


Основы помехоустойчивого кодирования

Рассматриваются основные методы помехоустойчивого кодирования, применяемые в современных системах передачи информации. В частности, приведено описание кодов BCH и Рида-Соломона, турбо-кодов, кодов с малой плотностью проверок на четность, полярных кодов. Представлены как теоретические положения, лежащие в основе рассматриваемых конструкций, так и вопросы их практической реализации. Приведены задачи и практические задания. Издание ориентировано как на студентов, так и на инженеров, занимающихся практической реализацией методов помехоустойчивого кодирования

ОСНОВЫ ПОМЕХОУСТОЙЧИВОГО КОДИРОВАНИЯ



КНИГА ВОРОГА

ВОРОЖОЮ МОВОЮ

Издательский дом
«СВАРОГ»
Киев – 2024

УДК 681.325
О-75

Основы помехоустойчивого кодирования. Книга ворога ворожою мовою. —
О-75 Киев: Изд. дом «СВАРОГ», 2024. — 230 с.

ISBN 978-611-01-3139-1

Рассматриваются основные методы помехоустойчивого кодирования, применяемые в современных системах передачи информации. В частности, приведено описание кодов БЧХ и Рида-Соломона, турбо-кодов, кодов с малой плотностью проверок на четность, полярных кодов. Представлены как теоретические положения, лежащие в основе рассматриваемых конструкций, так и вопросы их практической реализации. Приведены задачи и практические задания.

Издание ориентировано как на студентов, так и на инженеров, занимающихся практическое реализацией методов помехоустойчивого кодирования.

ISBN 978-611-01-3139-1

УДК 681.325

© Издательский дом «Сварог», 2024.

Оглавление

Сокращения, принятые в пособии	8
Введение	9
I Теоретические основы кодирования	12
1. Основные понятия	14
1.1. Кодирование в технических системах	14
1.1.1. Системы хранения и передачи информации	14
1.1.2. Стеганография и защита цифровых материалов	16
1.1.3. Поисковые системы	17
1.2. Модели каналов передачи информации	17
1.2.1. Понятие канала	17
1.2.2. q -ичный стирающий канал	18
1.2.3. q -ичный симметричный канал	19
1.2.4. Аддитивный гауссовский канал	20
1.3. Кодирование и декодирование	22
1.3.1. Виды канального кодирования	22
1.3.2. Критерии декодирования	23
1.3.3. Метрики	24
1.3.4. Параметр Бхаттачарьи	25
1.4. Теоретико-информационные предпосылки	27
1.4.1. Теоремы кодирования	27
1.4.2. Пропускная способность некоторых каналов	30
2. Блочные коды	33
2.1. Основные понятия	33
2.1.1. Параметры кодов	33
2.1.2. Границы	34
2.2. Линейные коды	35
2.2.1. Основные понятия	35
2.2.2. Синдромное декодирование	39
2.2.3. Границы	41
2.3. Анализ корректирующей способности	44
2.3.1. Обнаружение ошибок	45
2.3.2. Исправление ошибок	45
3. Универсальные алгоритмы декодирования	48

3.1.	Декодирование по информационным совокупностям	48
3.1.1.	Поиск ближайшего кодового слова	48
3.1.2.	Поиск кодового слова наименьшего веса	50
3.2.	Метод порядковых статистик	52
3.2.1.	Алгоритм	52
3.2.2.	Методы ускорения	53
3.3.	Декодирование по обобщенному минимальному расстоянию	54
3.3.1.	Исправление ошибок и стираний	54
3.3.2.	Метод Форни	55
3.4.	Метод Чейза	56
II	Алгебраические методы кодирования	59
4.	Конечные поля	61
4.1.	Некоторые алгебраические структуры	61
4.1.1.	Кольца, тела, поля	61
4.1.2.	Идеалы	64
4.2.	Алгебраические свойства конечных полей	67
4.2.1.	Основные факты о конечных полях	67
4.2.2.	Минимальные многочлены	70
4.3.	Вычисления в конечных полях	74
4.3.1.	Логарифмы	74
4.3.2.	Стандартный базис	75
5.	Коды Боуза-Чоудхури-Хоквингема	77
5.1.	Циклические коды	77
5.1.1.	Основные понятия	77
5.1.2.	Декодер Меггитта	79
5.1.3.	Корни порождающего многочлена	80
5.2.	Коды БЧХ	83
5.2.1.	Свойства и конструкция кодов	83
5.2.2.	Декодирование кодов БЧХ	85
5.2.3.	Спектральное описание декодера кодов БЧХ	88
5.2.4.	Алгоритм Берлекэмп-Месси	90
5.2.5.	Алгоритм Сугиямы	94
5.2.6.	Вопросы реализации	97
6.	Коды Рида-Соломона и производные от них	99
6.1.	Коды Рида-Соломона	99
6.1.1.	Конструкции кодов	99
6.2.	Декодирование до половины минимального расстояния	101

6.2.1.	Алгоритм Гао	101
6.2.2.	Декодирование с помощью многомерной интерполяции	102
6.3.	Списочное декодирование	106
6.3.1.	Алгоритм Гурусами-Судана	106
6.3.2.	Быстрая интерполяция	110
6.3.3.	Быстрый поиск функциональных корней	111
6.4.	Альтернативные коды	112
6.4.1.	Конструкция кодов	112
6.4.2.	Коды Гошпы	113
6.4.3.	Криптосистема Мак-Элиса	115
7.	Коды Рида-Маллера	118
7.1.	Конструкция кодов	118
7.1.1.	Построение с помощью полиномов Жегалкина	118
7.1.2.	Построение с помощью конструкции Плоткина	119
7.2.	Декодирование	119
7.2.1.	Жесткое декодирование	119
7.2.2.	Мягкое декодирование	122
8.	Полярные коды	126
8.1.	Поляризация канала	126
8.1.1.	Основная идея	126
8.1.2.	Общий случай	128
8.2.	Декодирование полярных кодов	129
8.2.1.	Алгоритм последовательного исключения	129
8.2.2.	Списочный алгоритм Тала-Варди	131
8.2.3.	Последовательное декодирование	131
8.3.	Усовершенствованные конструкции	133
8.3.1.	Полярные коды с CRC	133
8.3.2.	Полярные подкоды	134
8.4.	Полярные коды с ядром Арикана	139
8.4.1.	Декодирование	139
8.4.2.	Оценка надежности подканалов	141
8.4.3.	Сравнение кодов	144

III Коды на графах 147

9.	Сверточные коды	149
9.1.	Конструкция кодов	149
9.1.1.	Основные понятия	149
9.1.2.	Порождающая матрица	151

9.1.3.	Весовые свойства сверточных кодов	154
9.2.	Методы декодирования	156
9.2.1.	Алгоритм Витерби	156
9.2.2.	Алгоритм Бала-Коке-Елинека-Равива	159
9.2.3.	Анализ вероятности ошибки	162
10.	Коды с малой плотностью проверок на четность	167
10.1.	Основные понятия	167
10.2.	Декодирование	169
10.2.1.	Алгоритм инвертирования битов	169
10.2.2.	Алгоритм распространения доверия	170
10.2.3.	Эволюция плотностей	175
10.3.	Методы построения кодов	180
10.3.1.	Конструкция Галлагера	180
10.3.2.	Прогрессивное наращивание ребер	181
10.3.3.	Протографы	181
10.3.4.	Повторительно-накопительные коды	182
10.3.5.	Конструкция на базе кодов Рида-Соломона	183
10.3.6.	Сравнительный анализ	184
11.	Коды для стирающего канала	187
11.1.	Надежная доставка данных по ненадежным каналам	187
11.1.1.	Потери в сетях с коммутацией пакетов	187
11.1.2.	Цифровой фонган	188
11.2.	Конструкции кодов	189
11.2.1.	Преобразование Луби	189
11.2.2.	Волновые распределения	191
11.2.3.	Хищные коды	194
IV	Составные коды	195
12.	Методы комбинирования кодов	197
12.1.	Простые преобразования кодов	197
12.1.1.	Укорочение линейных блоковых кодов	197
12.1.2.	Выкалывание	197
12.1.3.	Расширение	198
12.2.	Составные коды	198
12.2.1.	Чередование кодов	198
12.2.2.	Прямая сумма кодов	198
12.2.3.	Конструкция Плоткина	199
12.3.	Каскадные коды	200

12.3.1. Прямое произведение кодов	200
12.3.2. Каскадные коды	201
13. Турбо-коды	203
13.1. Конструкция	203
13.1.1. Мотивация	203
13.1.2. Кодирование	204
13.1.3. Построение перемежителя	205
13.2. Декодирование	206
13.2.1. Турбо-декодер	206
14. Кодовая модуляция	208
14.1. Решетчато-кодовая модуляция	208
14.1.1. Сигнальные множества	208
14.1.2. Конструкция Унгербека	210
14.1.3. Хорошие решетчатые коды	212
14.2. Многоуровневые коды	213
14.2.1. Основные понятия	213
14.2.2. Правила выбора компонентных кодов	215
Предметный указатель	219
Библиографический список	223
Задания для курсовой работы	230

Сокращения, принятые в пособии

АМ	амплитудная модуляция
БКЕР	Бал-Коке-Елинек-Равив
БЧХ	Боуз-Чоудхури-Хоквингем
ДПФ	дискретное преобразование Фурье
КАМ	квадратурно-амплитудная модуляция
МППЧ	малая плотность проверок на четность
НОД	наибольший общий делитель
РКМ	решетчато-кодовая модуляция
РСЛОС	регистр сдвига с линейной обратной связью
ФМ	фазовая модуляция

Введение

Проблема надежной передачи информации возникла перед человеком еще в доисторические времена. Она всегда решалась путем внесения некоторой избыточности в передаваемые данные. Это делалось не только организационными методами (например, посылка нескольких гонцов с одним и тем же сообщением), но и подсознательно на уровне языка. Действительно, во многих случаях удается понять смысл предложения, даже если при его написании были допущены орфографические ошибки. Сведения о грамматических правилах, допустимых словах, взаимосвязи обозначаемых ими понятий, а также типовых ошибках при написании позволяют восстановить замысел автора текста. Вместе с тем, чем большее число ошибок допущено в документе (или чем сильнее он поврежден в результате каких-либо внешних воздействий), тем более трудоемким становится его понимание и тем больше вероятность неправильной его интерпретации. С ростом объема данных, накопленных человечеством, и развитием средств вычислительной техники потребность в обмене информацией многократно возросла. В простейших случаях избыточность естественного языка может оказаться достаточной и в случае передачи по техническим каналам связи. Однако такой подход абсолютно неприемлем при передаче больших объемов информации, а также в том случае, когда принятые данные должны интерпретироваться компьютером. Таким образом, возникла потребность в разработке математических методов помехозащиты.

Теория помехоустойчивого кодирования возникла в 1948 г. после публикации основополагающей работы К. Шеннона [62], в которой была показана принципиальная возможность обеспечения сколь угодно надежной передачи данных со скоростью, не превышающей пропускной способности канала. Однако конкретные методы, которые позволили бы достичь этого, в работе Шеннона предложены не были. В течение нескольких лет после ее публикации были предложены некоторые конструкции кодов, исправляющих ошибки, но их характеристики были чрезвычайно далеки от теоретически достижимых. С другой стороны, уровень развития вычислительной техники не позволял реализовать даже их, что привело к возникновению пессимистических настроений.

По мере развития электроники и вычислительной техники ситуация стала меняться. Одним из первых практических приложений теории кодирования стала информационная система сопровождения полета первого искусственного спутника Земли, созданная в СССР. Помехоустойчивое кодирование начало активно внедряться в системы космической связи. Постепенно, с ростом возможностей микроэлектроники, оно нашло применение в модемах, обеспечивавших взаимодействие ЭВМ, системах мобильной связи, накопителях на оптических и магнитных дисках и лентах. Была разработана богатая алгебраическая теория кодирования, которая, однако, не давала ответа на вопрос о том, как может быть практически достигнут предел Шеннона. Революция в помехоустойчивом кодировании состоялась в 1993 году, когда была предложена чрезвычайно простая конструкция турбо-кодов [18], обеспечивавшая близкую к оптимальной корректирующую способность. Позднее аналогичные свойства были обнаружены и у кодов с малой плотностью проверок на четность [50], которые были предложены еще в 1963 году [36], но не нашли применения из-за высокой сложности реализации. Наконец, в 2009 году, через 61 год после выхода работы Шеннона, была предложена конструкция полярных кодов [14], достигающих пропускной способности достаточно широкого класса каналов. Разработанный за эти годы математический аппарат нашел свое применение не только в системах хранения и передачи информации, но и в задачах обработки изображений, биометрике, биоинформатике и многих других отраслях.

Целью данного учебного пособия является систематическое изложение наиболее важных разделов теории помехоустойчивого кодирования с точки зрения инженера-разработчика системы передачи информации, решающего задачи выбора подходящих корректирующих кодов и реализации соответствующих алгоритмов, а также создания новых кодовых методов. В нем представлены конкретные численные результаты, характеризующие корректирующую способность различных кодов, которые могут быть полезны как при выборе наиболее подходящей для конкретного приложения конструкции, так и для оценки корректности реализации соответствующего алгоритма. Оно призвано также осветить недавние достижения теории кодирования, которые не отражены в классических учебниках и монографиях, изданных на русском языке. Представленный библиографический список включает статьи, оказавшие наибольшее влияние на развитие теории и практики помехоустойчивого кодирования. Несмотря на то, что некоторые из них относятся к 1960-ым

годам, представленные в них методы все еще широко используются в самых современных системах передачи и хранения информации. Вместе с тем, в список литературы включены ссылки на недавние результаты, которые уже нашли или в ближайшее время найдут практическое применение. Читателям рекомендуется самостоятельно изучить хотя бы некоторые из этих статей для более глубокого понимания рассматриваемых вопросов. Это может быть полезно при выполнении самостоятельной научной работы.

Данная книга может использоваться в качестве основного учебного пособия при изучении односеместрового курса “Основы помехоустойчивого кодирования”. Материал разбит на главы, каждая из которых соответствует одной или двум лекциям и освещает один из разделов теории кодирования. Типовая структура главы включает описание некоторого класса корректирующих кодов, их свойств, методов их кодирования и декодирования. В конце глав представлены задачи, выполнение которых способствует лучшему усвоению материалов. Предполагается, что эти задачи будут частично разобраны на практических занятиях, а частично решены обучающимися самостоятельно. Значительная часть этих задач заимствована из классических и современных учебников и монографий по теории кодирования [3, 8, 48, 1, 19, 51, 5, 7]. В приложении представлен примерный список тем для курсовой работы. Кроме того, подготовка устного сообщения по материалам статей, приведенных в списке литературы (на усмотрение преподавателя), включая строгое доказательство приведенных там утверждений, может быть альтернативой или дополнением курсовой работы или теоретического экзамена.

Пособие организовано следующим образом.

В части I изложены предпосылки развития теории кодирования и представлены её основные понятия и методы. Часть II посвящена алгебраической теории кодирования. В части III представлены результаты, касающиеся кодов на графах и вероятностных методов декодирования. Вопросы построения кодовой модуляции рассмотрены в части IV.

Автор глубоко признателен рецензенту Б.Д. Кудряшovu за внимательное ознакомление с рукописью и её конструктивную критику. Автор также выражает благодарность студентам А. Горбунову, А. Маркову, А. Мишиной, А. Чугрееву за многочисленные сообщения об ошибках и опечатках.

Часть I

Теоретические основы кодирования

1. Основные понятия

1.1. Кодирование в технических системах

1.1.1. Системы хранения и передачи информации

Исторически первым приложением помехоустойчивого кодирования являются системы хранения и передачи информации. На рис. 1.1 представлена типовая структура такой системы. Первым этапом обработки информации на передающей стороне является применение некоторого алгоритма сжатия данных (кодера источника), за счет которого во многих случаях можно существенно снизить объем реально передаваемой информации. Это достигается за счет устранения статистической избыточности, которая часто встречается в данных, формируемых современными информационными системами. В некоторых случаях на этом этапе производятся необратимые преобразования данных, т.е. сжатие с потерями, которые, однако, не являются значимыми для получателя. Принципы кодирования источников изложены, например, в [6]. Шенноном было показано, что кодирование источника может выполняться независимо от канального кодирования, поэтому в дальнейшем этот этап рассматриваться не будет. Вместе с тем, будем предполагать, что статистическая избыточность в передаваемых данных уже устранена, и они представляют последовательность независимых равномерно распределенных случайных величин из некоторого множества \mathbb{U} .

Далее в некоторых случаях может осуществляться шифрование данных с целью их защиты от несанкционированного доступа. Иногда эту операцию ошибочно также называют кодированием. Она, однако, не является предметом изучения теории помехоустойчивого кодирования.

После добавления к передаваемым данным необходимых служебных сведений, определяемых особенностями конкретной системы (например, адреса получателя), они разбиваются на блоки фиксированной длины. Операция канального кодирования состоит во внесении в эти блоки некоторой избыточной информации, которая будет позднее использована для исправления ошибок, возникающих при передаче. Результатом этой операции являются последовательности символов c_i , называемые кодовыми словами, которые преобразуются модулятором в сигналы, пригодные для передачи по некоторому каналу. Обозначим как $\mathcal{C}(u) : \mathbb{U} \rightarrow \mathbb{X}$

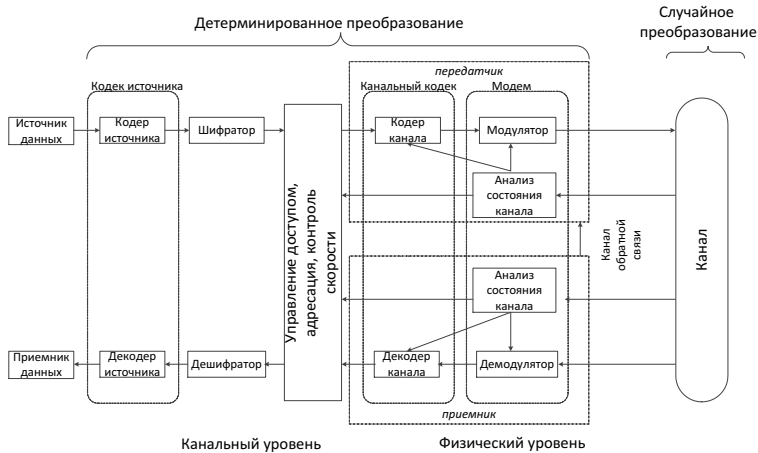


Рис. 1.1. Структура систем хранения и передачи информации

преобразование, выполняемое над сообщением u канальным кодером и модулятором. Это преобразование, как и все другие ранее описанные операции, является детерминированным.

В противоположность этому, *канал передачи информации* осуществляет стохастическое, т.е. недетерминированное преобразование данных $\mathcal{Y}(X) : \mathbb{X} \rightarrow \mathbb{Y}$, состоящее в наложении на них некоторых случайных помех. Он может быть охарактеризован некоторой условной плотностью распределения $p_{Y|X}(y|x)$, характеризующей многомерное распределение сигнала на его выходе при условии подачи на его вход последовательности сигналов x . Задачей приемника, состоящего из демодулятора и канального декодера, является нахождение $\hat{u} : \mathcal{Y}(C(\hat{u})) \approx y$, где y — сигнал, наблюдаемый на выходе канала. Смысл отношения \approx будет пояснен в разд. 1.3.2. Демодулятор преобразует принимаемые из канала сигналы в форму, пригодную для использования декодером. В простейшем случае это могут быть оценки для каждого из символов c_i , а в наиболее общем — вероятности равенства c_i всем возможным значениям при условии наблюдения части принятого сигнала, соответствующего этому символу. С учетом этого под каналом передачи информации иногда бывает удобно понимать также и комбинацию модулятора, собственно канала и демодулятора.

Канальный декодер осуществляет собственно нахождение \hat{u} . После проверки его правильности, обработки и удаления служебной информации осуществляется дешифрование и декомпрессия данных. В некоторых случаях приемник и/или передатчик могут анализировать состояние канала, динамически подстраивая свои параметры. Кроме того, иногда существует возможность организации канала обратной связи, который, например, может использоваться для запроса повторной передачи в случае неудачной попытки нахождения \hat{u} .

Предметом данной книги являются вопросы построения канальных кодера и декодера. *Задачей теории кодирования является разработка математических методов внесения избыточности в данные, а также алгоритмов, использующих эту избыточность с целью восстановления сообщений, подвергшихся случайным искажениям в результате передачи по зашумленному каналу.*

1.1.2. Стеганография и защита цифровых материалов

Методы помехоустойчивого кодирования могут быть использованы для сокрытия факта передачи данных, т.е. незаметного внедрения их в некоторый объект (контейнер), который может быть передан через открытые каналы, не вызывая при этом подозрений у лиц, заинтересованных в перехвате сообщения. Очевидно, что для реализации такого внедрения необходимо минимизировать изменения, которым подвергается контейнер. Синдромное кодирование [26] позволяет решить эту проблему путем представления сообщения как синдрома некоторого зашумленного вектора. Результат декодирования этого синдрома в некотором линейном коде приводит к вектору, показывающему те изменения, которые необходимо внести в части контейнера, выбранные для внедрения информации (например, наименее значащие биты пикселей изображения), чтобы они задавали кодируемые данные, причем количество таких изменений минимизируется.

Кроме того, методы помехоустойчивого кодирования могут использоваться для выявления путей распространения нелегальных копий цифровых материалов. Для этого каждому легальному их приобретателю должна выдаваться копия, в которую скрытно внедрена метка, идентифицирующая его. Однако несколько недобросовестных приобретателей могут сравнить свои копии, выявить их отличия и, предполагая, что именно в различающихся позициях содержится идентифицирующая их информация, изготовить новую копию, в которой соответствующие сим-

волы заменены случайными или средними значениями, вычисленными по имеющимся копиям. Вообще говоря, это приводит к разрушению меток и невозможности идентификации авторов построенной таким образом пиратской копии. Но если внедренные метки являются кодовыми словами соответствующим образом подобранного кода, возникает возможность алгебраическими методами построить список возможных нарушителей авторских прав [32].

1.1.3. Поисковые системы

Коды, исправляющие ошибки, могут быть использованы для повышения надежности автоматической классификации данных. Для этого различным категориям данных могут быть сопоставлены различные кодовые слова, после чего построены распознаватели, оценивающие каждый символ кодовых слов по известным признакам классифицируемых объектов. Некоторые из этих оценок могут быть неправильными, но при надлежащем выборе кодовых слов существует возможность исправления этих ошибок и повышения точности классификации [80].

1.2. Модели каналов передачи информации

1.2.1. Понятие канала

Очевидно, что для решения задачи, сформулированной в разд. 1.1.1, необходимо иметь некоторую модель канала передачи данных. Всякий *канал передачи информации* характеризуется своим входным и выходным алфавитами \mathbb{X} и \mathbb{Y} , а также условным распределением $P_{Y^m|X^n}\{y|x\}$ (или плотностью распределения $p_{Y^m|X^n}(y|x)$ в случае непрерывного алфавита), $y \in \mathbb{Y}^m, x \in \mathbb{X}^n$. Здесь X и Y обозначают случайные величины на входе и выходе канала, x и y — их значения, m и n — длины последовательностей. Далее, если не указано иное, будут рассматриваться *каналы без памяти*, для которых выполняется

$$\forall m : P_{Y^m|X^m}\{y_1, \dots, y_m|x_1, \dots, x_m\} = \prod_{i=1}^m P_{Y|X}\{y_i|x_i\},$$

т.е. прохождение каждого символа по нему осуществляется независимо. *Дискретным каналом* называют канал, у которого как \mathbb{X} , так и \mathbb{Y} являются конечными множествами. Более общая модель *дискретного по времени канала* характеризуется произвольными входным и выходным алфавитами, т.е. предполагается лишь, что передаваемое и принимаемое сообщения могут быть разбиты на некоторые буквы, каждая из которых

передается в свой интервал времени. Наибольший практический интерес представляет модель *полунепрерывного канала*, характеризующаяся конечным входным алфавитом и $\mathbb{Y} = \mathbb{R}$.

В случае дискретных алфавитов распределение $P_{Y|X} \{y|x\}$ задается в виде матрицы $P_{Y|X}$ переходных вероятностей, в которой строка x и столбец y содержат $P_{Y|X} \{y|x\}$. Очевидно, что сумма строк матрицы переходных вероятностей всегда равна вектору, состоящему из всех единиц. Дискретный канал называется *симметричным по входу*, если все строки матрицы переходных вероятностей являются перестановками первой строки. *симметричным по выходу*, если все столбцы матрицы переходных вероятностей являются перестановками первого столбца¹. Дискретный канал называется *полностью симметричным*, если он симметричен по входу и выходу.

1.2.2. q -ичный стирающий канал

Простейшей моделью является *q -ичный стирающий канал*. Его входным алфавитом является $\mathbb{X} = \{0, \dots, q-1\}$, а выходным — $\mathbb{Y} = \{0, \dots, q-1, \epsilon\}$. Появление символа ϵ , называемого *стиранием*, на выходе канала означает безвозвратную потерю соответствующего переданного символа. Матрица переходных вероятностей канала имеет вид

$$P_{Y|X} = \begin{pmatrix} 1-p & 0 & \dots & 0 & p \\ 0 & 1-p & \dots & 0 & p \\ \vdots & \vdots & \ddots & \dots & \vdots \\ 0 & 0 & \dots & 1-p & p \end{pmatrix}, \text{ где } p \text{ — вероятность стирания.}$$

Графическая модель канала при $q = 2$ представлена на рис. 1.2, а.

Данная модель может использоваться для описания IP-сетей, в которых, как известно, могут происходить потери пакетов. Несложно включить в пакеты, передаваемые по сети, их порядковый номер. В этом случае потеря пакета может быть легко обнаружена и интерпретирована как стирание. Заметим, что в рамках данной модели символы (например, пакеты), доставленные получателю, считаются безошибочными. Эта модель описывает также избыточные массивы жестких дисков (RAID-5,6), в которых факт отказа любого из дисков может быть легко обнаружен.

Ввиду простоты модели двоичный стирающий канал стал первым, для которого были предложены коды, достигающие его пропускной способности [49, 63]. В настоящее время эти коды нашли применение в си-

¹К сожалению, в литературе иногда симметричный по входу канал называют симметричным по выходу и наоборот.

WAR BOOKS
військова література

КУПИТИ