j=x^i(1+x^{j-i})=x^i(1+x^v)$, $0\le i<j\le n-1$ также не делится без остатка на $G(x)$, так как сомножитель x^i не делится без остатка ни на $(1+x)$, ни на многочлен $P(x)$. Второй сомножитель $(1+x^v)$ может делиться на примитивный многочлен $P(x)$ степени m только при наименьшем значении $v=2^m-1=n$, а в действительности $v<n-1$.

Многочлен трехкратной ошибки $e(x)=x^i+x^j+x^z$, имеющий нечетное число слагаемых, не может делиться без остатка на $(1+x)$. В противном случае элемент поля $x=1$ был бы корнем и $(1+x)$, и многочлена $e(x)$. Но «1» не может быть корнем многочлена $e(x)$, имеющего нечетное число членов. Действительно, подставив в $e(x)$ значение $x=1$, получим $e(1)=1(\mathrm{mod}\,2)$.

Таким образом, полный (n,k)-код с расширенной CRC и $n=2^m-1$ будет гарантированно обнаруживать все однократные, двукратные и все другие ошибки нечетной кратности. Это свойство выгодно отличает (n,k)-код с расширенной CRC от кода с простой CRC.

Приведенные выше свойства полного кода с расширенной CRC будут справедливы и для укороченного (n,k)-кода с расширенной CRC с $n<2^m-1$.

Для удлиненного (n,k)-кода с $n>2^m-1$ указанные выше свойства полного кода частично не выполняются. Это вызвано тем, что, как сказано выше, двукратные ошибки $e(x)=x^i+x^j=x^i(1+x^{j-i})=x^i(1+x^v)$, $0\le i<j\le n-1$, для которых величина v кратна 2^m-1, не будут обнаружены, так как такой многочлен $(1+x^v)$ делится без остатка и на $(1+x)$, и на многочлен $P(x)$. Следовательно, такую двукратную ошибку $e(x)$ код не обнаружит.

Особенностью кодов с расширенной CRC и $d_{\min} = 4$ является и то, что такие полные (n,k)-коды с $n = 2^m - 1$ могут работать как в режиме только обнаружения ошибок (обнаруживать все однократные, двукратные и все другие ошибки нечетной кратности), так и в режиме исправления однократных ошибок и гарантированного обнаружения всех двукратных ошибок. При этом декодер должен работать по двум этапам. Например, в режиме исправления однократных ошибок факт наличия одной ошибки сначала должен быть обнаружен проверкой на четность, которая покажет, что в комбинации нечетное число двоичных «1», а на втором этапе — делением принятой комбинации на многочлен $G(x)$ (или $P(x)$), в результате которого при однократной ошибке будет получен ненулевой синдром — ненулевой остаток от деления на многочлен. Далее исправление однократной ошибки происходит либо табличным способом, либо при последовательном считывании комбинации с буферного накопителя по определенной комбинации содержимого в ячейках регистра сдвига. Иногда такую комбинацию называют «замечательной».

Рассмотрим процедуру исправления *однократной ошибки* на примере кода $(n,k) = (15,10)$ с CRC-5 и примитивным многочленом $P(x) = 1 + x + x^4$, образующим многочленом $G(x) = (1+x)P(x) = 1 + x^2 + x^4 + x^5$ и нулевыми начальными состояниями ячеек регистра деления на $G(x)$. Для простоты будем считать, что была передана нулевая комбинация, в которой возникла однократная ошибка с одночленом в общем виде $e(x) = x^i$, где $0 \le i \le n-1$. Проверка на четность указывает на наличие ошибки. При исправлении однократной ошибки табличным способом значение синдрома $S(x) \neq 0$ укажет на номер ошибочной позиции и ошибка может быть сразу же, без задержек, исправлена. При этом в постоянной памяти должна содержаться таблица синдромов, вид которой для данного примера приведен в табл. 2.8.

Таблица 2.8

Таблица синдромов однократной ошибки кода $(15,10)$ *с CRC-5*

№ п/п	$e(x) = x^i$	$S_i(x) (\mathrm{mod}\ G(x))$	$[S_i] = (s_0,s_1,s_2,s_3,s_4)$
0	1	1	(10000)
1	x	x	(01000)
2	x^2	x^2	(00100)
3	x^3	x^3	(00010)
4	x^4	x^4	(00001)
5	x^5	$1 + x^2 + x^4$	(10101)
6	x^6	$1 + x + x^2 + x^3 + x^4$	(11111)
7	x^7	$1 + x + x^3$	(11010)
8	x^8	$x + x^2 + x^4$	(01101)
9	x^9	$1 + x^3 + x^4$	(10011)
10	x^{10}	$1 + x + x^2$	(11100)

Окончание табл. 2.8

Таблица синдромов однократной ошибки кода $(15,10)$ *с CRC-5*

№ п/п	$e(x)=x^i$	$S_i(x)(\text{mod } G(x))$	$[S_i]=(s_0,s_1,s_2,s_3,s_4)$
11	x^{11}	$x+x^2+x^3$	(01110)
12	x^{12}	$x^2+x^3+x^4$	(10111)
13	x^{13}	$1+x^2+x^3$	(10110)
14	x^{14}	$x+x^3+x^4$	(01011)

Предположим, что однократная ошибка возникла в 8 позиции, т. е. $e(x)=x^8$. Записав принятую комбинацию в накопитель и поделив ее на многочлен $G(x)$, получим синдром, равный $(x+x^2+x^4)$. Найдя этот синдром в табл. 2.8, определяем, что ошибка возникла в 8 позиции и подлежит исправлению, после чего в накопителе получим исходную кодовую комбинацию.

Другой вариант реализации декодера, исправляющего однократную ошибку, основан на последовательном считывании принятой комбинации с накопителя и исправлении ошибки в момент появления ее из накопителя.

Покажем математику такого исправления однократной ошибки с одночленом $e(x)=x^i$, где $0\le i\le n-1$ при оптимальной длине кодовой комбинации $n=2^m-1=15$. Принятой комбинации с однократной ошибкой соответствует многочлен $h(x)=f(x)+e(x)\equiv x^i\equiv S_i(x)[\text{mod } G(x)]$. Здесь учтено свойство циклического кода о том, что любая разрешенная комбинация $f(x)$ всегда делится на многочлен $G(x)$ без остатка. Итак, на момент приема всей n-элементной комбинации и записи ее в накопитель на n элементов, в регистре деления будет синдром $S_i(x)\equiv x^i[\text{mod } G(x)]$. Далее, при считывании комбинации с накопителя, каждому такту будет соответствовать один сдвиг содержимого регистра на один шаг, т. е. умножение содержимого ячеек регистра на x и приведение этого произведения по mod $G(x)$. Тогда через $(n-i)$ сдвигов на выходе накопителя появится ошибочный элемент h_i принятой комбинации $h(x)$. Содержимое регистра также умножится на x^{n-i} и станет равным:

$$x^{n-i}S_i(x)=x^{n-i}x^i=x^n\equiv 1[\text{mod } G(x)].$$

Таким образом, если к ячейкам регистра деления подключить дешифратор на «1», то он сработает в момент появления из накопителя ошибочного элемента и выдаст «1», которая просуммируется по mod 2 с ошибочным элементом h_i и тем самым исправит однократную ошибку. Так, если ошибка была в 8 позиции, т. е. $e(x)=x^8$, то соответствующий такой ошибке синдром, как следует из табл. 2.8, будет $S_8(x)\equiv x+x^2+x^4[\text{mod } G(x)]$. Тогда через $(n-i)=(15-8)=7$ сдвигов в ячейках регистра будет

$$x^8x^{n-i}=x^8x^7=x^{15}\equiv 1[\text{mod } G(x)].$$

Сработает дешифратор комбинации (10000) в ячейках регистра и выдаст «1», которая суммируется по mod 2 с ошибочным элементом h_8 и ошибка будет исправлена.

Функциональная схема декодера в общем виде показана на рис. 2.7.

Рис. 2.7. Функциональная схема декодера с исправлением однократной ошибки при последовательном считывании

Отметим, что ключ на выходе дешифратора будет разомкнут, пока поступает на вход комбинация $h(x)$, и замкнут после приема комбинации и записи ее в накопитель, т. е. с первым тактом считывания принятой комбинации из накопителя.

Обнаружение двукратной ошибки может происходить также в два этапа: сначала проверка на четность показывает, что в принятой комбинации ошибок нет, так как в ней будет четное число 1, а на втором этапе деление принятой комбинации на образующий многочлен $G(x)$ (или $P(x)$) указывает на ненулевой остаток (синдром), что говорит о наличии двукратной ошибки (хотя, как известно, это могут быть и ошибки более высокой четной кратности).

Для укороченного кода с длиной комбинации $n_1 < 2^m - 1$ дешифратор в схеме на рис. 2.7 должен быть настроен на «замечательную» комбинацию в ячейках регистра, соответствующую одночлену x^{n_1} по mod $G(x)$.

Примеры систем и рекомендаций по использованию (n,k)-кодов с расширенной CRC и с нулевыми начальными состояниями ячеек регистра деления для обнаружения ошибок

Рекомендация ITU-T G.704 1998 г. предписывает применение для обнаружения ошибок кода с CRC-5 и образующим многочленом

$$G(x) = (1+x)P(x) = (1+x)(1+x+x^4) = 1+x^2+x^4+x^5.$$

Для длины $n = 2^m - 1 = 15$, где m — степень примитивного многочлена $P(x)$, получим полный (оптимальный) $(n,k) = (15,10)$ циклический код с $d_{\min} = 4$. Такой код, как было доказано выше, будет обнаруживать все ошибки

нечетной кратности и все двукратные ошибки. В табл. 2.7 приведен весовой спектр разрешенных комбинаций этого кода, из которого следует, что код не будет обнаруживать определенные ошибки четной кратности, начиная с 4. Так, вероятность появления 4-кратной необнаруживаемой ошибки в канале ДСК будет определяться выражением:

$$P(4,n) = A(4)p^4(1-p)^{n-4},$$

где p — вероятность битовой ошибки в канале ДСК; $A(4)$ — количество разрешенных комбинаций кода с весом $w = 4$, число которых для данного кода равно 105 (табл. 2.7).

В реальных системах обычно $n > 2^m - 1$, т. е. применяют удлиненный код с расширенной CRC-5. Проведем анализ, насколько ухудшится обнаруживающая способность и общая эффективность кода с расширенной CRC-5 из-за возможных двукратных необнаруживаемых ошибок.

Как известно, примитивный многочлен $P(x) = (1 + x + x^4)$ является делителем двучлена $(1 + x^z)$ при наименьшем значении $z = 2^m - 1 = 15$. Обозначим такое значение $z = n_o$ и будем считать n_o оптимальной длиной комбинации, равной $n_o = 2^m - 1$. Тогда, как следует из свойств двучленных уравнений высшей алгебры, любой двучлен $(1 + x^{\lambda n_o})$, где $\lambda = 1, 2, \ldots$, будет делиться на $(1 + x^{n_o})$ без остатка. Из этого также следует, что $(1 + x^{\lambda n_o})$ будет делиться без остатка и на $(1 + x)$, и на многочлен $P(x)$. Таким образом, удлиненным кодом не будут обнаружены двукратные ошибки, многочлен которых будет иметь вид: $e(x) = (x^i + x^j) = x^i(1 + x^{\lambda n_o})$, где i и j — целые числа, $i \geq 0$, $\lambda = 1, 2, \ldots, s$, но такие, что $i + \lambda n_o \leq n - 1$ для всех λ. Величина s определяется из равенства

$$n = sn_o + r, \tag{2.20}$$

где r — остаток от деления n на $n_o = 2^m - 1$, т. е. $n \equiv r[\text{mod } n_o]$.

Для нашего примера с CRC-5 $m = 4$, следовательно $n_o = 2^4 - 1 = 15$. Пусть удлиненный $(n,k) = (50,45)$. Найдем количество двукратных необнаруживаемых ошибок в таком удлиненном коде как $B(2,n) = B(2,50)$. При этом $n = 50 \equiv 5(\text{mod } 15)$, т. е. $r = 5$. Тогда из (2.20) находим $s = 3$. Анализ конфигураций необнаруживаемых двукратных ошибок, выполненный авторами при подготовке настоящего пособия, а также исследования автора работы [8], показали, что количество таких ошибок точно определяется выражением:

$$B(2,n) = C_s^2 n_o + r \cdot s. \tag{2.21}$$

Подставив необходимые величины в (2.21), находим, что $B(2,n) = 60$.

Тогда вероятность двукратных необнаруживаемых ошибок для данного кода с CRC-5 будет определяться выражением:

$$P(2,n) = B(2,n)p^2(1-p)^{n-2} = 60p^2(1-p)^{n-2}.$$

Как видим, вероятность необнаруженной ошибки для удлиненного кода пропорциональна p^2, тогда как для оптимального кода с $n = 2^m - 1$ и $d_{\min} = 4$ эта вероятность пропорциональна p^4. Таким образом, эффективность удлиненного кода ухудшится приближенно в $p^2/p^4 = p^{-2}$ раз. В то же время, применение удлиненных кодов с расширенной CRC приводит к уменьшению избыточности и, следовательно, к увеличению скорости передачи данных.

Пример 2.3. Рассмотрим в качестве примера код $(n,k) = (33,29)$ с расширенной CRC-4 с образующим многочленом

$$G(x) = (1+x)P(x) = (1+x)(1+x+x^3) = 1+x^2+x^3+x^4.$$

Этот код образован на базе кода $(n,k) = (32,29)$ с простой CRC-3 и с образующим многочленом $P(x) = 1+x+x^3$, применяемого для передачи кадров в сети SDH [8] в соответствии с рекомендацией **ITU-T G.707**. В комбинации к $k = 29$ информационным элементам добавляются вместо трех четыре проверочных элемента, что вызвано введением сомножителя $(1+x)$ в образующий многочлен $G(x)$.

На рис. 2.8 представлена иллюстрация возможных двукратных ошибок, не обнаруживаемых удлиненным кодом с расширенной CRC-4, и поясняющая формулу (2.21). Так как $m = 3$, то получаем значение $n_o = 2^m - 1 = 7$. Тогда из (2.20) находим, что $s = 4$, а $r = 5$. На рис 2.8 условно наклонными линиями показаны $s = 4$ секции по $n_o = 7$ разрядов n-элементной комбинации. Двукратные не обнаруживаемые кодом ошибки располагаются по горизонтальным линиям. Это будут двукратные ошибки (переходы) по горизонтали из точек первого наклонного ряда во второй, как, например, переход $x^6 \to x^{13}$. Таких переходов из первого ряда во второй будет $n_o = 7$, и каждому из них соответствует двукратная ошибка с многочленом $e(x) = x^i(1+x)^7$ где i принимает значения от 0 до $n_o - 1 = 6$. Аналогичные переходы из точек первой наклонной линии в точки третьей и четвертой наклонных линий по $n_o = 7$ переходов в каждом случае, как, например, $x^5 \to x^{19}$ и $x^4 \to x^{25}$. Таким переходам соответствуют двукратные ошибки с многочленами $e(x) = x^i(1+x)^{14}$ и $e(x) = x^i(1+x)^{21}$. Всего таких двукратных ошибок (переходов) из $n_o = 7$ точек первого наклонного ряда в точки 2-го, 3-го и 4-го наклонных рядов будет равно $n_o(s-1) = n_o \cdot 3 = 21$.

Такими же необнаруживаемыми будут двукратные ошибки, соответствующие переходам из точек 2-го ряда в 3-й и 4-й, как, например, $x^9 \to x^{16}$ и $x^{10} \to x^{24}$. Таким переходам соответствуют двукратные ошибки с многочленами $e(x) = x^i(1+x)^7$ и $e(x) = x^i(1+x)^{14}$ где i меняется от 7 до $2n_o - 1 = 13$. Всего количество таких двукратных ошибок будет равно $n_o(s-2) = n_o \cdot 2 = 14$.

Не будут обнаружены также двукратные ошибки, соответствующие переходам из 3-го ряда в 4-й, как, например, $x^{20} \to x^{27}$. Таким переходам соот-

ветствуют двукратные ошибки с многочленами $e(x) = x^i(1+x)^7$ где i меняется от 14 до $3n_o - 1 = 20$. Всего количество таких двукратных ошибок будет равно $n_o(s-3) = n_o = 7$.

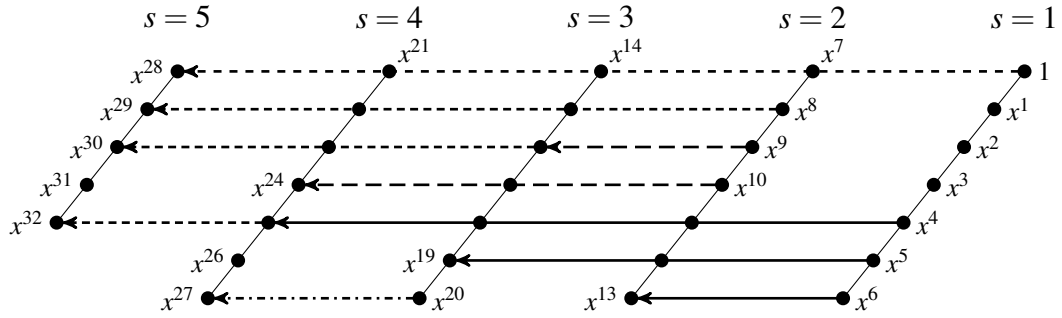


Рис. 2.8. Иллюстрация к возникновению двукратных необнаруживаемых ошибок в удлиненном коде с расширенной CRC-4 с образующим многочленом $G(x) = (1+x)(1+x+x^3)$ и длиной комбинации $n = 33$

Таким образом, суммарное количество необнаруживаемых двукратных ошибок между разрядами 1-го, 2-го ,3-го и 4-го рядов будет равно

$$n_o[1+2+\ldots+(s-1)] = n_o\frac{s(s-1)}{2} = n_oC_s^2.$$

Наконец, не обнаружатся двукратные ошибки, соответствующие переходам из точек 1-го, 2-го, 3-го и 4-го рядов в $r = 5$ точек 5-го ряда. Таких двукратных ошибок всего будет $s \cdot r$.

Итого, общее количество двукратных необнаруживаемых ошибок удлиненным кодом $(n,k) = (33,29)$ с CRC-4 будет равно

$$B(2,n) = s \cdot r + n_oC_s^2 = 4 \cdot 5 + 7 \cdot \frac{4 \cdot 3}{2} = 62.$$

Пример 2.4. Приведем пример *кодирования и декодирования*, а также схемную реализацию кодера и декодера оптимального систематического $(n,k) = (15,10)$ кода с расширенной CRC-5 с образующим многочленом

$$G(x) = (1+x)P(x) = (1+x)(1+x+x^4) = 1+x^2+x^4+x^5.$$

Рассмотрим одноэтапный вариант кодирования и декодирования. Пусть входная информационная комбинация имеет вид:

$$(a_0,a_1,a_2,a_3,a_4,a_5,a_6,a_7,a_8,a_9) = (1010010000).$$

Такой комбинации соответствует многочлен $\varphi(x) = 1+x^2+x^5$.

Процедура кодирования

Операция 1. Умножение $\varphi(x)$ на $x^{m+1} = x^5$, где m — степень примитивного многочлена $P(x)$:

$$x^5\varphi(x) = x^5(1 + x^2 + x^5) = x^5 + x^7 + x^{10}.$$

Операция 2. Деление $x^5\varphi(x)$ на образующий многочлен $G(x)$ и получение проверочных элементов $(r_0, r_1, \ldots, r_{m+1}) = (r_0, r_1, \ldots, r_4)$. В результате деления получен следующий многочлен остатка $r(x) = 1 + x^3 + x^4$, т. е. проверочные элементы будут равны $(r_0, r_1, \ldots, r_4) = (10011)$.

Операция 3. Формирование кодовой комбинации

$$f(x) = r(x) + x^5\varphi(x) = 1 + x^3 + x^4 + x^5 + x^7 + x^{10},$$

которой соответствует двоичный вектор (100111010010000).

Процедура декодирования

Деление принятой комбинации $h(x)$ на образующий многочлен $G(x)$ и проверка на равенство «0» синдрома $S(x)$. Равенство синдрома «0» воспринимается как отсутствие ошибок в принятой комбинации.

Пусть принятая комбинация не содержит ошибок, т. е. $h(x) = f(x)$. Поделив сформированную кодером комбинацию $f(x)$ на $G(x)$, убедимся, что синдром будет нулевым и, следовательно, ошибки в принятой комбинации отсутствуют.

Пусть теперь в принятой комбинации возникли две ошибки с многочленом $e(x) = x^5 + x^8$, т. е. $h(x) = f(x) + e(x) = 1 + x^3 + x^4 + x^7 + x^8 + x^{10}$. Поделив комбинацию $h(x)$ на $G(x)$, получим в остатке ненулевой синдром $S(x) = (1 + x)$, что свидетельствует о наличии ошибок в принятой на вход декодера комбинации.

Схемы кодера и декодера для рассмотренного примера представлены на рис. 2.9.

На вход кодера (рис. 2.9, а) в течение первых k тактов поступает информационная комбинация $\varphi(x)$ со старшего разряда. В течение этого времени ключ «Кл» находится в положении 1. Одновременно информационные элементы через схему «ИЛИ» поступают на выход кодера. После этого ключ переключается в положение 2 и на выход из ячеек регистра последовательно считываются проверочные элементы.

На вход декодера (рис. 2.9, б) в течение первых n тактов поступает комбинация $h(x)$ со старшего разряда. В течение этого времени ключ «Кл» разомкнут. После приема всей комбинации ключ «Кл» замыкается, а в ячейках регистра деления будет находиться синдром $S(x)$, который будет равен нулю, если ошибок в комбинации нет. При этом сработает дешифратор, на-

строенный на нулевой синдром, и выдаст сигнал, например «0», свидетельствующий об отсутствии ошибок в принятой комбинации. Напротив, если синдром не равен нулю, то на выходе дешифратора будет противоположный сигнал, указывающий на наличие ошибок в комбинации.

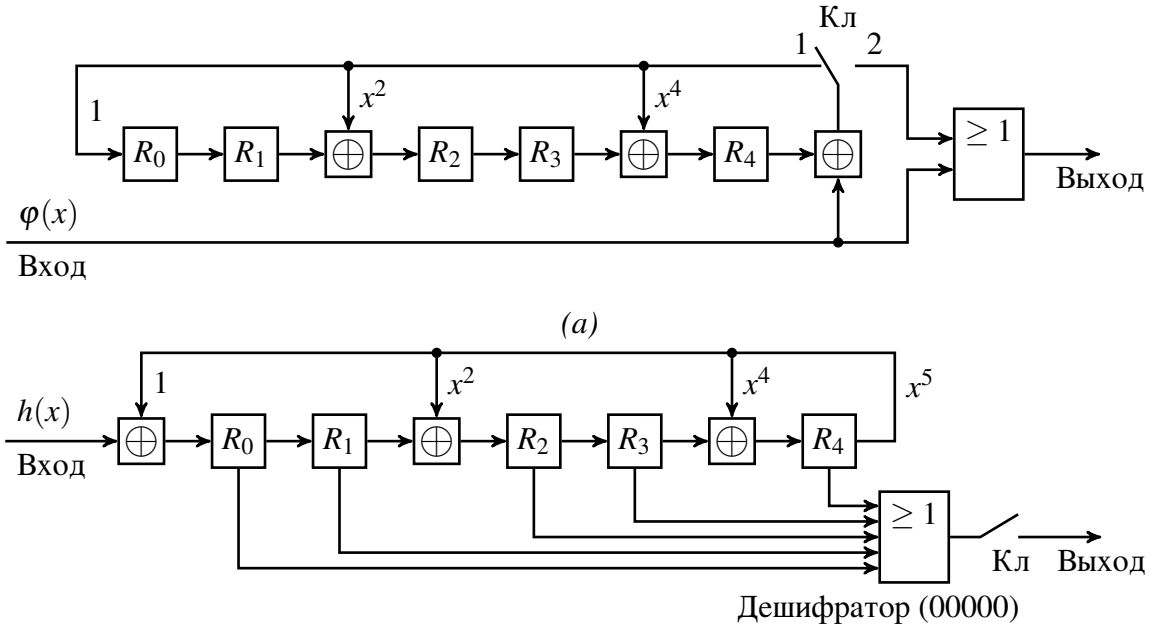


Рис. 2.9. Схемы кодера (а) и декодера (б) с расширенной CRC-5 и образующим многочленом $G(x) = (1+x)(1+x+x^4)$

Напомним, что в данном случае рассматривается вариант кодера и декодера с начальной установкой «0» в ячейки регистров сдвига с обратной связью.

Рассмотрим потактовую работу декодера при приеме комбинации $h(x)$ со старшего разряда из приведенного выше примера. Так как первые 4 старших разряда комбинации $h(x)$ являются нулями, то начнем рассматривать потактовую работу декодера с 5-го такта, когда на вход поступит «1», соответствующая двоичному коэффициенту при x^{10} (табл. 2.9).

Таблица 2.9

Потактовая работа декодера

№ такта	Разряд	$h(x)$	R_0 (0)	R_1 (0)	R_2 (0)	R_3 (0)	R_4 (0)	Выход дешифр.
5	x^{10}	1	1	0	0	0	0	
6	x^9	0	0	1	0	0	0	
7	x^8	1	1	0	1	0	0	
8	x^7	1	1	1	0	1	0	
9	x^6	0	0	1	1	0	1	
10	x^5	0	1	0	0	1	1	

Окончание табл. 2.9

Потактовая работа декодера

№ такта	Разряд	$h(x)$	R_0 (0)	R_1 (0)	R_2 (0)	R_3 (0)	R_4 (0)	Выход дешифр.
11	x^4	1	0	1	1	0	0	
12	x^3	1	1	0	1	1	0	
13	x^2	0	0	1	0	1	1	
14	x^1	0	1	0	0	0	0	
15	1	1	1	1	0	0	0	
								1

После приема комбинации в ячейках регистра находится ненулевой синдром, равный $S(x) = 1 + x$, поэтому на выходе дешифратора появится «1», свидетельствующая о наличии ошибок в принятой комбинации.

Приведем другие рекомендации по применению кодов с расширенными CRC и нулевыми начальными состояниями ячеек регистра деления.

В сетях с **технологией ATM** заголовки ATM-ячеек проверяются на наличие в них ошибок, в соответствии с рекомендацией **ITU-T I.432**, систематическим укороченным кодом $(n,k) = (40,32)$ с расширенной CRC-8 и образующим многочленом $G(x) = (1+x)P(x)$, где примитивный многочлен $P(x)$ степени 7 имеет вид:

$$P(x) = 1 + x^2 + x^3 + x^4 + x^5 + x^6 + x^7.$$

Еще одним широко применяемым кодом с расширенной CRC-16 с образующим многочленом $G(x) = 1 + x^2 + x^{15} + x^{16}$, который применяется в **протоколе бинарной синхронной связи BSC фирмы IBM**. Кодирование и декодирование осуществляется по алгоритму систематического циклического (n,k)-кода с нулевыми начальными состояниями ячеек регистра деления.

В **виртуальных локальных сетях VLAN** в соответствии со стандартом **IEEE 802.1Q** применяется (n,k)-код с расширенной CRC-32 с образующим многочленом

$$G(x) = 1 + x + x^3 + x^5 + x^7 + x^8 + x^{14} + x^{16} + x^{22} + x^{24} + x^{31} + x^{32}.$$

Наиболее сложным кодом является (n,k)-код с **расширенной CRC-64 стандарта ECMA-182** с образующим многочленом $G(x)$ 64 степени, имеющим вид в шестнадцатеричной форме записи: $(\texttt{142F0E1EBA9EA3693})_{16}$, при этом старшая степень слева.

2.3.3. Алгоритмы обнаружения ошибок двоичными (n, k)-кодами с CRC и ненулевыми состояниями ячеек регистров

Для рассмотренного выше алгоритма с нулевыми начальными состояниями ячеек регистра сдвига, реализующего деление на многочлен $G(x)$, решение декодера об отсутствии ошибок в принятой комбинации $h(x)$ выносится по нулевому остатку от деления $h(x)$ на многочлен $G(x)$. В другом, рассматриваемом ниже, алгоритме с ненулевыми состояниями ячеек регистров при отсутствии ошибок в принятой комбинации в результате деления $h(x)$ на многочлен $G(x)$ будет получен вполне определенный, не равный нулю остаток — синдром $S_o(x)$. Преимущество такого алгоритма в том, что, одновременно с контролем ошибок в принятой комбинации, осуществляется и контроль за исправностью канала. Так, при обрыве канала (или замирании, кратковременном прерывании) в первом алгоритме остаток от деления $h(x)$ на многочлен $G(x)$ будет нулевой, что будет восприниматься как отсутствие ошибок в принятой, в данном случае как бы нулевой, комбинации. Во втором алгоритме с ненулевыми начальными состояниями ячеек регистра сдвига эта ситуация будет обнаруживаться как ошибочная, так как по определению не может быть нулевого синдрома для любой разрешенной, даже нулевой, комбинации.

Как и в предыдущем случае, (n,k)-коды с ненулевыми начальными состояниями ячеек регистра сдвига могут быть как с «простой», так и с расширенной CRC. В приводимых ниже вариантах таких кодов во всех ячейках регистра деления в начальном состоянии установлены «1».

Варианты систематических кодов с «простой» CRC с $d_{\min} = 3$ и ненулевыми начальными состояниями ячеек регистров деления на образующий многочлен $P(x)$.

1. Широко применяемым таким кодом является **код CRC-5** для **USB** с образующим многочленом

$$P(x) = 1 + x + x^5.$$

2. Другим примером является **код CRC-6** для перспективной технологии **CDMA-2000-A** с образующим многочленом

$$P(x) = 1 + x + x^2 + x^5 + x^6.$$

3. В этой же технологии **CDMA-2000** применяется **код с CRC-16** с образующим многочленом

$$P(x) = 1 + x + x^2 + x^5 + x^6 + x^{11} + x^{14} + x^{15} + x^{16}.$$

4. Во многих современных системах применяется **код с «простой» CRC-32** с единичными начальными состояниями ячеек регистра образующего многочлена $P(x)$, имеющего вид в шестнадцатеричной форме записи

$(104C11DB7)_{16}$ со старшим разрядом слева. Одним из них является **код с CRC-32 для MPEG-2**.

Варианты систематических кодов с расширенной CRC с $d_{\min} = 4$ и ненулевыми начальными состояниями ячеек регистров деления на образующий многочлен $G(x)$.

1. Одним из примеров является **код CRC-6** для перспективной технологии **CDMA-2000-B** с образующим многочленом

$$G(x) = 1 + x + x^2 + x^6 = (1 + x)(1 + x^2 + x^3 + x^4 + x^5).$$

2. Аналогичным примером является **код CRC-8** для технологии **CDMA-2000** с образующим многочленом

$$G(x) = 1 + x + x^3 + x^4 + x^7 + x^8.$$

3. Во многих современных системах применяется **код с расширенной CRC-16** с единичными начальными состояниями ячеек регистра образующего многочлена $G(x) = (1 + x)P(x)$, $P(x)$ — примитивный многочлен 15 степени. Наиболее популярным является код с образующим многочленом

$$G(x) = 1 + x^5 + x^{12} + x^{16},$$

применяемый в протоколах **X.25**, **HDLC**, **V.42**, **XMODEM**, **Bluetooth** и др.

Рассмотрим алгоритмы кодирования и декодирования систематических (n,k)-кодов с CRC и ненулевыми (единичными) состояниями ячеек регистров деления кодера и декодера.

Процедура кодирования.

Шаг 1. Процесс кодирования исходной информационной комбинации в виде многочлена $\varphi(x)$ начинается с ее умножения на x^{n-k}.

Шаг 2. Одновременно с началом процесса кодирования во все $(n-k)$ ячеек регистра деления на многочлен $G(x)$, как стартовые состояния, записываются «1», т. е. в регистре кодера будет установлен многочлен

$$L(x) = 1 + x + x^2 + x^3 + \ldots + x^{n-k-1}.$$

Таким образом, этим двум первым шагам будет соответствовать добавление по mod 2 к старшим разрядам информационной комбинации $\varphi(x)$ единичной комбинации, соответствующей многочлену $L(x)$, т. е. получается сумма:

$$\varphi(x) \cdot x^{n-k} + x^k L(x).$$

Шаг 3. Последовательно с подачей на вход кодера информационной комбинации, начиная со старшего разряда, происходит потактовое деление

суммы $\varphi(x)\cdot x^{n-k}+x^kL(x)$ на образующий многочлен $G(x)$, в результате чего после окончания поступления на вход информационных элементов в ячейках регистра будут получены проверочные элементы

$$r(x)=r_0+r_1x+\ldots+r_{n-k-1}x^{n-k-1},$$

при этом будет справедливо следующее сравнение:

$$\varphi(x)\cdot x^{n-k}+x^kL(x)\equiv r(x)[\mathrm{mod}\ G(x)]. \tag{2.22}$$

При этом информационные элементы также последовательно поступают на выход кодера, что соответствует систематическому (n,k)-коду.

Шаг 4. После окончания поступления на вход кодера информационных элементов с ячеек регистра деления последовательно через инвертор считывается остаток от деления $r(x)$, т. е. многочлен $\overline{r(x)}$.

Шаг 5. Проверочные элементы инвертированного остатка $\overline{r(x)}$ добавляются к информационным элементам со стороны младших разрядов и в канал отправляется кодовая комбинация

$$f(x)=\overline{r(x)}+\varphi(x)\cdot x^{n-k}. \tag{2.23}$$

Процедура декодирования.

Рассмотрим в общем виде процедуру декодирования принятой комбинации $h(x)=f(x)+e(x)$ по шагам, в предположении, что ошибки в ней отсутствуют, т. е. $e(x)=0$ и $h(x)=f(x)$.

Шаг 1. С началом поступления на вход декодера принимаемой комбинации в ячейках регистра деления на образующий многочлен $G(x)$ устанавливается стартовая комбинация из всех «1», т. е. параллельным кодом записывается многочлен

$$L(x)=1+x+x^2+x^3+\ldots+x^{n-k-1}.$$

Относительно поступающей комбинации $h(x)=f(x)$ эти $(n-k)$ единиц займут k старших разрядов в n-элементной комбинации, т. е. это будет многочлен $x^kL(x)$.

Шаг 2. На умножитель на x^{n-k} начинает поступать комбинация $h(x)=f(x)$, суммируясь при этом с последовательными элементами, поступающими с выхода регистра деления, т. е. с многочленом $x^kL(x)$. При этом происходит потактовое деление получаемой суммы на многочлен $G(x)$. Таким образом, пока на вход декодера потактово поступает кодовая комбинация $f(x)$, начиная со старшего разряда при x^{n-1}, происходит деление суммы $x^{n-k}[f(x)+x^kL(x)]$ на образующий многочлен $G(x)$.

Шаг 3. После окончания поступления кодовой комбинации в ячейках регистра деления будет содержаться определенный синдром $S_o(x)$.

Приведем *математические выражения работы декодера*.

В результате деления будут происходить следующие преобразования:

$$x^{n-k}[f(x)+x^kL(x)] = x^{n-k}[x^{n-k}\varphi(x)+\overline{r(x)}+x^kL(x)] = \\ = x^{n-k}[x^{n-k}\varphi(x)+r(x)+L(x)+x^kL(x)].$$

Подставив вместо $r(x)$ выражение (2.22), получим:

$$x^{n-k}L(x) \equiv S_o(x)[\text{mod } G(x)]. \qquad (2.24)$$

Таким образом, в случае приема безошибочной кодовой комбинации $f(x)$ в результате ее декодирования в $(n-k)$ ячейках регистра деления будет содержаться вполне определенный синдром $S_o(x)$. Если синдром будет какой-либо другой, то это будет свидетельствовать о наличии в комбинации обнаруживаемых кодом ошибок.

Для приведенного выше примера кода с расширенной CRC-16, применяемого в протоколе HDLC (V.42), образующий многочлен имеет вид:

$$G(x) = 1+x^5+x^{12}+x^{16}.$$

Тогда, в соответствии с (2.24), синдром безошибочной комбинации $S_o(x)$ будет иметь вид:

$$S_o(x) = x^{16}L(x) = x^{16}(1+x+x^2+\ldots+x^{15}) \equiv \\ \equiv x^{12}+x^{11}+x^{10}+x^8+x^3+x^2+x+1[\text{mod } G(x)],$$

что в двоичной и в 16-ричной форме записи будет равняться

$$S_o = (0001110100001111)_2 = (1\text{D0F})_{16}.$$

Покажем, что рассматриваемые (n,k)-коды с CRC и единичными начальными состояниями ячеек регистров деления в кодере и в декодере не являются в полном смысле циклическими даже при $n = 2^{n-k}-1$.

Во-первых, такой систематический код не удовлетворяет свойству линейности, т. е. сумма двух или большего четного числа разрешенных кодовых комбинаций не образует некоторую другую разрешенную кодовую комбинацию. Рассмотрим это на примере двух разрешенных комбинаций $f_1(x)$ и $f_2(x)$, которые, в соответствии с (2.23), имеют вид:

$$f_1(x) = \overline{r_1(x)}+\varphi_1(x)\cdot x^{n-k}; \qquad f_2(x) = \overline{r_2(x)}+\varphi_2(x)\cdot x^{n-k}.$$

В приведенных выражениях $\varphi_1(x)$ и $\varphi_2(x)$ — многочлены исходных информационных элементов соответственно комбинаций $f_1(x)$ и $f_2(x)$; $\overline{r_1(x)}$ и $\overline{r_2(x)}$ — инвертированные остатки, которые равны:

$$\overline{r_1(x)} = r_1(x) + L(x) \qquad \text{и} \qquad \overline{r_2(x)} = r_2(x) + L(x),$$

где

$$r_1(x) \equiv x^{n-k}\varphi_1(x) + x^k L(x) \ [\mathrm{mod}\ G(x)]; \quad r_2(x) \equiv x^{n-k}\varphi_2(x) + x^k L(x) \ [\mathrm{mod}\ G(x)].$$

Подставив $\overline{r_1(x)}$, $r_1(x)$, $\overline{r_2(x)}$, $r_2(x)$ в выражения для разрешенных кодовых комбинаций $f_1(x)$ и $f_2(x)$, получим следующую сумму:

$$\begin{aligned} h(x) &= f_1(x) + f_2(x) = x^{n-k}\varphi_1(x) + r_1(x) + \cancel{L(x)} + x^{n-k}\varphi_2(x) + r_2(x) + \cancel{L(x)} = \\ &= \cancel{x^{n-k}\varphi_1(x)} + \cancel{x^{n-k}\varphi_1(x)} + \cancel{x^k L(x)} + \cancel{x^{n-k}\varphi_2(x)} + \cancel{x^{n-k}\varphi_2(x)} + \cancel{x^k L(x)} = 0. \end{aligned}$$

Таким образом, сумма двух разрешенных комбинаций не является также разрешенной комбинацией, так как среди множества разрешенных комбинаций нулевая отсутствует. Значит, код не удовлетворяет свойству линейности, которое характерно для классических циклических кодов.

Во-вторых, покажем, что также не работает свойство циклического сдвига, порождающего новую разрешенную комбинацию для классического циклического кода.

Пусть имеется разрешенная кодовая комбинация $f(x)$, при декодировании которой получен заранее известный синдром $S_o(x)$ в соответствии с (2.24).

Произведем теперь циклический сдвиг комбинации $f(x)$ на один шаг, в результате получим произведение $x \cdot f(x)$, которое подвергнем декодированию по рассмотренному выше алгоритму:

$$\begin{aligned} & x^{n-k}\left\{x \cdot f(x) + x^k L(x)\right\} = x^{n-k}\left\{x \cdot \left[x^{n-k}\varphi(x) + \overline{r(x)}\right] + x^k L(x)\right\} = \\ & = x^{n-k}\left\{x \cdot \left[x^{n-k}\varphi(x) + r(x) + L(x)\right] + x^k L(x)\right\} = \\ & = x^{n-k}\left\{x \cdot \left[\cancel{x^{n-k}\varphi(x)} + \cancel{x^{n-k}\varphi(x)} + x^k L(x) + L(x)\right] + x^k L(x)\right\} = \\ & = x^{n-k}L(x)\left(x + x^k + x^{k+1}\right) \neq S_o(x)[\mathrm{mod}\ G(x)]. \end{aligned}$$

Таким образом, циклический сдвиг разрешенной комбинации $f(x)$ на один шаг (умножение $f(x)$ на x) не порождает новую разрешенную комбинацию, т. е. при декодировании описанным выше алгоритмом синдром не равен $S_o(x)$. Поэтому такой систематический (n,k)-код с CRC не является в полном смысле циклическим и может быть назван *псевдоциклическим*.

Оценим *вероятностные характеристики* таких блочных систематических кодов с CRC и ненулевыми (единичными) начальными состояниями ячеек регистра деления на образующий многочлен $G(x)$.

Правильное декодирование будет происходить в случае отсутствия ошибок в принятой комбинации, состоящей из n элементов. Вероятность такого события в канале ДСК будет определяться выражением:

$$P_{\text{пп}} = (1 - p_0)^n,$$

где p_0 — вероятность ошибочного приема сигнального элемента в двоичном симметричном канале.

Определим ситуации, при которых ошибки обнаруживаться не будут. Пусть принимаемая комбинация будет: $h(x) = f(x) + e(x)$, где $e(x)$ — многочлен ошибок. Процедура декодирования в математических операциях будет следующей:

$$\begin{aligned}
&x^{n-k}\left\{h(x) + x^k L(x)\right\} = x^{n-k}\left\{f(x) + e(x) + x^k L(x)\right\} = \\
&= x^{n-k}\left\{x^{n-k}\varphi(x) + \overline{r(x)} + e(x) + x^k L(x)\right\} = \\
&= x^{n-k}\left\{x^{n-k}\varphi(x) + r(x) + L(x) + e(x) + x^k L(x)\right\} = \\
&= x^{n-k}\left\{\cancel{x^{n-k}\varphi(x)} + \cancel{x^{n-k}\varphi(x)} + L(x) + e(x) + \cancel{x^k L(x)} + \cancel{x^k L(x)}\right\} = \\
&= x^{n-k}[L(x) + e(x)] = x^{n-k}L(x) + x^{n-k}e(x) \equiv S_o(x) + x^{n-k}e(x)[\text{mod } G(x)].
\end{aligned}$$

Из полученного выражения следует, что необнаруживаемыми ошибками будут такие, многочлены которых $x^{n-k}e(x)$ делятся на $G(x)$ без остатка, т. е.

$$x^{n-k}e(x) \equiv 0[\text{mod } G(x)].$$

Таким образом, для оценки вероятности необнаруживаемых ошибок необходимо знать весовой спектр (n,k)-кода с образующим многочленом $G(x)$. Тогда вероятность необнаруживаемой ошибки $P_{\text{но}}$ в канале ДСК будет определяться выражением:

$$P_{\text{но}} = \sum_{w_i = d_{\min}}^{n} A(w_i) p_0^{w_i} (1 - p_0)^{n - w_i},$$

где $A(w_i)$ — число комбинаций классического (n,k)-кода с весом w_i, кратным образующему многочлену.

Вероятность приема комбинации с обнаруживаемыми ошибками $P_{\text{оо}}$, следовательно, будет равна

$$P_{\text{оо}} = 1 - P_{\text{пп}} - P_{\text{но}}.$$

Таким образом, в данном пункте рассмотрен практически весь спектр систематических кодов с CRC, применяемых в различных системах передачи данных для обнаружения ошибок.

2.4. Принцип обнаружения ошибок в протоколах межсетевого взаимодействия и транспортного уровня в сети Интернет

В глобальной сети Интернет применяется помехоустойчивый блочный код, предназначенный для обнаружения ошибок на уровне межсетевого взаимодействия в IP-пакетах, а также на транспортном уровне в протоколах TCP и UDP [42–44]. Алгоритмы кодирования и декодирования на различных уровнях одинаковы. При этом, в IP-пакетах код предназначен для контроля за ошибками только в заголовках IP-пакетов, тогда как на транспортном уровне контроль за ошибками осуществляется не только в заголовках, но и в поле данных TCP-сегментов и UDP-датаграмм. Особенности борьбы с ошибками в Интернете отличаются на каждом из уровней. Так, в случае обнаружения ошибок в заголовке IP-пакета весь пакет бракуется и переспрос на повторную передачу пакета не посылается. Обнаружение ошибок в TCP-сегменте приводит к тому, что ошибочный сегмент стирается и к отправителю TCP-сегмента посылается запрос на его повторную передачу. А вот если ошибки будут обнаружены в UDP-датаграмме, то последняя стирается и запрос на повторную передачу этой датаграммы не посылается.

Следующей особенностью (n,k)-кода является то, что длина кодируемой части не является постоянной, но она ограничена максимально возможной в соответствии с документами RFC (Request for Comments — запрос комментариев). Например, длина заголовка в IP-пакете 4 версии обычно равна 20 октетам. Максимальные размеры TCP-сегмента с заголовком без опций и UDP-датаграммы не превышают 65515 байт. Во всех указанных протоколах длина проверочной последовательности (контрольной суммы) равна 16 бит.

Помехоустойчивый код в Интернет не относится к классу CRC, а является кодом с вычислением контрольной суммы по модулю $(2^{16}-1)$ с переносом. Рассмотрим этот код подробнее.

2.4.1. Механизм вычисления и проверки контрольной суммы

2.4.1.1. Алгоритм кодирования

Кодируемая часть, длина которой в битах должна быть кратной 16, разбивается на участки по 16 двоичных элементов в каждом. Контрольная сумма формируется путем двоичного суммирования 16-элементных двоичных комбинаций кодируемой части пакета (сегмента, датаграммы) с переносом в следующие старшие разряды. Сложение происходит с приведением суммы 16-элементных комбинаций по модулю $(2^{16}-1)$. Полученная в результате суммирования 16-элементная двоичная комбинация на передающей стороне инвертируется, т. е. «1» меняется на «0», и наоборот — «0» меняется на «1». Полученная при этом двоичная 16-разрядная комбинация и будет представ-

лять собой контрольную сумму, которая записывается в поле контрольной суммы и передается в составе IP-пакета (TCP-сегмента, UDP-датаграммы) на приемную сторону. Следует учесть, что первоначально (до завершения процедуры кодирования) поле контрольной суммы должно быть обнулено. Кроме того, надо иметь ввиду, что в вычислении контрольных сумм TCP-сегмента и UDP-датаграммы как на передающей, так и на приемной стороне должны участвовать псевдозаголовки из 12 байт.

2.4.1.2. Алгоритм декодирования

На приемной стороне в декодере все 16-разрядные двоичные комбинации тех же самых полей, что и в кодере, а также принятая контрольная сумма суммируются по тому же правилу, что и на передаче. Отличие состоит лишь в том, что полученная после суммирования 16-разрядная двоичная комбинация на приемной стороне не инвертируется. В результате, если в принятом сообщении ошибки отсутствуют, то по окончании процедуры суммирования в декодере будет получена контрольная 16-разрядная комбинация, все элементы которой будут равны «1». Этот факт и будет свидетельствовать об отсутствии ошибок в принятом сообщении (заголовке IP-пакета, TCP-сегменте, UDP-датаграмме). Если в контрольной 16-разрядной комбинации будет хотя бы один «0», то это будет говорить о наличии ошибок в принятом сообщении.

На рис. 2.10, 2.11 и 2.12 приведен демонстрационный пример кодирования и декодирования контрольной суммы для трех двоичных 16-разрядных комбинаций с младшими разрядами справа в двоичном и шестнадцатеричном видах соответственно. При этом суммирование шестнадцатеричных чисел производится с переносом по mod 16.

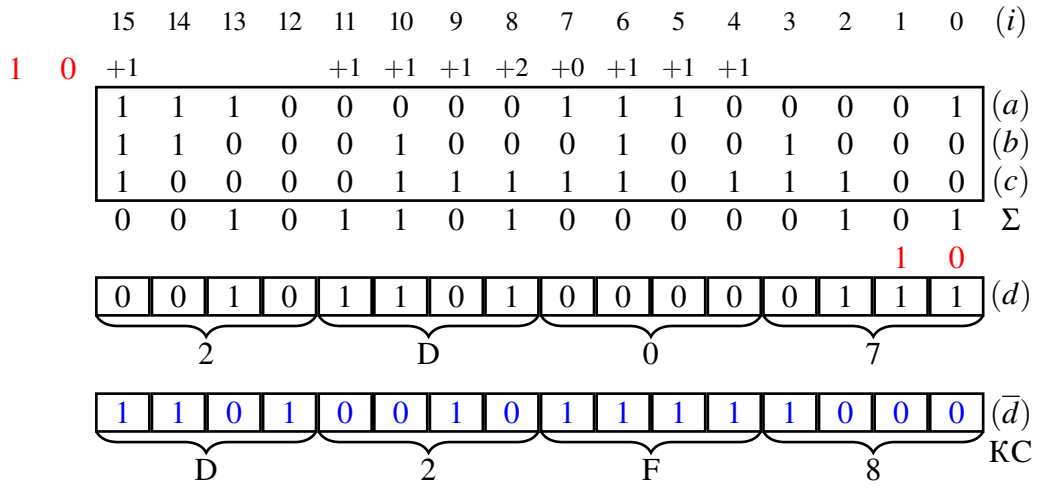


Рис. 2.10. Пример кодирования контрольной суммы для трех двоичных 16-разрядных комбинаций с младшими разрядами справа в двоичном виде

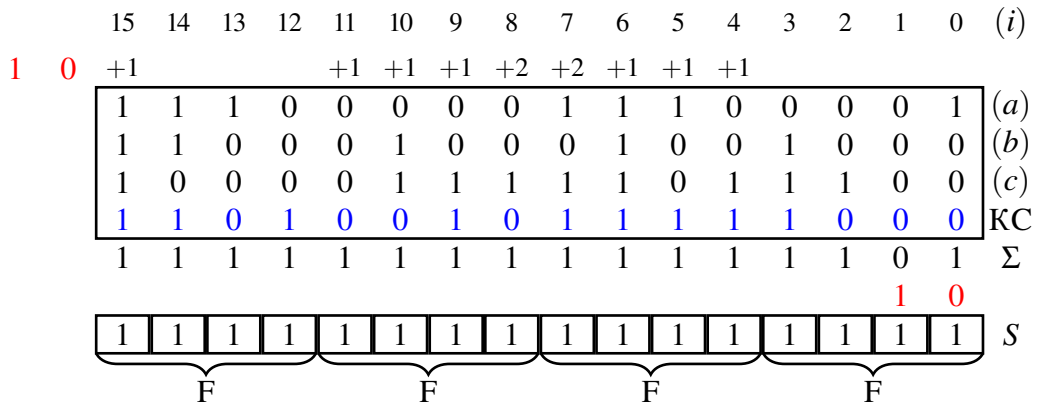


Рис. 2.11. Пример декодирования контрольной суммы для трех двоичных 16-разрядных комбинаций с младшими разрядами слева в двоичном виде

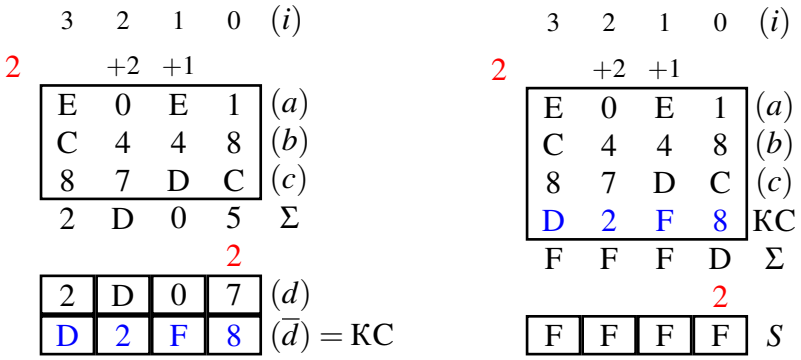


Рис. 2.12. Пример кодирования (а) и декодирования (б) контрольной суммы для трех двоичных 16-разрядных комбинаций с младшими разрядами слева в шестнадцатеричном виде

2.4.2. Вероятностная оценка кода по обнаружению ошибок

Обнаружение ошибок в данном коде может быть оценено аналогично рассмотренному в пп. 2.2.1 блочному коду байтовой структуры с длиной блока в 128 байт и вычислением контрольной суммы по mod 255. В частности, при длине блока в N байт вероятность правильного приема блока в канале ДСК с вероятностью битовой ошибки p может быть вычислена в соответствии с выражением $P_{\text{пп}} = (1-p)^{8N}$.

При вычислении контрольной суммы в Интернет происходит сложение N 16-элементных комбинаций по mod $(2^{16}-1)$, поэтому вероятность правильного приема блока будет определяться выражением $P_{\text{пп}} = (1-p)^{16N}$.

Прием блока с необнаруженной ошибкой возможен из-за возникновения так называемых ошибок замещения. Например, двукратная необнаруживаемая ошибка $(t=2)$ возникнет в случае, когда в одной из 16 N-элементных комбинаций блока возникнут ошибочные переходы одной «1» в «0» и одного «0» в «1». Вероятность такого события $P_{\text{но}}(t=2;1)$ в канале ДСК при равно-

вероятных 0 и 1 и среднем весе N-элементной комбинации $w = \frac{N}{2}$ может быть определена по выражению:

$$P_{\text{но}}(t = 2; 1) = 16\frac{N^2}{4}p^2(1-p)^{16N-2}. \tag{2.25}$$

Аналогично, 4-кратная ошибка $(t = 4)$ не будет обнаружена, если в одной из 16 N-элементных комбинаций блока возникнут ошибочные переходы двух «1» в два «0» и двух «0» в две «1». Вероятность $P_{\text{но}}(t = 4; 1)$ такого события оценивается выражением:

$$P_{\text{но}}(t = 4; 1) = 16\left[C^2_{N/2}p^2\right]^2(1-p)^{16N-4}. \tag{2.26}$$

В общем виде вероятность необнаруживаемых ошибок четной кратности $t = 2i$, $(1 \le i \le \frac{N}{2})$ типа замещений в одной из 16 N-элементных комбинаций может быть аналитически оценена, при равной вероятности 0 и 1 в сообщении, выражением:

$$P_{\text{но}}(t = 2i; 1) = 16\left[C^i_{N/2}p^i\right]^2(1-p)^{16N-2i}. \tag{2.27}$$

Тогда общая вероятность необнаруживаемой ошибки четной кратности типа замещения в одной из 16 N-элементных комбинаций блока может быть определена суммой:

$$P_{\text{но}}(t = 2,4,8,\ldots;1) = \sum_{i=1}^{N/2} P_{\text{но}}(t = 2i) = \sum_{i=1}^{N/2} 16\left[C^i_{N/2}p^i\right]^2(1-p)^{16N-2i}.$$

Для более полной приближенной оценки вероятности необнаруживаемых ошибок необходимо учесть также необнаруживаемые ошибки кратности 3. Тогда, кроме формул (2.25) и (2.26), следует также получить выражение для 3-кратных необнаруживаемых ошибок типа замещения. К таким ошибкам относятся однократная ошибка в j-й N-элементной комбинации, $1 \le j \le 16$, и двукратная ошибка в $(j-1)$-й комбинации. Причем, ошибки в j-й и в $(j-1)$-й комбинациях должны быть в противоположных символах, например, одна ошибка среди «1» в j-й и две ошибки среди «0» в $(j-1)$-й комбинации или наоборот. Заметим, при этом, что нулевой строке $(j = 0)$ соответствуют младшие разряды 16-разрядных комбинаций, участвующих в вычислении контрольной суммы.

При этих условиях вероятность трехкратных необнаруживаемых ошибок, аналогично формуле (2.14), можно определить из выражения:

$$P_{\text{но}}(t = 3; 2) = 2 \cdot 15\left[C^1_{N/2}C^2_{N/2}p^3(1-p)^{16N-3}\right]. \tag{2.28}$$

Кроме того, следует также учесть случай возникновения четырехкратных $(t = 4)$ необнаруживаемых ошибок в двух произвольных N-элементных комбинациях по две ошибки типа замещения в каждой из них. Вероятность $P_{\text{но}}(t = 4;2)$ такого события определяется как

$$P_{\text{но}}(t = 4;2) = C_{16}^{2}(Q_1)^2(1-p)^{16N}, \tag{2.29}$$

где Q_1 — вероятность (2.30) двукратной необнаруживаемой ошибки типа замещения в отдельно взятой N-элементной комбинации:

$$Q_1 = \left(\frac{N}{2}\right)^2 p^2(1-p)^{N-2}. \tag{2.30}$$

Таким образом, вероятность необнаруживаемых ошибок в протоколах IP, ICMP, TCP и UDP, в соответствии с (2.25), (2.26), (2.28), (2.29) и (2.30), можно приближенно определить выражением:

$$P_{\text{но}} = P_{\text{но}}(t = 2;1) + P_{\text{но}}(t = 4;1) + P_{\text{но}}(t = 3;2) + P_{\text{но}}(t = 4;2),$$

где в скобках $(t = i; j)$ обозначено: i — количество ошибок в j N-элементных комбинациях.

Считается, что в случае равномерного распределения, алгоритм контрольной суммы пропускает лишь 1 ошибку из 2^{16} пакетов. Для неравномерно распределенных данных обнаруживающая способность зависит от вида распределения. Так, исследование [45] показало, что в зависимости от вида трафика, используемый в протоколе TCP алгоритм вычисления контрольной суммы обеспечивает вероятность необнаруженной ошибки от 10^{-10} до $6{,}25 \cdot 10^{-8}$.

2.4.3. Примеры вычисления контрольной суммы для разных протоколов

2.4.3.1. Контрольная сумма в протоколе IPv4

В протоколе IPv4 контрольная сумма рассчитывается только для заголовка пакета. Данные не проверяются, поскольку инкапсулируемые в IPv4 протоколы имеют свою контрольную сумму, учитывающую, как их заголовок, так и данные. К тому же, заголовок пакета IPv4 меняется при прохождении маршрутизаторов и, следовательно, контрольная сумма должна вычисляться каждым маршрутизатором заново — если бы она учитывала и данные пакета IPv4, то это бы значительно повысило нагрузку на процессоры маршрутизаторов и увеличило время обработки каждого пакета [46].

Структура заголовка пакета IPv4 приведена на рис. 2.13 [46].

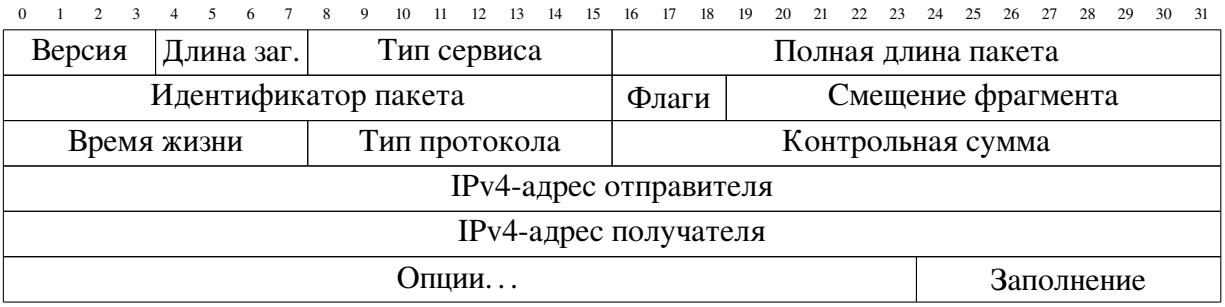


Рис. 2.13. Структура заголовка пакета IPv4

Контрольная сумма $\mathrm{CS_{IP}}$ заголовка передаваемого пакета IPv4 рассчитывается по следующему алгоритму:

1. Заголовок разбивается на слова W_i по 16 бит. При необходимости последнее слово заголовка дополняется нулями справа (биты заполнения), чтобы «выровнять» длину заголовка в битах кратно 16.

2. Значение поля контрольной суммы, которому соответствует слово W_6, принимается равным нулю:

$$W_6 = (0000)_{16}.$$

3. Полученные 16-битные слова W_i поэлементно суммируются между собой, как двоичные числа с переносом в старшие разряды:

$$W_s = \sum_i W_i.$$

4. В том случае, если результат сложения W_s в двоичном представлении превышает по длине 16 бит, он разбивается на два 16-битных слова, которые складываются между собой. Эту процедуру называют «круговым переносом», т. е. переполнение старшего разряда переносится в младший, например

$$\text{если } W_s = (2\mathrm{A4E3})_{16}, \quad \text{то } W_s = (0002)_{16} + (\mathrm{A4E3})_{16} = (\mathrm{A4E5})_{16}.$$

5. В случае, если результат сложения W_s снова превышает 16 бит, предыдущая операция повторяется.

6. Находится двоичное поразрядное дополнение результата сложения, которое и записывается в поле контрольной суммы:

$$\mathrm{CS_{IP}} = (\mathrm{FFFF})_{16} - W_s.$$

Для более подробного ознакомления с процедурой вычисления контрольной суммы в протоколах сетевого и транспортного уровня сети Интернет и вариантами ее реализации для различных языков программирования рекомендуется обратиться к RFC 1071 [42].

0 — 15	16 — 31
4500	0076
252D	4000
4011	0000
C0A8	010F
C1C8	B708

Рис. 2.14. Пример заголовка пакета IPv4 с обнуленным полем контрольной суммы

Для примера рассмотрим *расчет контрольной суммы заголовка IP-пакета*, приведенного на рис. 2.14. Пакет записан в шестнадцатеричной системе счисления. Поле контрольной суммы выделено цветом и обнулено перед началом формирования передаваемого IP-пакета.

1. Разбиваем заголовок с обнуленным полем контрольной суммы на слова по 16 бит и суммируем полученные 16-битные слова между собой:

$$(4500)_{16} + (0076)_{16} + (252D)_{16} + (4000)_{16} + (4011)_{16} + \\ + (0000)_{16} + (C0A8)_{16} + (010F)_{16} + (C1C8)_{16} + (B708)_{16} = (3253B)_{16}.$$

2. Поскольку результат сложения в двоичном представлении превышает 16 разрядов (или 4 шестнадцатеричных цифры), разбиваем его на два слова по 16 бит каждое и снова их суммируем:

$$(0003)_{16} + (253B)_{16} = (253E)_{16}.$$

3. Находим контрольную сумму, как двоичное поразрядное дополнение результата сложения:

$$CS_{IP} = (FFFF)_{16} - (253E)_{16} = (DAC1)_{16}.$$

Полученное число заносится в поле контрольной суммы заголовка IP-пакета (рис. 2.14).

Проверка контрольной суммы при приеме IP-пакета производится по аналогичному алгоритму, отличаясь только тем, что в расчете участвует и контрольная сумма принятого IP-пакета. Если итоговое поразрядное двоичное дополнение полученной суммы равно 0, т. е. $(0000)_{16}$, то это говорит о корректности контрольной суммы.

Для примера *проверим корректность контрольной суммы* заголовка IP-пакета, приведенного на рис. 2.14 с учетом значения поля контрольной суммы $(DAC1)_{16}$.

1. Суммируем все 16-битные слова заголовка между собой:

$$(4500)_{16} + (0076)_{16} + (252D)_{16} + (4000)_{16} + (4011)_{16} + \\ + (DAC1)_{16} + (C0A8)_{16} + (010F)_{16} + (C1C8)_{16} + (B708)_{16} = (3FFFC)_{16}.$$

2. Поскольку результат сложения превышает 16 бит, разбиваем его на два слова по 16 бит каждое и снова их суммируем:

$$(0003)_{16} + (\text{FFFC})_{16} = (\text{FFFF})_{16}.$$

3. Находим двоичное поразрядное дополнение результата сложения:

$$(\text{FFFF})_{16} - (\text{FFFF})_{16} = (0000)_{16}.$$

Таким образом, мы проверили, что приведенная в пакете на рис. 2.14 контрольная сумма верна.

Можно последнюю операцию поразрядного двоичного дополнения не проводить. Тогда правильность контрольной суммы принятого IP-пакета будет подтверждаться результатом суммирования $(\text{FFFF})_{16}$ на втором шаге алгоритма проверки.

2.4.3.2. Контрольная сумма в протоколе ICMP

В протоколе ICMP контрольная сумма рассчитывается для всего пакета. Структура пакета ICMP приведена на рис. 2.15 [47].

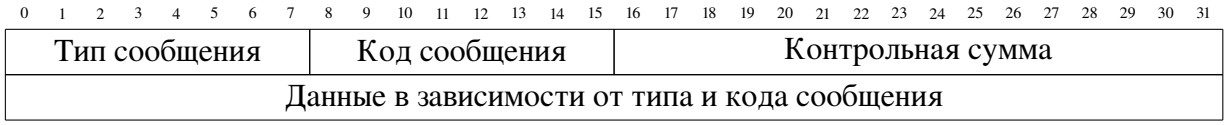


Рис. 2.15. Структура пакета ICMP

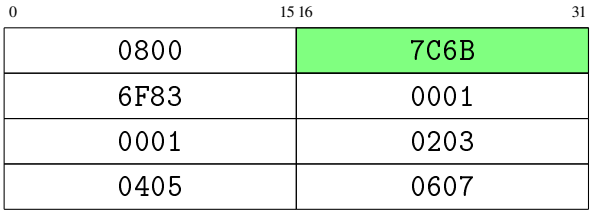


Рис. 2.16. Пример пакета ICMP

Алгоритм вычисления контрольной суммы полностью аналогичен таковому для заголовка пакета IP. Рассмотрим вычисление контрольной суммы на примере ICMP-пакета, приведенного на рис. 2.16. Поле контрольной суммы выделено цветом.

1. Разбиваем заголовок на слова по 16 бит, принимаем значение поля контрольной суммы равным нулю и суммируем полученные 16-битные слова между собой:

$$(0800)_{16} + (0000)_{16} + (6\text{F}83)_{16} + (0001)_{16} + \\ + (0001)_{16} + (0203)_{16} + (0405)_{16} + (0607)_{16} = (8394)_{16}.$$

2. Находим контрольную сумму, как двоичное поразрядное дополнение результата сложения:

$$\mathrm{CS}_{\mathrm{ICMP}} = (\mathrm{FFFF})_{16} - (8394)_{16} = (7\mathrm{C6B})_{16}.$$

Как можно видеть, результат совпадает со значением поля контрольной суммы, приведенным на рис. 2.16.

Проверка контрольной суммы ICMP-пакета аналогична рассмотренной для протокола IPv4.

2.4.3.3. Контрольная сумма в протоколах TCP и UDP

Алгоритм расчета контрольной суммы пакетов TCP и UDP, структура которых приведена на рис. 2.17 и 2.18 соответственно, практически аналогичен таковому для заголовка пакета IP. Контрольная сумма рассчитывается для всего пакета TCP/UDP, а также учитывает IP-адреса отправителя и получателя. Для этого перед расчетом контрольной суммы формируется специальный псевдозаголовок, структура которого показана на рис. 2.19 [48, 49].

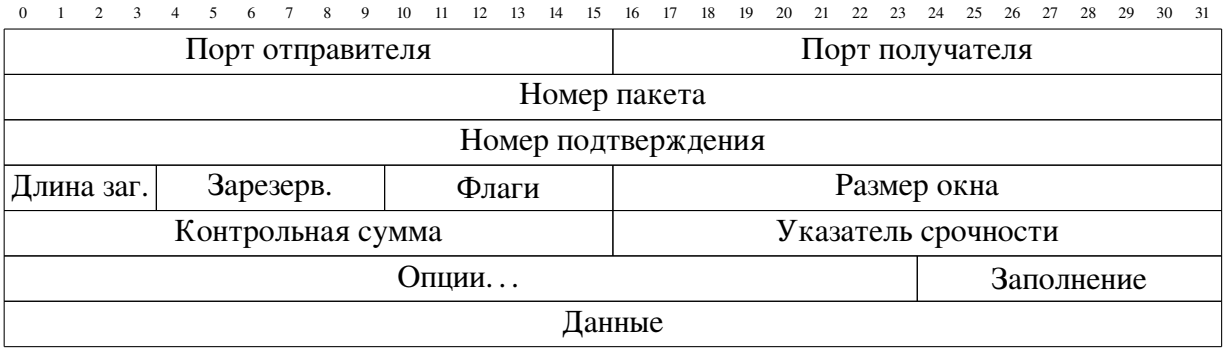


Рис. 2.17. Структура пакета TCP

Рис. 2.18. Структура пакета UDP

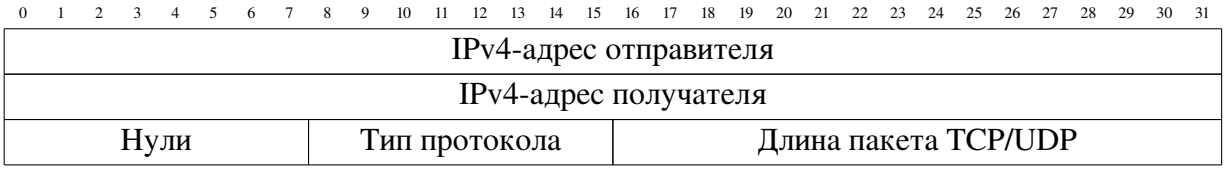


Рис. 2.19. Структура псевдозаголовка TCP/UDP

Рассмотрим вычисление контрольной суммы TCP/UDP на примере пакета UDP, показанного на рис. 2.20. На рис. 2.20 желтым выделен заголовок IPv4, который необходим для построения псевдозаголовка, а зеленым обозначена контрольная сумма пакета UDP.

0 — 15	16 — 31	
4500	0038	Заголовок IPv4
DAF5	0000	
4011	6537	
C0A8	010F	
C1C8	B708	
E4DD	0035	Заголовок UDP
0024	0B54	
C0FD	0100	Данные UDP
0001	0000	
0000	0000	
0667	6F6F	
676C	6503	
636F	6D00	
0001	0001	

Рис. 2.20. Пример пакета UDP с заголовком IPv4

Расчет контрольной суммы происходит в следующем порядке.

1. Формируется псевдозаголовок (рис. 2.21).

0 — 15	16 — 31
C0A8	010F
C1C8	B708
0011	0024

Рис. 2.21. Псевдозаголовок для пакета UDP, показанного на рис. 2.20

2. Разбиваем заголовок UDP, блок данных и псевдозаголовок на слова по 16 бит, принимаем значение поля контрольной суммы равным нулю и суммируем полученные 16-битные слова между собой:

$$\underbrace{[(\text{E4DD})_{16}+(0035)_{16}+(0024)_{16}+(0000)_{16}]}_{\text{Заголовок UDP}}+$$
$$+[(\text{C0FD})_{16}+(0100)_{16}+(0001)_{16}+(0000)_{16}+$$
$$+(0000)_{16}+(0000)_{16}+(0667)_{16}+(\text{6F6F})_{16}+(\text{676C})_{16}+$$
$$+\underbrace{(6503)_{16}+(\text{636F})_{16}+(\text{6D00})_{16}+(0001)_{16}+(0001)_{16}]}_{\text{Данные UDP}}+$$
$$+\underbrace{[(\text{C0A8})_{16}+(\text{010F})_{16}+(\text{C1C8})_{16}+(\text{B708})_{16}+(0011)_{16}+(0024)_{16}]}_{\text{Псевдозаголовок}}=(\text{5F4A6})_{16}.$$

3. Поскольку двоичная запись результата сложения превышает 16 бит, разбиваем его на два слова по 16 бит каждое и снова их суммируем:

$$(0005)_{16} + (\text{F4A6})_{16} = (\text{F4AB})_{16}.$$

4. Находим контрольную сумму, как двоичное поразрядное дополнение результата сложения:

$$\text{CS}_{\text{UDP}} = (\text{FFFF})_{16} - (\text{F4AB})_{16} = (0\text{B54})_{16}.$$

Как можно видеть, результат совпадает со значением поля контрольной суммы, приведенным на рис. 2.20.

Проверка контрольной суммы аналогична рассмотренной ранее для протокола IPv4.

Контрольные вопросы

1. Как реализуется кодирование и декодирование в кодах с проверкой на четность?
2. Каким образом расчитывается контрольная сумма блока по mod 255?
3. В каких случаях возникают необнаруживаемые ошибки при использовании метода контроля четности по строкам и столбцам блока?
4. Как реализуется алгоритм с простой CRC?
5. В каких системах применяются простые коды CRC?
6. Как строятся кодер и декодер расширенного кода CRC-5?
7. Как работает механизм обнаружения ошибок в сетевых и транспортных протоколах сети Интернет?

Рекомендуемая литература

1. Галлагер, Р. Теория информации и надежная связь / Р. Галлагер ; под ред. М. С. Пинскера, Б. С. Цыбакова. — М. : «Сов. радио», 1974.
2. Хэмминг, Р. В. Теория кодирования и теория информации / Р. В. Хэмминг. — М. : Радио и связь, 1983.
3. Braden, R. Computing the Internet Checksum. — Internet Requests for Comments. — 1988. — September. — URL: https://tools.ietf.org/html/rfc1071.
4. Морелос-Сарагоса, Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. / Р. Морелос-Сарагоса. — М. : Техносфера, 2005.
5. Власов, Е. Г. Конечные поля в телекоммуникационных приложениях. Теория и применение FEC, CRC и М-последовательностей : практическое пособие / Е. Г. Власов. — М. : Инфра-М, 2016.

3. ВЫБОР ПОМЕХОУСТОЙЧИВОГО КОДА В СИСТЕМАХ ПОВЫШЕНИЯ ДОСТОВЕРНОСТИ С РЕШАЮЩЕЙ ОБРАТНОЙ СВЯЗЬЮ

3.1. Общие положения

В системах повышения достоверности с обратной связью, упрощенный вид которых представлен на рис. 3.1, введение избыточности в передаваемые сообщения осуществляется с учетом состояния канала связи в момент передачи сообщения. С ухудшением состояния канала вводимая избыточность повышается, а по мере улучшения состояния канала она уменьшается. Устройства защиты от ошибок (УЗО), работающие по такому принципу, называют адаптивными.

В зависимости от характера информации, передаваемой по обратному каналу, различают системы повышения достоверности следующих видов:

- системы с решающей обратной связью (РОС);
- системы с информационной обратной связью (ИОС);
- системы с комбинированной обратной связью (КОС).

Название систем отражает характер информации, передаваемой по обратному каналу в целях повышения достоверности сообщений, передаваемых по прямому каналу.

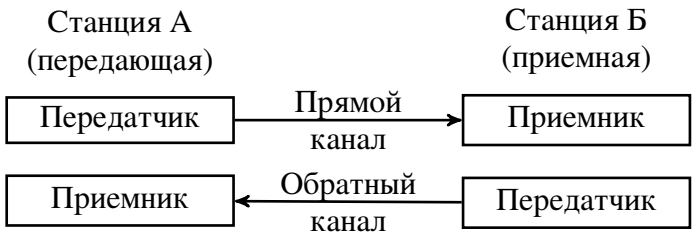


Рис. 3.1. Общий вид системы с обратной связью

В системах РОС активную роль в выявлении ошибок, возникающих в процессе передачи сообщения по прямому каналу, играет приемник.

В этих системах, как правило, используются циклические (n,k) коды в режиме обнаружения ошибок. Обнаружение ошибок осуществляется в декодере приемника, и по обратному каналу передается решение декодера приемника о наличии или отсутствии ошибок в принятом сообщении (кодовой комбинации). Это решение передается в виде специальных служебных комбинаций — «запрос» как требование повторения кодовой комбинации, в которой декодер обнаружил ошибку, или «подтверждение» как решение о передаче следующих кодовых комбинаций сообщения, если декодер не обнаружил ошибок в принятой комбинации (n,k) кода.

В системе ИОС решение о необходимости повторения переданного сообщения или передаче нового сообщения принимает передатчик. Для принятия такого решения по каналу обратной связи от приемной станции к передающей по обратному каналу возвращается вся принятая информация или ее признаки. В таких системах для передачи сообщений могут использоваться простые (неизбыточные) коды.

В системах КОС обратный канал может использоваться как для передачи решения приемника о наличии ошибок в принятом сообщении (как в системах РОС), так и для обратной передачи сообщения или его признака (как в системах ИОС).

Целью нашего рассмотрения является система РОС, характеризующаяся непрерывной последовательной передачей сообщений. Задача сохранения последовательности сообщений, в которой сообщения поступают от датчика, при выдаче их потребителю достигается использованием блокировки передатчика и приемника. Блокировка защищает потребителя от повторного получения сообщений, если они уже поступили к нему [50].

Блокировка является принципиальной характеристикой рассматриваемой системы и потому отражена в ее полном названии.

В системах РОС-ППбл есть еще одна особенность, требующая наличия блокировки. В целях упрощения логики работы устройства управления (УУ) в УЗО реализована одинаковая реакция УУ на комбинации с обнаруженной ошибкой и поступление на вход приемника комбинации «запрос».

В обоих случаях УУ УЗО обеспечивает передачу к противоположной станции служебной комбинации «запрос» и повторение h ранее переданных кодовых комбинаций. Блокировка приемника позволяет отсечь ненужную информацию, предотвращает реагирование на комбинацию «запрос» при поступлении повторяемой информации к станции, обнаружившей ошибку, а на станции, откуда ожидается повторная передача при приеме комбинации «запрос», устраняется повторный прием ранее правильно принятых сообщений.

Система РОС-ППбл имеет еще две принципиальные особенности, обусловленные необходимостью обеспечивать непрерывную последовательную передачу от передающей станции к приемной.

Это обязательное использование синхронного способа работы и отсутствие необходимости в сигнале «подтверждение».

Система РОС-ППбл имеет два режима работы — режим «нормальной работы» при отсутствии ошибок и режим «переспроса», вызванный обнаружением ошибок или приемом комбинации «запрос». Как правило, системы РОС-ППбл работают в режиме одновременной двухсторонней передачи (дуплекс) и при отсутствии ошибок сообщения передаются от двух взаимодействующих

станций до тех пор, пока приемник одной из станций не обнаружит ошибки или примет комбинацию «запрос».

В этом случае обе станции практически одновременно переходят в режим переспроса, обмениваются комбинациями «запрос» и повторно передаваемыми сообщениями. Режим переспроса завершается после того, как станция, обнаружившая ошибку, примет повторяемое сообщение без ошибок. После этого восстанавливается нормальный режим и обе станции начинают вводить новые сообщения от датчиков для передачи по каналам связи.

3.2. Описание работы системы РОС-ППбл

Рассмотрим работу системы РОС-ППбл, используя схему алгоритма функционирования (рис. 3.2), структурную схему одной из взаимодействующих станций (рис. 3.3) и временную диаграмму работы системы (рис. 3.4).

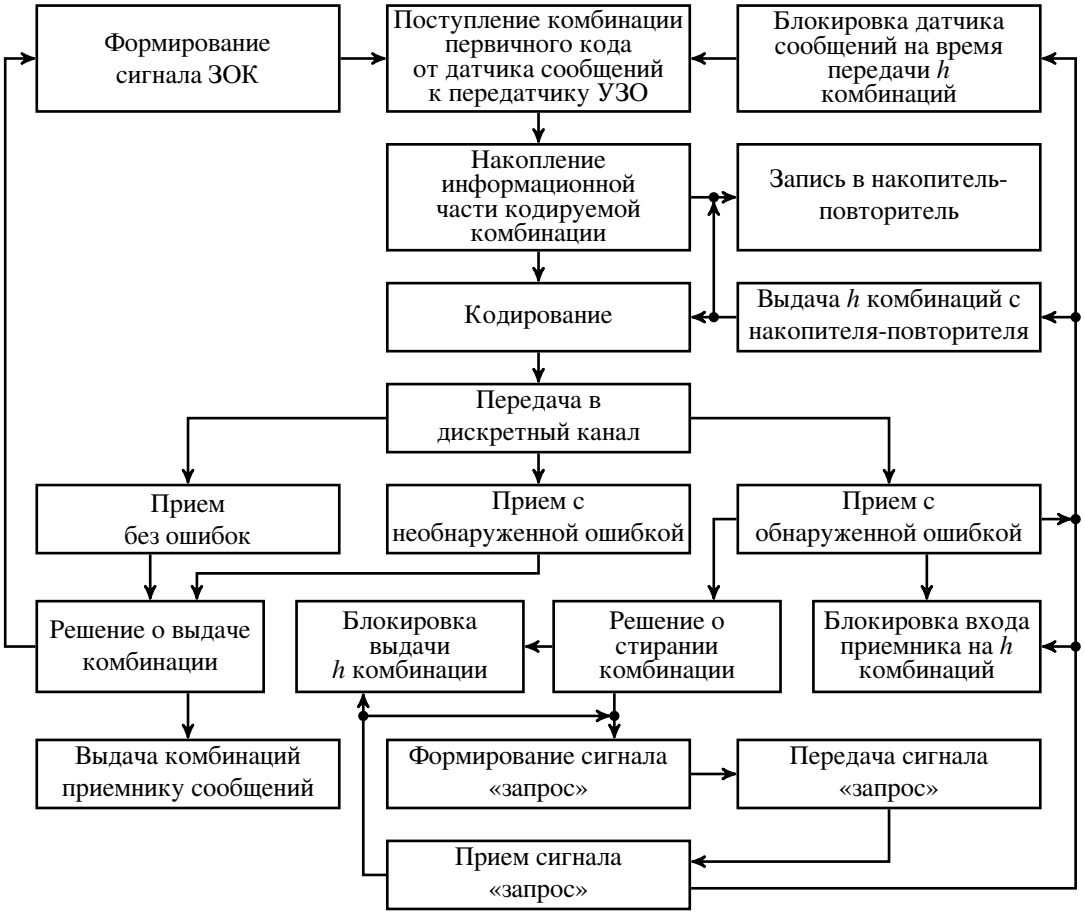


Рис. 3.2. Алгоритм функционирования системы РОС-ППбл

В этой системе выдача сообщений от источника в УЗО и от УЗО к источнику сообщений управляется от УЗО. В нормальном режиме работы УЗО формирует сигнал «запрос очередной комбинации» (ЗОК), разрешающей вывод l-элементной комбинации простого кода от датчика сообщений к УЗО. Эти комбинации накапливаются в накопителе информационных разрядов в

объеме k-элементного блока и вводятся в кодер, где формируется кодовая комбинация (n,k)-кода.

Для организации переспроса формируемой комбинации ее информационная часть, наряду с поступлением в кодер, поступает также в накопитель-повторитель, где будет храниться до тех пор, пока не будет принята приемником сообщений противоположной станции. Так как система синхронная, это время легко определяется. Одновременно в накопителе-повторителе находятся h ранее поступивших из накопителя информационных разрядов k-элементных блоков. Величину h называют емкостью накопителя-повторителя. Как правило в РОС-ППбл используются циклические коды БЧХ с большой избыточностью. В соответствии с требованиями руководящих документов рекомендуется использование циклических кодов с порождающим многочленом $g(x) = x^{16} + x^{12} + x^5 + 1$, обеспечивающим минимальное кодовое расстояние $d_{\min} = 4$.

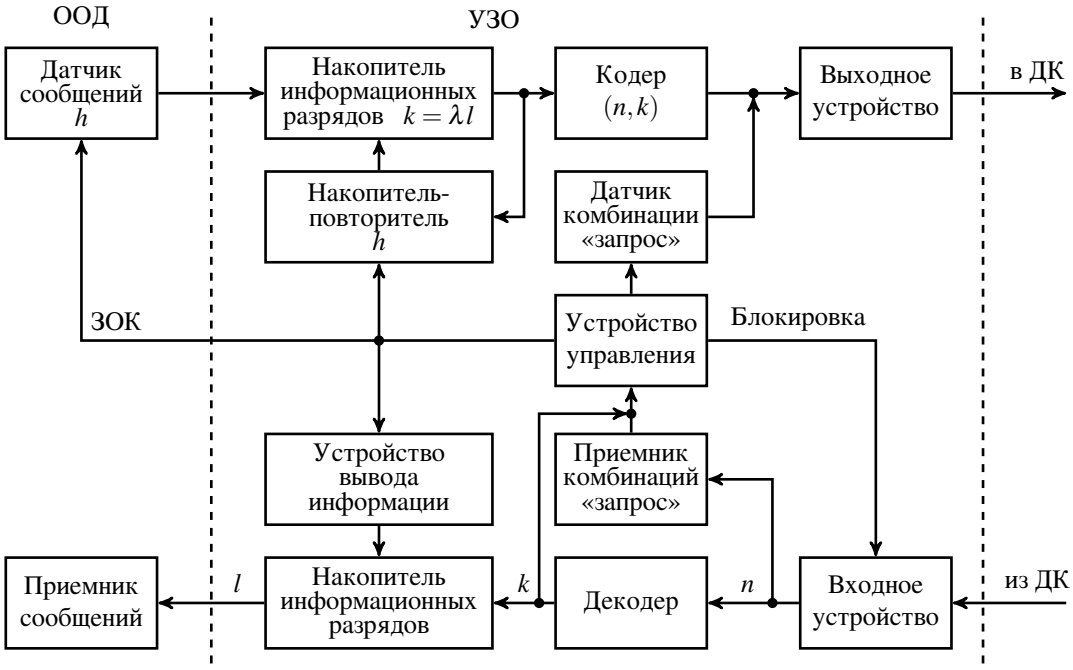


Рис. 3.3. Структурная схема системы РОС-ППбл

Сформированные кодовые комбинации непрерывно выдаются в дискретный канал и поступают к станции, с которой производится информационный обмен. Элементы принимаемой кодовой комбинации проходят процедуру регистрации во входном устройстве и поступают в декодер. Здесь осуществляется процедура обнаружения ошибок.

Одновременно принятая n-элементная комбинация поступает в приемник комбинации «запрос». На практике чаще всего применяют системы, у которых комбинация «запрос» является одной из разрешенных кодовых комбинаций. В том случае, когда принятая комбинация не содержит обнаруживаемых ошибок и не является комбинацией «запрос», принимается решение о

выдаче принятой комбинации приемнику сообщений, и УЗО сохраняет нормальный режим работы. Информационная часть принятой комбинации из накопителя информационных разрядов принудительно выводится в приемник сообщений.

По мере передачи кодовых комбинаций в нормальном режиме работы происходит обновление информации в накопителе-повторителе.

3.2.1. Режим переспроса

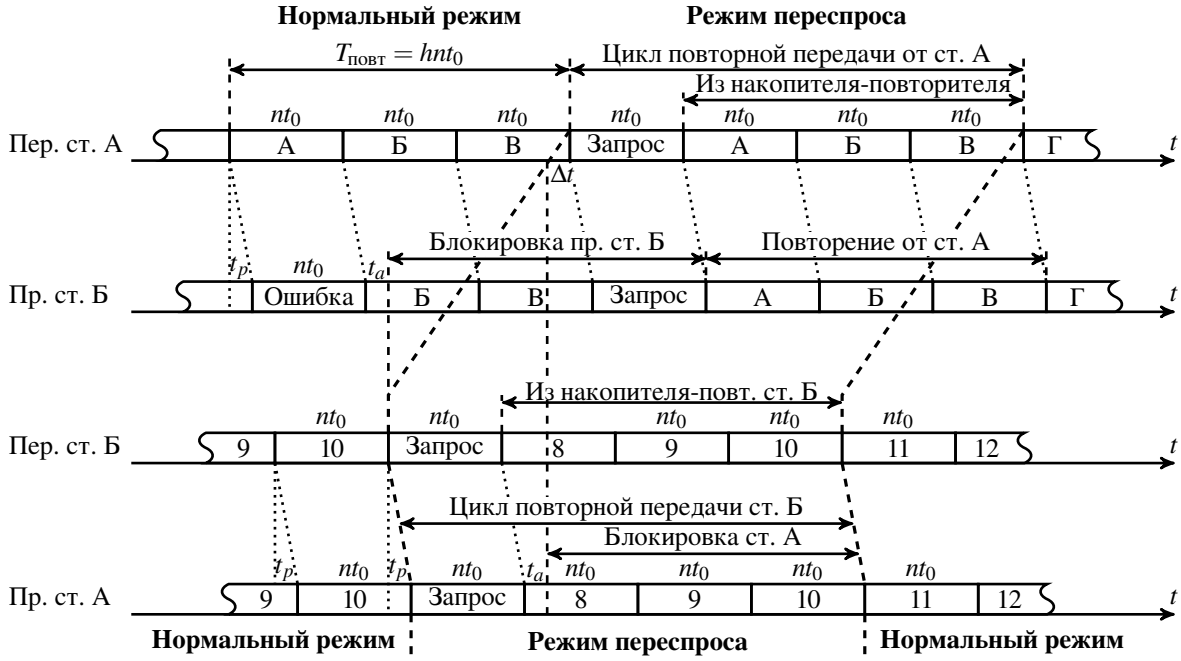
В рассматриваемой системе в целях упрощения логики работы устройства управления УЗО реакция системы управления на прием кодовой комбинации с ошибкой и прием комбинации «запрос» одинакова. Рассмотрим функционирование УЗО в режиме переспроса. Пусть в некоторый момент времени одна из взаимодействующих станций обнаруживает ошибку (станция Б на рис. 3.4). Информация об этом поступает с выхода декодера в УУ станции Б. В этом случае УУ станции Б выполняет следующие функции:

- прекращает выдачу комбинации «ЗОК» в датчик сообщений, и датчик сообщений прекращает ввод сообщений в накопитель информационных разрядов;
- подает сигнал в датчик комбинации «запрос», и комбинация «запрос» выводится в дискретный канал связи;
- подает сигнал на вывод информации из накопителя-повторителя; при этом h накопленных k-элементных блоков последовательно поступают в кодер и далее в дискретный канал; одновременно с подачей в кодер h k-элементных блоков вновь вводятся в накопитель повторитель;
- вырабатывает сигнал, запрещающий ввод информации во входное устройство приемника (блокировка входа приемника УЗО);
- прекращает подачу сигнала, разрешающего вывод информации из накопителя приема в сторону приемника сообщений (блокировка выхода приемника УЗО).

Таким образом, станция, обнаружившая ошибку, передает в дискретный канал комбинацию «запрос», а следом за нею h ранее переданных комбинаций и блокирует приемник УЗО. Блокировка с приемника УЗО станции, обнаружившей ошибку, будет снята к моменту поступления на ее вход повторно передаваемых комбинаций со станции, откуда пришла комбинация с ошибкой.

Вернемся к временной диаграмме рис. 3.4. Если в комбинации «запрос», переданной от станции Б к станции А при ее передаче по дискретному каналу ошибок не произошло, то информация о приеме комбинации «запрос» поступает в УУ станции А. УУ станции А при приеме комбинации «запрос»

выполняет в точности те же функции, что и УУ станции Б при обнаружении ошибок.



nt_0 — длительность передачи (приема) кодовой комбинации;
t_p — время распространения сигнала по каналу связи;
t_a — время анализа кодовой комбинации и комбинации «запрос»;
Δt — временной сдвиг в работе синхронных распределителей передатчика и приемника ст. А.

Рис. 3.4. Временная диаграмма работы системы РОС-ППбл

В результате приемник УЗО станции А блокируется по входу и выходу, а значит информация из накопителя-повторителя станции Б не поступает к приемнику сообщений станции А.

Передатчик УЗО станции А посылает в дискретный канал комбинацию «запрос», а следом за нею выводит в канал информацию из накопителя-повторителя.

Комбинация «запрос» от станции А попадает на заблокированный вход приемника и поэтому не воспринимается приемником УЗО станции Б.

Информация из накопителя-повторителя станции А поступает сразу же после снятия блокировки с приемника УЗО станции Б и анализируется, начиная с первой же комбинации, т. е. начиная с той комбинации, которая была ранее принята с ошибками.

Если при повторном приеме эта комбинация ошибок не имеет (или они не обнаруживаются), то эта комбинация передается в накопитель приема и далее приемнику сообщений. Таким образом осуществляется исправление ошибок в рассматриваемой схеме.

На станции Б прием повторяемой информации без ошибок восстанавливает нормальный режим работы.

Следом за комбинацией, в которой ранее были обнаружены ошибки, станция Б принимает комбинации из накопителя-повторителя станции А, ранее поступавшие в момент блокировки приемника УЗО станции Б.

Если в этих комбинациях станция Б ошибок не обнаруживает, то станция А сразу же за повторно передаваемыми комбинациями начинает передачу очередной информации из датчика сообщений.

В итоге в системе восстанавливается нормальный режим работы.

3.3. Расчет параметров системы РОС-ППбл

3.3.1. Относительная скорость передачи

Обозначим N — число кодовых комбинаций, переданных по каналу связи за некоторое время t; $N_{\text{пр}}$ — число комбинаций, поступивших на выход системы к приемнику сообщений за то же время; h — емкость накопителя-повторителя системы, равная числу повторно передаваемых по запросу комбинаций; ν — общее число переспросов за время передачи N комбинаций. Будем искать выражение для относительной скорости в виде

$$R = \frac{k}{n}\rho,$$

где $\frac{k}{n}$ — скорость передачи кода, а ρ — коэффициент, учитывающий снижение скорости передачи за счет переспросов.

При введенных обозначениях относительная скорость передачи в случае односторонней передачи подсчитывается как

$$R_1 = \frac{k}{n}\cdot\frac{N_{\text{пр}}}{N} = \frac{k}{n}\cdot\frac{N-(h+1)\cdot\nu}{N} = \frac{k}{n}\cdot\left(1-\frac{(h+1)\cdot\nu}{N}\right).$$

Выражение $(h+1)\cdot\nu$, равное общему числу повторяемых по запросам комбинаций (h из накопителя-повторителя и комбинация «запрос»), определяет отличие между N и $N_{\text{пр}}$. Выражение $\frac{(h+1)\cdot\nu}{N}$ можно трактовать как вероятность запроса — $P_{\text{запр}}$, т. е.

$$R_1 = \frac{k}{n}\cdot\left(1-P_{\text{запр}}\right) = \frac{k}{n}\cdot r,$$

где $r = 1-P_{\text{запр}}$ — снижение скорости передачи за счет переспросов. Здесь k и n — параметры используемого для передачи помехоустойчивого (n,k)-кода. Для случая двухсторонней передачи скорость будет уменьшаться на величину $(2-r)$, так как переспросы возможны в обоих направлениях, а r учитывает снижения скорости за счет переспросов в одном направлении. Окончательно получаем

$$R = \frac{k}{n}\cdot\frac{r}{2-r} = \frac{k}{n}\cdot\left(\frac{1-P_{\text{запр}}}{1+P_{\text{запр}}}\right).$$

Вероятность запроса приблизительно вычисляется по формуле:

$$P_{\text{запр}} \cong P[\geq 1,(h+1)n] = [(h+1)n]^{1-\alpha} \cdot p.$$

3.3.2. Расчет вероятности ошибок на выходе системы

N и $N_{\text{пр}}$ по-прежнему обозначают число кодовых комбинаций, переданных по каналу связи за некоторое время t, и число комбинаций, поступавших на выход системы (к приемнику сообщений) за то же время.

B — общее число кодовых комбинаций с необнаруженными ошибками среди N комбинаций; $B_{\text{пр}}$ — число комбинаций с необнаруженными ошибками среди $N_{\text{пр}}$ комбинаций; $B_{\text{бл}}$ — число комбинаций с необнаруженными ошибками, поступивших к приемнику УЗО в момент блокировки системы, $B_{\text{бл}} = B - B_{\text{пр}}$; h — емкость накопителя-повторителя системы, равная числу повторяемых при переспросе комбинаций; ν — число переспросов за время передачи N кодовых комбинаций.

$P_{\text{ош}}(C)$ — вероятность поступления комбинации с необнаруженной ошибкой с выхода системы в приемник сообщений; $P_{\text{ош}}(K)$ — вероятность необнаружения ошибок используемым помехоустойчивым кодом, т. е. вероятность необнаруживаемых ошибок в канале связи; $P_{\text{ош}}(\text{бл})$ — вероятность поступления комбинации с необнаруженными ошибками в момент блокировки приемника УЗО. При достаточно большом времени работы системы можно принять:

$$P_{\text{ош}}(C) = \frac{B_{\text{пр}}}{N_{\text{пр}}}; \qquad P_{\text{ош}}(K) = \frac{B}{N}; \qquad P_{\text{ош}}(\text{бл}) = \frac{B_{\text{бл}}}{\nu h}.$$

Установим связь между $P_{\text{ош}}(K)$ и $P_{\text{ош}}(C)$:

$$P_{\text{ош}}(C) = \frac{B_{\text{пр}}}{N_{\text{пр}}} = \frac{B - B_{\text{бл}}}{N_{\text{пр}}} = \frac{B}{N_{\text{пр}}} - \frac{B_{\text{бл}}}{N_{\text{пр}}} =$$

$$= \frac{B \cdot N}{N \cdot N_{\text{пр}}} - \frac{B_{\text{бл}}}{\nu h} \cdot \frac{\nu h}{N_{\text{пр}}} = P_{\text{ош}}(K) \cdot \frac{N}{N_{\text{пр}}} - P_{\text{ош}}(\text{бл}) \cdot \frac{\nu h}{N_{\text{пр}}}.$$

Заменяя величину νh на $N - N_{\text{пр}}$ и учитывая что $\frac{N_{\text{пр}}}{N} = \rho^{-1}$, где ρ — коэффициент снижения скорости за счет переспросов, получим:

$$P_{\text{ош}}(C) = P_{\text{ош}}(K) \cdot \rho^{-1} - P_{\text{ош}}(\text{бл})(\rho^{-1} - 1) =$$

$$= P_{\text{ош}}(K) \left[\rho^{-1} - \frac{P_{\text{ош}}(\text{бл})}{P_{\text{ош}}(K)} (\rho^{-1} - 1) \right] = \varepsilon P_{\text{ош}}(K),$$

где величина ε отражает отличие $P_{\text{ош}}(K)$ от $P_{\text{ош}}(C)$.

Приняв $\frac{P_{\text{ош}(\text{бл})}}{P_{\text{ош}}(K)} = \xi$ и проведя преобразования, получим

$$\varepsilon = \rho^{-1}\left[1 - \xi(1-\rho)\right].$$

Условие, при котором блокировки приводят к уменьшению числа необнаруживаемых ошибок на выходе системы, сводится к следующему:

$$\begin{cases} \rho^{-1}\left[1 - \xi(1-\rho)\right] < 1 & \text{или} \\ 1 - \xi(1-\rho) < \rho, & \text{или} \\ 1 - \rho < \xi(1-\rho), & \text{или} \\ \xi > 1. \end{cases}$$

Таким образом, система РОС-ППбл может обеспечивать дополнительное повышение достоверности за счет блокировки только в том случае, когда моменты блокировки совпадают с моментами появления комбинации с необнаруженными ошибками более частыми, чем в среднем по последовательности ошибок.

По экспериментальным данным для реальных каналов при $h = 5$ величина ε в большинстве случаев равна $0{,}1 \ldots 0{,}5$. Окончательно имеем:

$$P_{\text{ош}}(C) = \varepsilon P_{\text{ош}}(K) = \frac{\varepsilon}{2^{n-k}} P(\geq d, n) = \frac{\varepsilon}{2^{n-k}} \left(\frac{n}{d}\right)^{1-\alpha},$$

где n и k — параметры используемого для передачи помехоустойчивого (n,k)-кода, а d — его минимальное кодовое расстояние.

3.3.3. Расчет времени доведения сообщений

Под временем доведения сообщения будем понимать время от начала вывода сообщения из передатчика УЗО в дискретный канал до времени начала вывода сообщения из приемника УЗО в приемник сообщения. Так как l-элементные сообщения источника передаются по каналу в составе кодовых комбинаций (n,k)-кода, время доведения сообщений совпадает с временем, прошедшим от момента начала ввода кодовой комбинации в дискретный канал с выхода кодера передающей станции до момента окончания анализа об отсутствии ошибок в принятой комбинации декодером принимающей станции. В соответствии с логикой работы УЗО РОС-ППбл все принимаемые кодовые комбинации можно разделить на две группы:

1) комбинации, принятые в нормальном режиме работы;
2) комбинации, принятые в режиме переспроса.

Вероятность этих режимов соответственно равна $1 - P_{\text{запр}}$ и $P_{\text{запр}}$. Для комбинаций первой группы $t_{\text{дов1}} = nt_0 + t_p + t_a$, а для комбинации второй группы $t_{\text{дов2}} = (h+2)nt_0 + t_p + t_a$.

Результирующее выражение для $t_{\text{дов}}$ равно:

$$t_{\text{дов}} = \left[t_{\text{дов1}}(1 - P_{\text{запр}}) + t_{\text{дов2}} P_{\text{запр}}\right] \rho^{-1},$$

где ρ^{-1} — среднее число повторений кодовых комбинаций.

3.3.4. Расчет емкости накопителя-повторителя

Для расчета емкости накопителя-повторителя по временной диаграмме рис. 3.4 определим значения времени повторения: $T_{\text{повт}} = hnt_0$.

$T_{\text{повт}}$ — это то время, в течение которого в канале связи передается повторяемая по запросу информация из накопителя-повторителя. Из рис. 3.4 видно, что это время включает два цикла $t_p + nt_0 + t_a$.

1. Первый цикл — прием комбинаций с обнаруженной ошибкой (ось «прием станции Б»).

2. Второй цикл — прием комбинации «запрос» (ось «прием станции А»), а также интервал (ось «передачи станции А»).

Таким образом:

$$T_{\text{повт}} = hnt_0 = 2 \cdot (t_p + nt_0 + t_a) + \Delta T.$$

В синхронной системе временной интервал ΔT может иметь следующее значение:

$$0 \le \Delta T \le nt_0.$$

Примем $\Delta T = nt_0$, значит, $hnt_0 \ge 3nt_0 + 2(t_p + t_a)$, откуда находим

$$h \ge 3 + 2\frac{(t_p + t_a)}{nt_0}.$$

3.4. Рекомендации по выбору оптимального кода

3.4.1. Расчет оптимальных характеристик помехоустойчивого кода

При выборе помехоустойчивого кода используется критерий максимума скорости передачи. По этому критерию оптимальным считается такой код, применение которого в системе с решающей обратной связью обеспечивает заданные требования по достоверности и максимальное значение скорости передачи системы. Код будет оптимальным, если

$$P_{\text{ош}}(l) \le P_{\text{доп}}(l) \quad \text{и} \quad R = R_{\max},$$

где $P_{\text{доп}}(l)$ — допустимое значение вероятности ошибочного приема l-элементной комбинации первичного кода; $P_{\text{ош}}(l)$ — значение вероятности ошибочного приема l-элементной комбинации первичного кода, получаемое при использовании в системе РОС-ППбл помехоустойчивого кода.

Ранее была получена формула для оценки вероятности $P_{\text{ош}}(C)$ ошибочного приема используемых в РОС-ППбл комбинаций помехоустойчивого (n,k)-кода.

Получим формулу для расчета $P_{\text{ош}}(l)$.

В приемник сообщения поступают те ошибки, которые не обнаружены декодером, т. е. только те образцы ошибок, вид которых совпал с видом разрешенных комбинаций. Эти образцы ошибок в составе n-элементных комбинаций имели вес от d и более. Естественно, что в составе блоков, выдаваемых в приемник сообщений, будут исключены ошибки, приходящиеся на избыточные разряды. Будем также считать, что числом и вероятностью ошибок кратности до $d-1$ в информационных блоках, оставшихся после удаления избыточных разрядов, можно пренебречь по сравнению с числом и вероятностью ошибок кратности d и более. Это предположение оправдано тем, что d для большинства кодов, используемых в режиме обнаружения ошибок, невелико по сравнению с k и n. Кроме того, вероятность появления таких ошибок определяется вероятностью появления d и более ошибок в кодовой комбинации, передаваемой по каналу связи.

Охарактеризуем поток ошибок, пропущенных в приемник сообщений средней вероятностью ошибки на бит, равной $P_{\text{ПР}}$ и показателем группирования ошибок $\alpha_{\text{пр}}$.

Понятно, что $P_{\text{ПР}}$ существенно меньше вероятности ошибки на бит в канале связи, а показатель группирования $\alpha_{\text{пр}}$ имеет своей нижней границей показатель группирования ошибок в канале связи α, т. е. $P_{\text{ПР}} < P$ и $\alpha \le \alpha_{\text{пр}}$. Теперь можно записать равенство

$$\left(\frac{k}{d}\right)^{1-\alpha_{\text{пр}}} P_{\text{ПР}} = \frac{\varepsilon}{2^{n-k}} \left(\frac{n}{d}\right)^{1-\alpha} P.$$

Для упрощения расчетов примем $\alpha_{\text{пр}} = \alpha$, тогда

$$P_{\text{ПР}} = \frac{\varepsilon}{2^{n-k}} \left(\frac{n}{k}\right)^{1-\alpha} P.$$

Для используемых в РОС-ППбл кодов справедливо $\frac{k}{n} \to 1$ с ростом n (будет показано далее). Поэтому принимаем $P_{\text{ПР}} \cong \frac{\varepsilon}{2^{n-k}} P$. Следовательно, вероятность ошибки в l-элементном знаке первичного кода, поступающего с выхода декодера в приемник сообщений, определяется как

$$P_{\text{ош}}(l) = P(\ge 1, l) = l^{1-\alpha} P_{\text{ПР}} = \frac{\varepsilon l^{1-\alpha}}{2^{n-k}} P.$$

Теперь можно сформулировать алгоритм выбора помехоустойчивого (n,k)-кода, оптимального в смысле критерия максимума скорости передачи.

1. Выбирается класс помехоустойчивых кодов. В настоящее время в двоичных системах передачи для систем РОС чаще всего используют циклические (n,k)-коды БЧХ.

2. Для кодов БЧХ естественной длины для различных значений n и k рассчитывается вероятность необнаружения ошибок в соответствии с заданными значениями p и α. Результаты расчетов сводятся в табл. 3.1 в колонку $P_{\text{ош}}$. Данные о $g(x)$ в табл. 3.1 заимствованы из [51] и будут использованы при выборе порождающего многочлена для найденного оптимального кода.

Таблица 3.1

Таблица результатов расчета вероятности необнаружения ошибок

n	k	$\frac{k}{n}$	$n-k$	d	$P_{\text{ош}} = \frac{\varepsilon}{2^{n-k}}\left(\frac{n}{d}\right)^{1-\alpha} P$	$g(x)$		
						сомнож. $f_i(x)$	степени $f_i(x)$	корни (j)
15	11	0,73	4	3		$(23)_8$	4	1
	7	0,47	8	5		$(37)_8$	4	3
	6	0,4	9	6		$(03)_8$	1	0
31	26	0,84	5	3		$(45)_8$	5	1
	21	0,86	10	5		$(75)_8$	5	3
	16	0,52	15	7		$(67)_8$	5	5
	11	0,35	20	9		$(57)_8$	5	7
63	57	0,9	6	3		$(103)_8$	6	1
	51	0,81	12	5		$(127)_8$	6	3
	45	0,71	18	7		$(147)_8$	6	5
	39	0,62	24	9		$(111)_8$	6	7
127	120	0,94	7	3		$(211)_8$	7	1
	113	0,89	14	5		$(217)_8$	7	3
	106	0,83	21	7		$(235)_8$	7	5
	99	0,78	28	9		$(367)_8$	7	7
255	247	0,97	8	3		$(435)_8$	8	1
	239	0,94	16	5		$(567)_8$	8	3
	231	0,91	24	7		$(763)_8$	8	5
	223	0,87	32	9		$(551)_8$	8	7
511	502	0,98	9	3		$(1021)_8$	9	1
	493	0,96	18	5		$(1131)_8$	9	3
	484	0,95	27	7		$(1461)_8$	9	5
	475	0,93	36	9		$(1231)_8$	9	7
1023	1013	0,99	10	3		$(2011)_8$	10	1
	1003	0,98	20	5		$(2017)_8$	10	3
	993	0,97	30	7		$(2415)_8$	10	5
	983	0,96	40	9		$(3771)_8$	10	7

3. По данным табл. 3.1 по вычисленному значению $P_{\text{ош}}$ строятся графики семейства $P_{\text{ош}}(C) = f\left(\frac{k}{n}\right)$ для различных n. Пример графика представлен на рис. 3.5.

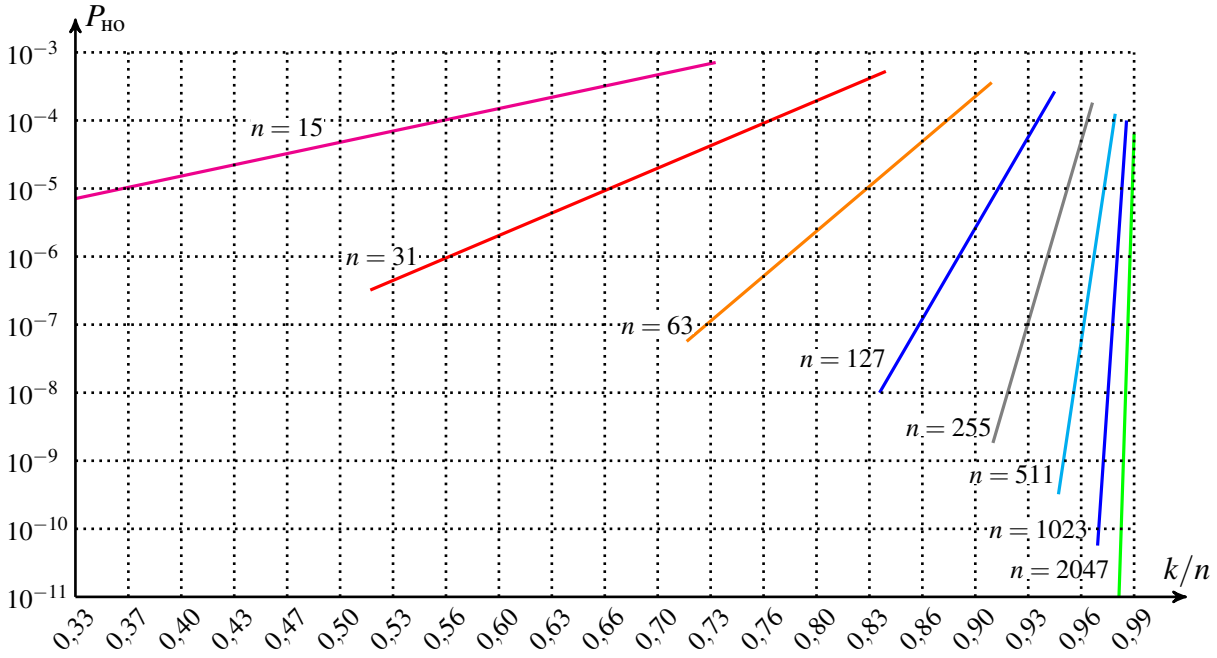


Рис. 3.5. Пример графиков семейства $P_{ош}(C) = f\left(\frac{k}{n}\right)$

4. На графике семейства $P_{\text{ош}}(C) = f\left(\frac{k}{n}\right)$ для каждого значения n находится такое значение $\frac{k}{n}$, которое удовлетворяет требованию по допустимой вероятности ошибки на выходе системы. Найденное значение $\frac{k}{n}$ заносится в табл. 3.2.

5. Для выбранных значений n и определенных в п. 4 значений $\frac{k}{n}$ в соответствии с заданными значениями p, α и рассчитанным h находятся значения r и R. Результаты сводятся в табл. 3.2.

Таблица 3.2

Таблица параметров для выбора кода

n	$\frac{k}{n}$	h	$r = 1 - [n(h+1)]^{1-\alpha} p$	$R_c = \frac{k}{n} r$	$R_{\text{д}} = \frac{k}{n} \frac{r}{2-r}$
15					
31					
63					
127					
255					
511					
1023					

6. По данным табл. 3.2 строятся графики $\frac{k}{n} = f(n)$, $r = f(n)$, $R_д = f(n)$. Пример графиков представлен на рис. 3.6.

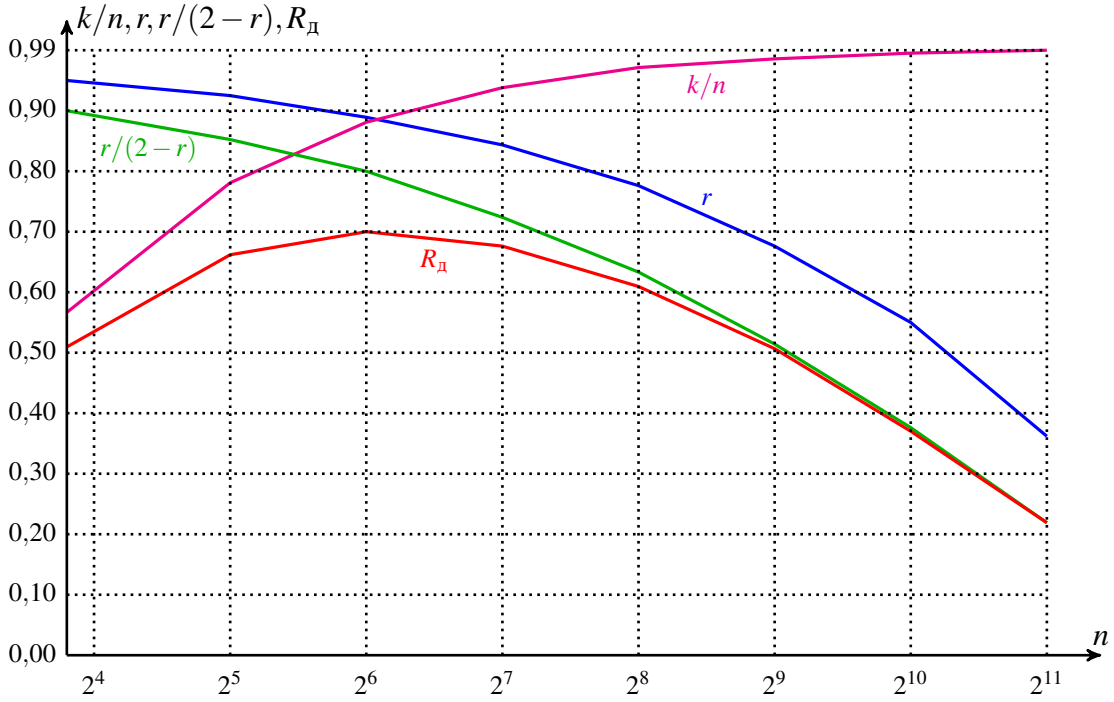


Рис. 3.6. Пример графиков $\frac{k}{n} = f(n)$, $r = f(n)$, $R_д = f(n)$

7. По графику $R_д = f(n)$ определяется максимальное значение относительной скорости $R_{\max}$ и соответствующие ему значения $n_{опт}$ и $\frac{k}{n}$. Умножением найденных значений $n_{опт}$ и $\frac{k}{n}$ находится значение k, соответствующее $R_{\max}$, а затем и $(n-k)_{опт}$.

Для найденных значений $n_{опт}$, $k_{опт}$, $(n-k)_{опт}$ находятся ближайшие числа n, k и $(n-k)$, кратные длине комбинации заданного первичного кода, но так, чтобы избыточность $(n-k)$ не уменьшалась по отношению к $(n-k)_{опт}$. Эта задача легко выполнима, так как максимум функции $R_д = f(n)$ достаточно «размытый». При этом допускается потеря скорости в пределах точности построения графика (1–2 %). На этом задача нахождения оптимального кода для РОС-ППбл считается выполненной. Эффективная скорость передачи определяется по формуле

$$R_{эфф} = R_{\max} \cdot N_e,$$

где N_e — заданная скорость передачи единичных элементов.

3.4.2. Проверка условия $P_{ош}(l) \le P_{доп}(l)$

Поиск оптимального кода основывался на выборе оптимальных параметров n и k кодов, удовлетворяющих заданным требованиям по достоверности. В ряде случаев может оказаться, что в пересчете достоверности с

n-элементного блока на l-элементный введенная избыточность $(n-k)$ будет значительно завышена. Поэтому, чтобы убедиться, что введенной избыточности достаточно для реализации требований по достоверности, предъявляемых к l-элементной комбинации первичного кода, дополнительно проводится проверка, основанная на проверке выполнения исходного неравенства $P_{\text{ош}}(l) \leq P_{\text{доп}}(l)$. Перепишем это выражение с учетом значения $P_{\text{ош}}(l) : \frac{\varepsilon \cdot l^{1-\alpha}}{2^{n-k}} p \leq P_{\text{доп}}(l)$. Логарифмируя это выражение, получаем $(n-k) \geq (1-\alpha)\log_2 l + \log_2 p + \log_2 \varepsilon - \log_2 P_{\text{доп}}(l)$.

Если выбранное в п. 7 значение $(n-k)$ удовлетворяет этому соотношению, то считают выбор (n,k)-кода обоснованным.

В ряде случаев можно уменьшить избыточность, выбранную в п. 7. Действительно, если найдется значение $(n-k)$ меньше выбранного в п. 7, но кратное l и удовлетворяющее проверке, то следует именно его принять за оптимальное $(n-k)$ и, сохраняя $n_{\text{опт}}$, кратное l, найти новое значение k. Эта процедура несколько повысит $R_{\max}$ при выполнении требований по достоверности и, следовательно, она корректна в рамках используемого критерия.

3.4.3. Выбор порождающего многочлена g(x)

Выбор порождающего многочлена для найденного оптимального кода основывается на вычисленных значениях $n_{\text{опт}}$ и $(n-k)_{\text{опт}}$. Для выбора $g(x)$ используется табл. 3.1. В этой таблице для представленных кодов БЧХ приведены порождающие многочлены $g(x)$ в виде произведения неприводимых многочленов $f_i(x)$, степень каждого $f_i(x)$ и минимальная степень последовательности корней каждого из сомножителей $(-\alpha^j)$. Индекс i неприводимого многочлена $f_i(x)$ возрастает с увеличением минимальной степени в последовательности корней. Например, $f_1(x)$ — неприводимый многочлен, последовательность корней которого содержит степень 1; $f_2(x)$ — соответствует многочлену с последовательностью корней, содержащей минимальную степень, не вошедшую в последовательность для $f_1(x)$ и т. д. Из приведенных в табл. 3.1 сомножителей порождающие многочлены циклических кодов можно получить следующим образом: $g_1(x) = f_1(x)$, $g_i(x) = g_{i-1}(x) f_i(x)$.

При этом степень $g(x)$ должна соответствовать параметру $(n-k)$ соответствующего кода. Такой метод составления порождающих многочленов позволяет построить циклические коды, у которых минимальное кодовое расстояние увеличивается по меньшей мере на 2 при увеличении числа сомножителей порождающего многочлена на 1.

В целях сокращения записи все многочлены указаны в восьмеричном представлении. Каждой восьмеричной цифре соответствует двоичная триада, как показано в табл. 3.3.

Таблица 3.3

Соответствие восьмеричных цифр и двоичных триад

Oct	0	1	2	3	4	5	6	7
Bin	000	001	010	011	100	101	110	111

Коэффициенты многочленов в двоичной записи располагаются в порядке убывания, т. е. коэффициенты при слагаемом высшего порядка расположены слева. Например, число $(2415)_8$ обозначает многочлен в двоичной записи: 010100001101. Учитывая, что старшая степень находится слева, имеем

$$f(x) = x^{10} + x^8 + x^3 + x^2 + 1.$$

Знание степени неприводимого многочлена и минимальной степени последовательности его корней позволяет найти всю последовательность корней для каждого многочлена $g(x)$ в таблице. Для этого используется известное правило: «Если α^i — корень $f(x)$, то и α^{2i} также его корень».

Надо помнить, что степени приводятся по mod n, где n — длина кодовой комбинации. Для приведенного многочлена $\alpha^i = 5$ и вся последовательность его корней имеет вид:

$$\alpha^5, \alpha^{10}, \alpha^{20}, \alpha^{40}, \alpha^{80}, \alpha^{160}, \alpha^{320}, \alpha^{640}, \alpha^{257}, \alpha^{514}.$$

Если найденный оптимальный код отсутствует в табл. 3.1 в явном виде, то следует его искать среди укороченных кодов $(n-i, k-i)$. При этом надо ориентироваться на число $(n-k)$, а i определить из выражения $i = n_т - n_{опт}$. Для этого выбираются табличные коды длины $n_т$, для которых $i > 0$.

Например, по результатам расчетов найден оптимальный код с параметрами $n_{опт} = 80$, $k_{опт} = 69$ т. е. $(n-k)_{опт} = 11$. По исходным данным $l = 5$.

Для окончательного решения по параметрам кода необходимо, чтобы n и k были кратны 5, т. е. $(n-k)$ может быть либо 10, либо 15. Следует проверить по условию $P_{ош}(l) \le P_{доп}(l)$ возможность использования $(n-k) = 10$. Если это возможно, то решением будет код $(80, 70)$. Если же проверка покажет, что $(n-k)$ должен быть больше 10, то следует выбрать код $(80, 65)$.

В первом случае $g(x)$ должен иметь степень 10, во втором — 15. В любом случае следует выбирать такой порождающий многочлен, который обеспечивает $d > 3$. Приемлемым решением является $d = 4$, но если при том же $(n-k)$ можно найти значение $g(x)$, обеспечивающее большее d, то надо выбирать $g(x)$ с большим d.

Для нашего примера с $n = 80$ следует рассматривать коды с длиной n от 127 и выше, ориентируясь на $(n-k)$. Для $(n-k) = 10$ решение можно найти, если выбрать $f_1(x)$ девятой степени, домножив его на $(x+1)$. В этом случае $f(x) = (1021)_8$, т. е. $f_1(x) = x^9 + x^4 + 1$, а $g(x) = (x+1)(x^9 + x^4 + 1)$.

Последовательность степеней корней выбранного $g(x)$ включает: α^0, α^1, α^2, α^4, α^8, α^{16}, α^{32}, α^{64}, α^{128}, α^{256}. В этой последовательности три степени $\alpha^0, \alpha^1, \alpha^2$ идут подряд, что позволяет сделать вывод, что $d_{\min}$такого кода равно 4. Итак, код $(80,70)$ является укорочением кода $(511,501)$.

Порождающий многочлен кода $(80,65)$ можно представить как произведение многочленов седьмой степени $(211)_8$ и $(217)_8$ и многочлена $x+1$.

Итак, для кода $(80,65)$:

$$g(x) = (x+1)(x^7+x^3+1)(x^7+x^3+x^2+x+1).$$

Его последовательность корней: α^0, α^1, α^2, α^4, α^8, α^{16}, α^{32}, α^{64}, a^3, a^6, a^{12}, a^{24}, a^{48}, a^{96}, a^{65}.

Здесь подряд идут степени α^0, α^1, α^2, α^3, α^4 т. е. $d_{\min} = 6$. Код $(80,65)$ является укорочением кода $(127,112)$.

Контрольные вопросы

1. Какие бывают виды систем обратной связи?
2. Как работает система РОС-ППбл?
3. Каким образом расчитывается вероятность ошибок на выходе системы РОС-ППбл?
4. Как выбирается оптимальный код для системы РОС-ППбл?
5. Объясните наличие максимума в функции $R = f(n)$.
6. По какому критерию осуществляется поиск оптимального кода для системы РОС-ППБл?
7. От каких факторов зависит относительная скорость передачи системы РОС-ППБл?
8. Объясните причину повышения достоверности за счет блокировки входа приемника. При каких условиях этот фактор имеет место?
9. От каких факторов зависит выбор емкости накопителя-повторителя для системы РОС-ППБл?
10. Сформулируйте требования к выбору порождающего многочлена для помехоустойчивого кода в системе РОС-ППБл.

Рекомендуемая литература

1. Питерсон, У. Коды, исправляющие ошибки / У. Питерсон, Э. Уэлдон. — М. : Мир, 1976.

2. Шварцман, В. О. Теория передачи дискретной информации : учебник для вузов связи / В. О. Шварцман, Г. А. Емельянов. — М. : Связь, 1979.

СПИСОК ЛИТЕРАТУРЫ

[1] Берлекемр, Э. Алгебраическая теория кодирования / Э. Берлекемр. — М. : Мир, 1972.

[2] Мак-Вильямс, Ф. Дж. Теория кодов, исправляющих ошибки / Ф. Дж. Мак-Вильямс, Н. Дж. А. Слоэн. — М. : Связь, 1979.

[3] Lin, S. Error Control Coding: Fundamentals and Applications / S. Lin, D. J. Costello. — New Jersey : Printice-Hall, 1983.

[4] Блейхут, Р. Теория и практика кодов, контролирующих ошибки / Р. Блейхут. — М. : Мир, 1986.

[5] Кларк, Д. К. Кодирование и исправление ошибок в системах цифровой связи / Д. К. Кларк, Д. Б. Кейн. — М. : «Радио и Связь», 1987.

[6] Морелос-Сарагоса, Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. / Р. Морелос-Сарагоса. — М. : Техносфера, 2005.

[7] Когновицкий, О. С. Двойственный базис и его применение в телекоммуникациях / О. С. Когновицкий. — СПб. : Линк, 2009.

[8] Власов, Е. Г. Конечные поля в телекоммуникационных приложениях. Теория и применение FEC, CRC и М-последовательностей : практическое пособие / Е. Г. Власов. — М. : Инфра-М, 2016.

[9] Когновицкий, О. С. Основы циклических кодов : учебное пособие / О. С. Когновицкий. — Л. : ЛЭИС, 1990.

[10] Владимиров, С. С. Математические основы теории помехоустойчивого кодирования : учебное пособие / С. С. Владимиров. — СПб. : СПбГУТ, 2016.

[11] Теория электрической связи : учебное пособие / К. К. Васильев, В. А. Глушков, А. В. Дормидонтов, А. Г. Нестеренко ; под ред. К. К. Васильева. — Ульяновск : УлГТУ, 2008.

[12] Золотарёв, В. В. Помехоустойчивое кодирование. Методы и алгоритмы: Справочник / В. В. Золотарёв, Г. В. Овечкин ; под ред. чл.-корр. РАН Ю. Б. Зубарева. — М. : Горячая линия–Телеком, 2004.

[13] Скляр, Б. Цифровая связь. Теоретические основы и практическое применение / Б. Скляр ; под ред. А. В. Назаренко. — М. : Издательский дом «Вильямс», 2003.

[14] Финк, Л. М. Теория передачи дискретных сообщений / Л. М. Финк. — М. : «Сов. радио», 1970.

[15] Гладких, А. А. Основы теории мягкого декодирования избыточных кодов в стирающем канале связи / А. А. Гладких. — Ульяновск : УлГТУ, 2010.

[16] Теория и техника передачи данных и телеграфия : учебник / Л. П. Пуртов, А. С. Замрий, А. И. Захаров, Н. И. Иванов, В. М. Охорзин. — СПб. : ВАС, 1973.

[17] Similarity of Discrete Gilbert-Elliot and Polya Channel Models to Continuous Rayleigh Fading Channel Model : Rep. / National Chiao Tung University ; Executor: Pen-Ting Sun. — Taiwan 30050, R.O.C. : 2002. — June.

[18] Jeruchim, M. C. Simulation of Communication Systems: Modeling, Methodology and Techniques / M. C. Jeruchim, P. Balaban, K. S. Shanmugan. Information Technology: Transmission, Processing and Storage. — New York : Springer US, 2006.

[19] Шеннон, К. Математическая теория связи / К. Шеннон // Работы по теории информации и кибернетике. — М. : Изд-во иностранной литературы, 1963.

[20] Прокис, Дж. Цифровая связь / Дж. Прокис ; под ред. Д. Д. Кловского. — М. : «Радио и Связь», 2000.

[21] MacKay, D. J. C. Information Theory, Inference, and Learning Algorithms / D. J. C. MacKay. — Cambridge : Cambridge University Press, 2003.

[22] Зайдлер, Е. Системы передачи дискретной информации / Е. Зайдлер ; под ред. Б. Р. Левина. — М. : «Связь», 1977.

[23] Вернер, М. Основы кодирования : учебник для ВУЗов / М. Вернер. — М. : Техносфера, 2006.

[24] Котов, П. А. Повышение достоверности передачи цифровой информации / П. А. Котов. — М. : Связь, 1966.

[25] Richardson, T. Modern Coding Theory / T. Richardson, R. Urbanke. — Cambridge : Cambridge University Press, 2008.

[26] Hasslinger, G. The Gilbert-Elliott Model for Packet Loss in Real Time Services on the Internet / G. Hasslinger, O. Hohlfeld // 14th GI/ITG Conference - Measurement, Modelling and Evalutation of Computer and Communication Systems. — Dortmund : VDE, 2008. — P. 1–15.

[27] Elliott, E. O. Estimates of error rates for codes on burst-noise channels / E. O. Elliott // Bell System Technical Journal. — 1963. — Vol. 42. — P. 1977–1997.

[28] Gilbert, E. N. Capacity of a burst-noise channel / E. N. Gilbert // Bell System Technical Journal. — 1960. — September. — Vol. 39. — P. 1253–1265.

[29] Rezaeian, M. Computation of capacity for Gilbert-Elliott channels, using a statistical method / M. Rezaeian // Communications Theory Workshop, 2005. Proceedings. 6th Australian. — Brisbane : IEEE, 2005. — P. 56–61.

[30] Охорзин, В. М. Выбор эффективных групповых корректирующих кодов для некоторых систем передачи двоичной информации / В. М. Охорзин // Труды Второй всесоюзной конференции по теории кодирования и ее приложениям. Секция 3, часть 2. — М. : Научный Совет по комплексной проблеме «Кибернетика» АН СССР, 1965.

[31] Гнеденко, Б. В. Курс теории вероятности / Б. В. Гнеденко. — М. : Физматгиз, 1961.

[32] Охорзин, В. М. Статистические характеристики систем передачи дискретных сообщений : учебное пособие / В. М. Охорзин, С. Л. Ерош. — СПб. : ВАС, 1974.

[33] Верещагин, Н. К. Информация, кодирование и предсказание / Н. К. Верещагин, Е. В. Щепин. — М. : ФМОП, МЦМНО, 2012.

[34] Sorger, U. Communication Theory / U. Sorger. — Norderstedt : BoD, 2009.

[35] Bitouze, N. Coding for a non-symmetric ternary channel / N. Bitouze, A. Graell i Amat // 2009 Information Theory and Applications Workshop / IEEE. — San Diego, CA, USA : IEEE, 2009. — Feb. — P. 113–118.

[36] Удалов, А. П. Избыточное кодирование при передаче информации двоичными кодами / А. П. Удалов, Б. А. Супрун. — М. : «Связь», 1964.

[37] Галлагер, Р. Теория информации и надежная связь / Р. Галлагер ; под ред. М. С. Пинскера, Б. С. Цыбакова. — М. : «Сов. радио», 1974.

[38] Тули, М. Справочное пособие по цифровой электронике / М. Тули. — М. : «Энергоатомиздат», 1990.

[39] Хэмминг, Р. В. Теория кодирования и теория информации / Р. В. Хэмминг. — М. : Радио и связь, 1983.

[40] Synchronous frame structures used at 1544, 6312, 2048, 8448 and 44 736 kbit/s hierarchical levels. — ITU-T Recommendation. — 1998. — October.

[41] Frame alignment and cyclic redundancy check (CRC) procedures relating to basic frame structures defined in Recommendation G.704. — ITU-T Recommendation. — 1991. — April.

[42] Braden, R. Computing the Internet Checksum. — Internet Requests for Comments. — 1988. — September. — URL: https://tools.ietf.org/html/rfc1071.

[43] Mallory, T. Incremental Updating of the Internet Checksum. — Internet Requests for Comments. — 1990. — January. — URL: https://tools.ietf.org/html/rfc1141.

[44] Rijsinghani, A. Computation of the Internet Checksum via Incremental Update. — Internet Requests for Comments. — 1994. — May. — URL: https://tools.ietf.org/html/rfc1624.

[45] Stone, J. When the CRC and TCP Checksum Disagree / J. Stone, C. Partridge // Proceedings of the Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication. — SIGCOMM '00. — New York, NY, USA : ACM, 2000. — P. 309–319. — URL: http://doi.acm.org/10.1145/347059.347561.

[46] Postel, J. Internet Protocol. — Internet Requests for Comments. — 1981. — September. — URL: http://www.rfc-editor.org/rfc/rfc791.txt.

[47] Postel, J. Internet Control Message Protocol. — Internet Requests for Comments. — 1981. — September. — URL: http://www.rfc-editor.org/rfc/rfc792.txt.

[48] Postel, J. User Datagram Protocol. — Internet Requests for Comments. — 1980. — August. — URL: http://tools.ietf.org/html/rfc768.

[49] Postel, J. Transmission Control Protocol. — Internet Requests for Comments. — 1981. — September. — URL: http://tools.ietf.org/html/rfc793.

[50] Шварцман, В. О. Теория передачи дискретной информации : учебник для вузов связи / В. О. Шварцман, Г. А. Емельянов. — М. : Связь, 1979.

[51] Питерсон, У. Коды, исправляющие ошибки / У. Питерсон, Э. Уэлдон. — М. : Мир, 1976.

Когновицкий Олег Станиславович
Охорзин Виктор Михайлович
Владимиров Сергей Сергеевич

ПРАКТИКА ПОМЕХОУСТОЙЧИВОГО КОДИРОВАНИЯ

ЧАСТЬ 1

СИСТЕМЫ С ОБНАРУЖЕНИЕМ ОШИБОК И ОБРАТНОЙ СВЯЗЬЮ

Учебное пособие

Редактор *Л. К. Паршина*

Компьютерная верстка *С. С. Владимирова*

План изданий 2018, п. 53

Подписано к печати 28.06.2018
Объем 6,25 усл.-печ. л. Тираж 30 экз. Заказ 868

Редакционно-издательский отдел СПбГУТ
193232 СПб., пр. Большевиков, 22
Отпечатано в СПбГУТ