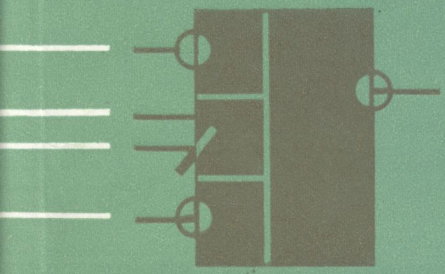
И. В. Кузьмин
В. И. Ключко
В. А. Литвин

КОДИРОВАНИЕ И ДЕКОДИРОВАНИЕ в информационных системах



И. В. Кузьмин,
В. И. Ключко,
В. А. Литвин

КОДИРОВАНИЕ И ДЕКОДИРОВАНИЕ в информационных системах

Под редакцией
профессора
доктора технических наук
И. В. КУЗЬМИНА

Киев
Головное издательство
издательского объединения
«Вища школа»
1985

УДК 621.391.1

Кодирование и декодирование в информационных системах. Кузьмин И. В., Ключко В. И., Литвин В. А./ Под ред. И. В. Кузьмина. — К.: Вища шк. Головное изд-во, 1985. — 190 с.

В монографии излагаются общие методы оценки эффективности и качества информации, методы защиты ее от ошибок в информационной системе (ИС). Рассматриваются кодовые методы повышения достоверности информации. Вводятся в рассмотрение поэтапные методы принятия решений, характеризуемые различным уровнем достоверности и позволяющие повысить эффективность защиты от ошибок. Проводится сравнение различных способов повышения достоверности информации и излагается методика оптимального проектирования средств защиты информации от ошибок ИС.

Для специалистов, занимающихся исследованием, проектированием и эксплуатацией информационных систем, а также студентов технических вузов, изучающих проблемы кодирования и декодирования информации.

Табл. 16. Ил. 65. Библиогр.: 35 назв.

Рецензенты: доктор технических наук *Г. В. Лавинский* (Киевский институт народного хозяйства), кандидат технических наук *В. П. Цымбал* (Украинский научно-исследовательский институт научно-технической информации)

Редакция литературы по кибернетике, электронике и энергетике

Зав. редакцией *М. С. Хойнацкий*

К $\frac{1504000000-105}{M211(04)-85}$ 445—85

ПРЕДИСЛОВИЕ

Автоматизированные системы измерения, контроля и управления широко применяются в научных исследованиях для управления всевозможными технологическими и организационными процессами, в том числе и вычислительными.

Эти системы включают сложные устройства, предназначенные для получения, преобразования, накопления и передачи информации. Показатели качества работы информационных систем во многом определяются достоверностью получения, передачи, хранения и обработки информации в системе, оперативностью управления, скоростью передачи информации, быстродействия аппаратных средств и сложностью аппаратурной реализации. Для улучшения перечисленных показателей должны быть учтены все основные факторы, влияющие на них, независимо от физических причин возникновения и этапов информационного процесса. Принцип системности требует рассмотрения и сравнения между собой совокупности способов улучшения рассмотренных параметров, повышения эффективности и качества ИС.

Причинами снижения эффективности информационных процессов в ИС являются:

воздействие помех при передаче, хранении и переработке информации;

отказы и сбои в работе аппаратуры;

ошибки, возникающие в процессе принятия решений и обусловленные различного типа ограничениями, накладываемыми на исходные данные, такими как конечная точность и информационная емкость, наличие временных задержек и т. п.;

ошибки человека как звена системы;

алгоритмическая и структурная реализация систем.

Относительная доля этих причин в общем количестве ошибок на выходе системы может быть различна. При проектировании информационных систем ощущается необходимость комплексного подхода для обеспечения заданных требований по защите информации от ошибок. Такой подход позволит избежать завышения требований к помехоустойчивости отдельных узлов и звеньев системы, неоправданного применения сложных и дорогостоящих способов повышения достоверности или наоборот, необоснованного отказа от применения тех или иных способов защиты от ошибок.

Информационные системы характеризуются большим количеством видов циркулирующей информации. Это и большие массивы измерительных данных, и отдельные показатели контроля, и команды управления адаптивных ИС. При этом информация (преимущественно в цифровой форме) может передаваться как на малые, так и на большие расстояния, что определяет различную стоимость используемых каналов связи.

Эти обстоятельства определяют применение в ИС широкого набора различных кодовых методов защиты информации от ошибок.

В монографии уделено внимание наиболее часто используемым новым и перспективным методам защиты информации от ошибок на основе использования избыточных кодов. Рассмотрены пути уменьшения сложности и повышения эффективности класса линейных кодов; приведены инженерные методики выбора и оценки циклических кодов, наиболее широко используемых в ИС различного назначения.

Развиваются методы декодирования кодов с повторением целесообразных для применения на каналах связи с пакетированием ошибок, а также при обработке и хранении информации в ИС.

Введены методы поэтапного кодирования и декодирования информации, позволяющие повысить эффективность защиты информации от ошибок. Показано, что поэтапные методы обработки информации могут быть применены к широкому классу систем, характеризуемых определенной временной избыточностью.

Изложена алгебраическая теория конструктивного построения сверточных кодов, хорошо совместимых с непрерывной передачей больших массивов измерительных данных и находящих все более широкое применение в ИС.

Оптимальные и близкие к ним методы приема и обработки информации находятся в стадии развития, поэтому наряду с известными техническими решениями в предлагаемой книге рассмотрен ряд новых квазиоптимальных решений, занимающих промежуточное положение между идеальным декодированием в целом и декодированием с обнаружением ошибок и позволяющих эффективнее использовать каналы связи.

Проводится сравнительный анализ систем передачи дискретной информации с решающей обратной связью, определяются области целесообразного использования тех или других систем и намечаются пути улучшения их характеристик.

Изложены вопросы селекции информации, включающие методы циклового фазирования и методы борьбы со вставками и выпадениями информации в ИС.

Основной материал рассматривается применительно к каналам связи с независимым и групповым распределением ошибок.

Рассматриваемые методы иллюстрируются примерами наиболее новых и эффективных технических решений, что позволяет использовать изложенный материал как при техническом проектировании информационных систем, так и в учебных целях.

Отзывы и пожелания просим направлять в Головное издательство издательского объединения «Вища школа» по адресу: 252054, Киев-54, ул. Гоголевская, 7.

1. ОБЩИЕ ПРИНЦИПЫ ПОСТРОЕНИЯ ИНФОРМАЦИОННЫХ СИСТЕМ (ИС)

1.1. Структурная схема ИС

Информационная система — система накопления, хранения, обновления, поиска и выдачи по запросам сведений различного характера [24—26].

На рис. 1.1 представлена обобщенная структурная схема ИС, содержащая следующие основные части: под-

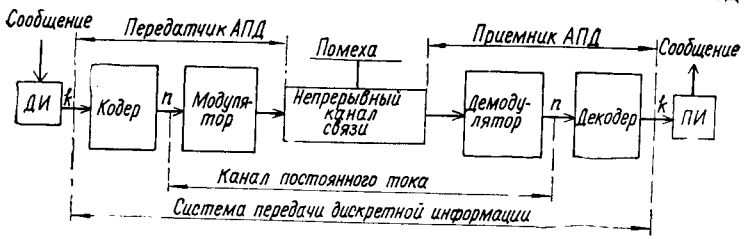


Рис. 1.1

систему измерений, подсистему передачи, подсистему обработки и представления информации и подсистему управления. Неотъемлемой частью ИС должна быть подсистема ввода и контроля данных.

Подсистема измерений включает в себя датчики, воспринимающие различные физические величины и преобразующие их в электрические сигналы, и собственно измерительные устройства. В эту же подсистему могут входить коммутатор, обеспечивающий поочередное подключение датчиков к системе, буферные запоминающие устройства, согласующие входной поток измерительной информации с пропускной способностью подсистемы передачи, и устройства сокращения избыточности измерений.

Структура и состав подсистемы передачи информации зависят от расстояния между объектами измерений и потребителями информации. При незначительных расстояниях подсистема передачи вырождается в соединительные электрические цепи. В частном случае данная подсис-

тема состоит из кодера и декодера канала связи, решающих задачу избыточного кодирования с целью уменьшения искажений информации при передаче, и передатчика с приемником, формирующих и наилучшим образом обрабатывающих передаваемые электрические сигналы.

Подсистема обработки и представления информации по заданному алгоритму осуществляет математическую обработку данных (например, декодирование, цифро-аналоговое преобразование, суммирование, обобщение, восстановление, прогнозирование и представление информации человеку-оператору (регистрация, наглядное отображение, звуковое сопровождение). Данная подсистема, как правило, содержит устройства хранения информации: постоянные запоминающие устройства (ПЗУ) — для хранения как документальной, так и фактографической информации констант, эталонных значений параметров и т. п.; оперативные запоминающие устройства (ОЗУ) — для хранения изменяющихся во времени данных.

Подсистема управления обеспечивает организацию взаимодействия всех подсистем и устройств, например, выбор очередности опроса датчиков, согласование параметров измерений с динамическими характеристиками измеряемых величин, согласование алгоритмов передачи и обработки информации с характеристиками каналов связи, включая реализацию алгоритмов управления.

Внешние воздействия проявляются в изменении технологических процессов, отказе или сбое элементов и устройств системы, действии помех в канале связи, изменении характеристик человека-оператора под воздействием климатических, температурных, шумовых и других факторов внешней среды.

Классификация информационных систем может быть выполнена по различным признакам, например по структуре, назначению, расстоянию до исследуемых объектов, характеру взаимодействия с объектом.

Информационно-измерительные системы являются частным случаем ИС. По структурному признаку их можно разделить на несколько групп:

а) системы с параллельными измерительными каналами;

б) системы с параллельно-последовательными измерительными каналами;

в) системы последовательного (сканирующего) типа;

г) мультиплицированные развертывающие системы.

По назначению информационно-измерительные системы подразделяются на:

в) собственно информационно-измерительные системы;
б) системы автоматического контроля и управления;
в) системы технической диагностики и т. д.

По расстоянию до исследуемого объекта информационно-измерительные системы обычно делят на системы ближнего и дальнего действия, или телеизмерительные (ТИ), телеконтролирующие (ТК) и телеуправляющие (ТУ). В системах первого типа стоимость каналов связи мала и может в меньшей степени учитываться при проектировании. В системах ТИ, ТК и ТУ каналы связи являются одним из наиболее сложных и дорогих устройств системы, и это необходимо учитывать при проектировании.

По характеру взаимодействия с объектом исследования структуры ИС подразделяются на пассивные и активные [24]. Пассивные системы только воспринимают информацию от объекта, а активные, действуя на объект, позволяют наиболее полно изучить его поведение.

Измерительная информация, проходя через различные части ИС, подвергается искажениям, что требует построения математических моделей источников ошибок, используемых при оценке эффективности методов и средств защиты информации от ошибок.

1.2. Математические модели источников ошибок

Математические модели, описывая последовательности цифровых ошибок, предназначены для аналитического решения задач, связанных с определением параметров систем передачи, обработки и хранения дискретной информации.

Наиболее простой из таких моделей является модель независимых ошибок. Если под вероятностью искажения комбинаций понимать вероятность появления n-элементных комбинаций хотя бы с одной ошибкой $P(\geqslant 1, n)$, то для канала с независимым распределением ошибок — дискретный симметричный канал (ДСК) без памяти

$$P(\geqslant 1, n) = 1 - (1 - P_0)^n, \qquad (1.1)$$

а при $nP_0 \ll 1$

$$P(\geqslant 1, n) \approx nP_0.$$

Вероятность искажения комбинаций $P(\geqslant 1, n)$ может быть определена также и через вероятности появления ис-

каженных комбинаций с одной $P(1, n)$, двумя $P(2, n)$... $P(i, n)$ и n ошибками $P(n, n)$:

$$P(\geqslant 1, n) = \sum_{i=1}^{n} P(i, n). \tag{1.2}$$

Для канала с независимыми ошибками

$$P(\geqslant 1, n) = \sum_{i=1}^{n} C_n^i P_0^i (1 - P_0)^{n-i}. \tag{1.3}$$

Вероятность появления искаженных комбинаций с m и более необнаруженными ошибками определяется выражением

$$P_{\text{н. о}} = P(\geqslant m, n) = \sum_{i=m}^{n} P(i, n). \tag{1.4}$$

Для канала с независимыми ошибками

$$P(\geqslant m, n) = \sum_{i=m}^{n} C_n^i P_0^i (1 - P_0)^{n-i}. \tag{1.5}$$

Обобщением модели независимых ошибок в каналах с группированием ошибок является модель, в которой принято, что на отдельных участках последовательности ошибок сохраняются закономерности, свойственные последовательности независимых испытаний, но интенсивность ошибок, характеризуемая вероятностью ошибочного приема элементарного символа P_0, меняется во времени. Достоинством такого подхода является возможность распространения теоретических результатов, полученных для канала с независимыми ошибками, на неоднородные каналы.

В [35] показано, что при практических расчетах можно ограничиться двумя-тремя состояниями канала с различными интенсивностями ошибок. Однако при этом экспериментальное определение вероятностей ошибочного приема символов в различных состояниях достаточно сложно. Поэтому наиболее приемлемой является следующая математическая модель дискретного канала, позволяющая описать последовательность ошибок лишь с помощью двух параметров.

Вероятность $P(\geqslant 1, n)$ является неубывающей функцией и при $n \to \infty$ $P(\geqslant 1, n) \to 1$ при любом значении P_0. Степень возрастания $P(\geqslant 1, n)$ с ростом n зависит от характера распределения ошибок. В реальных каналах, благодаря групповому характеру помех, величина

$P(\geqslant 1, n)$ зависит от длины комбинации в меньшей степени, чем для случая независимых ошибок и поэтому экспериментальные значения $P(\geqslant 1, n)$ располагаются примерно в средней части между границами $P_0 < P(\geqslant 1, n) < nP_0$.

На рис. 1.2 приведены зависимости $P(\geqslant 1, n)$ от n для радиорелейных телефонных каналов и КВ радиотелеграфных каналов. Масштаб по обеим осям логарифмический. Точками нанесены экспериментальные данные, которые для всех радиоканалов хорошо аппроксимируются прямыми линиями при числе элементов в комбинациях от 1 до 500. Для каналов различного вида наклон прямых различен. На основании уравнения прямой линии можно получить

$$P(\geqslant 1, n) = n^{1-\alpha}P_0 \text{ при } 0 < \alpha < 1. \qquad (1.6)$$

Коэффициент α, характеризующий степень возрастания вероятности $P(\geqslant 1, n)$ с увеличением n, является показателем группирования ошибок.

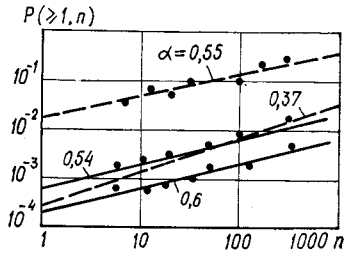


Рис. 1.2

Для двух границ величины вероятности $P(\geqslant 1, n)$ значения α следующие: для канала с независимыми ошибками $\alpha = 0$. Для гипотетического канала, когда все ошибки

Таблица 1.1

Номер канала	Тип канала	Вид модуляции	Скорость телеграфирования, Бод	Число переприемов или мощность передатчика	Средняя частность ошибок P_0	Показатель группирования α
1	Радиорелейный телефонный	ОВМ	1200	3	$2{,}66 \cdot 10^{-4}$	0,606
2	То же	ЧМ	1200	3	$7{,}03 \cdot 10^{-4}$	0,545
3	Тропосферный телефонный	ОФМ	1200	—	$7{,}03 \cdot 10^{-4}$	0,439
4	То же	ЧМ	1200	—	$7{,}05 \cdot 10^{-4}$	0,449
5	Радиотелеграфный КВ	ЧМ	150	20 кВт	$2{,}85 \cdot 10^{-4}$	0,373
6	То же	ЧМ	50	5 кВт	$5{,}85 \cdot 10^{-3}$	0,320
7	—»—	ЧМ	150	1 кВт	$1{,}64 \cdot 10^{-3}$	0,550

сосредоточены в одной группе, $\alpha = 1$. Таким образом, параметр α характеризует степень группирования ошибок в реальном канале связи и является вторым его параметром помимо P_0.

Значения показателя группирования для различных радиоканалов приведены в табл. 1.1.

Штриховой линией на рис. 1.2 нанесены зависимости $P(\geqslant 1, n)$ от n для независимого распределения ошибок.

Статистическая вероятность появления n-элементных комбинаций с m и более ошибками

$$P(\geqslant m, n) = \frac{\sum_{i=m}^{n} B(i, n)}{B_0(n)},$$

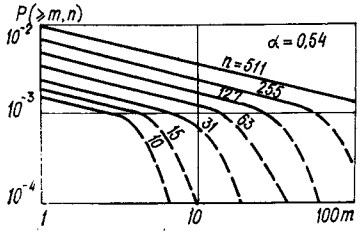


Рис. 1.3

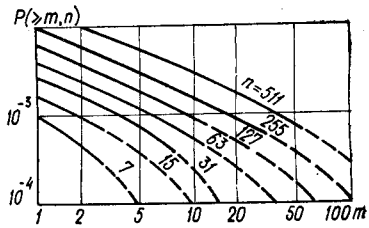


Рис. 1.4

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

На рис. 1.3, 1.4 в двойном логарифмическом масштабе показаны графики $P(\geqslant m, n)$ в зависимости от числа ошибок m в комбинациях различной длины n для радиорелейного телефонного и радиотелеграфного КВ каналов. Штриховые линии на этих рисунках отвечают экспериментальным данным, которые на участке $1 \leqslant m \leqslant n/3$ достаточно хорошо аппроксимируются прямыми линиями, что позволяет характеризовать групповое распределение ошибок в искаженных комбинациях тем же параметром α. В результате приближенная формула для определения $P(\geqslant m, n)$ приобретает следующий вид [35]:

$$P(\geqslant m, n) = \left(\frac{n}{m}\right)^{1-\alpha} P_0. \qquad (1.7)$$

На рис. 1.5 для сравнения приведены рассматриваемые зависимости для одного из радиотелеграфных КВ

каналов (сплошные линии) и для независимого распределения ошибок (штриховые линии), рассчитанные при той же вероятности $P_0 = 1{,}37 \cdot 10^{-2}$. В последнем случае с увеличением кратности ошибок вероятность их появления резко падает. Так, для ДСК без памяти вероятность $P(\geqslant 4{,}15) = 10^{-4}$, тогда как для реального канала $P(\geqslant 4{,}15) = 2 \cdot 10^{-2}$. Следовательно, групповой характер ошибок приводит к появлению искаженных комбинаций с большой кратностью ошибок.

Вероятности приема n-элементной комбинации с m ошибками $P(m, n)$ и m и более ошибками $P(\geqslant m, n)$ необходимы для расчета достоверности, обеспечиваемой корректирующими кодами и системами передачи дискретной информации.

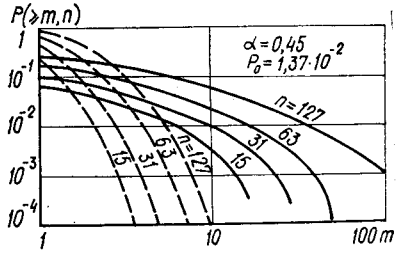


Рис. 1.5

Приведем формулу для определения $P(\geqslant m, n)$ [35]:

$$P(\geqslant m, n) = n^{1-\alpha} P_0 \prod_{i=2}^{m} \frac{\left(\frac{i-1}{n}\right)^{1-\alpha} - \frac{i-1}{n}}{\left(\frac{i}{n}\right)^{1-\alpha} - \frac{i-1}{n}} \cdot \quad (1.8)$$

Использовать формулу (1.8) для каналов с независимыми ошибками и каналов с малыми значениями α нельзя.

Большие возможности заложены в модели Аксенова, Александрова [2], которая описывается при помощи обобщенного потока Пуассона и позволяет отражать тонкую структуру зависимости ошибок в реальных каналах связи.

1.3. Форматизация сообщений в информационных системах

Каждое сообщение должно содержать служебную часть, в которой находятся служебные признаки, обеспечивающие автоматическую обработку информации в оконечной установке передачи данных. Из технологических соображений все сообщения целесообразно передавать в составе некоторого числа кодограмм стандартной или переменной длины, содержащих все необходимые признаки для автоматической обработки [21].

Под кодограммой или информационной кодограммой, понимают кодовое слово, в котором не приняты специальные меры по повышению достоверности передаваемой информации. Форматизованная служебная часть, находящаяся в начале каждой кодограммы, называется заголовком, а остальная часть кодограммы — информационной частью или текстом. Структура форматизованной части кодограммы определяет построение, расположение и взаимосвязь элементов заголовка, с помощью которых обеспечиваются автоматическая передача, контроль, обработка, хранение, поиск и регистрация сообщений. Служебная часть (заголовок) должна содержать все сведения, необходимые как для доведения информации от объекта-отправителя до объекта-получателя (адресата), так и для доведения их до непосредственных потребителей внутри объекта [21].

Структура заголовка должна обеспечивать:

возможность форматизации с целью сокращения времени доведения сообщений до абонентов, а также упрощения обработки информации в оконечных устройствах. Уменьшение времени доведения играет особо важную роль при передаче сообщений в системах управления, работающих в реальном масштабе времени;

возможность упаковки и распаковки сообщений в информационно-вычислительных сетях;

возможность организации передачи сообщений различной степени циркулярности в соответствии со структурой входящих в сеть систем управления;

наличие резервов и некоторой избыточности на случай последующих изменений и усовершенствований способов управления, методов обмена и увеличения количества передаваемых сообщений;

удобство и простоту формирования, обработки и представления информации для абонентов.

Учитывая перечисленные требования, служебная часть кодограммы должна содержать следующие признаки: начало или конец кодограммы; категорийность (срочность, секретность); вид сообщения; тип кода, используемого в текстовой части; время ввода кодограммы в сеть; порядковый номер кодограммы и их количество в сообщении, если последнее разбивается на несколько кодограмм; адрес абонента-отправителя и адреса абонентов-получателей; внутренние адреса, т. е. адреса конкретных устройств у абонентов, выдающих и принимающих сообщения; вид передачи: избирательная или циркулярная; контрольные признаки, необходимые для повышения достоверности

информации заголовка; маршрутные признаки — при наличии коммутационных узлов.

Для передачи различных сообщений требуется различный набор перечисленных выше признаков. Кодирование заголовка может осуществляться по позиционному признаку, когда смысловое значение каждого элемента служебной части однозначно определяется его положением в данном формате.

На рис. 1.6 показан один из возможных форматов заголовка. Все признаки в заголовке объединены в отдельные функциональные группы, имеющие общее смысловое значение. Состав каждой группы с первой по седьмую определяется признаком формата, расположенным в первой группе.

Группа	Наименование признаков
1	Начало кодограммы Признак формата
2	Категория срочности Вид сообщения Гриф секретности Вид кодирования
3	Исходящий регистрационный номер Время ввода информации в сеть Число к.д.г. в сообщении Порядковый номер к.д.г.
	Адрес абонента отправителя
4	Вариант передачи к.д.г. Адреса абонентов получателей Внутренние адреса
5	Контроль заголовка
6	Маршрутные признаки
7	Конец заголовка

Рис. 1.6

Вторая справочная группа содержит признаки, обеспечивающие приоритетность и выбор конкретной процедуры обработки информации.

Третья группа признаков используется для опознавания отправителя, контроля времени прохождения кодограмм (селекция по времени), учета и регистрации передаваемых сообщений. Кроме того, здесь же указываются признаки (порядковый номер кодограммы и число кодограмм в сообщении), которые используются для восстановления всего сообщения на приемной стороне. Внутренние адреса получателей в четвертой группе необходимы для распределения информации по конкретным устройствам на оконечных устройствах.

В основе построения большинства первичных кодов находятся системы счисления. Любой набор дискретных сообщений можно пронумеровать, а числа нумерации записать в определенной системе счисления. Наибольшее распространение в настоящее время получила двоичная система счисления и особенно ее разновидность — двоично-десятичная система, применяемая для форматизации сообщений в ИС. Произведем сравнительную оценку инфор-

мационных кодограмм, для форматизации которых используется двоичная и двоично-десятичная системы счисления.

Если необходимо передать Q различных десятичных чисел и S различных смысловых признаков, то потребуется $U =]1/4 \log_2(S + \Delta S)[$ тетрад для смысловых признаков и $V =]\lg(Q + \Delta Q)[$ тетрад для десятичных чисел, где ΔS, ΔQ — резервные смысловые признаки и десятичные числа, учитывающие развитие системы; $]x[$ — наименьшее из целых чисел не меньших x.

В большинстве реальных случаев необходимо передавать несколько групп десятичных чисел

$$Q_1, Q_2, \ldots, Q_\upsilon,$$

причем $Q = \prod_{i=1}^{\upsilon} Q_i$ — общее число всех передаваемых десятичных чисел, а также несколько различных групп смысловых признаков

$$S_1, S_2, \ldots, S_\mu,$$

где $S = \prod_{j=1}^{\mu} S_j$ — все возможные варианты смысловых признаков. Тогда можно записать, что

$$U_j = \left]\frac{1}{4}\log_2(S_j + \Delta S_j)\right[;$$

$$V_i = \left]\lg(Q_i + \Delta Q_i)\right[,$$

и необходимое число тетрад будет равно

$$\eta = \sum_{j=1}^{\mu} U_j + \sum_{i=1}^{\nu} V_i,$$

что составит $n_1 = 4\eta$ двоичных разрядов.

Общее количество различных собщений определяется выражением

$$N = QS,$$

что при двоичном кодировании потребовало бы

$$n_2 =]\log_2 N[$$

двоичных разрядов.

Во всех случаях $n_1 > n_2$ и относительная скорость передачи

$$R = \frac{n_2}{n_1} < 1{,}0.$$

Введенная на этапе форматизации избыточность не используется для повышения достоверности, что обусловлено следующими причинами:

использованием двоично-десятичной системы счисления, позволяющей упростить устройства шифровки и дешифровки информации;

наличием резервных числовых и смысловых признаков, учитывающих развитие системы.

1.4. Помехоустойчивое кодирование информации

Кодирование в широком смысле слова можно определить как процедуру взаимно однозначного отображения сообщений в сигналы, иными словами, преобразования сообщения в код. Таблица соответствия между совокупностью используемых сообщений и кодовыми комбинациями, которые их отображают, называется первичным кодом. В этом случае кодовая комбинация содержит k элементов. Кодовая комбинация избыточного кода содержит n элементов, где $n > k$.

Способность кода обнаруживать и исправлять ошибки обусловлена наличием избыточных элементов в кодовой комбинации $r = n - k$.

В этом случае общее число возможных кодовых комбинаций будет $N = 2^n$, число разрешенных комбинаций $M \leqslant 2^k$, а запрещенных — $2^n - 2^k$.

Искажение информации в процессе передачи сводится к тому, что некоторые из переданных элементов заменяются другими — неверными. При этом для систематических кодов из $2^k \cdot 2^n$ случаев передачи возможно 2^k $(2^k - 1)$ случаев перехода в другие разрешенные комбинации, что соответствует необнаруживаемым ошибкам, и 2^k $(2^n - 2^k)$ случаев перехода в неразрешенные комбинации, которые могут быть обнаружены [12]. Следовательно, часть опознанных ошибок от общего числа возможных случаев передачи составит

$$\frac{2^k (2^n - 2^k)}{2^k \cdot 2^n} = 1 - \frac{2^k}{2^n}.$$

Например, при использовании одного избыточного элемента ($r = 1$) часть опознанных ошибок составляет

$$1 - \frac{2^k}{2^{k+1}} = \frac{1}{2}.$$

Для того чтобы искаженная кодовая комбинация была опознана с наименьшей ошибкой, необходимо чтобы остальные $2^n - 2^k$ запрещенных комбинаций были разбиты на 2^k непересекающихся множеств $W_i (i = 1,2,\ldots,2^k)$, причем $2^{n-k} - 1$ кодовые комбинации, принадлежащие W_i, должны в наибольшей степени быть похожими на i-ю разрешенную комбинацию и должны быть приписаны ей.

Процедура опознания искаженной кодовой комбинации в этом случае будет состоять в ее сравнении со всеми 2^n кодовыми комбинациями. Когда произойдет совпадение с одной из комбинаций, принадлежащих W_i, осуществится отождествление искаженной комбинации с i-й разрешенной, т. е. исправление ошибки. Ошибка будет исправлена в $2^n - 2^k$ случаях из всех возможных. Отношение числа исправляемых кодом ошибочных кодовых комбинаций к числу обнаруживаемых ошибочных комбинаций равно [12]

$$\frac{2^n - 2^k}{2^k - (2^n - 2^k)} = \frac{1}{2^k}.$$

Степень отличия любых двух кодовых комбинаций характеризуется расстоянием между ними в смысле Хэмминга, называемым кодовым расстоянием. Оно выражается числом элементов, в которых комбинации отличаются одна от другой, и обозначается через d. Минимальное количество элементов, в которых все комбинации кода отличаются друг от друга, называется минимальным кодовым расстоянием d_0. Минимальное кодовое расстояние — параметр, определяющий помехоустойчивость избыточного кода. В общем случае для обнаружения всех ошибок до σ-кратных включительно минимальное кодовое расстояние

$$d_0 = \sigma + 1. \tag{1.9}$$

Минимальное кодовое расстояние, необходимое для одновременного обнаружения и исправления ошибок,

$$d_0 = \sigma + t + 1, \tag{1.10}$$

где t — число исправляемых ошибок.

Для кодов, только исправляющих ошибки,

$$d_0 = 2t + 1. \tag{1.11}$$

Соотношения (1.9), (1.10) и (1.11) определяют лишь кратность гарантийно обнаруживаемых и исправляемых ошибок. Обычно коды обнаруживают и исправляют часть ошибок и более высокой кратности.

К наиболее употребляемым избыточным кодам можно отнести блоковые и непрерывные коды.

Блоковые коды характеризуются тем, что исходная непрерывная информационная последовательность разделяется на отдельные части, каждая из которых кодируется отдельно и независимо от других частей, образуя разрешенные слова избыточного кода.

Равномерные блоковые коды характеризуются одинаковой длиной разрешенных кодовых слов, в отличие от неравномерных кодов.

В непрерывных кодах исходная информационная последовательность не разделяется на части, а кодируется непрерывно, причем избыточные элементы формируются на определенных позициях между информационными. Равномерные блоковые коды подразделяются на линейные и нелинейные

Линейные коды образуют наиболее обширный подкласс кодов и определяются тем, что сумма по модулю для двух и более разрешенных комбинаций кода дает комбинацию этого же кода.

Нелинейные коды не обладают этим свойством. Примером нелинейных кодов является код с постоянным весом, применяемый в телеграфии. В некоторых случаях линейные коды называют групповыми, что обусловлено математическим описанием подмножества разрешенных кодовых слов длины n как подгруппы в группе всех слов длины n. Линейный код, в котором информационные и проверочные элементы разделены и расположены на строго определенных позициях, называется систематическим, в отличие от несистематических кодов, в которых нельзя в явном виде выделить информационные и проверочные элементы. Систематические коды получили наибольшее распространение. Систематические коды, как правило, обозначаются (n, k) -кодами и включают: коды с проверкой на четность, коды Хэмминга, циклические коды, коды с повторением, итеративные коды, каскадные, коды Рида—Малера, дециклические коды и много других [4, 32].

В информационных системах для передачи коротких команд управления нашли наибольшее применение циклические коды; для обнаружения ошибок при встроенном контроле аппаратуры обработки — коды с одной проверкой на четность; при хранении информации — коды с повторением; при непрерывной передаче больших массивов измерительных данных — сверточные коды. Для повышения эффективности обработки избыточных кодов развиваются

различные квазиоптимальные методы декодирования, использующие дополнительную информацию о ненадежных элементах передаваемых данных.

2. КРИТЕРИЙ ОЦЕНКИ ЭФФЕКТИВНОСТИ И КАЧЕСТВА ИС

2.1. Выбор критерия

Синтез и анализ любой системы и, в частности ИС, включающей кодирующие и декодирующие устройства, необходимо начинать с выбора и обоснования критериев оценки качества, эффективности и оптимизации. При этом необходимо выбрать такие критерии, которые бы позволили синтезировать оптимальную ИС с учетом наиболее важных показателей эффективности и качества работы. К этим показателям прежде всего следует отнести:

точность работы и контролеспособность собственно системы; быстродействие; объем, массу, сложность; стоимость; информационную способность; вероятность выполнения задачи или надежность системы; помехоустойчивость.

Кроме этих требований, критерии должны обладать определенной конструктивностью, позволяющей легко оценивать их численное значение, качество и эффективность не только процесса получения информации или системы самой по себе с точки зрения приближения ее к потенциальному совершенству, но и сравнительно, по совокупности однотипных систем или процессов.

2.2. Точность работы ИС

Рассмотрим точность работы ИС, реализующей систему алгоритмов контроля по допускам, для чего воспользуемся понятием идеальной и реальной системы контроля и управления, включающей аппаратуру измерения, принятия решения и восстановления [15]. Точность работы ИС обусловливается точностью системы алгоритмов и точностью аппаратуры. Введем понятие идеальной и реальной ИС.

Идеальной назовем такую ИС, которая реализует систему алгоритмов и работает без ошибок в процессе получения информации. При теоретических исследованиях понятием идеальной часто пользуются с целью упрощения анализа и получения качественных показателей различных процессов и систем.

Реальной назовем такую ИС, которая работает с конечной точностью. Под точностью реальной системы будем понимать такую точность, с которой реальная система воспроизводит физическую величину или процесс.

Реальная аппаратура точно как же, как и реальный алгоритм, дает некоторую потерю информации в процессе ее получения. Суммарные потери информации, например при контроле ИС по допускам a, b на параметр x, обусловливаются ошибками первого рода или вероятностью необнаруженных отказов и ошибками второго рода, или вероятностью ложных отказов [4,15,16].

Под необнаруженными отказами понимают существующие отказы ИС, которые не обнаруживаются в процессе контроля и управления вследствие конечной точности работы ИС, или работы ИС с ошибками первого рода. Под ложными отказами понимаются отсутствующие на самом деле отказы, которые ложно обнаруживаются в процессе контроля и управления вследствие конечной точности работы ИС, или работы ИС с ошибками второго рода.

Если ложные отказы имеют место только при измерении параметров вследствие некоторой конечной точности аппаратуры, то необнаруженные отказы имеют место как при проводимых измерениях, так и тогда, когда параметр не измеряется. Вероятность существования необнаруженных отказов параметров, измерение которых не проводится, зависит от собственной безотказности систем, а также от момента измерения параметров и определяется известными методами теории надежности. Полную вероятность необнаруженных отказов необходимо определять с учетом проводимых измерений и без них.

Вероятность необнаруженных отказов и вероятность ложных отказов при контроле параметра x можно определить соответственно формулами [4]

$$P_{\text{н. о}}(t, \tau) = \int_{\infty}^{a} f(x, t, \tau)\left[\int_{a-x}^{b-x} f(z, t, \tau)\, dz\right] dx + \\ + \int_{b}^{\infty} f(x, t, \tau)\left[\int_{a-x}^{b-x} f(z, t, \tau)\, dz\right] dx, \qquad (2.1)$$

где $f(x, t, \tau)$ — закон распределения контролируемого параметра x, имеющего предельно допустимые значения a, b; $f(z, t, \tau)$ — закон распределения ошибок приборов конт-

роля ИС z; t, τ — соответственно текущее время и момент времени, до которого рассматривается ИС:

$$P_{л.\,о}(t, \tau) = \int_a^b f(x, t, \tau)\left[\int_{-\infty}^{a-x} f(z)\,dz + \int_{b-x}^{\infty} f(z, t, \tau)\,dz\right]dx. \quad (2.2)$$

При нормальных законах распределения контролируемых параметров и погрешностей приборов соответственно

$$f(x, t, \tau) = \frac{1}{\sqrt{2\pi}\sigma_x} \exp\,[-(x - m_x)^2/2\sigma_x^2]; \quad (2.3)$$

$$f(t, \tau) = \frac{1}{\sqrt{2\pi}\sigma_z} \exp\,[-z^2/2\sigma_z^2]; \quad (2.4)$$

$$P_{н.\,о}(t, \tau) = \frac{1}{2\sqrt{2\pi}\sigma_x} \int_{-\infty}^{a} \left[\Phi\left(\frac{b-x}{\sqrt{2}\sigma_z}\right) - \Phi\left(\frac{a-x}{\sqrt{2}\sigma_z}\right)\right] \times$$

$$\times \exp\left[-\left\{\frac{(x - m_x)^2}{2\sigma_x^2}\right\}\right] dx + \frac{1}{2\sqrt{2\pi}\,\sigma_x} \int_b^{\infty} \left[\Phi\left(\frac{b-x}{\sqrt{2}\,\sigma_z}\right) -$$

$$-\Phi\left(\frac{a-x}{\sqrt{2}\,\sigma_z}\right)\right] \exp -\left\{\frac{(x - mx)^2}{2\sigma_x^2}\right\} dx. \quad (2.5)$$

$$P_{л.о}(t, \tau) = \frac{1}{2\sqrt{2\pi}\,\sigma_x} \int_a^b \exp\left[-\left\{\frac{(x - m_x^2)}{2\sigma_x^2}\right\} \times\right.$$

$$\left. \times \left[2 + \Phi\left(\frac{a-x}{\sqrt{2}\,\sigma_z}\right) - \Phi\left(\frac{b-x}{\sqrt{2}\,\sigma_z}\right)\right] dx, \quad (2.6)\right.$$

где m_x — математическое ожидание контролируемого параметра; σ_x; σ_z — среднее квадратическое отклонение контролируемого параметра и ошибки прибора, соответственно; $\Phi(a, b, x, \sigma_z)$ — функции Лапласа.

Из выражений (2.5) и (2.6) численным интегрированием находятся вероятности $P_{н.\,о}$ и $P_{л.\,о}$.

Вероятность выполнения задачи ИС, параметр которой контролируется, определяется по теореме о полной вероятности [15]:

$$P(t, \tau) = \frac{P_{S,R}(t, \tau)^*}{P_R(t, \tau)}, \quad (2.7)$$

где

$$P_{S.R}(t, \tau) = [1 - P_{л.\,о}(t, \tau)]\,P_0(t, \tau)$$

— вероятность того, что ИС в результате контроля допущена к выполнению задачи (событие R) и она является в то же

время исправной (событие S); $P_0(t, \tau)$ — вероятность выполнения задачи ИС до контроля; $P_R(t, \tau)$ — вероятность допуска ИС к выполнению задачи, которую можно вычислить с использованием логической табл. 2.1.

Таблица 2.1

Состояние ИС	ИС годна я S	Ложный отказ z'	Необнаруженный отказ z''	ИС допущена к выполнению задачи R
Аппаратура контроля ИС не работает	1	—	—	1
	0	—	—	0
	1	0	—	1
Аппаратура контроля ИС работает	1	1	—	0
	0	—	0	0
	0	—	1	1

Из табл. 2.1 следует, что при работающей аппаратуре контроля логическая функция допуска ИС к выполнению задачи складывается из двух членов

$$F(R) = Sz' \vee Sz'',$$

где S и z рассматриваются как логические переменные.

Переходя от логического оператора к вероятностному, получим вероятность суммы двух несовместных событий

$$P_R(t, \tau) = P_{Sz'}(t, \tau) + P_{Sz''}(t, \tau). \qquad (2.8)$$

Переходя от логических функций к вероятностям, имеем

$$R_R(t, \tau) = P_0(t, \tau)[1 - P_{л.о}(t, \tau)] + P_{н.о}(t, \tau) \times \\ \times [1 - P_0(t, \tau)]. \qquad (2.9)$$

Подставляя выражения (2.8), (2.9) в формулу (2.7), окончательно получим [15]

$$P(t, \tau) = \frac{[1 - P_{л.о}(t, \tau)] P_0(t, \tau)}{[1 - P_{л.о}(t, \tau)] P_0(t, \tau) + [1 - P_0(t, \tau)] P_{н.о}(t, \tau)}. \qquad (2.10)$$

Зная эту вероятность, нетрудно определить оставшуюся энтропию после контроля i-го параметра, формирующего вероятность выполнения ИС задачи

$$H_i(t, \tau) = -\{P_i(t, \tau) \log_2 P_i(t, \tau) + \\ + [1 - P_i(t, \tau)] \log_2 [1 - P_i(t, \tau)]\}, \qquad (2.11)$$

и общую энтропию ИС при контроле независимых параметров

$$H(t,\ \tau) = \sum_{i=1}^{m} H_i(t,\ \tau). \qquad (2.12)$$

Таким образом, на вероятность выполнения задачи ИС существенно влияют вероятности $P_{л.о}(t,\ \tau)$ и $P_{н.о}\ (t,\tau)$, определяемые заданными допусками и точностью ИС.

2.3. Время получения информации

Время, необходимое для получения информации с учетом частоты отказов ИС в первым приближении, можно определить [4] по формуле

$$T_{F_i} = a_{F_i} T_{0F_i} [1 - P_i]^{\mu_{TF_i}}, \qquad (2.13)$$

где a_{F_i} — постоянный коэффициент, определяемый в процессе разработки и эксплуатации системы; в частных простейших случаях его можно полагать равным либо 0, либо 1; T_{0F_i} — время контроля системы, в которой не принимались специальные меры по повышению вероятности безотказной работы; P_i — вероятность безотказной работы системы; μ_{TF_i} — постоянная, характеризирующая степень резервирования, определяемая в процессе производства и эксплуатации.

Время, необходимое для получения информации в зависимости от сложности и вероятности безотказной работы, в первом приближении можнс определить по формуле

$$T_c = a_{c_i} T_{0\,c_i} \left[\frac{1 - P_{0i}}{1 - P_i}\right]^{\mu_{Tc_i}}, \qquad (2.14)$$

где a_{ci} — постоянный коэффициент, определяемый в процессе разработки и эксплуатации системы; в частных простейших случаях его можно полагать равным либо 0, либо 1; T_{0c_i} — время, затрачиваемое в простейшей системе, неусложненной с целью повышения вероятности безотказной работы ее; P_{0_i} — вероятность безотказной работы простейших систем; μ_{Tc_i} — постоянная, определяемая в процессе производства и эксплуатации, характеризующая степень резервирования.

Одним из способов увеличения вероятности безотказ-
гой работы ИС является резервирование ее блоков и подсистем. При резервировании, с одной стороны, уменьшается время контроля и управления ИС в результате увеличения вероятности ее безотказной работы, с другой стороны, увеличивается время контроля и управления за счет усложнения [15].

2.4. Масса и объем аппаратуры ИС

Масса и объем аппаратуры ИС не имеет существенного значения для стационарной системы. В случая передвижной системы характер изменения массы и объема в зависимости от вероятности безотказной работы в первом приближении можно оценить, воспользовавшись формулами для массы:

$$G(t,\ \tau) = G_{\text{А}}(t,\ \tau) + G_{\text{э}}(t,\ \tau), \tag{2.15}$$

где

$$G_{\text{А}}(t,\ \tau) = g_{\text{А}} G_{0\text{А}} \left[\frac{1 - P_0(t,\ \tau)}{1 - P(t,\ \tau)}\right]^{\mu_{G_{\text{А}}}} \tag{2.16}$$

— масса собственно ИС;

$$G_{\text{э}}(t,\ \tau) = g_{\text{э}} C_{0_{\text{э}}} [1 - P(t,\ \tau)]^{\mu_{G_{\text{э}}}} \tag{2.17}$$

— масса оборудования для эксплуатации ИС;
для объема оборудования

$$V(t,\ \tau) = V_{\text{А}}(t,\ \tau) + V_{\text{э}}(t,\ \tau), \tag{2.18}$$

где

$$V_{\text{А}}(t,\ \tau) = e_{\text{А}} V_{\text{ор}}(t,\ \tau) \left[\frac{1 - P_0(t,\ \tau)}{1 - P(t,\ \tau)}\right]^{\mu_{V_{\text{А}}}} \tag{2.19}$$

— объем ИС;

$$V_{\text{э}}(t,\ \tau) = e_{\text{э}} V_{\text{оэ}}(t,\ \tau) [1 - P(t,\ \tau)]^{\mu_{V_{\text{э}}}} \tag{3.20}$$

— объем оборудования для эксплуатации ИС.

Коэффициенты $g_{\text{А}}$, $g_{\text{э}}$, $e_{\text{А}}$, $e_{\text{э}}$ являются постоянными, значение которых определяется в процессе производства и эксплуатации. В простейших случаях эти коэффициенты могут принять значения 0 или 1. В таком случае, когда затраты на снижение массы и объема включаются в общую стоимость, коэффициенты $g_{\text{А}}$, $g_{\text{э}}$, $e_{\text{р}}$, $e_{\text{э}}$ представляют затраты на единицу массы или объема соответственно.

При оценке эффективности и оптимизации процесса получения информации могут учитываться также и другие показатели, например затраты энергии.

2.5. Стоимость получения информации

Средняя стоимость системы определяется суммарными затратами на разработку и эксплуатацию [4]:

$$C = C_{\text{р}} + C_{\text{э}},$$

где $C_{\text{р}}$ — стоимость разработки и изготовления системы $C_{\text{э}}$ — стоимость эксплуатации системы.

В свою очередь,

$$C_{\text{р}} = b_{\text{р}} C_{0\text{р}} \left(\frac{1 - P_0}{1 - P}\right)^{\mu c_{\text{р}}}, \qquad (2.21)$$

где $b_{\text{р}}$ — некоторый постоянный коэффициент, значение которого определяется в процессе производства; в простейшем случае коэффициент $b_{\text{р}}$ может принять значение 0 или 1; $C_{0\text{р}}$ — стоимость простейшей системы при первоначальной вероятности безотказной работы P_0; $C_{\text{др}} \left(\frac{1-P_0}{1-P}\right)^{\mu c_{\text{р}}}$ — стоимость усложненной системы с учетом дополнительных затрат по достижению заданной вероятности безотказной работы P; $\mu c_{\text{р}}$ — постоянная величина, определяемая в процессе контроля и управления.

Стоимость эксплуатации системы

$$C_{\text{э}} = b_{\text{э}} C_{\text{д.э}} (1 - P)^{\mu c_{\text{э}}}, \qquad (2.22)$$

где $b_{\text{э}}$ — постоянный коэффициент, значение которого определяется в процессе эксплуатации; в простейшем случае коэффициент $b_{\text{э}}$ может принимать значение 0 или 1; $C_{\text{д.э}}$ — стоимость эксплуатации простейшей системы; $C_{\text{д.э}}(1 - P)^{\mu c_{\text{э}}}$ — стоимость системы при заданной вероятности безотказной работы P.

Общая стоимость процесса получения информации определяется формулой

$$C_{\Sigma}(t, \tau) = C_c(t, \tau) + \Delta C_T(t, \tau) + \Delta C_G(t, \tau) + \\ + \Delta C_V(t, \tau) + \ldots, \qquad (2.23)$$

где $C(t, \tau)$ — стоимость ИС; $\Delta C_T(t, \tau)$ — стоимость затрат

на получение заданного быстродействия ИС; $\Delta C_G(t, \tau)$ — стоимость затрат на получение заданной массы ИС; $\Delta C_V(t, \tau)$ — стоимость затрат на получение заданного объема системы.

2.6. Обобщенный функционально-статистический критерий оценки эффективности

При выводе критерия оценки эффективности процесса получения информации прежде всего необходимо, чтобы он действительно характеризовал эффективность. Критерий удовлетворит этому требованию, если он характеризует информационную способность ИС [15].

Количество информации, получаемое ИС за интервал времени τ, t при контроле m параметров,

$$I_{\text{р}}(t, \tau) = H_0(t, \tau) - H(t, \tau), \tag{2.24}$$

где $H_0(t,\tau)$ — энтропия ИС, определяемая по формуле, аналогичной (2.12), и характеризующая неопределенность до начала процесса получения информации; $H(t,\tau)$ — оставшаяся энтропия, определяемая по формуле (2.12).

Равенство (2.24) характеризует реальную информационную способность ИС; потенциальная способность ИС

$$I_{\text{п}}(t, \tau) = H_0(t, \tau). \tag{2.25}$$

Эффективность ИС с информационной точки зрения можно оценить критерием

$$\Э_I(t, \tau) = \frac{I_{\text{р}}(t, \tau)}{I_{\text{п}}(t, \tau)} \tag{2.26}$$

или с учетом равенств (2.24), (2.25).

$$\Э_I(t, \tau) = \frac{H_0(t, \tau) - H(t, \tau)}{H_0(t, \tau)}. \tag{2.27}$$

Этот критерий обладает следующими достоинствами. Критерий имеет физический смысл и действительно характеризует эффективность ИС однозначно некоторым числом, изменяющимся от 0 до 1. При этом идеальная ИС имеет эффективность, равную единице, реальная — меньше единицы. При $\Э_I(t, \tau) \leqslant 0$ применять ИС не имеет смысла, так как при $\Э_I(t, \tau) = 0$ она не дает информации, а при $\Э_I(t, \tau) < 0$ дает дезинформацию. Критерий достаточно полно учитывает отношение ИС к самой главной характе-

ристике состояния ИС — вероятности ее безотказной работы, а также к точности и качеству работы ИС.

Однако наряду с указанными достоинствами критерий (2.27) имеет существенные недостатки:

является статической оценкой эффективности, не учитывающей динамики работы ИС; не учитывает сложности и стоимости ИС, а также некоторых других показателей (масса и объем), которые в зависимости от условий применения могут оказаться весьма важными.

Критерием, не обладающим указанными недостатками, можно считать обобщенный статистический критерий оценки эффективности [15]

$$Э(t,\ \tau) = \frac{K_I(t,\ \tau)}{K_{I0}(t,\ \tau)}, \qquad (2\ 28)$$

где

$$K_I(t,\ \tau) = \frac{I_{\max}(t,\ \tau)}{C_\Sigma(t,\ \tau)} \qquad (2.29)$$

— обобщенная статистическая характеристика реальной ИС;

$$I_{\max}(t,\ \tau) = \sum_{i=1}^{m} I_{i\,\max}(t,\ \tau) \qquad (2.30)$$

— максимальное среднее количество информации, получаемое при контроле m параметров за m опытов, выполняемых наилучшей ИС с точки зрения получения $I_{\max}(t,\tau)$; $C_\Sigma(t,\tau)$ — математическое ожидание стоимости реальной ИС, определяемое, например, по формуле (2.23);

$$K_{I_0}(t,\ \tau) = \frac{I_{\max\,\max}(t,\ \tau)}{C_{\min}(t,\ \tau)} \qquad (2.31)$$

— обобщенная потенциальная статистическая характеристика идеального процесса и ИС;

$$I_{\max\,\max}(t,\ \tau) = \sum_{i=1}^{m} I_{i\,\max\,\max}(t,\ \tau) = m(t,\ \tau) \qquad (2.32)$$

— максимальное среднее количество информации, получаемое при контроле m параметров за m опытов, выполняемых наилучшей в указанном ранее смысле ИС при максимальной неопределенности объекта;

$$C_{\min}(t,\ \tau) = C_0(t,\ \tau)$$

— стоимость идеализированной ИС.

С учетом равенств (2.24), (2.25), (2.29), (2.32) можно записать окончательно

$$\Э(t,\ \tau) = \frac{\sum\limits_{i=1}^{m} \{H_{i\,0}(t, \tau) - H_i(t, \tau)\}\, C_{i\,\min}(t,\ \tau)}{H_0 \sum\limits_{i=1}^{m} C_{\Sigma i}(t, \tau)}. \qquad (2.33)$$

Таким образом, для оценки эффективности ИС необходимо:

определить энтропию каждой системы объекта и ИС до получения информации;

определить энтропию объекта и ИС с учетом энтропии, обусловленной ошибками ИС;

определить среднее количество информации, получаемое за каждый опыт;

подсчитать первоначальную стоимость $C_{\min}$ и окончательную реальную стоимость C_{Σ};

произвести расчеты по формуле (2.33).

Достоинством обобщенного статистического критерия оценки эффективности является полнота, наглядность, сравнительная простота и общность, позволяющая одним числом характеризовать как весь процесс контроля и управления, так и по частям, включающим сложные и простые опыты.

При этом диапазон изменения обобщенного статистического критерия для ИС, дающих информацию.

$$0 \leqslant \Э(t,\ \tau) \leqslant 1. \qquad (2.34)$$

Несовершенные ИС имеют $\Э\ (t,\ \tau) \leqslant 0$. При этом $\Э\ (t,\ \tau) < 0$ для систем, дающих дезинформацию о состоянии объекта. Совершенные системы имеют $\Э(t,\ \tau)$, близкий к единице.

2.7. Особенности оценки детерминированных вероятностных характеристик цифровых автоматических систем

Характерной особенностью информационных дискретных систем является наличие квантования по времени и уровню. Кроме того, в дискретных элементах как входные, так и выходные сигналы имеют всего лишь два значения — 0 и 1 и называются двоичными переменными. В связи с этим для анализа и синтеза дискретных

систем применяется алгебра логики и вероятностная логика [15].

Как и для непрерывных систем, математическое соотношение, связывающее входные и выходные переменные дискретной схемы, называется оператором. Оператор определяет функциональные свойства схемы и может быть задан при n входных и m выходных логических переменных в виде некоторой логической функции $F_j(z_1, \ldots, z_n)$, $j = 1, \ldots, m$, где логическим переменным и операторам могут соответствовать различные состояния системы, соответствующие определенным детерминированным критериям оценки эффективности и качества.

В однотактных дискретных системах в один и тот же такт работы набор значений m выходных переменных полностью определяется заданием набора n входных переменных. В многотактных дискретных системах (системах с памятью) набор значений m выходных переменных в данный такт определяется набором значений n входных переменных и состоянием систем в момент их поступления.

Оператор бесповторной дискретной системы с n входами может иметь 2^n различных независимых состояний, каждое из которых может быть описано конъюнкцией всех n переменных в виде $z^{\sigma_1}, \ldots, z_n^{\sigma_n}$, где σ_i равно 0 или 1, при этом $z^0 = \bar{z}$, $z^1 = z$.

Состояние дискретной системы, при котором она выполнит задачу по получению нужного эффекта и качества хотя бы одним из возможных способов, есть

$$F(\bar{z}) = \mathrm{V}_1 \bar{z}_1^{\sigma_1} \ldots \bar{z}_n^{\sigma_n}. \qquad (2.35)$$

Состояние дискретной системы, при которой она не выполнит задачу, есть

$$F(z) = \mathrm{V}_0 z_1^{\sigma_1} \ldots z_n^{\sigma_n}. \qquad (2.36)$$

Следовательно,

$$F(z) \vee \bar{F}(z) \equiv 1. \qquad (2.37)$$

При известных вероятностях логических переменных статистический анализ дискретной системы позволяет выявить общие и усредненные свойства.

Так как логические переменные между собой независимы, то вероятность выполнения задачи системой по получению нужного эффекта и качества определенным способом в соответствии с формулой (2.35)

$$P(t, \tau) = p_1^{\sigma_1}(t, \tau) \ldots p_n^{\sigma_n}(t, \tau), \qquad (2.38)$$

где

$$p_i^{\sigma_i}(t,\ \tau) = \begin{cases} p_i(t,\ \tau) \text{ при } \sigma_i = 1; \\ p_i(t,\ \tau) = 1 - p_i(t,\ \tau) \text{ при } \sigma_i = 0. \end{cases} \quad (2\ 39)$$

Различные возможные способы выполнения задачи системой независимы и несовместимы, поэтому вероятность выполнения задачи системой хотя бы одним способом

$$P(t,\ \tau) = \sum_1 p_1^{\sigma_1}(t,\ \tau) \ldots p_n^{\sigma_n}(t,\ \tau). \quad (2.40)$$

Вероятность невыполнения задачи системой

$$\bar{P}(t,\ \tau) = \sum_0 p_1^{\sigma_1}(t,\ \tau) \ldots p_n^{\sigma_n}(t,\ \tau). \quad (2.41)$$

Очевидно, что

$$P(t,\ \tau) + P(t,\ \tau) = 1. \quad (2.42)$$

Однако для сложных логических функций $F(\bar{z})$ при большом числе логических переменных составление совершенной дизъюнктивно-конъюнктивной нормальной формы представляет известные трудности. В этих случаях значительное упрощение можно получить, применяя методы вероятностной логики, позволяющей непосредственно по любой логической функции $F(\bar{z})$, представленной в виде конъюнкции, определить вероятность $P(t,\ \tau)$.

Пример. Предположим, что работа схемы описывается оператором

$$F(z) = z_1 \vee z_2 z_3.$$

Применяя закон инверсии, представим логическую функцию в виде

$$F(z) = \overline{\bar{z}_1 \bar{z}_2 \bar{z}_3}.$$

Для определения вероятности $P(t,\ \tau)$ заменим

$$z_i \to p_i;$$
$$\bar{z}_i \to \bar{p}_i = 1 - p_i.$$

Получим окончательно

$$P(t,\ \tau) = \overline{\overline{p_1(t,\ \tau)}\, p_2(t,\ \tau)\, p_3(t,\ \tau)} = 1 - [1 - p_1(t,\ \tau)] \times$$
$$\times [1 - p_2(t,\ \tau)\, p_3(t,\ \tau)],$$
$$\bar{P}(t,\ \tau) = 1 - P(t,\ \tau).$$

Кроме того, как это видно из примера, вероятностная логика позволяет одним и тем же выражением описывать как алгоритм, реализуемый дискретной схемой, так и вероятностные характеристики реализации этого алгоритма.

3. ЛИНЕЙНЫЕ КОДЫ

3.1. Постановка задачи

Линейные коды занимают наиболее значимое место среди известных избыточных кодов, и поэтому последующие разделы книги будут в основном посвящены данному типу кодов.

Наибольший интерес представляют линейные коды, которые при заданных k и n обеспечивают наибольшее значение минимального кодового расстояния d_0. Возможно несколько постановок задачи отыскания таких кодов [4]:

1. Из множества $N(n) = 2^n$ кодовых комбинаций выбрать заданное число M комбинаций так, чтобы кодовое расстояние d_0 было максимально возможным.

2. Из множества $N(n)$ выбрать максимально возможное число $M_{\max}$ комбинаций так, чтобы кодовое расстояние оказалось равным заданному.

3. Найти линейный оператор L, однозначно преобразующий k-значные комбинации в n-значные при обеспечении максимально возможного кодового расстояния d_0,

$$X_i(n) = L[X_i(k)],$$

где $X_i(n)$ — i-е кодовое слово из множества $N(n)$; $X_i(k)$— i-е кодовое слово из подмножества $M = 2^k$, причем $k < n$.

Наибольший интерес представляет третья задача, как наиболее конструктивная, непосредственно приводящая к построению кодирующих и декодирующих устройств линейных кодов.

3.2. Построение линейных кодов

Линейные формы. Линейные систематические коды строятся путем добавления к каждой k-значной комбинации исходного кода r проверочных элементов, выбираемых по определенному правилу. Если комбинацию кода записать в виде

$$\alpha_1, \alpha_2 \ldots \alpha_i \ldots \alpha_k, \beta_1 \ldots \beta_j \ldots \beta_r,$$

то α_i — один из k информационных элементов, а β_j — один из r проверочных элементов комбинации, причем α_i и β_j могут принимать значения 0 или 1. В линейных кодах

для определения проверочных элементов β_j используются линейные формы, т. е.

$$\beta_j = L_j(\alpha) = \sum_i \alpha_i, \qquad (3.1)$$

где i принимает значения от 1 до k; Σ — означает, что сложение производится по определенным правилам (для кодов с основанием 2 это правило означает сложение по модулю два).

Порождающая матрица. Зная закон построения кода, можно определить все множество разрешенных кодовых комбинаций и, расположив их друг под другом, получить матрицу, содержащую n столбцов и $(2^k - 1)$ строк. Однако при больших значениях n и k такое описание кода оказывается громоздким. Поэтому код записывается в более компактной форме. Это достигается за счет выбора из всех строк матрицы только линейно независимых, например,

$$G = \begin{bmatrix} 0\ 0\ 1 : 0\ 1\ 1 \\ 0\ 1\ 0 : 1\ 0\ 1 \\ 1\ 0\ 0 : 1\ 1\ 1 \end{bmatrix} = [IG']. \qquad (3.2)$$

Матрица G, содержащая только линейно независимые строки (комбинации) линейного кода, называется порождающей или образующей. Это название обусловлено тем, что матрица дает возможность получить любую разрешенную комбинацию кода путем суммирования по модулю два определенных строк порождающей матрицы.

Проверочная матрица. Существует еще один вариант матричной формы описания линейных кодов, тождественно эквивалентный описанию с помощью линейных форм. Эта матрица содержит r строк и n столбцов и называется проверочной. Ее образование иллюстрируется с помощью табл. 3.1.

Таблица 3.1

Линейные формы	x_1	x_2	x_3	$\beta_1 = x_1 + x_2$	$\beta_2 = x_1 + x_3$	$\beta_3 = x_1 + x_2 + x_3$
Вид	$H = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$	1 0 1	0 1 1	1 0 0	0 1 0	$\begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} = [H'I]$

В проверочной матрице H в каждой строке проставляется 1 на позиции, соответствующей только одному прове-

рочному разряду, а на информационных позициях данной строки 1 записывается для элементов, участвующих в формировании данного проверочного разряда. Проверка включает r этапов по числу строк проверочной матрицы. На каждом этапе осуществляется суммирование по модулю два элементов проверяемой комбинации на тех позициях, на которых стоят единицы данной строки проверочной матрицы. Если результат на всех этапах проверки равен нулю, то проверяемая комбинация принадлежит к разрешенным комбинациям данного кода.

3.3. Процедуры декодирования

Обнаружение ошибок. После того, как исходная кодовая комбинация закодирована в полное кодовое слово X, оно передается по зашумленному каналу. Канал накладывает на кодовое слово вектор помехи

$$l = [l_1,\ l_2,\ \ldots,\ l_n],$$

где $l_i = \begin{cases} 0, & \text{если канал не искажает } i\text{-й элемент} \\ 1, & \text{если канал искажает } i\text{-й элемент.} \end{cases}$

Полученное слово описывается последовательностью

$$Y = [y_1,\ y_2,\ \ldots,\ y_n],$$

где $y_i = X_i + l_i$, или в векторной записи

$$Y = X + l.$$

Декодер вычисляет синдром

$$S^t = HY^t.$$

Если $S^t = 0$, это значит, что или помеха в канале отсутствует [$l = 0$], или вектор помехи совпадает по своей конфигурации с одним из разрешенных кодовых слов. Если синдром $S^t \neq 0$, что свидетельствует о наличии ошибки, то принятое слово Y стирается. Рассмотренный метод декодирования с обнаружением ошибок называется синдромным.

Исправление ошибок методом сопоставления. При сопоставлении принимаемого кодового слова Yl, возможно искаженного, со всеми разрешенными словами, фиксируется число несовпадений и отождествление производится с тем разрешенным словом Xm, от которого Yl отличается в наи-

меньшем числе элементов, т. е. отыскивается минимум выражения

$$\min\{\vartheta(Yl \oplus Xm)\}, \ (m = 1, 2, \ldots, k),$$

где $\oplus$ — операция суммирования по модулю два, с помощью которой осуществляется сравнение комбинаций; ϑ — число несовпадений комбинаций Yl и Xm.

Для двоичных симметричных каналов (ДСК) без памяти метод сопоставлений эквивалентен декодированию по критерию максимума отношения правдоподобия. Он позволяет получить наименьшую величину ошибки декодирования.

Если d_0— минимальное кодовое расстояние, то правильное декодирование произойдет, если комбинация Yl будет отличаться от комбинации Xm числом позиций, не превышающим величины

$$t = \left[\frac{d_0 - 1}{2}\right], \tag{3.3}$$

где знак $[\cdot]$ означает целую часть $\frac{d_0 - 1}{2}$.

В этом случае принято, что избранный код корректирует все ошибки кратности t и менее.

Исправление ошибок методом контрольных чисел. Эквивалентными названиями метода являются табличный метод декодирования или синдромный метод. В основе реализации этого метода находится операция вычисления синдрома (контрольного числа) S для принимаемой кодовой комбинации и его сравнение с табличными значениями. При совпадении с одним из контрольных чисел из таблицы выбирается комбинация ошибки, соответствующая данному контрольному числу. Комбинация ошибки вычисляется из принятой кодовой комбинации, восстанавливая исходную кодовую комбинацию (исправляя ошибки).

Описанное декодирование для ДСК совпадает с декодированием методом сопоставлений и при условии, что все кодовые векторы линейного кода равновероятны. Такое декодирование обеспечивает максимально возможную для данного кода среднюю вероятность правильного декодирования.

При избыточном кодировании очень важным является понимание предельных возможностей рассматриваемых кодов, а именно какое максимальное значение минимального кодового расстояния d_0 может быть достигнуто для (n, k)-кода, и может ли быть улучшен код с параметрами n, k и d_0. Ответ на поставленные вопросы дают верхняя и ниж-

няя границы для минимального кодового расстояния. В настоящее время имеется несколько верхних границ — Плотнина, Хэмминга, Элайеса и др., и одна нижняя граница — Варшамова—Гилберта [28].

3.4. Оценка сложности кодеров и декодеров линейных кодов

Сложность кодеров $S(K, L)$ и декодеров $S(D, L)$ линейных кодов будем характеризовать числом запоминающих элементов (ячеек) $S_p(K, L)$, $S_p(D, L)$ и числом операций, необходимых для кодирования $S_t(K, L)$ или декодирования $S_t(D, L)$ информации.

Такой выбор критериев обусловлен следующими соображениями. Элементы памяти составляют основную долю среди всех элементов кодеров и декодеров, а число необходимых операций обусловливает быстродействие устройств при заданной тактовой частоте.

Кодер линейного кода может быть построен на основе порождающей матрицы G (3.2) или проверочной матрицы H (табл. 3.1). При этом в элементах памяти кодера необходимо хранить только подматрицы G' или H', так как вторая половина матриц G и H представляет собой единичные подматрицы I. Как в одном, так и в другом случае потребуется число элементов памяти [28]

$$S_p(K, L) = kr = R(1 - R)n^2, \qquad (3.4)$$

где R — относительная скорость передачи информации.

При вычислении элементов на проверочных позициях в соответствии с матрицей H необходимо произвести не более k умножений и k сложений по модулю два для одного проверочного элемента. Умножения производятся на элементы, расположенные в строке подматрицы H'. Таким образом, число операций при линейном кодировании не превосходит

$$S_t(K, L) = 2kr = 2R(1 - R)n^2. \qquad (3.5)$$

Далее будет показано, что для некоторых линейных кодов можно значительно уменьшить число ячеек памяти и число операций по сравнению с величинами, которые получаются из (3.4), (3.5).

Декодер линейного кода, осуществляющий обнаружение ошибок, по существу и по сложности не отличается от кодера, так как также требует запоминания подматрицы H' и вычисления проверочных соотношений, определяемых матрицей H.

Более сложным оказывается декодер, исправляющий ошибки в кодовых комбинациях.

Декодер, реализующий метод сопоставлений, должен содержать в памяти полный набор 2^k разрешенных кодовых комбинаций, чтобы осуществлять сравнение с ними принятой кодовой комбинации. В этом случае сложность декодера будет

$$S'_p(D,\ L) = n2^{nR}, \tag{3.6}$$

число операций

$$S'_t(D,\ L) = n2^{nR}. \tag{3.7}$$

Декодер линейного кода, реализующий метод контрольных чисел (рис. 3.1), должен содержать приемный регистр Р на n разрядов, память П1 для подматрицы H' на $R\ (1 - R)n^2$ элементов и память П2, содержащую 2^r лидеров смежных классов по n разрядов каждый. Это позволит по принятому кодовому слову Y вычислить синдром S_i^t, выбрать соответствующий вектор l_t, на сумматоре по модулю М2 исправить ошибку и исправленную комбинацию X выдать получателю. Сложность декодера в этом случае будет

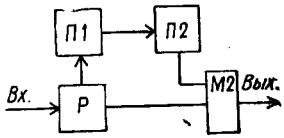


Рис. 3.1

$$S''_p(D,\ L) = n + R\,(1 - R)\,n^2 + n2^{(1-R)n}.$$

Первыми двумя членами при больших значениях n можно пренебречь и тогда окончательно получим

$$S''_p(D,\ Z) = n2^{(1-R)n}. \tag{3.8}$$

Число операций в этом случае будет определяться вычислением синдрома S, что потребует $2kr = 2R\ (1 - R)n^2$ операций; выбором вектора l_t — r операций и сложением $Y \oplus l_t$ — n операций.

Пренебрегая вторым и третьим составляющим при больших значениях n, получим

$$S''_t(D,\ L) = \text{const}\, n^2. \tag{3.9}$$

Сравнение (3.8) и (3.9) с выражениями (3.6) и (3.7) показывает, что декодирование по методу контрольных чисел не приводит к радикальному уменьшению сложности декодера линейного кода. Возрастающее вместе с n как показательная функция число двоичных элементов памяти в декодере приводит к тому, что при современной техноло-

гии построение оптимального декодера в соответствии со схемой, представленной на рис. 3.1, становится нереальным. В последующих разделах будет показано, как можно преодолеть эти трудности.

3.5. Некоторые пути уменьшения сложности декодирующих устройств

Почти во всех случаях представляется возможным за счет снижения быстродействия достичь существенного уменьшения сложности декодирующего устройства при заданной помехоустойчивости.

Рассмотрим принципы построения некоторых типов декодирующих устройств, реализующих эту идею.

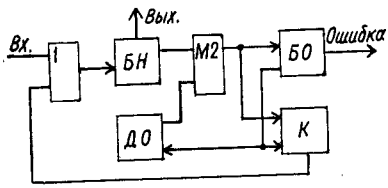


Рис. 3.2

Исправление одиночных и обнаружение многократных ошибок. На рис. 3.2 представлена функциональная схема устройства для исправления одиночных и обнаружения многократных ошибок [12].

Работает устройство следующим образом. Принятая комбинация (n, k)-кода записывается в n-разрядный буферный накопитель (БН) и затем через сумматор по модулю два поступает в блок обнаружения ошибок (БО). При первой выдаче комбинации датчик одиночных ошибок (ДО) не работает и на второй вход сумматора по модулю два сигнал не подается. Это равносильно наложению на комбинацию нулевого вектора ошибки. При необнаружении ошибки БО выдает сигнал на управляющий вход ключа (К) в ДО. Ключ открывается, а ДО по этому сигналу выдает вектор ошибки, аналогичный предыдущему, т. е. нулевой. Комбинация второй раз из БН через сумматор по модулю два и ключ поступает на выход устройства и перезаписывается в БН для обеспечения возможности параллельного съема информации.

При обнаружении ошибки в комбинации после первой ее выдачи включается в работу ДО и комбинация выдается из БН второй раз. На сумматоре по модулю два на комбинацию накладывается вектор ошибки, формируемый ДО, и результат с выхода сумматора поступает в БО. При обнаружении ошибки комбинация из БН выдается в третий раз с наложением очередного вектора ошибок и анализом

в БО. Этот процесс происходит до первого необнаружения ошибки, но не более $(n + 1)$ раз. Если при очередной проверке ошибка в анализируемой комбинации не обнаруживается, то БО выдает сигнал на ключ и ДО. Ключ открывается, а ДО формирует вектор ошибок, аналогичный предыдущему. При очередной выдаче комбинации из БН на сумматоре по модулю два происходит исправление ошибки, и исправленная комбинация через ключ К поступает на выход *1* и перезаписывается в БН. Если в течение $(n + 1)$ проверок отождествления комбинации с кодовой не происходит, то БО вырабатывает сигнал «ошибка».

Определенный интерес представляет рассмотрение принципа действия датчика одиночных ошибок.

На рис. 3.3 и 3.4 изображены функциональные схемы двух вариантов ДО. На рис. 3.3 представлена функцио-

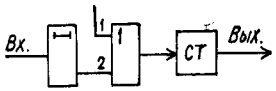


Рис. 3.3

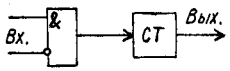


Рис. 3.4

нальная схема ДО, выполненного по схеме деления на $(n + 1)$ с добавлением одного импульса при необнаружении ошибки. Двоичный счетчик СТ, выполненный по схеме деления на $(n + 1)$, при подаче на его вход импульсов тактовой частоты выдает импульсы, сдвинутые относительно друг друга на $(n + 1)$ тактов. При подаче одного импульса добавления при обнаружении ошибки на вход *2* схемы ИЛИ очередной импульс с выхода СТ будет выдан через n тактов, т. е. сформируется вектор ошибки, аналогичный предыдущему. Схема задержки обеспечивает сдвиг импульса добавления на $\tau_з$ для того, чтобы он не совпал с импульсами тактовой частоты.

На рис. 3.4 изображена функциональная схема ДО, выполненного по схеме деления на $(\tau_з - 1)$ с вычислением одного импульса при необнаружении ошибки.

При отсутствии импульса вычитания импульсы тактовой частоты проходят через схему запрета, записываются в двоичный счетчик СТ, на выходе которого появляются импульсы, сдвинутые относительно друг друга на $(n - 1)$ тактов. При поступлении импульса вычитания на запрещающий вход схемы запрета запрещается прохождение одного импульса тактовой частоты в СТ, очередной импульс на выходе которого появится через n тактов, т.е. будет сформирован вектор ошибки, аналогичный предыдущему.

Сложность ДО может быть оценена в элементах памяти как

$$Sd = \mu] \log_2 n [, \qquad (3.10)$$

где μ — коэффициент, учитывающий наличие кроме памяти дополнительных элементов.

Буферный накопитель содержит n элементов памяти, а блок обнаружения ошибок, если он, например, обнаруживает ошибки в комбинациях циклического (n, k)-кода, содержит λn элементов памяти, где λ — коэффициент, зависящий от избыточности кода. Таким образом, сложность рассмотренного декодирующего устройства можно оценить выражением

$$S_p = (1 + \lambda) n + \mu] \log_2 n [. \qquad (3.11)$$

Так как второй член выражения (3.16) значительно меньше первого, то можно записать

$$S_p \approx (1 + \lambda) n, \qquad (3.12)$$

т. е. имеет место линейная зависимость роста сложности декодера от длины комбинации. Это выгодно отличает данное устройство от декодеров, сложность которых оценивается выражениями (3.6) и (3.8).

Однако простота схемной реализации рассмотренного декодера достигается за счет снижения его быстродействия, так как в наихудшем случае для исправления или обнаружения ошибок требуется дополнительная n-кратная прокрутка принятой комбинации с поочередным наложением всех векторов одиночных ошибок, т.е. требуется n^2 дополнительных тактов работы устройства. Это накладывает более жесткие требования на быстродействие элементной базы, используемой для построения схем декодеров. Если не так давно это требование практически исключало применение устройств данного типа; то в настоящее время и в перспективе, учитывая тенденцию непрерывного увеличения быстродействия элементной базы, эти устройства будут находить все более широкое применение.

Возможно некоторое увеличение быстродействия за счет видоизменения процедуры наложения векторов одиночных ошибок и конструкции датчика одиночных ошибок. На рис. 3.5 изображена функциональная схема соответствующего декодера, который работает следующим образом. Принятая комбинация записывается в буферный накопитель

БН и одновременно проверяется на отсутствие ошибок в БО. При отсутствии ошибок комбинация из БН выдается получателю, а при обнаружении ошибок устройство переходит в режим исправления одиночной ошибки. Комбинация из БН с наложенным на сумматоре по модулю два вектором одиночной ошибки выдается в БО и перезаписывается в БН. Если и в данном случае ошибка обнаруживается, комбинация в третий раз выдается в БО и перезаписывается в БН. При этом на сумматоре будет происходить восстановление исходной комбинации и наложение на нее очередного вектора одиночной ошибки, т. е. наложение вектора, являющегося суммой по модулю два очередного и предыдущего векторов одиночных ошибок. Этот процесс происходит до первого необнаружения ошибки, но не более

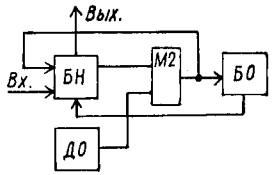


Рис. 3.5

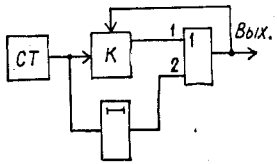


Рис. 3.6

($n + 1$) раза. Если при очередной проверке ошибка в анализируемой комбинации не обнаруживается, то БО разрешает выдачу записанной в БН комбинации на выход устройства.

Если в результате ($n + 1$) проверки отождествления комбинации не произойдет, то последняя стирается, а устройство переходит в режим приема очередного сообщения.

В этом декодере ДО выполняется по схеме, изображенной на рис. 3.6. В исходном состоянии ключ К закрыт. С началом первой выдачи комбинации из БН в БО включается счетчик СТ емкостью ($n + 1$). При обнаружении ошибки после первой проверки СТ не прекращает своей работы. Поэтому при повторной выдаче комбинации из БН счетчик выдает импульс переполнения, который, пройдя элемент задержки на один такт, инвертирует второй разряд комбинации на сумматоре по модулю два. Если ошибка обнаруживается, то при следующей выдаче комбинации сигнал счетчика через открытый ключ восстанавливает второй инвертированный в предыдущей проверке разряд и с помощью элемента задержки инвертирует третий элемент комбинации и т. д.

Если максимальное время декодирования в устройстве (рис. 3.2) составляет

$$t_1^{max} = q\Delta t,$$

где Δt — время одного цикла проверки и q — максимальное число проверок, то максимальное время декодирования в устройстве (рис. 3.5) будет

$$t_2^{max} = (q-2)\,\Delta t.$$

Модифицированный метод сопоставлений. При исправлении ошибок методом сопоставлений (3.2) необходимо запоминание всех разрешенных комбинаций, что обусловливает значительную сложность декодера (3.6).

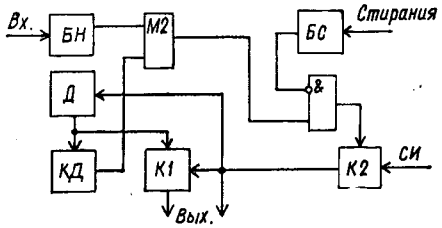


Рис. 3.7

Возможно не запоминание, а последовательное формирование всех комбинаций (n, k)-кода и поочередное сравнение принятой комбинации с формируемыми. В этом случае упрощение декодера также достигается за счет уменьшения его быстродействия.

На рис. 3.7 представлена функциональная схема устройства исправления стираний, в основу построения которого положен модифицированный принцип сопоставлений [8].

Работает устройство следующим образом. Принимаемая кодовая комбинация после записи в буферном накопителе БН поступает на первый вход сумматора по модулю М2. На второй вход сумматора поступают комбинации избыточного (n, k)-кода, формируемые датчиком безызбыточного кода Д и кодером (n, k)-кода КД. Результат сравнения подается на вход схемы запрета, на запрещающий вход которой поступают стирания (ненадежные элементы) из блока стираний БС. Отсутствие сигналов на выходе схемы запрета в течение какого-либо цикла проверки указывает на то, что комбинация безызбыточного кода, формируемая в этом цикле датчиком Д, является информационной. Сигнал опроса в этом случае открывает ключ К2 и проходит в датчик

Д, который формирует комбинацию, аналогичную предыдущей. Эта комбинация как результат декодирования поступает на выход устройства.

3.6. Поэтапное кодирование и декодирование дискретной информации

Под поэтапным кодированием будем понимать такой процесс введения информационной избыточности, который позволяет определить заданную корректирующую способность кода в зависимости от числа учитываемых проверочных элементов.

Линейный код, заданный проверочной матрицей H в канонической форме (см. табл. 3.1), частично удовлетворяет этому определению. Действительно, учет только первого проверочного элемента β_1 позволяет обнаружить часть ошибок, связанных с информационными элементами x_1 и x_2. Второй проверочный элемент β_2 позволяет дополнительно обнаружить ошибки, связанные с элементами x_1 и x_3.

Однако в такой форме записи оказывается затруднительным определение действительных корректирующих возможностей укороченных кодов. Известна процедура I-укорочения кода с минимальным кодовым расстоянием d_0 [12], в соответствии с которой может быть удалено P проверочных элементов. В этом случае полученный I-укороченный код будет иметь минимальное кодовое расстояние $\geqslant d_0 - P$, т. е. кодовое расстояние будет не меньше указанной величины, но в каких случаях оно будет больше и насколько, сказать затруднительно.

Так, линейный (31, 21) — код имеет $d_0 = 5$. Если удалить четыре проверочных элемента, то I-укороченный (27, 21) -код будет иметь $d_0 \geqslant 1$, т. е. определить его корректирующие возможности фактически не представляется возможным. В то же время известно, что циклический укороченный (27, 21) - код имеет минимальное кодовое расстояние $d_0 = 4$.

Полностью удовлетворяет определению поэтапного кодирования информации линейный код, задаваемый проверочной матрицей

$$H = \left[\begin{array}{c|c} H_1 & \\ H_2 & I \\ \vdots & \\ H_q & \end{array}\right] = |H_1, H_2, \ldots, H_q; I|, \qquad (3.13)$$

где H_1 — подматрица размерности $(n_1 - k) \times k$, определяющая проверочные соотношения для (n_1, k)-кода; H_2 — подматрица размерности $(n_2 - k) \times k$, определяющая проверочные соотношения (n_2, k) - кода, и т. д.; H_q — подматрица размерности $(n_q, - k)$, определяющая проверочные соотношения для (n_q, k) - кода; I — единичная матрица размерности $(r_1 + r_2 + \ldots + r_q) \times (r_1 + r_2 + \ldots + r_q)$, где $r_i = n_i - k$.

Этот же код может быть задан при помощи порождающей матрицы

$$G = \left[\begin{array}{|c|c|c|c|c|}\hline I & G_1 & G_2 & \cdots & G_q \\ \hline \end{array}\right] = \left[I; G_1, G_2, \ldots, G_q\right], \qquad (3.14)$$

где I — единичная матрица размерности $k \times k$; G_1 — подматрица размерности $k \times (n_1 - k)$, определяющая проверочные (r_1) элементы (n_1, k) - кода, и т. д.; G_q — подматрица размерности $k \times (n_q - k)$, определяющая проверочные (r_q) элементы (n_q, k) - кода.

В этом случае (n_i, k) - код, где $i = 1,2,\ldots,q$, обладает вполне определенными корректирующими свойствами, характеризуемыми кратностью гарантийно исправляемых (t_i) или гарантийно обнаруживаемых (σ_i) ошибок. Выделение r_i проверочных элементов на i -м этапе декодирования позволяет в простейшем случае гарантийно обнаружить все ошибки до σ_i - кратных включительно, или исправить все ошибки до t_i - кратных включительно. В общем случае оказывается затруднительным определение минимального кодового расстояния $(K + \sum_{j=1}^{\mu} r_j, k)$, которое обозначим d_Σ, μ (при $\mu = 1,2 \ldots, q$). Эта задача решена только для рассеченных кодов максимальной длины (коды Соломона—Штифлера) и для кодов Рида—Соломона, получаемых с помощью китайской теоремы об остатках [12].

Положим, что $(k + r_i, k)$ - код является циклическим, задаваемым образующим полиномом $P_i(X)$, входящим в разложение двучлена $X^n + 1$, причем

$$K + \sum_{j=1}^{q} r_j < n,$$

и образующие полиномы $P_i(X)$ не имеют делителей, кроме единицы.

Произведем оценку минимального кодового расстояния рассеченного кода данного класса. Для этого докажем следующие теоремы.

Теорема 1. Для рассеченного $(K + \sum_{j=1}^{q} r_j, k)$-кода, задаваемого образующими полиномами $P_1(x)$ и $P_2(x)$, всегда выполняется неравенство

$$d_{\Sigma,2} \geqslant \max\{d_1, d_2\} + 1.$$

Рассмотрим $(K + r_1, K)$-код. Если $I(x)$ — произвольная комбинация безызбыточного кода, то возможны следующие случаи:

$$I(x) = F(x) P_1(x).$$

Тогда вес информационной части

$$\omega_i \geqslant d_1, \tag{3.15}$$

а вес проверочной части $\omega_{r_1} = 0$

$$I(x) \neq F(x) P_1(x). \tag{3.16}$$

В этом случае $\omega_{r_1} \geqslant 1$ и $\omega_i + \omega_{r_1} \geqslant d_1$.

Рассмотрим $(K + r_1 + r_2, k)$-код. Если

$I(x) = F(x) P_1(x)$ и $F(x) \neq f(x) P_2(x)$, то $\omega_{r_2} \geqslant 1$ и $\omega_i + \omega_{r_2} \geqslant d_2 + d_1 - 1$.

Следовательно, с учетом (3.15) и (3.16) суммарный вес кодового слова рассеченного кода определится как

$$\omega_{\Sigma_1} \geqslant \max\{d_1 + 1, d_2 + d_1 - 1\} = d_2 + d_1 - 1. \tag{3.17}$$

При $I(x) \neq F(x) P_1(x)$ и $F(x) \neq f(x) P_2(x)$

$$\omega_{r_1} \geqslant 1, \ \omega_{r_2} \geqslant 1, \ \omega_i + \omega_{r_1} \geqslant d_1 \text{ и } \omega_i + \omega_{r_2} \geqslant d_2.$$

Тогда суммарный вес кодового слова рассеченного кода

$$\omega_{\Sigma_2} \geqslant \max\{d_1 + 1, d_2 + 1\} \geqslant \max\{d_1, d_2\} + 1, \tag{3.18}$$

а оценка для нижней границы минимального кодового расстояния может быть получена из (3.17) и (3.18)

$$\omega_{\Sigma} \geqslant \min\{\omega_{\Sigma_1}, \omega_{\Sigma_2}\} = \max\{d_1, d_2\} + 1,$$

что и требовалось доказать

Теорема 2. Если рассчитанный $(K + \sum_{j=1}^{q} r_j, k)$-код задан образующими полиномами $P_1(x), P_2(x), \ldots, P_q(x)$, то

нижняя граница его минимального кодового расстояния определяется выражением

$$d_{\Sigma, q} \geqslant \max\{d_i [i = 1, 2, \ldots, q]\} + (q - 1).$$

Доказательство теоремы сведено в табл. 3.2, где $P_i(x) \sim 1$ указывает на наличие, а $P_j(x) \sim 0$ — на отсутствие данного многочлена в числе сомножителей комбинации $I(x)$. В каждой строке рассматривается один из возможных вариантов структуры исходной комбинации $I(x)$. Так, для первой строки $I(x)$ не содержит в качестве сомножителей ни одного из многочленов $P_i(x)$ $[i = 1,2,\ldots,q]$.

Для второй строки $I(x)$ содержит в качестве одного из сомножителей только многочлен $P_i(x)$. Для последней строки $I(x)$ содержит в качестве сомножителей все многочлены $P_i(x)$. В каждом варианте определяются веса ω_{r_i} проверочных элементов и ω_{Σ_j} — оценки нижней границы для суммарочного веса комбинаций рассеченного кода. В качестве нижней границы выбирается наибольшая из оценок

$$\omega_{\Sigma}^{i} \geqslant \max\{\omega_{\Sigma j} [j = 1, 2, \ldots]\}$$

для каждой строки таблицы. А в качестве оценки нижней границы минимального кодового расстояния рассеченного кода выбирается наименьшая из нижних границ для суммарного веса различных вариантов комбинаций

$$d_{\Sigma, q} = \min\{\omega_{\Sigma}^{i} (i = 1, 2, \ldots)\}. \qquad (3.19)$$

Заметим, что $d_{i,j}$ означает минимальное кодовое расстояние циклического (ni, j, k) - кода, образующим полиномом которого является многочлен

$$P_{ij}(x) = P_i(x) P_j(x).$$

Анализируя последний столбец таблицы в соответствии с (3.19), определяем, что этому условию удовлетворяет содержимое первой строки данного столбца, т. е.

$$\min\{\omega_{\Sigma}^{i}\} = \max\{d_i + q - 1 (i = 1, 2, \ldots, q)\} = \\ = \max\{d_i\} + (q - 1), \qquad (3.20)$$

что и требовалось доказать.

Если $d_i = d [i = 1, 2, \ldots, q]$, то $d_{\Sigma, q} = d + q - 1$ Это вытекает из (3.20) при подстановке значения d_i.

Следствие 2. Если $d_i > d_{i-1}$, то $d_{\Sigma q} = d_q + q - 1$, что следует из аналогичной подстановки.

Таблица 3.2

№ п. п	$P_1(x)$	$P_2(x)$	$P_3(x) \dots P_q(x)$	ω_{r_i}	$\omega_{\Sigma j}$
1	0	0	0 ... 0	$\omega_{r_1} \geqslant 1;\ \omega_{r_2} \geqslant 1,\ \dots\ \omega_{r_q} \geqslant 1$	$\omega_{\Sigma_1} \geqslant d_1 + q - 1;\ \omega_{r_2} \geqslant d_2 + q - 1,\ \dots\ \omega_{\Sigma_q} = d_q + q - 1 \geqslant \max\{\omega_{\Sigma_j}\}$
2	1	0	0 0	$\omega_{r_1} = 0;\ \omega_{r_2} \geqslant 1,\ \dots\ \omega_{r_q} \geqslant 1$	$\omega_{\Sigma_1} \geqslant d_1 + q - 1$ $\omega_{\Sigma i} \geqslant d_{1,j} + q - 2\ (i = 2, 3, \dots\ q) \geqslant \max\{\omega_{\Sigma_j}\}$
3	0	1	0 ... 0	$\omega_{r_1} \geqslant 1;\ \omega_{r_2} = 0,\ \dots\ \omega_{r_q} \geqslant 1$	$\omega_{\Sigma_2} \geqslant d_2 + q - 1$ $\omega_{\Sigma_i} \geqslant d_{2,i} + q - 2\ (i = 1, 3, \dots\ q) \geqslant \max\{\omega_{\Sigma_j}\}$
4	1	1	0 ... 0	$\omega_{r_1} = 0;\ \omega_{r_2} = 0,\ \dots\ \omega_{r_q} \geqslant 1$	$\omega_{\Sigma_1} \geqslant d_{1,2} + q - 2;\ \omega_{\Sigma_2} \geqslant d_{1,2} + q - 2$ $\omega_{\Sigma_i} \geqslant d_{1,2,i} + q - 3 (i = 3, 4 \dots\ q) \geqslant \max\{\omega_{\Sigma_j}\}$
5	0	0	1 ... 0	$\omega_{r_1} \geqslant 1;\ \omega_{r_2} \geqslant 1;\ \omega_{r_3} = 0;\ \dots,\ \omega_{r_q} \geqslant 1$	$\omega_{\Sigma_3} \geqslant d_3 + q - 1$ $\omega_{\Sigma_i} \geqslant d_{3,i} + q - 2\ (i = 1, 2, 4 \dots\ q) \geqslant \max\{\omega_{\Sigma_j}\}$
⋮	⋮	⋮	⋮	⋮	⋮
N	1	1	1 ... 1	$\omega_{r_1} = 0;\ \omega_{r_2} = 0;\ \omega_{r_3} = 0;\ \omega_{r_q} = 0$	$\omega_{\Sigma} \leqslant d_{1,2,3,\dots,q} \geqslant \max\{\omega_{\Sigma_j}\}$

Доказанные теоремы позволяют определить потенциальную корректирующую способность рассмотренного класса рассеченных кодов при их использовании в системах передачи дискретной информации с обратной связью.

3.7. Области применения поэтапных методов принятия решений

В соответствии с теоремой кодирования Шеннона при скоростях передачи сколь угодно близких, но не превышающих пропускную способность канала, может быть достигнута сколь угодно малая вероятность приема сообщения с ошибкой. Математически эта теорема представляется в виде

$$P(\varepsilon) \leqslant \exp\{-nE(R)\},$$

где n — длина блока сообщения; $E(R)$ — функция надежности, зависящая от соотношения скорости передачи R и пропускной способности канала связи С. Она уменьшается при увеличении этого соотношения, равна нулю при $R=C$ и положительна при всех значениях $R < C$.

Таким образом, можно добиться экспоненциального уменьшения вероятности ошибки при возрастании длины блока n. При этом сложность декодеров возрастает как показательная функция (3.6) и основные усилия направляются на создание декодеров, сложность которых возрастала бы медленнее.

Однако, анализируя теорему Шеннона и методы построения кодов, удовлетворяющих этой теореме, приходим к выводу, что помимо сложности существенным недостатком этих кодов является временная задержка в декодировании, обусловленная длиной блока сообщения

$$Z = n\frac{1}{V},$$

где V — скорость модуляции.

Для определенного класса систем этот недостаток становится существенным, приводящим к потере точности и устойчивости систем, или к ограничению области их существования.

Известны работы [19], в которых учитывается старение информации, обусловленное задержкой Z, и устанавливаются зависимости достижимой достоверности информации с учетом фактора задержки.

Известны и традиционные методы уменьшения времени задержки за счет увеличения скорости модуляции в каналах связи с большей пропускной способностью.

Возможен и другой путь [6,12], состоящий в нейтрализации вредного воздействия задержки и основанный на методе поэтапного принятия решений, обладающих различной точностью (достоверностью).

Реальное решение R_d может с определенной вероятностью соответствовать некоторому идеальному решению R_i, что обусловлено конечной точностью представляемой для принятия решения информации. Таким образом, решение может характеризоваться точностью

$$\lambda = F(R_i - R_d)^{-1},$$

или достоверностью, определяемой вероятностью соответствия действительного решения идеальному,

$$P = P(R_d \to R_i).$$

Для обеспечения эффективности управления необходимо, чтобы выполнялись неравенства

$$\lambda \geqslant \lambda_{доп};\ P \geqslant P_{доп},$$

где $\lambda_{доп}$, $P_{доп}$ — допустимые значения указанных характеристик. Решение формируется в течение определенного времени

$$t_р = t_с + t_{пр},$$

где $t_с$ — время сбора информации, а $t_{пр}$ — время обработки и принятия решения. При этом для обеспечения большей точности и достоверности решения требуется большее время $t_р$.

Как правило, в системах задаются одним значением точности или достоверности решения, что не позволяет обеспечить эффективное согласование решающего органа и объекта управления, характеризуемого определенной временной избыточностью.

Передаточная функция объекта с временной избыточностью может быть представлена в виде

$$K(P) = e^{-p\tau} K_0(P),$$

где τ — запаздывание; $K_0(P)$ — оператор движения объекта на фазовой плоскости.

Более эффективное согласование решающего органа с объектом управления указанного типа может быть осуществлено при условии поэтапного формирования и выда-

чи решений, обладающих различной степенью точности для каждого этапа. Это значит, что за время $t_{р_1} < t_р$ формируется предварительное решение R_{D_1}, точность которого меньше заданной, так как для его формирования используется не в полном объеме и менее достоверная информация. Сформированное решение выдается объекту управления, который приступает к его реализации. Решающий орган продолжает прием и обработку более достоверной и полной информации, на основе которой формирует последующее более точное решение R_{D_2}. При этом $t_{р_1} < t_{р_2} < t_р$. Последующее решение сравнивается с предварительным. При совпадении предварительное решение не изменяется, а при несовпадении производится корректировка предварительного решения и объект управления отрабатывает последующее решение до формирования окончательного решения R_D, характеризуемого заданной точностью. В частном случае может быть два решения: предварительное R_{D_1} и окончательное R_D, но всегда должно выполняться условие

$$t_р - t_{р_1} \leqslant \tau,$$

что исключает возникновение необратимых процессов на объекте управления до момента выработки окончательного решения.

Рассмотрим примеры реализации способа поэтапного формирования решения.

В том случае, когда решающий орган формирует решение для человека-оператора в системе человек — машина, первый этап может заключаться в выдаче на индикатор «грубого» отсчета контролируемого параметра, а второй этап — в представлении уточненных данных. Это позволяет уменьшить объем симультанного восприятия информации, что уменьшает напряженность оператора и сокращает число ошибок и время считывания информации.

Рассматривая фрагмент функционирования типовой автоматизированной системы управления, можно отметить, что информация о состоянии объекта управления передается по каналам связи в вычислительный центр для выработки решения, которое возвращается на объект, реализуя алгоритм управления. Допустим, что передача осуществляется с использованием помехоустойчивого составного кода, задаваемого матрицами (3.13) или (3.14), причем $q = 2$, т.е. имеет место два этапа кодирования и декодирования. В этом случае после приема $n_1 = K - r_1$ элементов

и необнаружении ошибок начинается вычислительный процесс по выработке решения. Если прием второй группы (r_2) проверочных элементов не изменяет предварительное решение о принятом сообщении, то время цикла управления будет равно

$$T_{ц_1} = t_{c_1} + t_k + t_{пр},$$

где $t_c = \frac{n_1}{V}$ — время передачи информации о состоянии объекта; t_k — время передачи сигнала управления; $t_{пр}$ — время принятия решения.

В противном случае время одного цикла управления будет

$$T_{ц_2} = t_{c_2} + t_k + t_{пр},$$

где

$$t_{c_2} = \frac{n_1 + r_2}{V}.$$

При этом всегда выполняется условие

$$T_{ц_2} > T_{ц_1}.$$

Поскольку реальные каналы связи характеризуются тем, что большую часть времени в них ошибки отсутствуют, а в отдельные промежутки появляются пачки ошибок, то N циклов управления будут включать V циклов с временем $T_{ц_1}$ и W циклов с временем $T_{ц_2}$, причем $V \gg W$.

Среднее время цикла управления составит

$$\bar{T}_ц = \frac{1}{N}(VT_{ц_1} + WT_{ц_2}),$$

и поскольку $V \gg W$, то $\bar{T}_ц \to T_{ц_1}$ при $N \to \infty$.

Таким образом, всегда будет выполняться условие

$$\bar{T}_ц < T_{ц_2}$$

и, следовательно, точность реализации алгоритма управления повышается.

В информационных сетях с коммутацией каналов применение предлагаемого способа ведет к уменьшению среднего времени задержки сообщения на объекте коммутации. В этих системах выбор канала, по которому необходимо передать принятую информацию, определяется теми указаниями, которые в информации содержатся. Для приема информации требуется время $t_п$, для коммутации канала — $t_к$, для передачи по скоммутированному каналу — $t_{пд}$.

Поскольку время принятия предварительного решения $t_{пр}$ относительно поступающей информации меньше времени $t_п$ приема всей информации, постольку работы по коммутации канала начнутся раньше на время $(t_п — t_{пр})$. В большинстве случаев коммутация будет проведена правильно и передача сообщения начнется на время $(t_п — t_{пр})$ раньше. В тех редких случаях, когда предварительное решение окажется ошибочным, коммутация будет проводиться по окончательному решению, словно предварительной коммутации не было. Следовательно, математическое ожидание времени задержки сообщения на объекте коммутации составит

$$M(t_з) = M(t_{пр}) + M(t_к) + M(t_{пд})$$

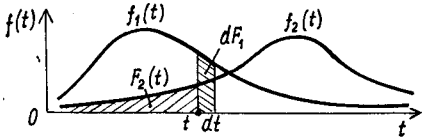


Рис. 3.8

и будет на величину $[M(t_п) — M(t_{пр})]$ меньше времени задержки в существующих системах.

Таким образом, под классом систем, допускающих поэтапную обработку информации, будем понимать системы, обладающие инерционностью $\tau_н$ в отработке управляющих воздействий. При этом область реализации процедур поэтапной обработки задается неравенством

$$\tau_з < \tau_н, \qquad (3.21)$$

где $\tau_з = t_2 — t_1$, t_1 — задержка в принятии предварительного решения; t_2 — задержка в формировании окончательного решения.

В общем случае величины $\tau_н$ и $\tau_з$ могут быть случайными, задаваемыми плотностями распределения вероятностей $g(t)$ и $f(t)$ (рис.3.8).

Предпосылкой к реализации неверного решения является выполнение неравенства

$$\tau_н < \tau_з,$$

которое означает, что окончательное решение будет сформировано к моменту, когда предварительное решение уже выполнилось. Определим вероятность β того, что случайная величина $\tau_н$ примет значение меньшее, чем $\tau_з$. Рассмотрим плоскость $(\tau_з, \tau_н)$. Чтобы $\tau_н$ оказалось меньшим $\tau_з$, необходимо, чтобы точка $(\tau_з, \tau_н)$ попала в полуплоскость

$\tau_н < \tau_з$. Вероятность совместного осуществления неравенств

$$t \leqslant \tau_з < t + dt, \ \tau_н < \tau_з$$

равна $G(t)\, dF(t)$. И так как t может оказаться любым от 0 до $+\infty$, то в силу формулы полной вероятности, обобщенной очевидным образом, искомая вероятность

$$\beta = \int_0^{+\infty} G(t)\, dF(t).$$

Очевидно, если достоверность предварительного решения характеризуется вероятностью P_1, а окончательного — P_2, то необходимо выполнение неравенства

$$(1 - P_1)\, \beta \leqslant 1 - P_2.$$

Рассмотрение существа вопроса и анализ известных систем позволяет определить области возможного использования процедур поэтапного принятия решений: управляющие системы односторонней направленности; системы передачи информации с обратными связями; автоматизированные системы управления; автоматические системы регулирования; системы человек—машина; информационные сети с коммутацией каналов и коммутацией сообщений; системы массового обслуживания; системы передачи данных; системы обработки информации с использованием ЭВМ.

Таким образом, несмотря на то что линейные коды относятся к самым исследованным и потому наиболее используемым кодам, вопрос о соотношении сложности и эффективности кодирующих и особенно декодирующих устройств данных кодов остается открытым.

Это обусловлено развитием элементной базы проектирования и соответственно изменяющимися тенденциями и возможностями построения дискретных устройств, что определяет применение некоторых методов обработки, еще совсем недавно не представляющих интереса для практического использования, а также разработку новых алгоритмов и процедур обработки, совместимых с аппаратно-программными принципами построения устройств передачи и обработки информации в ИС.

Анализ известных методов принятия решений позволяет выделить как наиболее перспективные поэтапные

методы принятия решений, которые характеризуются важным свойством нейтрализации негативных последствий старения информации в ИС и повышения на этой основе эффективности управления.

4. ЦИКЛИЧЕСКИЕ КОДЫ

4.1. Задание циклических кодов

Наиболее распространенным подклассом линейных кодов являются циклические коды. Это обусловлено относительно простым построением кодера и декодера, обнаруживающего ошибки, при достаточно высоких корректирующих способностях кода. Эти коды позволяют преодолеть некоторые трудности, связанные с технической реализацией, свойственные линейным кодам, на которые указывалось в п.3.3. В ИС циклические коды предпочтительны для передачи сообщений небольшой длины, например, команд управления объектами.

Алгебраическая структура циклических кодов впервые была исследована Боузом, Чоудхури и Хоквингемом, поэтому они известны как БЧХ-коды. Эти коды характеризуются следующими свойствами [14]: длиной кодовых последовательностей

$$n = 2^m - 1, \tag{4.1}$$

где $m = 1,2,3,\ldots$;

числом проверочных элементов, не превышающим величины $0,5\ \sigma_m$, т.е.

$$\sigma \geqslant \frac{2r}{m}; \tag{4.2}$$

способностью обнаруживать все пакеты ошибок длины

$$l \leqslant r; \tag{4.3}$$

циклическим сдвигом разрешенной комбинации кода, приводящим к образованию разрешенной комбинации этого же кода.

Возможно задание циклических БЧХ-кодов при помощи порождающих или проверочных матриц аналогично общим правилам построения линейных кодов. Однако воспользуемся более простыми инженерными методиками, базирующимися на алгебраических понятиях. В этом слу-

чае более удобной является запись кодовых комбинаций в виде полинома переменной x:

$$G(x) = a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \cdots + a_1x + a_0.$$

Коэффициенты a_i представляют собой цифры данной системы счисления. В двоичной системе счисления коэффициенты могут принимать одно из двух значений 0 или 1. Так, двоичное четырехразрядное число 1001 может быть записано в виде полинома

$$G(x) = 1x^3 + 0x^2 + 0x + 1 = x^3 + 1 \approx 1001.$$

Это выражение устанавливает однозначное соответствие между двумя формами записи кодовых комбинаций.

Циклические коды образуются умножением каждой комбинации k-элементного безызбыточного кода, выраженной в виде многочлена $G(x)$, на образующий полином $P(x)$ степени $(n - k)$. При этом умножение производится по обычным правилам с приведением подобных членов по модулю два [13]. Следовательно, в случае отсутствия ошибок любая разрешенная кодовая комбинация циклического кода должна разделиться на образующий полином $P(x)$ без остатка. Появление остатка от деления указывает на наличие ошибок в кодовой комбинации. При этом гарантийно обнаруживаются ошибки, определяемые выражениями (4.2) и (4.3). Кроме того, обнаруживается большая часть $\left(\frac{2^r-1}{2^r}\right)$ ошибок более высокой кратности.

Широкое применение нашел другой метод, который в отношении степени избыточности и помехоустойчивости приводит к построению эквивалентного циклического кода. В соответствии с этим методом каждая кодовая комбинация первичного кода $G(x)$ умножается на одночлен X^{n-k}. Это эквивалентно приписыванию справа к комбинации $G(x)$, записанной в двоичной форме, $(n - k)$ нулей. Произведение $G(x)\ x^{n-k}$ делится на образующий полином $P(x)$ степени $(n - k)$:

$$\frac{x^{n-k}G(x)}{P(x)} = Q(x) + \frac{R(x)}{P(x)}, \qquad (4.4)$$

где $Q(x)$ — частное от деления такой же степени, как и $G(x)$; $R(x)$ — остаток.

Так как частное $Q(x)$ имеет такую же степень, как и кодовая комбинация $G(x)$, то, следовательно, $Q(x)$ является кодовой комбинацией этого же простого k-элементного кода.

Умножая обе части равенства на $P(x)$ получим

$$M(x) = Q(x)\,P(x) = x^{n-k}G(x) + R(x). \qquad (4.5)$$

Здесь знак минус заменен знаком плюс, так как сложение и вычитание по модулю два — операции эквивалентные.

Из полученного равенства видно, что кодовая комбинация циклического кода может быть получена двумя эквивалентными методами, причем второй метод приводит к построению систематического циклического кода, в котором информационные и проверочные элементы разделены. А так как информационные элементы непосредственно принимаются из канала связи, то эффект размножения ошибок в информационной части кодовой комбинации будет отсутствовать.

4.2. Коды с постоянной четностью единиц

Наименьшей избыточностью обладают циклические $(k + 1, k)$ - коды, имеющие один проверочный элемент и получившие название кодов с постоянной четностью единиц. Построение этих кодов осуществляется при помощи образующего полинома

$$P(x) = x + 1$$

методами, изложенными в п.4.1. При этом разрешенные кодовые слова циклического $(k + 1, k)$-кода во всех случаях содержат четное число единиц. Докажем это свойство, используя метод построения циклических кодов, основанный на умножении комбинаций $G(x)$ на образующий полином $P(x) = x + 1$.

Так как образующий полином $P(x)$ является двучленом, то произведение $G(x)P(x)$ независимо от числа членов первого сомножителя $G(x)$ всегда будет содержать четное число членов.

Доказанное свойство определяет метод построения кодов с постоянной четностью единиц, наиболее пригодный для технической реализации и приводящий к получению кодовых комбинаций систематического кода.

Коды с постоянной четностью единиц позволяют обнаружить любые ошибки нечетной кратности, т. е. для этих кодов $\sigma = 1,3,5,\ldots, l$, где $l = k$ для нечетных значений k и $l = k + 1$ для четных значений k.

4.3. Помехоустойчивость циклических кодов

Циклические коды можно использовать в следующих режимах: для исправления ошибок; для обнаружения ошибок; для исправления и обнаружения ошибок.

Достоверность передаваемой информации. Наиболее предпочтительным является использование циклических кодов в режиме обнаружения ошибок, так как при этом достигается наибольшая достоверность передаваемой информации, определяемая вероятностью необнаруженных ошибок (1.7):

$$P_{\text{н. о}} = \frac{1}{2^r} P[\geqslant (\sigma + 1), n], \tag{4.6}$$

где $P[\geqslant (\sigma + 1), n]$ — вероятность ошибок кратности, большей чем σ; σ — кратность гарантийно обнаруживаемых циклическим кодом ошибок; $\frac{1}{2^r}$ — коэффициент, учитывающий долю необнаруживаемых ошибок более высокой кратности, чем σ.

Для ДСК без памяти с учетом выражения (1.5) получим

$$P_{\text{н. о}} = \frac{1}{2^r} \sum_{i=\sigma+1}^{n} C_n^i P_0^i (1 - P_0)^{n-i}. \tag{4.7}$$

При $nP_0 \ll 1$, ограничиваясь первым членом суммы, получим приближенное выражение, пригодное для инженерных расчетов:

$$P_{\text{н. о}} \cong \frac{1}{2^r} C_n^{\sigma+1} P_0^{(\sigma+1)}. \tag{4.8}$$

При передаче информации в канале связи с группирующимися ошибками, определяя $P[\geqslant(\sigma + 1), n]$ из (1.7) и подставляя в (4.6), получим приближенное выражение

$$P_{\text{н. о}} = \frac{1}{2^r} \left[\frac{n}{\sigma + 1}\right]^{1-\alpha} P_0. \tag{4.9}$$

Для точных расчетов вероятность $P[\geqslant(\sigma + 1), n]$ должна определяться из выражения (1.8).

Использование циклических кодов для исправления ошибок приводит к снижению достоверности передаваемой информации, которая может быть определена по формулам (4.6), (4.7) и (4.9), если исключить коэффициент $\frac{1}{2^r}$ и вместо

параметра σ подставить параметр t, который определяет кратность гарантийно исправляемых циклическим кодом ошибок и связан с σ соотношением

$$t = \left[\frac{\sigma}{2}\right]. \tag{4.10}$$

Режим одновременного исправления и обнаружения ошибок по достигаемой достоверности занимает промежуточное положение между рассмотренными режимами. Вероятность необнаружения ошибок в этом случае может быть вычислена по формулам (4.6) — (4.8), если параметр σ уменьшить на величину t.

В режиме исправления ошибок достоверность снижается по сравнению с режимом обнаружения ошибок. Это позволяет сделать вывод, что наиболее рациональными следует считать такие системы передачи дискретной информации, в которых циклические коды используются для обнаружения ошибок.

В некоторых случаях, когда используются каналы связи достаточно низкого качества, находит применение режим одновременного исправления и обнаружения ошибок. Это позволяет уменьшить потери информации и увеличить относительную скорость передачи.

Потери информации. Потери информации имеют место в том случае, когда возникает ошибка, необнаруживаемая циклическим кодом, поэтому для режима обнаружения ошибок можно записать, что

$$P_{\text{п}} = P_{\text{о. о}} = P_{\text{ош}} - P_{\text{н. о}}, \tag{4.11}$$

где $P_{\text{ош}}$ — вероятность появления любой ошибки в кодовой комбинации, определяемая выражением (1.1)—(1.3) или (1.6). Так как в реальных системах $P_{\text{н. о}} \ll P_{\text{ош}}$, то можно положить, что

$$P_{\text{п}_1} \approx P_{\text{ош}}. \tag{4.12}$$

В режиме одновременного исправления и обнаружения ошибок исправляются ошибки до t-кратных включительно. Поэтому потери будут обусловлены абсолютным большинством ошибок, кратность которых превышает t, т.е.

$$P_{n_2} \cong \sum_{i=t+1}^{n} P(i, n), \tag{4.13}$$

где $P(i, n)$ — вероятность появления i-кратных ошибок.

Для ДСК без памяти

$$P_{\text{п}_3} = \sum_{i=t+1}^{n} C_n^i P_0^i (1 - P_0)^{n-t} \approx C_n^{t+1} P_0^{t+1}. \qquad (4.14)$$

Для канала с группирующимися ошибками с учетом (1.7) получим приближенное выражение

$$P_{\text{п}_3} \cong \left(\frac{n}{t+1}\right)^{1-\alpha} P_0, \qquad (4.15)$$

а на основании (1.8) будем иметь точную формулу для определения потерь информации

$$P_{\text{п}_3} = n^{1-\alpha} P_0 \prod_{i=2}^{t+1} \frac{\left(\frac{i-1}{n}\right)^{1-\alpha} - \frac{i-1}{n}}{\left(\frac{i}{n}\right)^{1-\alpha} - \frac{i-1}{n}}. \qquad (4.16)$$

Вероятностные характеристики кодов с постоянной четностью единиц. Как отмечалось ранее, коды с постоянной четностью единиц обнаруживают все ошибки нечетной кратности, поэтому с учетом (1.2) вероятность необнаружения ошибок может быть вычислена по формуле

$$P_{\text{н. о}} = \sum_{i=2,4,\ldots}^{n} P(i, n), \qquad (4.17)$$

где i принимает только четные значения.

Для ДСК без памяти выражение (4.17) на основании (1.3) преобразуется к виду

$$P_{\text{н. о}} = \sum_{i=2,4,\ldots}^{n} C_n^i P_0^i (1 - P_0)^{n-i} \approx C_n^2 P_0^2. \qquad (4.18)$$

В каналах с группирующимися ошибками приближенное выражение для определения вероятности необнаружения ошибок может быть получено из (1.7):

$$P_{\text{н. о}} \cong \left(\frac{n}{2}\right)^{1-\alpha} P_0, \qquad (4.19)$$

а точная формула — путем подстановки (1.8) в (4.16):

$$P_{\text{н. о}} = \sum_{i=2,4,\ldots}^{n} [P(\geqslant i, n) - P(\geqslant i+1, n)] =$$

$$= \sum_{i=2,4,\ldots}^{n} n^{1-\alpha} P_0 \prod_{j=2}^{i} \frac{\left(\frac{j-1}{n}\right)^{1-\alpha} - \frac{j-1}{n}}{\left(\frac{j}{n}\right)^{1-\alpha} - \frac{j-1}{n}} \left(1 - \frac{\left(\frac{i}{n}\right)^{1-\alpha} - \left(\frac{i}{n}\right)}{\left(\frac{i+1}{n}\right)^{1-\alpha} - \left(\frac{i}{n}\right)}\right). \qquad (4.20)$$

Циклический (n,k)-код, построенный при помощи образующего полинома $P(x)$ и не обладающий свойством постоянной четности единиц, может прибрести это свойство, если образующий полином $P(x)$ домножить на двучлен $(x-1)$ и формировать кодовые комбинации нового $(n+1, k)$-кода на основании полинома

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

В этом случае циклический $(n+1, k)$-код приобретает свойство дополнительно обнаруживать все ошибки нечетной кратности и, следовательно, для определения вероятности необнаружения ошибок по выражениям (4.6) — (4.9) необходимо σ увеличить на единицу и присваивать i только четные значения.

4.4. Алгоритм нахождения циклического кода, удовлетворяющего заданной достоверности

Исходными данными для построения циклического кода являются: $P^{\partial}_{\text{н.о}}$ — допустимое значение вероятности необнаружения ошибок; k — число информационных элементов исходного безызбыточного кода; P_0 — вероятность искажения одного элемента кодовой комбинации, характеризующая качество канала связи. При использовании канала связи с группирующимися ошибками дополнительно задается коэффициент группирования α.

На рис. 4.1 приведена структурная схема алгоритма нахождения образующего полинома циклического кода, удовлетворяющего заданной достоверности.

1. На первом этапе определяют n^* как функцию m, используя выражение (4.1), удовлетворяющее условию

$$n^*(m-1) < k < n^*(m). \qquad (4.21)$$

2. По заданному k и найденному значению $n^*(m)$ определяют число проверочных элементов

$$r^* = n^*(m) - k. \qquad (4.22)$$

3. Уточняют число проверочных элементов по таблице в [35], выбирая ближайшее значение $r_{\text{т}} \leqslant r^*$.

4. Определяют табличное значение кратности гарантийно обнаруживаемых ошибок $\sigma_{\text{т}}$, соответствующее $r_{\text{т}}$.

5. Так как все табличные коды могут быть дополнены проверкой на четность, то определяют максимальную избыточность

$$r_{\max} = r_{\text{т}} + 1$$

и максимальную кратность гарантийно обнаруживаемых ошибок

$$\sigma_{max} = \sigma_т + 1.$$

6. Уточняют длину кодовой комбинации циклического кода

$$n = k + r_{max}.$$

Если $n < n^*(m)$, то будет иметь место так называемый укороченный циклический (n, k)-код, который по коррек-

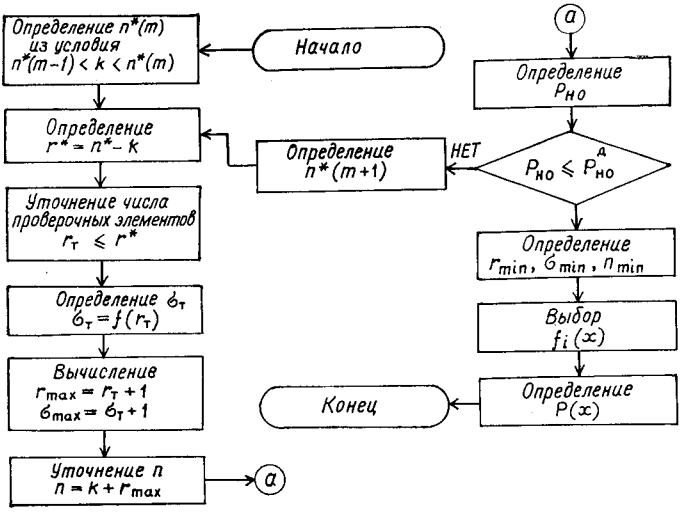


Рис. 4.1

тирующей способности эквивалентен полному циклическому $(n^*, n^* - r_{max})$-коду, число информационных элементов которого больше на величину $(n^* - n)$.

7. Для найденных значений n, r_{max} и σ_{max}, используя выражения (4.7), (4.8) или (4.9) определяют вероятность необнаружения ошибок $P_{н.о}$.

8. Проверяют условие

$$P_{н.о} \leqslant P^{д}_{н.о}. \qquad (4.23)$$

9. При невыполнении условия (4.23) выбирают $n^*(m+1)$ и повторяют п. 2—8.

10. Если условие (4.23) выполняется, то методом последовательного приближения, например дихотомии (половин-

ного разбиения), или методом перебора, определяют минимальное число проверочных элементов r_{min} и соответствующие значения n_{min} и σ_{min}, для которых выполняется условие (4.23).

В этом случае

$$n_{min} = k + r_{min},$$

и

$$r_{min} = r_{т\,min} \text{ и } \sigma_{min} = \sigma_{тmin} \tag{4.24}$$

при отсутствии дополнительной проверки на четность или

$$r_{min} - r_{т\,min} + 1 \text{ и } \sigma_{min} + \sigma_{т\,min} + 1 \tag{4.25}$$

при введении дополнительной проверки на четность.

11. По таблицам [35] выбирают образующий полином $P(x)$, соответствующий вычисленным значениям r_{min} и σ_{min}. Для случая, определенного выражением (4.24),

$$P(x) = \prod_{i=1}^{\lambda} f_i(x),$$

где $f_i(x)$ — неприводимые многочлены, индекс i которых возрастает с увеличением числа проверочных элементов $r_т$; λ — индекс, соответствующий $r_{т\,min}$.

При введении дополнительной проверки на четность (4.25)

$$P(x) = \prod_{=1}^{\lambda} f_i(x)(x+1).$$

С целью сокращения записи все многочлены в [35] указаны в восьмеричном представлении. При такой записи каждый символ обозначает три двоичных знака в соответствии со следующим кодом:

0 ↔ 000	4 ↔ 100
1 ↔ 001	5 ↔ 101
2 ↔ 010	6 ↔ 110
3 ↔ 010	7 ↔ 111

Коэффициенты многочленов в двоичной записи расположены в порядке убывания, так что коэффициент при слагаемом высшего порядка расположен слева.

Например, число 45 в коде $C\,n^* = 31$ обозначает многочлен 5-й степени. В двоичной записи этому числу эквивалентно число

100 101

и соответствующий многочлен равен

$$f(x) = x^5 + x^2 + 1.$$

Образующий полином $P(x)$ является предпосылкой для построения кодирующего и декодирующего устройств циклического кода.

4.5. Принципы построения кодирующих и декодирующих устройств

Схемные реализации кодирующих и декодирующих устройств определяются способами задания циклических кодов. Рассмотрим некоторые варианты этих устройств.

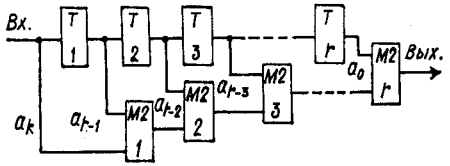


Рис. 4.2

Кодирующие и декодирующие устройства, задаваемые умножением на образующий полином. В основу построения этого типа устройств положены многотактные линейные фильтры Хаффлина (28). На рис. 4.2 представлена функциональная схема кодирующего устройства (кодера), осуществляющего умножение информационного многочлена $G(x)$ (4.4) на образующий полином

$$P(x) = a_{n-k}x^{n-k} + a_{n-k-1}x^{n-k-1} + \cdots + a_i x^i + \cdots + a_1 x + a_0.$$

Устройство содержит регистр сдвига, число разрядов которого обусловливается степенью образующего полинома, и сумматоры по модулю два, число в связи с которыми определяются коэффициентами a_i. Если $a_i = 1$, то сумматор по модулю два и соответствующая связь имеют место, если $a_i = 0$ — сумматор и соответствующая связь отсутствуют.

Работа кодера сводится к следующему. При подаче на его вход информационного элемента a_{k-1} (коэффициента при старшем члене многочлена $G(x)$) на выходе образуется произведение $a_{k-1}\, a_{n-k}$, а значение a_{k-1} запоминается в первом разряде регистра сдвига. При втором такте работы схемы на выходе образуется элемент, равный $a_{k-1}\, a_{n-k-1} \oplus \oplus a_{k-2}\, a_{n-k}$, причем в первом разряде регистра сдвига

оказывается записанным коэффициент a_{k-2}, а во втором — коэффициент a_{k-1}.

После n-го такта процесс формирования комбинации заканчивается. При этом первыми на выходе кодера образуются коэффициенты при старших членах многочлена $M(x) = G(x)\,P(x)$. Кодирующее устройство описанного типа, осуществляющее умножение на образующий полином

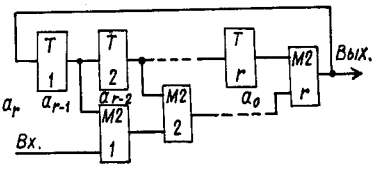


Рис. 4.3

$P(x) = x^3 + x + 1$, приведено на рис. 4.3. Процесс формирования комбинации $M(x) = G(x)\,P(x) = (x^3 + 1) + (x^3 + x + 1)$ по тактам представлен в табл. 4. 1.

Таблица 4.1

Вход $[G(x)]$	Состояние разрядов регистра сдвига			Выход $[M(x)]$
	1	2	3	
1	1	0	0	1
0	0	1	0	0
0	0	0	1	1
1	1	0	0	0
0	0	1	0	0
0	0	0	1	1
0	0	0	0	1

Декодирующее устройство (декодер), осуществляющее деление на образующий полином $P(x)$, также выполняется на регистре сдвига с обратными связями через сумматоры по модулю два. На рис. 4.4 приведена схема декодера для деления на полином $P(x)$. Он содержит число разрядов регистра сдвига, соответствующее степени полинома $P(x)$, а количество сумматоров по модулю два с соответствующими связями определяется коэффициентами a_i.

Декодирующее устройство описанного типа, осуществляющее деление на образующий полином $P(x) = x^3 + x + 1$,

приведено на рис. 4.5, а процесс декодирования (деления) представлен в табл. 4.2, 4.3.

В декодере (рис. 4.5) информационные элементы формируются на k последних тактах работы схемы и остаток от деления оценивается по состоянию разрядов регистра сдвига после n тактов работы.

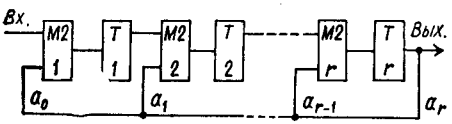


Рис. 4.4

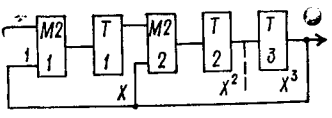


Рис. 4.5

Таблица 42

Вход [M (x)]	Состояние разрядов регистра сдвига			Выход [G (x)]
	1	2	3	
1	1	0	0	0
0	0	1	0	0
1	1	0	1	0
0	1	0	0	1
0	0	1	0	0
1	1	0	1	0
1	0	0	0	1
	$R(x)=0$			

Таблица 43

Вход [M'(x)]	Состояние разрядов регистра сдвига			Выход [G'(x)]
	1	2	3	
1	1	0	0	0
1	1	1	0	0
1	1	1	1	0
0	1	0	1	1
0	1	0	0	1
1	1	1	0	0
1	1	1	1	0
	$R(x)=x^2+x+1$			

Для примера в табл. 4.3 демонстрируется процесс декодирования комбинации $M'(x) = M(x) \oplus l(x)$, где вектор ошибки $l(x) = x^5 \approx 0100000$, т. е ошибка имеет место во втором разряде кодовой комбинации.

На рис. 4.6. в общем виде, а на рис. 4.7 для полинома $P(x) = x^3 + x + 1$ приведены схемы декодеров, эквивалентных декодерам на рис. 4.4 рис. 4.5 соответственно, которые также позволяют получить частное и оценить наличие или отсутствие ошибок в декодируемой комбинации.

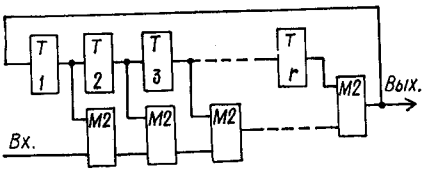


Рис. 4.6

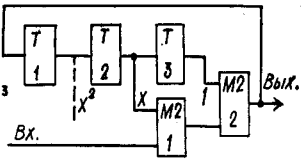


Рис. 4.7

Процесс декодирования декодером (рис. 4.7) комбинаций $M(x)$ и $M'(x)$ представлен в табл. 4.4. 4.5, из которых видно, что информационные элементы формируются на первых k тактах, а наличие или отсутствие ошибок оцени-

Таблица 4.4

Вход $[M'(x)]$	Состояние разрядов регистра сдвига			Выход $[G(x)]$
	1	2	3	
1	1	0	0	1
1	1	1	0	1
1	0	1	1	0
0	0	0	1	0
0	1	0	0	1
1	1	1	0	1
1	0	1	1	0
		$R'(x)$		$R'(x)$

Таблица 5.5

Вход $[M(x)]$	Состояние разрядов регистра сдвига			Выход $[G'(x)]$
	1	2	3	
1	1	0	0	1
0	0	1	0	0
1	0	0	1	0
0	1	0	0	1
0	0	1	0	0
1	0	0	1	0
1	0	0	0	0
		$R'(x)$		$R'(x)$

вается по $(n - k)$ последним элементам на выходе декодера или по состоянию разрядов регистра сдвига после n тактов работы. При этом нулевые элементы характеризуют отсутствие ошибок, а наличие хотя бы одного ненулевого элемента фиксирует факт искаженности комбинации (вых. 2 декодера). Преимуществом декодеров (рис. 4.6 и 4.7) является большее быстродействие, обусловленное тем, что в большинстве случаев факт искаженности комбинации устанавливается до истечения n тактов работы схемы. Так, для рассмотренного примера декодер (табл. 4.5) обнаружит ошибку на $(k + 1)$ такте работы схемы.

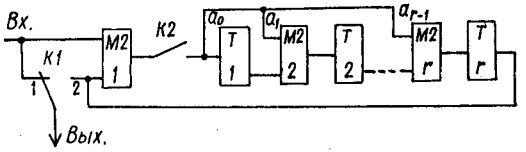


Рис. 4.8

Кодирующие и декодирующие устройства, основанные на вычислении остатка от деления. В основу построения кодирующего устройства положена схема деления (рис. 4.4) на полином. На рис. 4.8 изображена структурная схема кодера, работающего на указанном принципе. В исходном состоянии ключ К1 находится в положении *1*, ключ К2 замкнут. В течение K тактов информационные элементы поступают одновременно на выход кодера и в регистр сдвига, где за k тактов образуется остаток $R(x)$ от деления $G(x)\,x^{n-k}$ на образующий полином $P(x)$. Затем ключ К2 размыкается, а К1 переводится в положение *2* и остаток $R(x)$ поступает на выход кодера.

На рис. 4.9 структурная схема (рис. 4.8) детализирована применительно к случаю $P(x) = x^3 + x + 1$, а в табл. 4.6 показан процесс вычисления остатка $R(x)$.

Таблица 4.6

Вход [G(x)]	Состояние разрядов регистра сдвига			Выход [M(x)]
	1	2	3	
1	1	1	0	1
0	0	1	1	0
0	1	1	1	0
1	0	1 →	1	1
		R(x)		

Для построения декодеров могут быть использованы схемы деления на полином $P(x)$ (рис. 4.4), но, как правило, применяется схема вычисления остатка, принцип построения которой соответствует схеме кодера (рис. 4.9). Отличие состоит в том, что отсутствует ключ К2, ключ К1

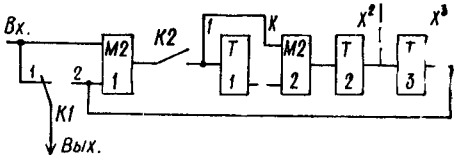


Рис. 4.9

имеет только положение *1* и для анализа остатка введена схема ИЛИ с $(n - k)$ входами и схема *И*, на которой синхроимпульсом СИ на $(n + 1)$-м такте опрашивается состояние разрядов регистра сдвига (рис. 4.10).

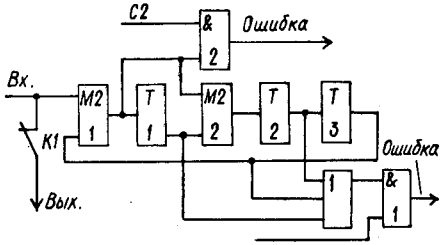


Рис. 4.10

В табл. 4.7 показан процесс вычисления остатка для неискаженной комбинации $M(x)$, а в табл. 4. 8 — для комбинации $M'(x)$, у которой искажен второй разряд.

Таблица 4.7

Вход	Состояние разрядов регистра сдвига			Выход
	1	2	3	
1	1	1	0	1
0	0	1	1	0
0	1	1	1	0
1	0	1	1	1
1	0	0	1	
1	0	0	0	
0	0	0	0	

Таблица 4.8

Вход [M'(x)]	Состояние разрядов регистра сдвига			Выход [G'(x)]
	1	2	0	
1	1	1	0	1
[1]	1	0	1	[1]
0	1	0	0	0
1	1	0	0	1
1	1	0	0	
1	1	0	0	
0	0	1	0	

Из табл. 4. 7, 4.8 видно, что анализировать остаток можно по состоянию первого разряда сдвига в течение $(n - k)$ последних тактов приема информации. В это время подается синхросигнал С2. Появление сигнала на выходе схемы И2 свидетельствует об искаженности комбинации.

Сложность кодеров циклических кодов и декодеров, работающих в режиме обнаружения ошибок, определяется числом разрядов регистра сдвига и количеством сумматоров по модулю два. В элементах памяти сложность оценивается выражением

$$S_p \approx \lambda n, \tag{4.26}$$

где λ — коэффициент пропорциональности, зависящий от избыточности кода.

В отличие от выражений (4.22) и (4.23) зависимость (4.26) носит линейный характер, что и обусловливает широкое применение циклических кодов в режиме обнаружения ошибок.

Уменьшение сложности кодеров и декодеров циклических кодов. В некоторых случаях возможно дополнительное упрощение кодеров и декодеров, построенных на базе устройств для умножения на неприводимый полином $P(x)$ [12]. Это оказывается возможным, если полином $P(x)$ обладает полной или частичной симметрией.

Так, если неприводимый полином

$$P(x) = x^5 + x^4 + x^3 + x + 1 \approx 111011 \approx \overbrace{(x^2 + x + 1)}^{P_1(x)} x^3 + \overbrace{+ (x + 1)}^{P_2(x)},$$

то известное устройство для умножения (рис. 4.2) должно

содержать пять разрядов регистра сдвига и четыре двухвходовых сумматора по модулю два. На рис. 4.11 приведена функциональная схема устройства для умножения на полином $P(x)$, эквивалентного известному по выполненным функциям и содержащего пять разрядов регистра сдвига и три двухвходовых сумматора.

Работает устройство следующим образом. С поступлением информационной последовательности $G(x)$ в регистр *1* на выходе сумматора *2* появляются двоичные элементы, соответствующие произведению $G(x)\,P_1(x) = G(x)\,(x^2 + x + 1)$, так как сумматор связан с входом и параллельными выходами регистра *1* через сумматор В. В эти же мо-

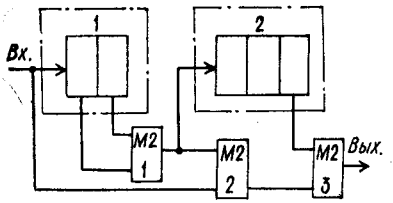


Рис. 4.11

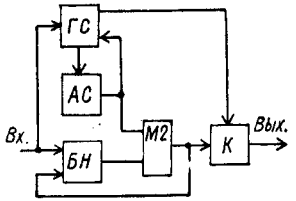


Рис. 4.12

менты времени появляются двоичные элементы, соответствующие произведению $G(x)\,P_2(x) = G(x)\,(Ox^2 + x + 1) = G(x)\,(x + 1)$, поскольку сумматор *1* связан с параллельными выходами регистра *1*. Выход сумматора *1* дополнительно связан с входом линии задержки *2*, чем достигается деление произведения $G(x)\,P_2(x)$ на величину x^3 (т.е. задержка на три такта). С выхода линии задержки *2* сигнал произведения поступает на один из входов сумматора *3*, на другой вход которого с выхода сумматора *2* подается произведение $G(x)\,P_1(x)$.

На выходе сумматора 3 получаем сумму по модулю два указанных сигналов, т. е.

$$G(x)\,P_1(x) + G(x)\,P_2(x)\,\frac{1}{x^3} = G(x)\,[P_1(x)\,x^3 + P_2(x)]\,\frac{1}{x^3} =$$

$$= G(x)\,P(x)\,\frac{1}{x^3}.$$

В полученном выражении дробь $\frac{1}{x^3}$ означает задержку сигнала в линии задержки *2* и на результат произведения на влияет.

Исправление ошибок для коротких циклических кодов. Процедура исправления ошибок для циклических кодов

основывается на вычислении синдрома (остатка от деления) и установления взаимно однозначного соответствия между синдромом и имеющей место ошибкой с последующим ее исправлением.

Структурная схема устройства, осуществляющего исправления ошибок в циклических кодах, представлена на рис. 4.12.

Кодовая последовательность одновременно поступает в буферный накопитель БН и генератор синдрома ГС. После n тактов БН будет заполнен принятой кодовой комбинацией, а ГС будет сформирована комбинация синдрома (опознавателя), соответствующая вектору ошибки. Синдром исследуется анализатором синдрома АС, представляющим комбинационную логическую схему. При выдаче кодовой комбинации в момент прохождения ошибочного элемента АС выдает корректирующий сигнал, который на сумматоре по модулю два инвертирует (исправляет) ошибочный элемент и исправленная комбинация перезаписывается в БН. Этот же сигнал поступает в ГС, перестраивая его на исправление очередного ошибочного элемента. Если через n тактов ГС окажется в нулевом состоянии, то сигнал с его выхода откроет ключ К и кодовая комбинация выдается на дальнейшую обработку. В противном случае комбинация стирается, так как содержит неисправляемые ошибки.

Сложность декодеров, исправляющих ошибки, определяется сложностью анализатора синдрома и резко возрастает с увеличением длины кодовой комбинации и кратности исправляемых ошибок. Поэтому эти устройства нашли ограниченное применение в основном для циклических кодов небольшой длины.

Напомним, что во многих случаях, когда требуется исправление или одновременно обнаружение и исправление ошибок, могут оказаться более эффективными методы и устройства, рассмотренные в п. 3.5. Особенно следует подчеркнуть целесообразность их использования в сочетании с циклическими кодами, работающими в режиме обнаружения ошибок.

4.6. Циклические коды, допускающие мажоритарное декодирование

Задача построения достаточно простых декодирующих устройств, работающих в режиме исправления ошибок, в определенной степени решается при использовании цикли-

ческих кодов, допускающих мажоритарное декодирование (принцип голосования) $M(n, \kappa)$ - кодов [14], из которых наиболее просто реализуемыми являются коды, основанные на системе разделенных проверок.

Циклический (n, κ) - код, как всякий линейный код, может быть задан при помощи проверочной матрицы H, определяющей систему контрольных проверок (проверок на четность) для элементов проверяемой кодовой комбинации.

Системой разделенных проверок называется такое множество контрольных проверок, которое удовлетворяет следующим условиям:

некоторый элемент, например, α_j, входит в каждую контрольную проверку множества;

любой другой элемент α_i $(i \neq j)$ входит не более чем в одну контрольную проверку.

Например, если циклический (7.3) - код задан образующим полиномом $P(x) = (x + 1)(x^3 + x + 1)$, то его проверочная матрица в канонической форме имеет вид

$$H = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}. \qquad (4.27)$$

Следующие линейные комбинации строк h_i матрицы H задают соотношения, удовлетворяющие определению системы разделенных проверок,

$$\begin{aligned} h_1 &= 1\ 1\ 0\ 1\ 0\ 0\ 0; \\ h_2 + h_3 &= 1\ 0\ 0\ 0\ 1\ 1\ 0; \\ h_4 &= 1\ 0\ 1\ 0\ 0\ 0\ 1. \end{aligned}$$

Дополняя систему тривиальным соотношением $\alpha_1 = \alpha_1$, получим четыре независимых выражения для α_1:

$$\left.\begin{aligned} \alpha_1 &= \alpha_2 + \alpha_4; \\ \alpha_1 &= \alpha_5 + \alpha_6; \\ \alpha_1 &= \alpha_3 + \alpha_7; \\ \alpha_1 &= \alpha_1. \end{aligned}\right\} \qquad (4.28)$$

Каждая проверка системы разделенных проверок позволяет представить α_j (например, α_1) в виде линейной комбинации элементов, которые не входят более ни в одну из проверок. Поэтому одиночное искажение кодового слова может нарушить только ту проверку, в которую входит

искаженный элемент. Две ошибки могут исказить не более двух проверок; t ошибок исказят не более t проверок.

Для правильного декодирования элемента α_j, если при передаче исказились $l \leqslant t$ элементов кодового слова, достаточно, чтобы система разделенных проверок содержала не менее $2t + 1$ контрольных соотношений. Тогда значение элемента α_j можно определить с помощью решения по большинству.

Так как код — циклический, то для декодирования остальных элементов также может быть использована выбранная система разделенных проверок, поскольку конт-

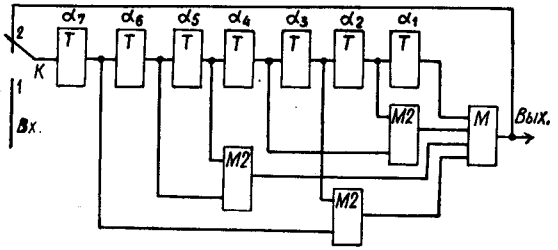


Рис. 4.13

рольным соотношениям удовлетворяет любое кодовое слово, и в том числе слово, получаемое из принятой последовательности циклическим сдвигом (четвертое свойство циклических кодов, п.4.1).

Продолжая рассмотрение примера (4.27), систему проверок (4.28) необходимо дополнить следующими соотношениями:

$$\left.\begin{array}{l} \alpha_2 = \alpha_3 = \alpha_5; \\ \alpha_2 = \alpha_6 = \alpha_1; \\ \alpha_2 = \alpha_4 = \alpha_1; \\ \alpha_2 = \alpha_2; \end{array}\right| \quad \left|\begin{array}{l} \alpha_3 = \alpha_4 + \alpha_6; \\ \alpha_3 = \alpha_7 + \alpha_1; \\ \alpha_3 = \alpha_5 + \alpha_2; \\ \alpha_3 = \alpha_3. \end{array}\right\}. \qquad (4.29)$$

Таким образом, системы контрольных проверок (4.28) и (4.29) позволяют исправить по критерию большинства любую одиночную ошибку и обнаружить любую двойную ошибку (случай, когда два уравнения дают $\alpha_j = 1$, а два других $\alpha_j = 0$).

Функциональная схема декодирующего устройства для данного кода представлена на рис. 4.13. В исходном состоянии ключ К находится в положении *1* и кодовая комбинация в течение семи тактов вводится в регистр сдвига.

После этого ключ К переводится в положение *2* и начинается процесс мажоритарного декодирования. При этом за первые K-тактов формируются информационные, а за последующие $(n - k)$-тактов — проверочные элементы. Сформированные элементы по цепи обратной связи через ключ К перезаписываются в регистр и участвуют в последующих контрольных проверках. Так, если передаваемая комбинация

$$M(x) \approx 1100101$$

оказалась принятой комбинацией

$$M'(x) \approx 1110101$$

с искаженным элементом α_3, то на первом такте декодирования на мажоритарный элемент М поступят сигналы

$$\alpha_1 = \alpha_2 + \alpha_4 = 1;$$
$$\alpha_1 = \alpha_5 + \alpha_6 = 1;$$
$$\alpha_1 = \alpha_3 + \alpha_7 = 0;$$
$$\alpha_1 = 1$$

и на его выходе сформируется значение $\alpha_1 = 1$, которое перезапишется в последний разряд регистра сдвига.

На втором такте на мажоритарный элемент М поступит сигнал 0111 и сформируется значение $\alpha_2 = 1$. Далее на М поступят 0001, а на выходе появится исправленное значение $\alpha_3 = 0$ и т. д.

Для систематического кода, работающего только в режиме исправления ошибок, декодирование может быть закончено через K тактов, так как при этом будут выделены исправленные информационные элементы. В некоторых случаях (например, применяемый код несистематический) декодирование осуществляется в течение n тактов.

Системы разделенных проверок могут использоваться не только для исправления, но также и для обнаружения ошибок. При этом вместо мажоритарного элемента используется решающий элемент, который реализует более сложную пороговую функцию. Сравнение с другими способами декодирования циклических кодов с исправлением ошибок показывает, что мажоритарное декодирование является наиболее простым и удобным. Декодер для $M(n, k)$-кодов содержит число элементов памяти, возрастающее линейно с ростом длины комбинации n. Кроме того, он содержит не более чем k пороговых логических элементов и не более чем kd_0 сумматоров по модулю, где d_0 — минимальное кодовое расстояние. При этом известные [14] $M(n, k)$-

коды проигрывают в скорости передачи соответствующим БЧХ-кодам не более чем на 5 — 10% . Однако такое сравнение недостаточно точно, так как не учитывает способности мажоритарной декодирующей схемы исправлять некоторые комбинации ошибок кратности выше t.

Выбор $M(n, k)$ - кодов, обладающих заданной корректирующей способностью, осуществляется из таблицы [14], а расчет вероятностных характеристик выполняется по методике, изложенной в п. 4.3.

4.7. Поэтапное формирование и обработка циклических кодов

Методы поэтапного кодирования и декодирования дискретной информации, рассмотренные в п.3.6, могут быть распространены на циклические коды, что в определенных случаях позволяет уменьшить время приема информации без снижения ее достоверности [6].

Определение метода. На передающей стороне исходное кодовое слово, которое может быть представлено с помощью многочлена $G(x)$ степени $k - 1$, кодируют первым циклическим кодом с образующим полиномом $P_1(x)$ степени r_1. Получают кодовое слово циклического $(k + r_1, k)$ -кода

$$Q(x) = G(x)\, x^{r_1} + R_1(x),$$

где $R_1(x)$ — остаток от деления $G(x)\, x^{r_1}$ на образующий полином $P_1(x)$.

В частном случае степень r_1 образующего полинома $P_1(x)$ может быть равна 1.

Кодовое слово $Q(x)$ кодируют последующим циклическим кодом с образующим полиномом $P_2(x)$ степени r_2.

Этот полином обеспечивает обнаружение пачек ошибок большой длины и, следовательно,

$$r_2 \gg r_1.$$

Получают кодовое слово

$$M(x) = Q(x)\, x^{r_2} + R_2(x),$$

где $R_2(x)$ — остаток от деления $Q(x)\, x^{r_2}$ на образующий полином $P_2(x)$.

Таких этапов кодирования может быть несколько.

В результате получают кодовое слово, где за k информационными элементами следует r_1 проверочных элементов,

определяемых первым этапом кодирования, далее r_2 проверочных элементов, определяемых вторым этапом кодирования, и т.д. Сформированное кодовое слово поступает в дискретный канал.

На приемной стороне после приема из дискретного канала $(k + r)$ элементов декодируют сообщение, закодированное первым циклическим кодом. Проверяют выполнение проверочных соотношений, например, по вычисляемому синдрому. При неудовлетворении проверочных соотношений (синдром не равен нулю) полагают, что сообщение принято с ошибкой. При этом сообщение стирается и для исполнения не выдается. При удовлетворении проверочных соотношений (синдром равен нулю) декодированное сообщение анализируют с целью выявления запрещенных сообщений, исполнение которых приводит к необратимым процессам. В частном случае запрещенных сообщений для конкретной системы может не быть.

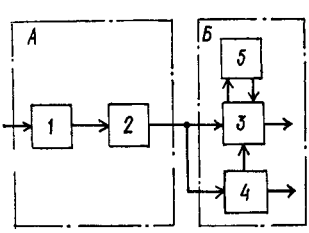


Рис. 4.14

Если в результате анализа окажется, что сообщение разрешенное, оно в качестве предварительного решения выдается для исполнения. При этом время приема

$$t_{\text{п}_1} = \frac{k + r_1}{V}.$$

После приема $(k + r_1 + r_2)$ элементов декодируют с обнаружением ошибок сообщение, закодированное последующим циклическим кодом с образующим полиномом $P_2(x)$.

При удовлетворении проверочных соотношений и имевшей место блокировке декодированное сообщение выдают для исполнения, поскольку после данного этапа декодирования сообщение будет обладать требуемой достоверностью, а при отсутствии блокировки продолжают исполнение предварительного решения. В случае неудовлетворения проверочных соотношений прекращают исполнение предварительного решения, а при имевшей место блокировке запрещают выдачу и стирают декодированное сообщение.

Реализация метода. На рис. 4.14 представлен вариант структурной схемы устройства защиты от ошибок, реализующей рассмотренный способ.

Схема содержит передающую станцию A, приемную станцию $Б$, кодирующий блок *1*, кодирующий блок *2*, декодирующий блок *3*, декодирующий блок *4* и дешифратор *5*.

Кодирующий блок *1* осуществляет первый этап кодирования с образующим полиномом $P_1(x) = x + 1$ степени $r_1 = 1$, кодирующий блок *2* предназначен для кодирования полученного кодового слова циклическим кодом с образующим полиномом $P_2(x) = x^3 + x + 1$ степени $r_2 = 3$, декодирующий блок *3* выполнен по схеме вычисления остатка от деления принимаемого кодового слова на образующий полином $P_1(x) = x + 1$, декодирующий блок *4* выполнен по схеме вычисления остатка от деления принимаемого кодового слова на образующий полином $P_2(x)$, дешифратор *5* выполнен по схеме выявления запрещенного сообщения, например

$$x^2 + 1 \sim 101.$$

Исходное кодовое слово, например $x^2 + 1$, кодируют в кодирующем блоке *1* и на выходе получают

$$Q(x) = (x^2 + 1)x - 1010.$$

Кодовое слово $Q(x)$ циклического (4.3)-кода поступает на вход кодирующего блока *2*, на выходе которого образуется кодовое слово

$$M(x) = [(x^2 + 1)x]\, x^3 + x + 1 = x^6 + x^4 + x + 1 \sim 1010011$$

циклического (7.4)-кода, поступающего в дискретный канал.

На приемной станции $Б$ кодовое слово $M(x)$ поступает одновременно в декодирующие блоки *3* и *4*.

Через время

$$t_{п_1} = \frac{k + r_1}{V} = \frac{4}{V}$$

без учета времени, необходимого на обработку информации, декодирующий блок *3* произведет декодирование части сообщения (первые $k + r_1$ элементов) $1010 \sim (x^2 + 1)x$. Результат декодирования $x^2 + 1$, поскольку остаток от деления равен нулю, анализируется дешифратором *5*, который настроен на данную комбинацию и, следовательно, выдает сигнал блокировки выдачи сообщения для исполнения в декодирующий блок *3*.

Через время $t_п = \frac{k + r_1 + r_2}{V} = \frac{7}{V}$ декодирующий блок *4* декодирует кодовое слово $M(x)$ и, так как полученный остаток равен нулю, подает сигнал в декодирующий блок *3*, разрешающий выдачу сообщения для исполнения.

Все незапрещенные сообщения при отсутствии ошибок декодируются блоком *3* и выдаются для выполнения, так как дешифратор *5* не блокирует выдачу. При этом после срабатывания декодирующего блока *4* предварительное решение не меняется, т.е. продолжает исполняться ранее декодированное сообщение.

При возникновении двойных ошибок декодирующий блок *3* последних не обнаружит и выдает декодированное разрешенное сообщение для исполнения.

В этом случае декодирующий блок *4* по наличию остатка от деления выдает сигнал на прекращение исполнения предварительного решения.

Если, например, состояние S_1 канала связи характеризуется вероятностью ошибки $P_1 = 10^{-5}$, состояние S_2 — вероятностью ошибки $P_2 = 0{,}5$, вероятность перехода из состояния S_1 в состояние S_2 $\alpha = 10^{-6}$ и вероятность перехода из состояния S_2 в состояние $S_1\beta = 10^{-2}$, то можно определить вероятности возникновения состояний S_1 и S_2

$$Q_1 = \frac{\beta}{\alpha + \beta} \approx 1 - 10^{-4};\ Q_2 = \frac{\alpha}{\alpha + \beta} \approx 10^{-4}.$$

Вероятность необнаружения ошибки при первом декодировании в состоянии S_1 определяется как

$$P_{н.\,о}^{S_1} \leqslant [1 - (1 - P_1)^n] - nP_1(1 - P_1)^{n-1} \approx n(n-1)P_1^2 \approx 10^{-8}.$$

Вероятность необнаружения ошибки при первом декодировании в состоянии S_2

$$P_{н.\,о}^{S_2} = 0{,}5.$$

В этом случае вероятность необнаружения ошибки при первом декодировании определяется как

$$P_{н.\,о} = P_{н.\,о}^{S_1} Q_1 + P_{н.\,о}^{S_2} Q_2 \approx 0{,}5 \cdot 10^{-4}.$$

Это значит, что в среднем только одно из 10000 декодированных и выданных для исполнения сообщений будет корректироваться на последующем этапе декодирования.

Таким образом, выбором соответствующего полинома $P_1(x)$ можно обеспечить для абсолютного большинства

переданных сообщений уменьшение времени приема в m раз, где

$$m = \frac{k + r_2}{k + r_1}.$$

Декодирование циклических мажоритарных кодов с повторением. При декодировании циклических кодов, допускающих мажоритарную обработку, процесс декодирования может быть осуществлен только после приема всей комбинации циклического (n, k)-кода. Для кодов с повторением мажоритарная обработка заканчивается после приема всех повторений комбинации. Использование для помехоустойчивого кодирования сообщений одновременно циклических мажоритарных кодов и метода многократных повторений позволяет обеспечить требуемые характеристики по достоверности и надежности передачи информации при использовании каналов связи низкого качества.

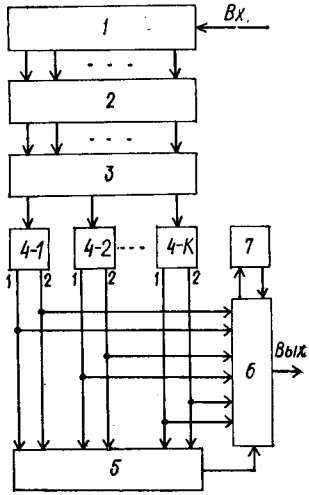


Рис. 4.15

На рис. 4.15 изображена функциональная схема декодирующего устройства для циклических мажоритарных кодов с повторением. Устройство содержит регистр сдвига *1*, сумматоры по модулю два *2*, распределитель *3*, счетчики мажоритарных проверок *4 — 1*, *4 —2*, ..., *4 — k*, блок запоминания *5*, блок сравнения *6* и дешифратор *7*.

Регистр сдвига установлен для записи n элементов одной кодовой комбинации циклического (n, k) -кода и перезаписи комбинации по цепи обратной связи при формировании результатов мажоритарных проверок.

Сумматоры по модулю два *2* предназначены для вычисления мажоритарных проверок путем суммирования импульсов с различных ячеек регистра сдвига *1* с целью получения серии импульсов, из которых затем по большинству определяется значение информационного элемента. Входы сумматоров подключены к ячейкам регистра сдвига в соответствии с системой мажоритарных проверок для конкретного циклического кода.

Распределитель *3* служит для направления результатов мажоритарных проверок с выходов сумматоров в счетчик того информационного элемента, которому соответствуют эти проверки.

Счетчики мажоритарных проверок *4—1*, *4—2*, ..., *4—k* используются для подсчета результатов мажоритарных проверок. Они выполнены по схеме с несколькими порогами срабатывания. Каждый порог определяется числом принятых кодовых комбинаций, по результатам мажоритарных проверок которых вычисляются информационные элементы. В общем случае число счетчиков равняется числу информационных элементов k в исходной кодовой комбинации. Если l — число мажоритарных проверок для одного информационного элемента за одно повторение, то минимальный порог определится величиной $0{,}5l$ (l — четное) или $0{,}5 \cdot (l+1)$, где l — нечетное. За m повторений порог определится величиной $0{,}5\ lm$ или $0{,}5\ (lm+1)$. За все N повторений порог определится величиной $0{,}5\ lN$ или $0{,}5\ (lN+1)$. Так, для циклического (7,3)-кода с трехкратным повторением $l = 4$, минимальный порог за одно повторение равен двум, порог за два повторения равен четырем и порог за все повторения равен 6.

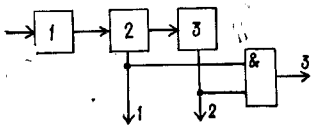


Рис. 4.16

При этом счетчик мажоритарных проверок для одного информационного элемента (рис. 4.16) будет состоять из трех двоичных разрядов и значение информационного элемента для минимального порога определится состоянием второго разряда счетчика после обработки первого повторения, для второго порога — состоянием третьего разряда счетчика после обработки двух повторений и для третьего порога за все повторения — состоянием второго и третьего разрядов счетчика после обработки трех повторений.

В частном случае порогов срабатывания может быть два: первый порог за одно или часть повторений определяет первый этап обработки, второй порог за все повторения определяет второй этап обработки.

Счетчики мажоритарных проверок *4—1*, *4—2*, ..., *4—к* выполнены по схеме с двумя порогами и соответственно имеют по два выхода.

Блок запоминания *5* служит для поочередного запоминания результатов мажоритарной обработки, соответствую-

щих реализованным порогам срабатывания счетчиков *4—1*, *4—2*,..., *4—к*.

Блок сравнения *6* первый результат мажоритарной обработки выдает для исполнения, сравнивает каждый последующий результат с предыдущим и при их несовпадении выдает сигнал на прекращение исполнения предыдущего решения и выдает для исполнения последующее решение.

Дешифратор *7* анализирует результаты мажоритарных обработок и при выявлении запрещенной комбинации блокирует ее выдачу до окончания приема всех повторений. К запрещенным комбинациям могут быть отнесены сообщения, исполнение которых приводит к необратимым процессам у получателя и которые не могут быть скорректированы последующими результатами мажоритарных проверок. В частном случае для систем, в которых отсутствуют запрещенные комбинации, дешифратор *7* будет отсутствовать.

Работа устройства происходит следующим образом.

Принимаемая n-разрядная кодовая комбинация вводится в регистр сдвига 1. Далее, в течение $к$ тактов при помощи регистра сдвига *1* и сумматоров *2* формируются результаты мажоритарных проверок для каждого из $к$ информационных элементов, которые через распределитель *3* вводятся в соответствующий счетчик мажоритарных проверок *4—1*, *4—2*, ..., *4—k*. Вся процедура декодирования осуществляется за время $t = \frac{1}{V}$, где V — скорость модуляции для принимаемой кодовой комбинации. Аналогично обрабатывается каждое повторение циклического кода.

После приема и обработки m повторений, определяющих первый порог срабатывания, информационные элементы с первых выходов счетчиков мажоритарных проверок поступают одновременно в блок запоминания *5* и блок сравнения *6*. Из блока сравнения *6* декодированная комбинация поступает в дешифратор *7*, который анализирует и не препятствует выдаче для исполнения разрешенной комбинации, или подачей сигнала в блок сравнения *6* блокирует выдачу запрещенной комбинации.

После приема и обработки N повторений, определяющих второй порог срабатывания, информационные элементы со вторых выходов счетчиков мажоритарных проверок поступают одновременно в блок запоминания *5* и блок сравнения *6*. Поступившие информационные элементы вытесняют из блока запоминания *5* в блок сравнения *6* ранее запомненный результат. В блоке сравнения *6* сравниваются результаты первого и второго этапов обработки. При их

совпадении продолжает исполняться сообщение, декодированное на первом этапе. При несовпадении блок сравнения *6* выдает сигнал на прекращение исполнения сообщения, декодированного на первом этапе и выдает для исполнения сообщение, декодированное на втором этапе.

В случае имевшей место на первом этапе блокировки блок сравнения *6* выдает для исполнения сообщение, декодированное на втором этапе. Выбором соответствующего значения m обеспечивается то, что в абсолютном большинстве случаев сообщения, декодированные на первом и втором этапах, будут совпадать и время приема определится величиной

$$t_{\text{п}} = \frac{mn}{V},$$

что в $S = \frac{N}{m}$ раз меньше, чем время приема в известных устройствах.

Если δ — реализуемое кодовое расстояние циклического мажоритарного $M(n, \kappa)$ - кода [14], которое аналогично минимальному расстоянию, то кратность гарантийно исправляемых ошибок определяется соотношением

$$t = \left[\frac{\delta - 1}{2}\right].$$

В общем виде реализуемое расстояние определяется выражением $\delta = t + \sigma + 1$, причем $\sigma \geqslant t$.

Реализуемое кодовое расстояние, соответствующее m повторениям первого этапа обработки,

$$\delta_m = m\delta,$$

а кратность исправляемых ошибок

$$t_m = \left[\frac{m\delta - 1}{2}\right]. \qquad (4.30)$$

Второй этап обработки характеризуется приемом N повторений, реализуемое кодовое расстояние которых

$$\delta_N = N\delta,$$

а кратность исправляемых ошибок

$$t_N = \left[\frac{N\delta - 1}{2}\right]. \qquad (4.31)$$

Характеристики (4.30) и (4.31) позволяют определить достоверность информации первого и второго этапов обработки по методике (п.4.3).

Таким образом, можно отметить, что наряду с разработанными процедурами обнаружения и исправления ошибок циклические коды хорошо совместимы с процедурой поэтапного принятия решений, что повышает эффективность их использования при передаче информации в ИС.

5. КОДЫ С ПОВТОРЕНИЕМ

5.1. Определение

Если коды с одной проверкой на четность относятся к наиболее высокоскоростным, так как обладают наименьшей избыточностью, то коды с повторением относятся к диаметрально противоположному предельному классу кодов

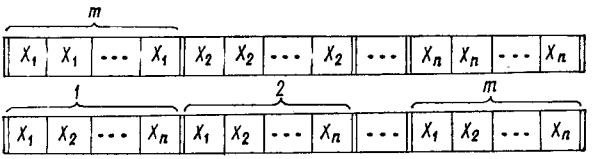


Рис. 5.1

и характеризуются значительной корректирующей способностью [3], которая достигается введением большой избыточности. Это снижает относительную скорость передачи, но сохраняет основное преимущество кодов с повторением, которая заключается в простоте технической реализации. Указанные обстоятельства объясняют их широкое применение для самых различных классов используемых каналов связи невысокой стоимости, а также при хранении и обработке информации в ИС [3].

Известны два варианта представления кодов с повторением (рис. 5.1, *а*, *б*). В первом случае имеет место m-кратное повторение каждого элемента кодовой комбинации, а во втором случае кодовая комбинация повторяется m раз, т. е. одноименные элементы разнесены на длину кодовой комбинации.

Проверочная матрица для одного информационного элемента кода с повторением имеет следующий вид:

$$H_i = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{matrix} 1 \\ 2 \\ \vdots \\ m-1 \end{matrix}. \qquad (5.1)$$

Кодовое расстояние кодов с повторением не зависит от способа представления их и равно

$$d_m = md,$$

где d — минимальное число позиций, в которых отличаются между собой комбинации кода $X_1, X_2, \ldots, X_n$.

Если повторяются элементы или комбинации безызбыточного кода, то $d = 1$ и $d_m = m$. При этом относительная скорость передачи

$$R = \frac{1}{m}.$$

На рис. 5.2 изображены структурные схемы декодирующих устройств для двух методов (рис. 5.1, *а*, *б*) представ-

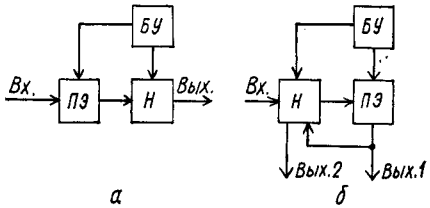


Рис. 5.2

ления кодов с повторением. В соответствии с первым методом m одноименных элементов из канала поступают в пороговый элемент ПЭ, где применяется решение относительно передаваемого элемента. Это решение 0 или 1 записывается в накопитель Н, емкость которого равна числу элементов кодовой комбинации n. Блок управления БУ синхронизирует процесс приема, обработки и выдачи информации. В качестве порогового элемента используется чаще всего двоичный счетчик, емкость которого должна быть равна $\frac{m+1}{2}$, а число разрядов — $\left]\log_2 \frac{m+1}{2} + 1\right[$. Таким образом, сложность декодера в элементах памяти

$$S_1 \approx n + \left]\log_2 \frac{m+1}{2} + 1\right[. \qquad (5.2)$$

В соответствии со вторым методом (рис. 5.1, *б*; рис. 5.2, *б*) информация из канала связи (повторения кодовых комбинаций) накапливается в накопителе Н, обрабатывается пороговым элементом ПЭ и результат обработки переза-

писывается в накопитель Н и выдается на выход устройства. Сложность декодера в этом случае определяется емкостью накопителя и равна

$$S_2 \approx n \left]\log_2 \frac{m+1}{2} + 1\right[. \qquad (5.3)$$

Анализ показывает, что декодер второго типа сложнее декодера первого типа на η %, где

$$\eta = \frac{S_2 - S_1}{S_1} \cdot 100 = \frac{(n-1)\left[\log_2 \frac{m+1}{2} + 1\right[- n}{n + \left]\log_2 \frac{m+1}{2} + 1\right[} \cdot 100\ \%. \qquad (5.4)$$

Если $m = 7$ и $n = 50$, то $\eta = 180$ %.

В дискретном симметричном канале ДСК без памяти помехоустойчивость обоих методов одинаковая, поэтому предпочтение должно быть отдано первому методу и соответствующему устройству, как более простому (рис. 5.2, *а*). Тем не менее, более широкое распространение получил второй метод и соответствующее декодирующее устройство. Это обусловлено тем, что реальные каналы характеризуются памятью, а второй метод представления кодов с повторением обладает свойством декорреляции ошибок. Именно поэтому основное внимание в дальнейшем будет сосредоточено на данном методе, представляющем интерес для использования в реальных каналах связи ИС.

5.2. Обработка по критерию «два из двух» избыточных (n, k) -кодов

Отличительной особенностью рассматриваемой модификации кода с двухкратным повторением является то, что на передающей стороне дважды повторяется комбинация избыточного (n, $к$)-кода, а на приемной стороне два повторения поразрядно сравниваются и проверяются на отсутствие ошибок избыточным (n, $к$)-кодом. Декодер принимает решение об отсутствии ошибок, если все одноименные элементы двух повторений совпадают и удовлетворяются контрольные проверки избыточного (n, $к$)-кода.

Основные соотношения. Так как избыточный (n, $к$)-код, например циклический, обнаруживает все ошибки до σ-кратных включительно и $\frac{2^r-1}{2^r}$ часть ошибок более высо-

кой кратности, то вероятность необнаружения ошибок для ДСК без памяти

$$P_{\text{н. о}} = \frac{1}{2^r} \sum_{i=\sigma+1}^{n} C_n^i P_0^{2i} (1 - P_0)^{2(n-i)}, \tag{5.5}$$

а приближенное выражение определится, как

$$P_{\text{н. о}} = \frac{1}{2^r} C_n^{\sigma+1} P_0^{2(\sigma+1)}. \tag{5.6}$$

Для канала с группирующимися ошибками из (1.7) получим формулу

$$P_{\text{н. о}}(\alpha) = \frac{1}{2^r} \sum_{i=\sigma+1}^{n} \frac{C_n^i}{C_{2n}^{2i}} (2n)^{1-\alpha} P_0 [(2i)^{\alpha-1} - (2i+1)^{\alpha-1}] \tag{5.7}$$

или упрощенное выражение

$$P_{\text{н. о}}(\alpha) = \frac{1}{2^r} \frac{C_n^{\sigma+1}}{C_{2n}^{2(\sigma+1)}} (2n)^{1-\alpha} P_0 [[2(\sigma+1)^{\alpha-1} - [2(\sigma+1)+1]^{\alpha-1}]. \tag{5.8}$$

Увеличение объема передаваемых сигналов. Недостатком рассмотренных методов передачи и приема кодов с повторением является то, что они не позволяют без введения дополнительной избыточности определить начало и конец кодовых комбинаций, т. е. осуществить синхронизацию по циклам. Это обусловлено тем, что рассмотренные коды не являются самосинхронизирующимися, т. е. не содержат в своем составе сигналов цикловой синхронизации. Способ, устраняющий отмеченный недостаток, описан в [23]. В соответствии с этим способом на передающей стороне исходное сообщение кодируют избыточным (n, κ)-кодом и осуществляют двухкратное повторение посылок. При этом на первую комбинацию накладывают по модулю два рекуррентный синхросигнал. На приемной стороне каждый элемент, поступающий из канала связи, суммирует по модулю два с ранее поступившим и задержанным на время приема одной комбинации элементов. Результат суммирования непрерывно анализируют на наличие рекуррентного синхросигнала и при его выделении декодируют задержанные элементы. В случае отсутствия ошибок результат декодирования выдают получателю.

Рассмотрим действие данного способа на примере циклического (13,9)-кода с образующим полиномом $P(x) = x^4 + x^3 + 1$ и рекуррентной последовательностью, порождаемой многочленом $Q(x) = x^4 + x + 1$. Выберем в качестве начальной фазы синхросигнала комбинацию 1001. В этом случае синхросигнал имем вид

$$S \sim 1001.\ 101011110.$$

Если комбинация исходного неизбыточного кода $I(x) = x^8 + x + 1$, то комбинация циклического (13,9)-кода будет

$$M \sim 1000000110001.$$

В этом случае 1-я посылка, представляющая собой сумму по модулю два комбинации $M(x)$ и синхросигнала $S(x)$, определится следующим образом:

$$N = M \oplus S = \oplus \begin{array}{l} 1000000110001 \\ 1001101011110 \\ \hline 0001101101111. \end{array}$$

На приемной стороне сначала принимается комбинация N — 1-я посылка, а затем комбинация M — 2-я посылка. При этом элементы N задерживают на время приема одной посылки, т. е. на 13 тактов, и складывают их по модулю два с одноименными элементами 2-й посылки:

$$N \oplus M = \oplus \begin{array}{l} 0001101101111 \\ 1000000110001 \\ \hline \underline{1001}101011110. \end{array}$$

Полученную комбинацию анализируют и, если ее начало совпадает с начальной фазой синхросигнала 1001 и остальные элементы соответствуют синхросигналу заданного вида, то считают, что цикловое фазирование осуществлено правильно и декодируют комбинацию M, элементы которой в данный момент находятся в линии задержки. Если остаток от деления на образующий полином равен нулю, то декодированное сообщение выдают для дальнейшей обработки.

Рассмотренный способ имеет относительную избыточность кода

$$H_1 = \frac{2n - k}{k},$$

а в тех случаях, когда цикловая синхронизация осуществляется при помощи синхросигнала маркера, состоящего

из n' дополнительных элементов, относительная избыточность будет

$$H_2 = \frac{(2n + n') - k}{R}.$$

Таким образом, избыточность рассмотренного способа меньше на γ %, где

$$\gamma = \frac{H_2 - H_1}{H_2} \cdot 100\ \% = \frac{n'}{(2n + n') - R} \cdot 100.$$

Если $n = n' = 31$, $k = 21$, то $\gamma = 43$ %.

Возможно дополнительное увеличение объема передаваемых сигналов при той же относительной избыточности кода [23]. Это достигается за счет того, что на передающей стороне при передаче информационного сигнала на 1-ю посылку накладывают рекуррентный синхросигнал одной конфигурации. При передаче одновременно информационного и служебного сигналов накладывают рекуррентный синхросигнал другой конфигурации. Служебными сигналами могут быть сигналы типа «квитанция», «запрос» и др. В том случае, когда на приемной стороне выделяют синхросигнал другой конфигурации, дополнительно фиксируют прием служебного сигнала. Число служебных сигналов обусловливается количеством используемых синхросигналов различной конфигурации.

Если циклический (14.9)-код задается образующим полиномом $P(x) = x^5 + x^3 + x + 1$, а рекуррентные синхросигналы S_1 и S_2 — порождающими многочленами $Q_1(x) = x^4 + x^3 + x + 1$ и $Q_2(x) = x^4 + x + 1$, то синхросигналы имеют вид

$$S_1 \sim \underbrace{1001}0001111010;$$

$$S_2 \sim \underbrace{1001}1010111100,$$

с начальными фазами 1001.

Выберем комбинацию исходного неизбыточного кода

$$I(x) = x^2 + x + 1 — 100000011,$$

тогда комбинация циклического (14,9)-кода будет

$$M \sim 10000001100010.$$

В этом случае при передаче только информационного сигнала 1-я посылка представляет собой сумму по модулю два комбинации M и синхросигнала S_1:

$$N_1 = M \oplus S_1 = \oplus \begin{array}{l} 10000001100010 \\ 10010001111010 \\ \hline 00010000011000. \end{array}$$

При одновременной совместной передаче информационного и служебного сигнала 1-я посылка является суммой по модулю два комбинации M и синхросигнала S_2:

$$N_2 = M \oplus S_2 = \begin{array}{r} 10000001100010 \\ 10011010111100 \\ \hline 00011011011110. \end{array}$$

На приемной стороне сначала принимают комбинацию N_i ($i = 1,2$) — 1-ю посылку, а затем комбинацию M — 2-ю посылку. При этом элементы комбинации N_i задерживают на время приема одной посылки, т. е. на 14 тактов, и складывают их по модулю два с одноименными элементами 2-й посылки. В тех случаях, когда передается только информационный сигнал, будем иметь

$$N_1 \oplus M = 10010001111010.$$

Анализируют полученную комбинацию известными методами анализа рекуррентых последовательностей и, если ее начало совпадает с начальной фазой синхросигнала, а остальные элементы соответствуют синхросигналу S_1, считают, что цикловое фазирование осуществлено правильно. В этом случае декодируют комбинацию M, элементы которой в данный момент находятся в линии задержки.

При совместной передаче информационного и служебного сигналов 1-ю посылку N_2 складывают по модулю два со 2-й комбинацией M.

$$N_2 \oplus M = 10011010111100.$$

Полученную комбинацию анализируют и, если ее начало совпадает с начальной фазой, а остальные элементы соответствуют синхросигналу S_2, считают, что цикловое фазирование осуществлено правильно. В этом случае декодируют комбинацию M и дополнительно фиксируют прием служебного сигнала. Увеличение объема передаваемых сигналов позволяет в системах передачи дискретной информации с обратной связью увеличить относительную скорость передачи. Так, если в указанных системах квитанционный подканал формируется временным разделением сигналов и время работы квитанционного подканала составляет $\frac{1}{\mu}$ часть работы информационного подканала, то относительная скорость передачи

$$R_1 = \frac{k}{2n\left(1 + \frac{1}{\mu}\right)}.$$

Рассмотренный способ характеризуется относительной скоростью

$$R_2 = \frac{k}{2n},$$

что на γ % больше, где

$$\gamma = \frac{R_2 - R_1}{R_1} \cdot 100\ \% = \frac{1}{\mu} \cdot 100\ \%.$$

при $\frac{1}{\mu} = 0{,}25$; $\gamma = 25\ \%$. Настолько же сократится время задержки сигналов.

Техническая реализация. На рис. 5.3. изображена структурная схема устройства для приема и обработки (n, k)-ко-

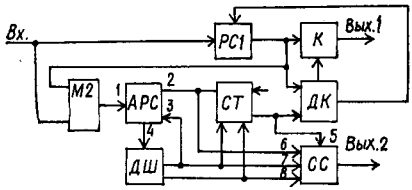


Рис. 5.3

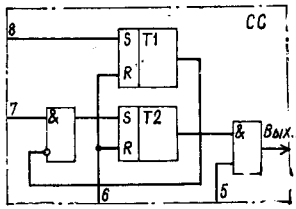


Рис. 5.4

дов с повторением. Устройство содержит регистр сдвига РС1, ключ К, сумматор по модулю два, анализатор рекуррентного синхросигнала АРС, счетчик СТ зачетного интервала, декодер ДК, дешифратор ДШ начальной фазы и селектор служебного сигнала СС, возможный вариант которого представлен на рис. 5.4.

Работает устройство следующим образом. Напоминаем, что информационный сигнал закодирован избыточным (n, k)-кодом и имеет двухкратное повторение, причем на 1-ю посылку наложен по модулю два рекуррентный синхросигнал. Первая посылка при приеме записывается в регистр РС1, число разрядов которого соответствует длине одной посылки. Поступающая на вход устройства 2-я посылка одновременно вводится в регистр РС1 и поступает на вход сумматора по модулю два, на другой вход которого из регистра РС1 вводятся элементы 1-й посылки. На сумматоре происходит сложение по модулю два 1-й и 2-й посылок и на его выходе выделяется рекуррентный синхросигнал, который поступает в анализатор АРС. После выделения начальной фазы синхросигнала ДШ запускает счетчик СТ и с

этого момента начинается проверка поступающей последовательности на соответствие закону построения рекуррентного синхросигнала. Результаты проверки выдаются на вход СТ. При каждом удовлетворении рекуррентному закону на суммирующий вход СТ подается импульс тактовой частоты. При наличии серии из l нулей с выхода АРС счетчик СТ переполняется, что свидетельствует о правильном выделении синхросигнала и окончании циклового фазирования. Отметим, что

$$l = n - \nu,$$

где ν — число элементов начальной фазы синхросигнала. Сигнал с выхода СТ разрешает декодирование 2-й посылки, которая поступает из регистра РС1 в декодер ДР, где проверяется на наличие или отсутствие ошибок, и результат декодирования перезаписывается в РС1. При отсутствии ошибок ДК выдает сигнал на ключ $К_1$, который открывается, и декодированный сигнал поступает на выход *1* устройства.

В том случае, когда одновременно с информационным передается служебный сигнал, ДШ выделяет начальную фазу другого синхросигнала, в результате чего появляется управляющий сигнал на другом выходе ДШ. Этот сигнал поступает на вход *7* селектора СС и переводит в единичное состояние триггер Т2, который подготавливает к срабатыванию схему И. Если другой синхросигнал выделяется правильно, то с окончанием его выделения появляется импульс на выходе СТ, который поступает через вход 5 СС на второй вход схемы И и проходит на выход *2* устройства, фиксируя прием служебного сигнала. При этом декодирование 2-й посылки и выдача результата на выход *1* устройства осуществляется аналогично рассмотренному ранее. Если начальная фаза другого синхросигнала была выделена ложно, то поступающие вслед за этим импульсы с выхода АРС на вход *6* СС установят в нулевое состояние Т2. Триггер Т1 устанавливается в единичное состояние при выделении начальной фазы основного синхросигнала (передается только информация). Сигнал с его выхода проходит на запрещающий вход схемы «запрета», исключая срабатывание Т2 от комбинации, совпадающей с начальной фазой другого синхросигнала, но не являющейся ею, так как она расположена внутри принимаемого синхросигнала.

В том случае, когда используемые синхросигналы порождаются различными многочленами, применяют перестра-

иваемый анализатор АРС (рис. 5.5), содержащий регистр сдвига РС2; коммутатор КМ и многовходовой сумматор по модулю два. При этом, когда выделяется синхросигнал, соответствующий совместной передаче информационного и служебного сигналов, импульс с выхода ДШ дополнительно продается через вход 5АРС на коммутатор КМ, который переключает выходы разрядов РС2 на входы многовходового сумматора в соответствии с законом построения данного синхросигнала. По окончании цикла приема КМ возвращается в исходное состояние, настраивая АРС на основной синхросигнал.

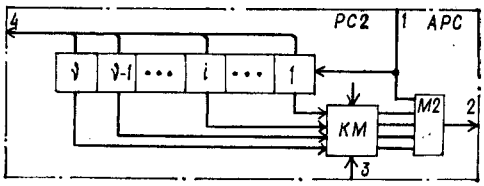


Рис. 5.5

5.3. Обработка избыточных (n, κ)-кодов с повторением по критерию «один из двух»

Рассмотренный ранее метод обработки кодов с повторением по критерию «два из двух» позволяет получить наибольшее значение достоверности принимаемой информации. Однако это достигается за счет некоторого увеличения потери информации, так как даже при наличии ошибки только в одной из посылок стираются обе посылки.

Излагаемый метод в определенных случаях лишен указанного недостатка, хотя достигается это за счет снижения достоверности.

Основные характеристики. Сущность метода обработки по критерию «один из двух» [1,12] состоит в том, что на приемной стороне две посылки избыточного (n, κ)-кода поразрядно сравнивают и проверяют на отсутствие ошибок. Если ошибки не обнаруживаются и комбинации двух посылок поразрядно совпадают, то фиксируют правильный прием и декодированное сообщение подвергают дальнейшей обработке. При обнаружении ошибки в одной посылке и необнаружении в другой дальнейшей обработке подвергают ту посылку, в которой ошибка не обнаружена.

Если же ошибки не обнаруживаются, но имеет место хотя бы одно несовпадение одноименных разрядов двух посылок, то фиксируют наличие ошибок и информация стирается.

Для каждого из повторений возможно одно из трех случайных событий: ошибки отсутствуют, т. е. имеет место правильный прием, вероятность которого — $P_{\text{п.п}}$; ошибки обнаружены, что характеризуется вероятностью $P_{\text{о.о}}$; ошибки не обнаружены, чему соответствует вероятность $P_{\text{н.о}}$. Указанные характеристики для каждого повторения определяются известными методами с использованием выражений (1.1), (1.3), (4.7), (4.8) или (1.6), (4.9). При этом всегда имеет место равенство

$$P_{\text{п. п}} + P_{\text{о. о}} + P_{\text{н. о}} = 1.$$

Определим вероятность необнаружения ошибки $P^{\Sigma}_{\text{н.о}}$, вероятность потери $P^{\Sigma}_{\text{п}}$ и вероятность правильного приема $P^{\Sigma}_{\text{п.п}}$, являющиеся финальными и характеризующими результат обработки двух посылок по критерию «один из двух». Сделаем допущение о независимости событий между двумя посылками, что справедливо даже для каналов с группирующимися ошибками вследствие обеспечиваемой кодами с повторением декорреляции ошибок. Представим в табл. 5.1 все возможные события для 1-й (П1) и 2-й (П2) посылок их вероятностями.

Каждое из девяти совместных независимых событий для 1-й и 2-й посылок соотнесем в соответствии с выражением (5.18) с правильным приемом $[P^{\Sigma}_{\text{п. п}}]$, потерями информации $[P^{\Sigma}_{\text{п}}]$ или с необнаружением ошибок $[P^{\Sigma}_{\text{н. о}}]$, что дает

$$\begin{aligned} P^{\Sigma}_{\text{п. п}} &= P^{2}_{\text{п. п}} + 2P_{\text{п. п}}P_{\text{о. о}}; \\ P^{\Sigma}_{\text{п}} &= P^{2}_{\text{о. о}} + 2P_{\text{п. п}}P_{\text{н. о}} + P^{2}_{\text{н. о}}; \\ P^{\Sigma}_{\text{н. о}} &= 2P_{\text{о. о}}P_{\text{н. о}}. \end{aligned} \qquad (5.9)$$

Тот факт, что событие, характеризуемое вероятностью $P^{2}_{\text{н.о}}$, отнесено к потерям информации, объясняется тем, что в абсолютном большинстве случаев необнаруживаемые ошибки в 1-й и 2-й посылках совпадать не будут. Поэтому необнаруживаемыми ошибками в одноименных элементах можно пренебречь. Кроме того, считая, что $P_{\text{н.о}} \ll 1$, $P_{\text{п.п}} \approx$

Таблица 5.1

№ п.п	П1	П2	$P_{\text{п. п}}$	$P_{\text{п}}$	$P_{\text{н. о}}$
1	$P_{\text{п. п}}$	$P_{\text{п. п}}$	$P^2_{\text{п. п}}$		
2	$P_{\text{п. п}}$	$P_{\text{о. о}}$	$P_{\text{п. п}} \cdot P_{\text{о. о}}$		
3	$P_{\text{п. п}}$	$P_{\text{н. о}}$		$P_{\text{п. п}} \cdot P_{\text{н. о}}$	
4	$P_{\text{о. о}}$	$P_{\text{п. п}}$	$P_{\text{о. о}} \cdot P_{\text{п. п}}$		
5	$P_{\text{о. о}}$	$P_{\text{о. о}}$		$P^2_{\text{о. о}}$	
6	$P_{\text{о. о}}$	$P_{\text{н. о}}$			$P_{\text{о. о}} \cdot P_{\text{н. о}}$
7	$P_{\text{н. о}}$	$P_{\text{п. п}}$		$P_{\text{н. о}} \cdot P_{\text{п. п}}$	
8	$P_{\text{н. о}}$	$P_{\text{о. о}}$			$P_{\text{н. о}} \cdot P_{\text{о. о}}$
9	$P_{\text{н. о}}$	$P_{\text{н. о}}$		$P^2_{\text{н. о}}$	

≈ 1 и $P^2_{\text{н.о}} \ll 2\,P_{\text{п.п}}\,P_{\text{н.о}}$ выражения (5.19) преобразуем к виду

$$P^{\Sigma}_{\text{п. п}} \cong P^2_{\text{п. п}} + 2P_{\text{о. о}}P_{\text{п. п}};$$
$$P^{\Sigma}_{\text{п}} \cong P^2_{\text{о. о}} + 2P_{\text{н. о}}; \qquad (5.10)$$
$$P^{\Sigma}_{\text{н. о}} = 2P_{\text{о. о}}P_{\text{н. о}}.$$

Вероятность правильного приема информации для рассматриваемого метода больше, чем аналогичная характеристика п. 5.2. Это достигается значительным снижением достоверности. Рассмотренный метод применяется при хранении информации в ИС с использованием дублированных запоминающих устройств.

Техническая реализация. На рис. 5.6 изображена функциональная схема устройства для приема информации по двум параллельным каналам связи, реализующая критерий обработки «один из двух». Устройство содержит два одинаковых подканала, включающих декодер ДК1 (2), накопитель Н1 (2) и ключ К1 (2), а также сумматор по модулю два, блок опроса БО, логическую схему ЛС и схему ИЛИ.

Работает устройство следующим образом. Элементы кодовых комбинаций поступают в ДК1 и ДК2, где подвергаются обработке, и одновременно записываются в накопители Н1, Н2 и сравниваются на сумматоре по модулю два. Результат сравнения всех разрядов комбинаций, принятых по обоим каналам, учитывается только в тех случаях, когда с управляющих выходов ДК1, ДК2 не поступают

сигналы отбраковки данной кодовой комбинации ввиду наличия в ней ошибок. Сигнал несовпадения одноименных элементов, формируемый сумматором по модулю два и записанный в триггер блока опроса БО, не попадает на выход схемы запрета ЛС всякий раз, когда имеется хотя бы один из сигналов отбраковки в одном из подканалов. Возможны следующие варианты в работе устройства:

Сигналы отбраковки в подканалах отсутствуют и все элементы комбинаций совпадают. В этом случае ключи К1 и К2 открыты и комбинации через схему ИЛИ выдаются на выход устройства.

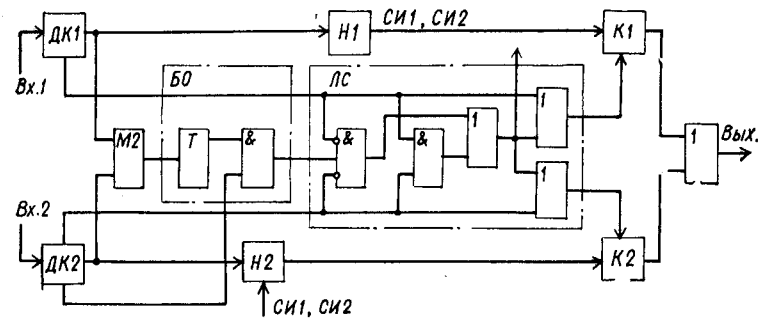


Рис. 5.6

Сигналы отбраковки в подканалах отсутствуют, но имеет место несовпадение одноименных элементов комбинаций. Тогда сигнал выхода БО проходит через ЛС и закрывает ключи К1 и К2. Информация на выход не поступает.

Сигнал отбраковки поступает в одном подканале, например, первом. Этот сигнал закрывает ключ К1 и на схеме запрета ЛС запрещает прохождение сигнала несовпадения одноименных элементов. В этом случае независимо от результата анализа одноименных элементов двух комбинаций на выход поступает комбинация второго подканала через открытый ключ К2.

5.4. Исправление ошибок в избыточных (n, κ)-кодах с повторением

При передаче дискретной информации в системах с обратной связью оказывается целесообразным использование комбинированных методов защиты от помех, предусматривающих как обнаружение, так и частичное исправ-

ление ошибок. Это позволяет без существенного снижения достоверности повысить относительную скорость передачи информации.

Исправление одиночных ошибок в ДСК без памяти. Если в одной из посылок избыточного $(n, к)$ -кода ошибки не обнаруживаются, а в другой обнаруживаются и при этом имеет место несовпадение в одном элементе сравниваемых повторений, то этот элемент исправляется (инвертируется) в комбинации с обнаруженной ошибкой.

К трансформации сообщения, т. е. к появлению необнаруживаемых ошибок, приводят случаи, когда искажено

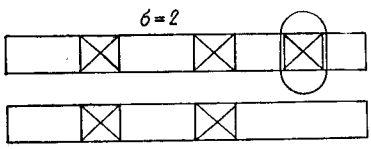


Рис. 5.7

σ (где σ — кратность гарантийно обнаруживаемых ошибок) одноименных элементов в двух повторениях и имеет место еще одна дополнительная одиночная ошибка в одной из посылок (рис. 5.7). Вероятность необнаружения ошибок в этом случае будет

$$P_{\text{н. о}} = P_{\text{н. о}_1} + P_{\text{н. о}_2},$$

где $P_{\text{н. о}_1}$ определяется выражением (5.5), а

$$P_{\text{н. о}_2} = \frac{1}{2^{r-1}} \sum_{i=\sigma}^{n} C_n^i (n-i) P_0^{2i+1} (1-P_0)^{2n-(2i+1)}. \quad (5\ 11)$$

Так как $P_{\text{н. о}_1} \ll P_{\text{н. о}_2}$, то, ограничившись первым членом суммы и выполнив преобразования, получим приближенное выражение

$$Y_{\text{н. о}} \approx \frac{1}{2^{r-1}} C_n^{\sigma} (n-\sigma) P_0^{2\sigma+1}. \quad (5.12)$$

Потери информации обусловливаются появлением ошибок кратности 2 и более и поэтому оцениваются в общем виде вероятностью $P(\geqslant 2{,}2\ n)$. Для ДСК без памяти эта вероятность определяется выражением

$$P_{\text{п}} = \sum_{i=2}^{2n} C_{2n}^i P_0^i (1-P_0)^{2n-i}. \quad (5.13)$$

Приближенное соотношение будет иметь следующий вид:

$$P_{\text{п}} \approx C_{2n}^2 P_0^2. \quad (5.14)$$

Таким образом, исправление одиночных ошибок снижает достоверность и уменьшает потери информации.

Исправление одиночных ошибок в каналах с памятью. Предполагая ошибки одинаковой кратности равновероятными и используя соотношения (1.6) и (1.7), получим выражение для определения вероятности необнаружения ошибок в каналах с памятью

$$P_{\text{н. о}}(\alpha) = P_{\text{н. о}_1}(\alpha) + P_{\text{н. о}_2}(\alpha),$$

где $P_{\text{н. о}}(\alpha)$ определяется соотношением (5.7), а

$$P_{\text{н. о}_2}(\alpha) = \frac{1}{2^{r-1}} \sum_{i=\sigma}^{n} \frac{C_n^i (n-i)}{C_{2n}^{2i+1}} (2n)^{1-\alpha} P_0 [(2i+1)^{\alpha-1} - [2(i+1)^{\alpha-1}]]. \quad (5.15)$$

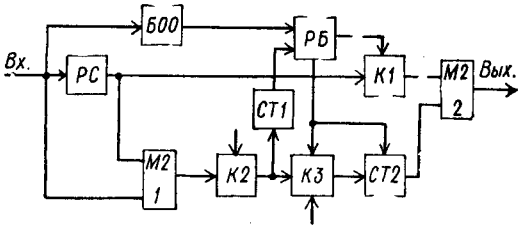


Рис. 5.8

Ограничившись первым членом выражения (5.15) и полагая $P_{\text{н. о}_1}(\alpha) \ll P_{\text{н. о}_2}(\alpha)$, получим приближенное соотношение

$$P_{\text{н. о}}(\alpha) = \frac{1}{2^{r-1}} \frac{C_n^{\sigma}(n-\sigma)}{C_{2n}^{2\sigma+1}} (2n)^{1-\alpha} \cdot P_0 [(2\sigma+1)^{\alpha-1} - [2(\sigma+1)]^{\alpha-1}]. \quad (5.16)$$

Потери информации оцениваются вероятностью $P(\geqslant 2{,}2\,n)$, которая определяется из (5.6):

$$P_{\text{п}}(\alpha) = (2n)^{1-\alpha} P_0 \cdot 2^{\alpha-1}. \quad (5.17)$$

Техническая реализация. На рис. 5.8 изображена функциональная схема декодирующего устройства, осуществляющего исправление одиночных ошибок в избыточных (n, κ)-кодах с повторением [11].

Работает устройство следующим образом. Поступающая на вход устройства комбинация 1-й посылки записы-

вается в регистр сдвига РС и проверяется в блоке обнаружения ошибок БОО. Ключ К2 закрыт и открывается по окончании приема 1-й посылки. Комбинация 2-й посылки, осуществляя последовательный сдвиг предыдущей, подается на один из входов сумматора по модулю два, на другой вход которого поступает комбинация 1-й посылки. Таким образом, одновременно с процедурой оценки достоверности, производимой БОО, происходит поэлементное сравнение обеих комбинаций. В случае необнаружения ошибок БОО и идентичности двух повторений решающий блок РБ, открывая ключ К1, обеспечивает вывод записанной в РС комбинации на выход устройства.

В том случае, когда БОО не обнаруживает ошибку в 1-й посылке, а комбинация 2-й посылки окажется искаженной, в результате поэлементного сравнения двух посылок на выходе сумматора М2 (*1*) появляется импульс несовпадения для соответствующего разряда комбинации, который включает счетчик СТ1 и через ключ К3 счетчик СТ2. Емкость СТ1 равна двум, а СТ2 — n. СТ2 начинает счет поступающих на вход сумматора элементов комбинации. Если в результате дальнейшего сравнения двух посылок не произойдет несовпадения элементов, на выходе СТ1 сигнал будет отсутствовать. Решающий блок РБ по окончании приема 2-й посылки открывает ключ К1, через который комбинация 2-й посылки поступает на вход сумматора М2 (*2*). Поскольку емкость СТ2 равна n, остаток его в момент окончания приема 2-й посылки соответствует местоположению искаженного элемента. Поэтому импульс переполнения СТ2 поступает на второй вход сумматора М2 (*2*) в тот момент, когда на первый вход последнего подается искаженный элемент комбинации. В результате осуществляется исправление одиночной ошибки и исправленная комбинация поступает на выход устройства.

Если БОО обнаруживает ошибку в 1-й посылке и не обнаруживает во 2-й и СТ1 фиксирует только одно несовпадение (это соответствует случаю, когда одиночная ошибка имеет место в 1-й посылке и, следовательно, нет необходимости в коррекции 2-й посылки), РБ сбрасывает СТ2 в исходное состояние, закрывает К3 и открывает К1. Комбинация без коррекции выдается на выход устройства. В тех случаях, когда СТ1 фиксирует более одного несовпадения, сигнал с его выхода поступает в РБ, который запрещает выдачу комбинации на выход.

Можно уменьшить потери информации, а следовательно, увеличить относительную скорость передачи и оператив-

ность, если в регистре сдвига сохранять неискаженное повторение комбинации, которое использовать в проверках при приеме последующих повторений.

На рис. 5.9 представлена функциональная схема декодирующего устройства, реализующего отмеченный принцип. Поступающая на вход устройства комбинация через переключатель ПК записывается в регистр сдвига РС и проверяется в БОО. Если ошибка не обнаружена, БОО выдает сигнал в РБ, а с помощью ПК выход РС соединяет с его входом. Комбинация 2-й посылки подается на один из входов сумматора по модулю два М2. При этом комбинация 1-й посылки одновременно с поступлением на второй вход сумматора М2 переписывается в РС. Таким образом, одновременно с перезаписью 1-й посылки происходит поэлементное сравнение обеих комбинаций. Если окажется, что сравниваемые комбинации идентичны или произошло лишь одно несовпадение, учитываемое одноразрядным счетчиком СТ, то РБ, открывая ключ К1, выдает комбинацию из РС на выход устройства.

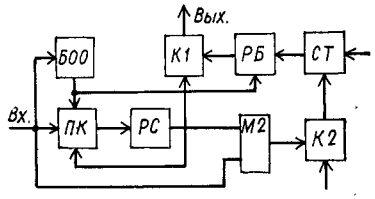


Рис. 5.9

В случае обнаружения ошибки в 1-й посылке в РС через ПК вводится 2-я посылка, которая сравнивается с первой на сумматоре М2. При этом учитывается результат анализа второй посылки в БОО. Если повторная комбинация окажется неискаженной и произойдет не более одного несовпадения, то на выход устройства выдается 2-я посылка сообщения. В случае обнаружения ошибок в обеих посылках или при возникновении более одного несовпадения в сравниваемых комбинациях осуществляется прием и обработка очередного повторения.

Обеспечение заданной вероятности потери сообщения $P_{п1}(m)$ для первого варианта декодирующего устройства достигается m-кратным повторением кодовой посылки, представляющим двухкратное повторение комбинации избыточного (n, k) -кода.

$$P_{п1}(m) = [P_п(1)]^m,$$

где $P_п(1)$ — вероятность потери сообщения при однократной передаче.

Второй вариант декодирующего устройства при тех же предположениях позволяет значительно уменьшить потери информации

$$P_{п2}(m) = [P_п(1)]^{2m-1}.$$

Так, если $P_п(1) = 10^{-2}$ и $m = 3$, то $P_{п1}(m) = 10^{-6}$ и $P_{п2}(m) = 10^{-10}$.

Таким образом, коды с повторением, являясь совершенными, вместе с тем относятся к самым низкоскоростным кодам и поэтому целесообразны для применения в ИС только в тех случаях, когда выполняются определенные условия:

сообщения имеют небольшую длину;

отсутствуют каналы обратной связи;

ошибки при передаче имеют тенденцию к группированию;

предъявляются высокие требования по надежности доведения информации;

требуется невысокая сложность технической реализации;

отсутствует непрерывная передача сообщений;

используются каналы связи невысокой стоимости.

Модификация алгоритмов неполного декодирования избыточных кодов с повторением повышает эффективность их использования при защите информации от ошибок как в реальных каналах связи, так и при контроле информации в запоминающих устройствах ИС.

При этом формирование самосинхронизирующихся кодов с повторением на основе рекуррентных последовательностей увеличивает объем передаваемых сигналов и расширяет функциональные возможности средств передачи информации.

6. МАЖОРИТАРНОЕ ДЕКОДИРОВАНИЕ КОДОВ С ПОВТОРЕНИЕМ

6.1. Адаптивное мажоритарное декодирование кодов с повторением

Представляет интерес разработка мажоритарных декодирущих устройств, имеющих возможность перестраиваться в зависимости от качества каналов связи и вместе с тем сохраняющих простоту технической реализации. Рассмотрим некоторые из наиболее перспективных направлений построения такого типа устройств [12].

Определение метода. В соответствии с этим методом запоминают 1-ю посылку, сравнивают его со следующей и дополнительно запоминают позиции несовпадающих элементов. При приеме каждого последующего повторения производят его сравнение и выявляют несовпадения с предыдущим результатом, на место которого записывают совпадающие элементы принимаемого повторения, те несовпадающие элементы, которые соответствуют хранимым в данный момент несовпадениям, а остальные элементы принимаемого повторения перед записью инвертируют. Кроме того, при приеме нечетного повторения логически складывают выявленные и хранимые несовпадения, на место которых записывают результат логического сложения. При приеме четного повторения выполняют операцию логического умножения для выявленных и хранимых несовпадений, на месте которых записывают результат логического перемножения. На рис. 6.1 изображен граф,соответствующий данному методу, где показано H_{ij} $[i = 1,0; j = 1,0]$ — состояние одноименных элементов памяти; $1/r$, $0/r$, $1/H$, $0/H$ — «1» и «0» четного и нечетного повторений.

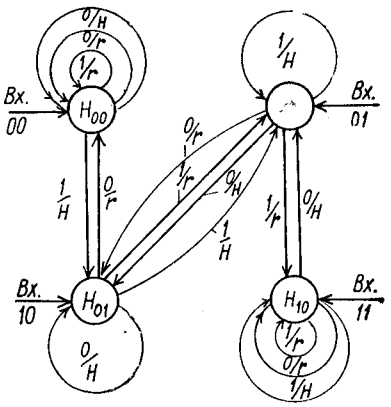


Рис. 6.1

Начальное состояние памяти устанавливается после приема первой пары элементов $00 \rightarrow H_{00}$; $01 \rightarrow H_{11}$; $10 \rightarrow H_{01}$; $11 \rightarrow H_{10}$.

Ориентированный граф (стрелка) определяет переход системы из одного состояния в другое в зависимости от вида последующих принимаемых элементов.

Рассмотрим действие метода на примере мажоритарного анализа кода с тремя и пятью посылками. Для наглядности предполагаем, что имеют место искажения и поэтому посылки 1, 2, 3-я не совпадают:

1. 1 0 1 1 0 1;

2. 1 1 1 0 1 1;

3. 1 1 0 1 0 1.

Запоминают 1-ю посылку. Сравнивают 2-ю и 1-ю посылки и запоминают 2-ю посылку на месте 1-й.

Позиции несовпадений

$$0\,1\,0\,1\,1\,0 \qquad (6.1)$$

запоминают дополнительно. Таким образом, используют $2n$ элементов памяти, где n — число элементов в одной посылке (в примере $n = 6$). Третью посылку сравнивают со второй. Совпадающие элементы 3-й посылки без изменения записывают на место 2-й посылки:

$$1\,1\,.\;.\;.\;1.$$

Аналогично записывают несовпадающие элементы 3-й посылки, которым соответствуют ранее запомненные несовпадения, а именно 4-й и 5-й элементы

$$.\;.\;.\;1\,0.$$

Остальные несовпадающие элементы 3-й посылки перед записью инвертируют, следовательно, 3-й элемент

$$.\;.\;1\;.\;.\;.$$

Таким образом, вместо 2-й посылки окажется записан результат мажоритарной обработки «два из трех»

$$1\,1\,1\,1\,0\,1. \qquad (6.2)$$

Несовпадения 2-й и 3-й посылок

$$0\,0\,1\,1\,1\,0$$

логически складывают с хранимыми несовпадениями

$$\begin{array}{r} 010110 \\ +\;001110 \\ \hline 011110, \end{array} \qquad (6.3)$$

а результат логического сложения (6.3) записывают на место ранее хранимых несовпадений (6.1).

Таким образом, к концу приема 3-й посылки в n элементах памяти хранится результат мажоритарной обработки и в n элементах памяти — несовпадения (6.3). Если к концу приема 3-й посылки оценка состояния канала связи указывает на необходимость продолжения приема посылок и декодирования по критерию «три из пяти», то осуществляют прием 4-й и 5-й посылок

$$4.\;0\,1\,0\,0\,1\,1;$$
$$5.\;0\,1\,0\,1\,0\,1.$$

Четвертую посылку сравнивают с результатом мажоритарной обработки (6.2) и выявляют несовпадения

$$1\,0\,1\,1\,1\,0. \qquad (6.4)$$

На место результата (6.2) записывают совпадающие элементы 4-й посылки, т.е. 2-й и 6-й:

$$.\ 1\ .\ .\ .\ 1 \qquad (6.5)$$

и несовпадающие элементы, которым соответствуют хранимые несовпадения (6.3), т.е. 3, 4 и 5-й элементы:

$$.\ .\ 0\,0\,1. \qquad (6.6)$$

Остальные элементы 4-й посылки перед записью инвертируют, поэтому 1-й элемент

$$1\ .\ .\ .\ .\ .\ . \qquad (6.7)$$

Таким образом, из (6.5), (6.6) и (6.7) формируется промежуточный результат

$$1\,1\,0\,0\,1\,1. \qquad (6.8)$$

Ранее хранимые несовпадения (6.3) логически перемножают с выявленными несовпадениями (6.4):

$$\begin{array}{r} 011110 \\ \times\ 101110 \\ \hline 001110 \end{array} \qquad (6.9)$$

и результат (6.9) записывают на место несовпадений (6.3).

Таким образом, и на этом этапе оказываются задействованными только $2n$ элементов памяти.

Продолжают прием 5-й посылки, сравнивают ее с промежуточным результатом (6.8) и выявляют несовпадения:

$$1\,0\,0\,1\,1\,0. \qquad (6.10)$$

Совпадающие 2, 3, 6-й элементы 5-й посылки записывают на место промежуточного результата (6.8) без изменения

$$.\ 1\,0\ .\ .\ 1.$$

Аналогично записывают несовпадающие элементы, которым соответствуют хранимые несовпадения (6.9), т. е. 4 и 5-й элементы:

$$.\ .\ .\ 1\,0. \qquad (6.11)$$

Остальные элементы 5-й посылки перед записью получают 1-й элемент

$$1 \quad . \quad . \quad . \quad . \quad . \quad . \qquad (6.12)$$

В результате из (6.10), (6.11) и (6.12) формируется результат мажоритарной обработки «три из пяти»

$$1\,1\,0\,1\,0\,1,$$

который записывается на место промежуточного результата (6.8). Вероятностные характеристики метода «m из (2 m — — 1)» имеют следующий вид:

$$P_э \approx C^m_{2m-1} P^m_0, \qquad (6.13)$$

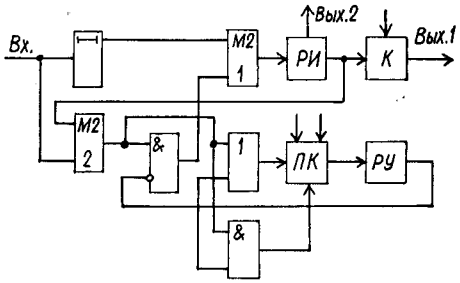


Рис. 6.2

$$P_{ош} = 1 - \sum_{j=0}^{n} \sum_{i=0}^{n-j} \sum_{\nu=0}^{n-j-i} \frac{(C^{m-1}_{2m-1})^j C_n (C^{m-2}_{2m-1})^i C^i_{n-j} \dots (C^1_{2m-1})^\nu \cdot C^\nu_{n-j-i} \dots}{C^{(m-1)j+(m-2)i+\dots+\nu}_{(2m-1)n}} \times$$

$$\times P\{[(m=1)j + (m-2)i + \dots + \nu],\ (2m-1)n\}. \qquad (6.14)$$

Техническая реализация. На рис. 6.2 изображена функциональная схема декодирующего устройства, реализующего рассмотренный метод адаптивного мажоритарного декодирования.

Перед приемом информации все разряды информационного регистра РИ находятся в состоянии 0, а управляющего регистра РУ — в состоянии 1.

Первая посылка сообщения через элемент задержки и сумматор по модулю два М2(1) поступает в РИ. При этом единицы, выданные с выхода РУ, запрещая прохождение информации на второй вход сумматора М2(1), вновь перезаписываются в РУ. Во время приема 2-й посылки на сумматоре

по модулю два М2(2) происходит поэлементное сравнение обеих посылок и запись 2-й посылки в РИ. При этом результат сравнения через элемент И (на второй вход последнего поступают единицы из РУ) и переключатель ПК вводится в РУ.

Во время приема 3-й посылки на сумматоре М2(2) происходит поэлементное сравнение 2-й и 3-й посылок. При этом совпавшие элементы непосредственно через сумматор М2(1) поступают в РИ, поскольку на втором входе сумматора М2(1) сигнал отсутствует. В случае несовпадения сравниваемых элементов возможны два варианта.

Если имеет место несовпадение одноименных элементов первых двух посылок, то в РИ соответствующие элементы 3-й посылки записываются без изменения, так как на второй вход сумматора М2(1) сигнал не подается ввиду наличия на запрещающем входе схемы запрета сигнала, поступающего с выхода РУ.

Если в первой паре сравниваемых посылок произошло совпадение одноименных элементов, то соответствующие элементы 3-й посылки изменяются на противоположные, поскольку импульсы несовпадения с выхода сумматора М2(2) через элемент запрета беспрепятственно поступят на другой вход сумматора М2(1). При этом через элемент ИЛИ и переключатель ПК в РУ перезаписываются импульсы несовпадения первой пары сравниваемых комбинаций и добавляются импульсы несовпадения 2-й и 3-й посылок. Таким образом, в РИ вводится результат мажоритарного декодирования трехкратного дублированного сообщения, а в РУ — логическая сумма несовпадений принятых посылок.

Во время приема 4-й посылки происходит ее сравнение с последовательностью, записанной в РИ. При этом совпавшие элементы непосредственно без изменения через сумматор М2 (1) поступают в РИ, поскольку на втором входе М2 (1) сигнал отсутствует. В случае несовпадения аналогично предыдущему возможны также два варианта.

Если имеет место несовпадение одноименных элементов первых трех посылок, то в РИ соответствующие элементы 4-й посылки записываются без изменения, так как на второй вход сумматора М2 (1) сигнал не подается ввиду наличия на запрещающем входе схемы запрета сигнала, поступающего с выхода РУ.

Если в первых трех посылках произошло совпадение одноименных элементов, то соответствующие элементы 4-й посылки изменяются на противоположные, поскольку им-

пульс несовпадения с выхода сумматора М2 (2) через схему запрета поступит на другой вход сумматора М2(1). При этом через элемент И и ПК в РУ записываются единицы только в те разряды, в которых вновь произошло несовпадение. Таким образом, в РИ вводится последовательность, являющаяся промежуточным результатом, а в РУ — логическое произведение несовпадений, записанных после приема 3-й посылки, с несовпадениями, выявленными после приема 4-й посылки.

Во время приема 5-й посылки вновь происходит сравнение с последовательностью, записанной в РИ. При этом без изменения в РИ вводятся все совпавшие на сумматоре М2(2) элементы, а также те несовпавшие, на местах которых в РУ записаны единицы, которые запрещают прохождение сигнала несовпадения с сумматора М2(2) через элемент запрета на второй вход сумматора М2(1). Все остальные несовпавшие элементы инвертируются на сумматоре М2 (1) и записываются в РИ. Таким образом, в РИ вводится результат мажоритарного декодирования «три из пяти». После приема 5-й посылки результат в последовательном коде через ключ К снимается с выхода *1* устройства, а в параллельном коде — с выхода *2*.

Таким образом, рассмотренное устройство при изменении состояния каналов связи позволяет без потери промежуточной информации изменять критерий мажоритарного решения.

6.2. Расширение области адаптивного мажоритарного декодирования кодов с повторением

При снижении качества канала связи в течение длительного времени оказывается целесообразным введение дополнительной избыточности путем увеличения числа передач кодов с повторением, с последующей мажоритарной обработкой. При этом возможна поэтапная обработка принимаемых посылок без потери промежуточных результатов [12].

Определение метода. В соответствии с этим методом подсчитывают число единиц в одноименных элементах $(2^m - 1)$ посылок, где $m = 2,3,\ldots, M$, и полученное число μ_i $[i = 1,2,\ldots,n]$ для каждого из n элементов в виде цифрового кода последовательно записывают. При приеме очередной посылки упомянутые цифровые коды последовательно и синхронно считывают. Корректируют, увеличивая на единицу,

те числа μ_i, которым соответствуют единичные элементы очередной посылки, при условии, что $\mu_i < M$, и вновь последовательно перезаписывают. При этом результат мажоритарной обработки образуют каждый раз в момент приема нечетных посылок по правилу: если $\mu_i \geqslant m$ — формируют информационную единицу, а если $\mu_i < m$ — формируют нуль.

Рассмотрим действие способа на примере мажоритарного декодирования кодов с $(2m-1)$ повторением, где $m = 2,3,\ldots, 7$, т.е. $M = 7$. Как было отмечено, для записи цифровых кодов необходимо $3n$ элементов памяти. Если $n = 5$, то в частном случае можно использовать три пятиразрядных регистра сдвига. Для наглядности предположим, что имеют место искажения и поэтому посылки, приведенные в табл. 6.1, на совпадают:

Таблица 6.1

Номер посылки	Номер разрядов посылок				
	1	2	3	4	5
1	1	1	0	1	1
2	0	1	1	0	1
3	1	1	0	1	1
4	0	0	1	0	0
5	1	1	0	0	0
6	1	1	0	0	1
7	0	1	0	1	1
8	1	0	1	0	1
9	1	1	1	0	0
10	0	0	0	1	0
11	1	1	0	0	1
12	0	1	1	0	1
13	1	0	0	0	0

Память представим в виде трех регистров сдвига Р1, Р2 и Р3, где i-й столбец предназначен для записи цифрового кода, соответствующего числу единиц в i -х элементах принятых комбинаций.

Так, для пяти комбинаций из табл. 6.1 цифровые коды в памяти будут следующие:

т.е. для первого элемента принято 3 единицы, для второго — 4, для третьего — 2 и т.д. Рассмотрим действие способа для приведенных в табл. 6.1 данных.

Принимают первую посылку, подсчитывают число единиц и цифровые коды записывают в регистры сдвига со стороны 5-х разрядов, продвигая их с каждым новым при-

нимаемым элементом влево. Таким образом к концу приема 1-й посылки содержимое регистров будет следующее:

Регистр	1	2	3	4	5	
P1	1	0	0	0	1	2^0
P2	1	0	1	1	1	2^1
P3	0	1	0	0	0	2^2

Регистр	1	2	3	4	5	
P1	1	1	0	1	1	2^0
P2	0	0	0	0	0	2^1
P3	0	0	0	0	0	2^2

т.е. в регистре P1 запишется 1-я посылка. Принимают 2-ю посылку и одновременно последовательно и синхронно считывают цифровые коды (6.15), начиная с первых разрядов регистров. Цифровые коды (6.15) корректируют — увеличивают на единицу для тех элементов, для которых в данный момент принимают единицу, т. е. для 2,3, 5-го элементов, и новый результат опять перезаписывают (так как в данный момент все $\mu_i < M$). По окончании приема 2-й посылки в регистрах будем иметь цифровые коды:

$$\begin{array}{l} 1\,0\,1\,1\,0; \\ 0\,1\,0\,0\,1; \\ 0\,0\,0\,0\,0. \end{array} \qquad (6.15)$$

При приеме 3-й посылки рассмотренные операции повторяются и одновременно из скорректированных цифровых кодов формируют результат по критерию «два из трех» и перезаписывают в регистры цифровые коды

$$\begin{array}{l} 0\,1\,1\,0\,1; \\ 1\,1\,0\,1\,1; \\ 0\,0\,0\,0\,0. \end{array} \qquad (6.16)$$

Так как $m = 2$ (трехкратное повторение), то $\mu_1 = m$, $\mu_2 > m$, $\mu_3 < m$, $\mu_4 = m$ и $\mu_5 > m$ и результат мажоритарной обработки будет

$$1\,1\,0\,1\,1.$$

Этот же результат можно получить повторно, считывая цифровые коды (6.16) из регистров и применяя к ним известное правило. При необходимости осуществляют прием очередных посылок.

После приема 4-й посылки цифровые коды в регистрах будут

$$\begin{array}{l} 0\,1\,0\,0\,1; \\ 1\,1\,1\,1\,1; \\ 0\,0\,0\,0\,0, \end{array}$$

а после приема 5-й посылки —

1 0 0 0 1;
10 1 1 1;
0 1 0 0 0.

Так как в этом случае $m = 3$ (пятикратное повторение), то $\mu_1 = m$, $\mu_2 > m$, $\mu_3 < m$, $\mu_4 < m$, $\mu_5 = m$ и результат мажоритарной обработки будет

1 1 0 0 1.

Аналогично осуществляется прием и обработка очередных посылок и после окончания приема 10-й посылки в регистрах будет следующие цифровые коды:

0 1 0 0 0;
1 1 0 0 1;
1 1 1 1 1.

Так как $\mu_2 = M = 7$, то при приеме 11-й посылки μ_2 остается без изменения (не корректируется) и в регистры перезапишутся цифровые коды

1 1 0 0 1;
1 1 0 0 1;
1 1 1 1 1.

В этом случае $m = 6$, $\mu_1 > m$, $\mu_2 > m$, $\mu_3 < m$, $\mu_4 < m$, $\mu_5 > m$. Поэтому результат мажоритарной обработки будет

1 1 0 0 1.

При приеме 12-й посылки $\mu_1 = \mu_2 = \mu_5 = 7 = M$ и, следовательно, μ_1, μ_2, и μ_5 не корректируются. В регистры перезапишутся цифровые коды

1 1 1 0 1;
1 1 0 0 1;
1 1 1 1 1.

Те же цифровые коды и по той же причине не корректируют при приеме 13-й посылки. Поэтому в регистры перезапишутся цифровые коды

1 1 1 0 1;
1 1 0 0 1;
1 1 1 1 1.

В этом случае $m = M = 7$, $\mu_1 = m$, $\mu_2 = m$, $\mu_4 = m$, $\mu_5 = m$ и результат мажоритарной обработки будет

1 1 0 0 1.

Реализация известных способов для рассмотренных кодов потребовала бы 12 n элементов памяти, т.е. сложность этого устройства оказалась бы в четыре раза больше. Чрезмерная сложность и ограничивала до настоящего времени применение указанных устройств в адаптивных системах связи.

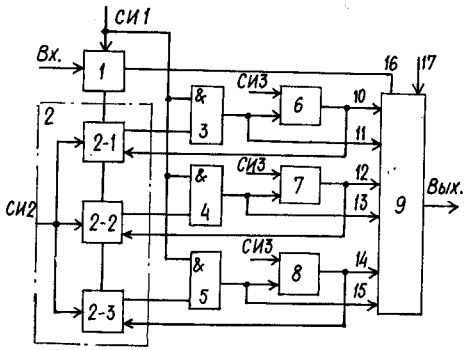


Рис. 6.3

Техническая реализация. Функциональная схема адаптивного мажоритарного декодирующего устройства, реализующего рассмотренный метод, представлена на рис. 6.3. Устройство содержит ключ *1*, счетчик *2*, логические схемы *3,4* и *5*, регистры сдвига *6,7,8* и решающий блок *9*, функциональная схема которого изображена на рис. 6.4.

Работает устройство следующим образом. Исходное состояние счетчика *2* и регистров сдвига *6*, *7*, *8* — нулевое, ключ *1* открыт. Первая посылка через ключ *1* поступает на вход счетчика *2*. Если принимаемый элемент — единица, то в первый разряд *2—1* счетчика *2* записывается единица в регистр сдвига *6*, а СИ2 устанавливает счетчик *2* в состояние нуль, подготавливая его к приему очередного элемента. Синхроимпульс СИ3 обеспечивает сдвиг единицы из первого разряда регистра сдвига *6* во второй. При приеме нулевого элемента состояние счетчика *2* не меняется, а в регистр *6* записывается нуль (имеет место только сдвиг информации).

Таким образом, по окончании приема 1-й посылки она окажется записанной в регистр сдвига *6*. Состояние регистров *7* и *8* — нулевое. Синхроимпульс СИ3 сдвигает информацию в регистре *6* на один разряд, и первый элемент 1-й посылки с выхода регистра *6* поступает на установочный вход первого разряда *2—1* счетчика *2*. Если этот элемент единица, то первый разряд счетчика *2* устанавливается в это же состояние. Если первый элемент 2-й посылки также есть единица, то состояние счетчика *2* изменится — первый разряд установится в нуль, а второй —

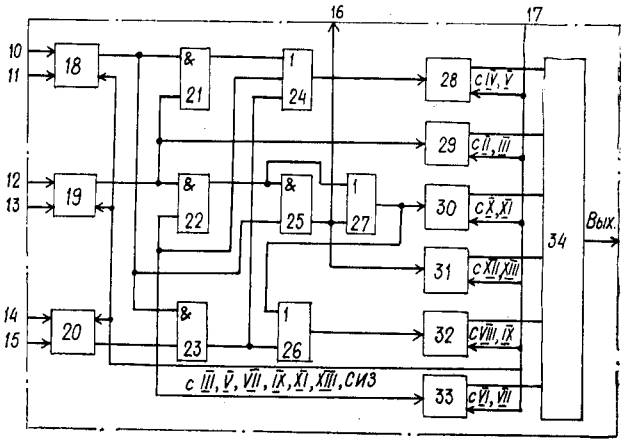


Рис. 6.4

в единицу. Действующий вслед за этим СИ1 считывает состояние счетчика *2* и при этом в первый разряд регистра *6* записывается нуль, а в первый разряд регистра *7* — единица. Далее СИ2 сбрасывает счетчик *2* в нуль, а СИ3 сдвигает информацию в регистрах на один разряд и устанавливает счетчик *2* в состояние, соответствующее второму элементу 1-й посылки. Далее на вход счетчика *2* поступает второй элемент *2*-й посылки и переводит счетчик *2* в соответствующее состояние, которое считывается СИ1 и записывается в регистры *6* и *7*, после чего СИ2 сбрасывает счетчик *2* в нуль, а СИ3 сдвигает информацию в регистрах *6,6* и подготавливает счетчик *2* установкой его в соответствующее состояние к приему очередного элемента из канала связи и т. д. При приеме каждого элемента 3-й посылки первый и второй разряды счетчика *2* могут оказаться в одном из следующих состояний — 00, 10, 01

и 11. Синхросигнал II, соответствующий окончанию приема 2-й посылки и необходимому качеству канала связи, открывает ключ 29 решающего блока *9*. Информационная единица формируется и выдается на выход устройства для состояний 01 и 11 счетчика *2* (две или три единицы из трех возможных). Информационный нуль формируется и выдается на выход устройства для состояний 00 и 10 счетчика *2* (три или два нуля из трех возможных). Если результат мажоритарной обработки «два из трех» необходимо выдать повторно, то на вход *17* решающего блока *9* попадается синхросигнал III, который поступает на управляющие входы переключателей *18, 19, 20* и на управляющий вход ключа *29*. Переключатели *18, 19, 20* подключают решающую схему блока *9* на выход регистров *6, 7* и *8*, а ключ *29* открывается. Содержимое регистров *6* и *7* поступает в решающий блок *9*, где формируется мажоритарный результат, выдаваемый повторно через ключ *29* на выход устройства.

Если состояние каналов связи на момент окончания приема 2-й и 3-й посылок таково, что результат мажоритарной обработки не будет удовлетворять требованию по верности информации, то синхросигналы II и III не формируются и результат мажоритарной обработки на выход устройства не выдается. Продолжается прием 4-й посылки, которая обновляет содержимое регистров сдвига *6*, *7* и *8*. Так, если для *i*-го элемента сообщения после приема трех посылок было зафиксировано состояние *11* (принята единица во всех трех посылках), то при поступлении единицы и в 4-х посылках счетчик *2* перейдет в состояние 001 и в регистры сдвига *6* и *7* при считывании информации СИ1 запишется нуль, а в регистр *8* — единица. После окончания приема 4-й посылки состояние регистров сдвига *6*, *7* и *8* будет характеризовать в двоичном коде число принятых единиц для каждого разряда сообщения (см. табл. 6.2).

Таблица 6.2

Р6	Р7	Р8	Число единиц
2^0	2^1	2^2	
0	0	0	0
1	0	0	1
0	1	0	2
1	1	0	3
0	0	1	4

При необходимости выдачи результата мажоритарной обработки «три из пяти» синхросигнал IV открывает ключ *28* и с поступлением очередных элементов 5-й посылки обновляется состояние счетчика *2*, результат считывается и запоминается в регистрах *6*, *7*, *8* и одновременно проходит в решающий блок

9. Для состояния 110, 001 и 101 формируется единица, а для состояний 000, 100 и 010 — нуль. Результат через ключ *28* выдается на выход устройства. Повторная выдача производится при подаче синхросигнала V, который подключает решающую схему блока *9* к выходу регистров *6*, *7* и *8* и открывает ключ *28*. Запомненный в регистрах *6,7* и *8* двоичный код, соответствующий числу принятых единиц для каждого разряда сообщений, аналогично рассмотренному ранее выдается в решающий блок *9*, где формируется и выдается (повторно) на выход устройства результат мажоритарной обработки «три из пяти».

Если на данном этапе результат мажоритарной обработки не должен выдаваться, то синхросигналы четвертый и пятый не формируются и продолжается прием *6*-й посылки. Результат мажоритарной обработки по критерию «четыре из семи» полностью определяется состоянием третьего разряда 2—3 счетчика *2* после приема соответствующего элемента 7-й посылки, а следовательно, содержимым регистра сдвига *8*. Поэтому этот результат снимается или с выхода разряда 2—3 счетчика *2* через схему И *5*, переключатель *20* и ключ *33* (при действии синхросигнала VI), или с выхода регистра *8* через переключатель 20, ключ *33* (при действии синхросигнала VII).

Аналогично происходит прием и обработка по критериям «пять из девяти», «шесть из одиннадцати» и «семь из тринадцати». В этом случае действуют соответствующие синхросигналы и элементы решающей схемы блока *9* и соответственно открываются ключи *32*, *30* и *31*. Отличие состоит в том, что максимальная емкость счетчика *2* $V_{max} = 7$ (состояние разрядов 111). Следовательно, при приеме числа единиц $V > V_{max}$ состояние счетчика *2* не должно меняться. Это достигается подачей СИ3 на управляющие входы переключателей *18*, *19*, *20*. При этом на время считывания информации с регистров *6,7* и *8* решающий блок *9* подключается к выходам последних. Если считывается состояние 111, то появляется сигнал на выходе *16*, срабатывают схемы И *22* и *25* блока *9*, который закрывает ключ *1*, исключая возможный прием единицы очередной посылки. Состояние счетчика *2* 111 не меняется и вновь перезаписывается в регистры *6*, *7* и *8*. При считывании СИ1 одновременно открывает ключ *1*, подготавливая устройство к приему очередного элемента сообщения.

Рассмотренное устройство обладает более высокой технико-экономической эффективностью, чем известные, так как выполняет операции мажоритарной обработки для

любых кодов с $(2m-1)$ повторением, где $m = 2, 3, 4, 5, 6, 7$.

В общем случае устройства для мажоритарного декодирования кодов с $(2m-1)$ повторением, построенные по известным принципам, имеют сложность, характеризуемую S_1 элементами памяти

$$S_1 \approx 2(m-1)n,$$

а сложность рассмотренного устройства оценивается выражением

$$S_2 \approx]\log_2(m+1)[n,$$

где $]x[$ — ближайшее целое число, не меньшее X.

Таким образом, устройство, построенное по известному принципу, сложнее на η %, где

$$\eta = \frac{S_1 - S_2}{S_2} \cdot 100\ \% = \frac{2(m-1) -]\log_2(m+1)[}{]\log_2(m+1)[} \cdot 100\ \%.$$

Если $m = 7$, то $\eta = 300$ %.

Разработанный метод и устройства являются перспективными для использования [3] в ИС при многократном считывании информации магнитных носителей. Это позволяет снизить исходные требования к вероятности ошибки на один знак и соответственно повысить плотность записи информации.

6.3. Мажоритарное декодирование избыточных (n, κ)-кодов с повторением

Данный метод относится к комбинированным методам защиты информации от ошибок, в которых сочетаются исправление части ошибок посредством мажоритарной обработки $(2m-1)$ повторений с последующей проверкой полученного результата на наличие или отсутствие ошибок по контрольным проверкам избыточного (n, κ)-кода.

Вероятностные характеристики метода для ДСК без памяти. Если используется трехкратное повторение комбинаций избыточного (n, κ)-кода, для которого σ — кратность гарантийно обнаруживаемых ошибок, то после мажоритарной обработки будем иметь

$$P_э \cong 3P_0^2.$$

Вероятность необнаружения ошибок в этом случае

$$P_{н.о} = \frac{1}{2^r} \sum_{i=\sigma+1}^{n} C_n^i P_э^i (1-P_э)^{n-i} \qquad (6.17)$$

или

$$P_{\text{н. о}} \approx \frac{1}{2^r} C_n^{\sigma+1} P_э^{\sigma+1}, \qquad (6.18)$$

где (6.18) — приближенное выражение.
Потери информации при этом оцениваются по формуле

$$P_п = 1 - (1 - P_э)^n \approx nP_э. \qquad (6.19)$$

В тех случаях, когда мажоритарной обработке подвергается $(2m - 1)$ повторений, $P_э(m)$ может быть получено из следующего приближенного выражения:

$$P_э(m) \approx C_{2m-1}^m P_0^m. \qquad (6.20)$$

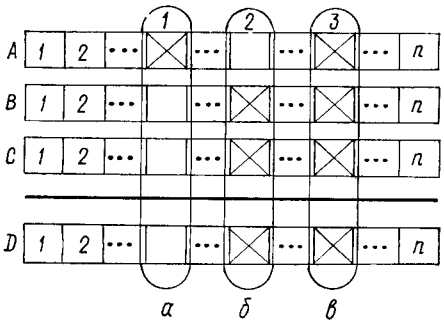


Рис. 6.5

Характеристики метода для канала с группирующимися ошибками. Из рис. 6.5 следует, что к необнаруживаемым ошибкам относятся ошибки, содержащие $t (t = 0,1 \ldots, \omega)$ искажений типа единицы, j $(j = 0,1,2,\ldots, \omega - t)$ искажений типа двойки при $t + j \leqslant \omega$ и i искажений типа тройки $(i = \sigma + 1 - j, \ \sigma + 2 - j, \ldots, \ n - t - j)$. Отметим, что $\omega < n$; в этом случае число необнаруживаемых ошибок определенной кратности

$$N_{t,\,j,\,i} = 3^t 3^j C_n^t C_n^j C_{n-t}^j C_{n-t-j}^i,$$

а общее число ошибок данной кратности — $N_{t,\,j,\,i}^{\Sigma} = C_{3n}^{t+2j+3i}$.

Предполагая все ошибки равновероятными и зная суммарную вероятность этих ошибок $P[(t + 2j + 3i), 3n]$, можно определить вероятность необнаруженных ошибок рассматриваемой кратности

$$P_{\text{н. о}}(t,\ j,\ i) = \frac{3^t 3^j C_n^t C_{n-t}^j C_{n-t-j}^i}{C_{3n}^{t+2j+3i}} P[(t + 2j + 3i),\ 3n].$$

Суммируя $P_{\text{н. о}}(t, j, i)$ по всем значениям t, j и i, получим выражение для определения полной вероятности необнаружения ошибок

$$P_{\text{н. о}}(\alpha) = \frac{1}{2^r} \sum_{t=0}^{\omega} \sum_{i=0}^{\omega-t} \sum_{i=\sigma+i-j}^{n-t-j} \operatorname{sign}(i) \frac{3^t 3^j C_n^t C_{n-t}^j C_{n-t-j}^i}{C_{3n}^{t+2j+3i}} \times \\ \times P[(t+2j+3i)\, 3n], \qquad (6.21)$$

где $\operatorname{sign}(i) = \begin{cases} 1, & \text{если } i \geqslant 0, \\ 0, & \text{если } \quad 0; \end{cases}$ $\frac{1}{2^r}$ — коэффициент, учитывающий обнаружение ошибок более высокой кратности, чем σ.

В определенных случаях можно уменьшить вероятность необнаруженных ошибок соответствующим выбором верхнего предела для переменных t и j, если независимо от результата контрольных проверок избыточного кода браковать информацию в случаях, когда число несовпадений (искажения типа единицы и двойки) в одноименных элементах превысит некоторый порог ω.

Не все составляющие выражения (6.21) имеют одинаковый вес. Некоторые из них убывают очень быстро. Это позволяет использовать приближенную формулу

$$P_{\text{н. о}}(\alpha) \approx \frac{1}{2^r} \frac{3^{\omega} C_n^{\sigma+1} C_{n-(\sigma+1)}^{\omega-(\sigma+1)}}{C_{3n}^{\omega+\sigma+1}} P[(\omega+\sigma+1),\ 3n]. \qquad (6.22)$$

Считая, что потери информации обусловливаются неисправляемыми ошибками, последние можно оценить при помощи выражения (6.14). В том случае, когда число несовпадений ограничивается параметром $\omega < n$, необходимо в выражении (6.14) в качестве верхнего предела использовать ω. Потери информации при этом несколько возрастают.

6.4. Поэтапная обработка кодов с повторением

В [6] рассматривается способ передачи и приема поэтапно закодированных сообщений. Использование этого способа для кодов с повторением позволяет наилучшим образом использовать вводимую избыточность, обеспечивая наибольшую верность без снижения оперативности управления и увеличения потерь информации.

Сравнительный анализ алгоритмов декодирования кодов с повторением. В соответствии с первым алгоритмом прием посылок и декодирование с обнаружением ошибок осуществляют до тех пор, пока в очередном сообщении не будут обнаружены ошибки. В этом случае достоверность определяется как функция

$$P_{\text{н. о}_1} = F_1(d_0)$$

и оперативность управления как

$$t_{q_1}^{\min} = \frac{k+r}{V}, \qquad (6.23)$$

где V — скорость модуляции. Следовательно, имеет место высокая оперативность и низкая достоверность, поскольку для повышения достоверности не используется вся вводимая избыточность.

В соответствии со вторым алгоритмом декодирования осуществляют $(2m-1)$ посылок, мажоритарную обработку по критерию большинства и декодирование с обнаружением ошибок результата мажоритарной обработки.

В данном случае достоверность определяется как функция

$$P_{\text{н. о}_2} = F_2[(2m-1)d], \text{ причем } P_{\text{н. о}_2} \ll P_{\text{н. о}_1}.$$

Однако оперативность управления резко снижается и характеризуется выражением

$$t_{q_2}^{\min} = (2m-1)\frac{(k+r)}{V},$$

т. е.

$$t_{q_2}^{\min} = (2m-1)\, t_{q_1}^{\min}.$$

Алгоритм поэтапного декодирования кодов с повторением сочетает преимущества как первого, так и второго из рассмотренных выше алгоритмов. В соответствии с этим алгоритмом осуществляется прием и декодирование повторных посылок сообщения и первое правильно декодированное сообщение в качестве предварительного решения выдается для начала исполнения. Этим обеспечивается высокая оперативность управления. Повторные посылки сообщения накапливаются, обрабатываются мажоритарным способом и декодируются. Декодированное сообщение сравнивается с предварительным решением. При их совпадении предварительное решение не изменяется. При несовпадении предварительное решение бракуется и в качестве окончательного решения выдается сообщение, декодированное после накопления и мажоритарной обработки. Этот

метод характеризуется высокой оперативностью управления ($t_{g_1}^{min}$) и большим значением достоверности передаваемой информации ($P_{н.\,о_2}$). Возможны различные модификации разработанного алгоритма поэтапного декодирования, обусловленные заданными требованиями по достоверности доведения информации и оперативности управления. Определим области целесообразного применения тех или других алгоритмов декодирования кодов с повторением.

Области применения алгоритмов декодирования кодов с повторением. Решение поставленной задачи выполняется в предположении использования каналов связи с независимыми ошибками, характеризуемых одним параметром—вероятностью искажения одного элемента комбинации P_0.

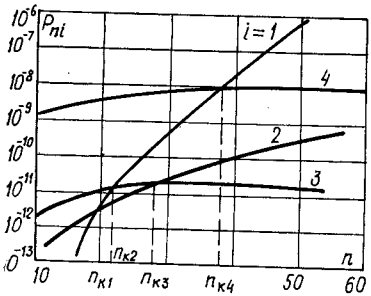


Рис. 6.6

Алгоритм декодирования, в соответствии с которым первая правильно декодированная посылка сообщения выдается получателю, обеспечивает следующие характеристики.

Достоверность информации может быть вычислена по формуле

$$P_{н.\,о_1} = \frac{1}{2^r} \sum_{i=\sigma+1}^{n} C_n^i P_0^i (1 - P_0)^{n-1}.$$

Потери информации характеризуются выражением

$$P_{п_1} \approx [1 - (1 - P_0)^n]^{2m-1}.$$

При $nP_0 \ll 1$ может быть использовано приближенное выражение

$$P_{п_1} \approx (nP_0)^{2m-1}.$$

Минимальное время доведения информации до получателя характеризуется выражением (6.23).

На рис. 6.6 приведена зависимость $P_{п_1} - f_1(n)$ для $P_0 - 10^{-2}$ при условии, что $2m - 1 = 15$.

В соответствии со вторым алгоритмом осуществляется накопление $l < 2m - 1$ повторных посылок сообщения,

мажоритарная обработка по критерию большинства и декодирование с обнаружением ошибок результата мажоритарной обработки. Правильно декодированное сообщение выдается получателю. В случае обнаружения ошибок сообщение бракуется и осуществляется очередной цикл, состоящий из накопления новых l посылок, мажоритарной обработки и декодирования. Таких циклов может быть от 1 до $\frac{2m-1}{l}$.

Достоверность, надежность доведения информации и оперативность управления могут быть вычислены по следующим формулам:

$$P_{\text{н. о}_2} = \frac{1}{2^r} \sum_{i=\sigma+1}^{n} C_n^i P_{э_1}^i (1 P_{э_1})^{n-1};$$

$$P_{э_1} \approx C_l^{\frac{l+1}{2}} P_o^{\frac{l+1}{2}};$$

$$P_{п_2} = [1 - (1 - P_{э_1})^n]^{\frac{2m-1}{l}} \approx (nP_{э_1})^{\frac{2m-1}{l}};$$

$$\text{tg}_2^{\min} = \frac{(k+r)\,l}{V}.$$

Сравнительный анализ показывает, что

$$P_{\text{н. о}_2} < P_{\text{н. о}_1} \text{ и } \text{tg}_2^{\min} > \text{tg}_1^{\min}.$$

На рис. 6.6 приведена зависимость $P_{п_2} = f_2(n)$, из которой видно, что при $n < n_{k_1}$

$$P_{п_1} < P_{п_2},$$

а при $n > n_{k_1}$, $P_{п_1} > P_{п_2}$.

Критическое значение длины кодовой комбинации может быть вычислено по формуле

$$n_{k_1} = [C_l^{0,5(l+1)}]^{\frac{1}{l-1}} P_o^{-0,5}.$$

Третий алгоритм предусматривает выдачу получателю 1-й правильно декодированной посылки сообщения, накопление всех повторных посылок, мажоритарную обработку по критерию большинства, декодирование результата мажоритарной обработки и его сравнение с результатом первого правильного декодирования.

Достоверность, надежность доведения информации и оперативность управления вычисляются по следующим формулам:

$$P_{\text{н. о}_3} = \frac{1}{2^r} \sum_{i=o+1}^{n} C_n^i P_{э_2}^i (1 - P_{э_2})^{n-i};$$

$$P_{э_2} \approx C_{2m-1}^m P_o^m;$$

$$P_{п_3} = 1 - (1 - P_{э_2})^n \approx nP_{э_2};$$

$$tq_3^{min} = tq_1^{min}.$$

Сравнительный анализ показывает, что

$$P_{\text{н. о}_3} < P_{\text{н. о}_2} < P_{\text{н. о}_1}, \text{ а } tq_3^{min} = tq_1^{min} < tq_2^{min}.$$

На рис. 6.6 приведены зависимости, из которых видно, что при $n < n_{k_1} P_{п_1} < P_{п_2} < P_{п_3}$; при $n_{k_1} < n < n_{k_2} P_{п_2} < P_{п_1} < P_{п_3}$; при $n_{k_2} < n < n_{k_3} P_{п_2} < P_{п_3} < P_{п_1}$, а при $n > n_{k3} P_{п3} < P_{п2} < P_{п1}$.

Критические значения длины кодовой комбинации n_{k2} и n_{k3} могут быть определены по следующим формулам:

$$n_{k_2} \approx (C_{2m-1}^m)^{\frac{1}{2(m-1)}} P_o^{-0,5};$$

$$n_{k3} \approx (C_{2m-1}^m)^{\frac{l}{2m-1-l}} (C_l^{0,5(l+1)})^{\frac{2m-1}{l-2m+1}} P_o^{0,5}.$$

В соответствии с четвертым алгоритмом накапливают l повторных посылок сообщения, обрабатывают их по критерию большинства, декодируют и при необнаружении ошибок результат декодирования выдают получателю и запоминают. Запоминается также результат мажоритарной обработки. Продолжают накапливать повторные посылки сообщения и при этом каждые l посылок обрабатывают по критерию большинства и запоминают результат обработки. После приема всех посылок сообщения $\frac{2m-1}{l}$ результатов мажоритарных обработок обрабатывают по критерию большинства, результат обработки декодируют и сравнивают с результатом первого правильного декодированного сообщения. При их совпадении первое решение не меняется, а при несовпадении отменяется исполнение предварительного решения и получателю выдается последнее решение.

Достоверность, надежность доведения информации и оперативность управления вычисляются по следующим формулам:

$$P_{\text{н. о}_4} = \frac{1}{2^r} \sum_{i=\sigma+1}^{n} C_n^i P_{\text{э3}}^i (1 - P_{\text{э3}})^{n-i};$$

$$P_{\text{э3}} \approx C_{\frac{2m-1}{l}}^{0,5\left(\frac{2m-1}{l}+1\right)} P_{\text{эl}}^{0,5\left(\frac{2m-1}{l}+1\right)};$$

$$P_{\text{п4}} = 1\,(1 - P_{\text{э3}})^n \approx nP_{\text{э3}};$$

$$\text{tq}_4^{\min} = \frac{(k+r)\,l}{V}.$$

Сравнительный анализ показывает, что

$$P_{\text{н. о3}} < P_{\text{н. о4}} < P_{\text{н. о2}} < P_{\text{н. о1}};\ \text{tq}_4^{\min} = \text{tq}_2^{\min} > \text{tq}_3^{\min}.$$

Однако достоверность предварительного решения четвертого алгоритма выше, чем третьего. Проще оказывается и аппаратурная реализация четвертого алгоритма.

На рис. 6.6 приведена зависимость $P_{\text{п4}} = f_4(n)$, из которой можно сделать вывод, что для всех значений $nP_{\text{п3}} < P_{\text{п4}}$. При $n < n_{k_1} P_{\text{п1}} < P_{\text{п2}} < P_{\text{п3}} < P_{\text{п4}}$;

$$\begin{aligned}
&n_{k1} < n < n_{k2}\ \ P_{\text{п2}} < P_{\text{п1}} < P_{\text{п3}} < P_{\text{п4}};\\
&n_{k2} < n < n_{k3}\ \ P_{\text{п2}} < P_{\text{п3}} < P_{\text{п1}} < P_{\text{п4}};\\
&n_{k3} < n < n_{k3}\ \ P_{\text{п3}} < P_{\text{п3}} < P_{\text{п1}} < P_{\text{п4}};\\
&n_{k4} < n < n_{k4}\ \ P_{\text{п3}} < P_{\text{п2}} < P_{\text{п4}} < P_{\text{п1}};\\
&n > n_{k5} < n_{k5}\ \ P_{\text{п3}} < P_{\text{п4}} < P_{\text{п2}} < P_{\text{п1}}.
\end{aligned}$$

Критические значения длины кодовой комбинации можно вычислить по формулам:

$$n_{k4} \approx \left[C_{\frac{2m-1}{l}}^{\frac{2m-1+l}{2l}} (C^{0,5(l+1)})^{\frac{2m-1+l}{2l}} P_{\text{o}}^{\frac{l^2+2m-1+l-3l(2m-1)}{4l}} \right]^{\frac{1}{2(m-1)}};$$

$$n_{k5} \approx \left[C_{\frac{2m-1}{l}}^{\frac{2m-1+l}{2l}} \right]^{\frac{l}{2m-1-l}} [C_l^{0,5(l+1)}]^{\frac{l(2m-1+l)}{2(2m-1)(2m-1-l)}} P_{\text{o}}^{-\left(\frac{l+1}{4}\right)}.$$

Методика выбора алгоритмов декодирования. Исходными данными для выбора алгоритмов декодирования кодов

с повторениями являются заданные значения достоверности $P^{з}_{н.\,о}$, надежности доведения информации до управляемых объектов $P^{з}_{н}$, оперативности управления $tq^{з}$ и длины информационной части кодовой комбинации κ, обусловленной количеством передаваемых сообщений и разнообразием их признаков, а также характеристиками каналов P_0.

На первом этапе выбираются характеристики обнаруживающего ошибки кода (r и σ) для кодирования одного повторения сообщения.

Вычисляются основные параметры с использованием приведенных формул и строятся графические зависимости $P_{пi} = f_i(n)$ для заданных характеристик канала связи и различных значений m.

Когда $n > n_{k5}$ и $tq_4^{min} < tq^{з}$ при $P_{нач} < P^{з}_{н.\,о}$ выбирается четвертый алгоритм декодирования. При $P_{нач} > P^{з}_{н.\,о}$ следует отдать предпочтение третьему алгоритму, хотя это и приведет к усложнению аппаратурной реализации.

При $n_{k4} < n < n_{k5}$, а также $tq^{з} < tq_2^{min}$ выбирается третий алгоритм при условии, что $P_{п3} < P^{з}_{п}$. В противном случае следует увеличить m_{min} и произвести новую оценку.

При $tq^{з} > tq_2^{min}$ может быть выбран четвертый алгоритм при условии $P_{п4} < P^{з}_{п}$, как обладающий большей достоверностью, или второй алгоритм при $P_{п2} < P^{з}_{п} < P_{п4}$ и $P_{н.\,о2} < P^{з}_{н.\,о}$.

Таким образом, на основе метода адаптивного мажоритарного декодирования кодов с повторением, базирующегося на принципе циклического сдвига с насыщением индексов состояния одноименных элементов принимаемой информации, синтезированы мажоритарные декодирующие устройства, обеспечивающие достижение требуемой помехоустойчивости приема при значительно меньшей сложности технической реализации. Новый метод является перспективным для использования в ИС при многократном считывании информации с магнитных носителей, так как позволяет снизить исходные требования к вероятности ошибки на один знак и соответственно повысить плотность записи информации.

Сравнительная оценка различных алгоритмов поэтапного декодирования избыточных (n, κ)-кодов с повторением позволила определить области их предпочтительного использования и разработать методику выбора требуемого алгоритма.

7. ОПТИМАЛЬНЫЕ И БЛИЗКИЕ К НИМ МЕТОДЫ ПРИЕМА И ОБРАБОТКИ СООБЩЕНИЙ С ИЗБЫТОЧНОСТЬЮ

7.1. Общие положения

Рассмотренные ранее методы основаны на поэлементном приеме сообщений. В этом случае процедуры демодуляции и декодирования оказываются между собой не связанными, что определяет простоту технической реализации устройств но одновременно снижает помехоустойчивость приема сообщений. Это происходит потому, что первая решающая схема по установленному правилу идентифицирует принятый элементарный сигнал с сиволом 0 или 1, который направляется в декодер (вторая решающая схема), а информация о форме сигнала теряется и в дальнейшей обработке не принимает участия. В результате увеличиваются потери информации и уменьшается вероятность правильного приема.

Поэтому все более широкое распространение получают методы, в которых процедуры демодуляции и декодирования объединяются в большей или меньшей степени, чем обусловливается их большая или меньшая оптимальность.

В случае приема в целом вся информация, содержащаяся в принятом сигнале относительно переданного сообщения, может быть использована объединенной решающей схемой, что увеличивает вероятность правильного приема. Реализация этого метода встречает значительные трудности, поэтому разрабатываются методы сопряжения процедур демодуляции и декодирования при фиксированном приемнике. Это прежде всего декодирование в целом, прием по наиболее надежным символам, метод Вагнера, прием с использованием сигналов стирания и другие методы, занимающие промежуточное положение между поэлементным приемом и приемом в целом.

Так как в основе построения идеального декодера находится метод сопоставлений с полным набором 2^k кодовых комбинаций, то это определяет его применение для небольших значений κ. Поэтому в настоящее время большое распространение получили квазиоптимальные методы декодирования, допускающие определенные ограничения, несколько снижающие помехоустойчивость, но приводящие к существенному уменьшению сложности декодирующих устройств.

7.2. Метод Вагнера и прием по наиболее надежным элементам

Характерной особенностью метода Вагнера [4] является его возможность применения к избыточным (n, κ) -кодам, имеющим четкое значение минимального кодового расстояния d_0, и исправления всех ошибок кратности $t \leqslant \frac{d_0}{2}$.

Напомним, что кратность гарантийно исправляемых ошибок для избыточных (n, κ)-кодов в общем случае определяется соотношением

$$t \leqslant \left[\frac{d_0 - 1}{2}\right].$$

Следовательно, если $d_0 = 4$, то возможно исправить только однократные ошибки, в то время как метод Вагнера позволяет исправить однократные и двухкратные ошибки.

Структурная схема декодирующего устройства, реализующего данный метод, приведена на рис. 7.1. В накопитель Н записывается принимаемая кодовая комбинация, а вероятностный декодер ВД вычисляет вероятности ошибки P_{ji} $(j = 1,2..., m + 1;\ i = 1,2,...,n)$ для каждого принимаемого элементарного сигнала, сравнивает их между собой и определяет номер ρ самого ненадежного элемента, для которого $P_{j\rho} = P_{j\rho\max}$.

Одновременно кодовая комбинация проверяется на наличие или отсутствие ошибок в декодере Д, который в данном цикле настроен на режим обнаружения ошибок кратности $\sigma \leqslant d_0 - 1$.

При необнаружении ошибок комбинация выдается из накопителя Н через схему ИЛИ на выход устройства. При необнаружении ошибки декодер Д перестраивается в режим исправления ошибок кратности $t \leqslant \left[\frac{d_0 - 1}{2}\right]$ и выдает сигнал в Н и ВД.

Кодовая комбинация из Н поступает на один из входов сумматора по модулю два, на другой вход которого подается импульс в ВД в момент прохождения самого ненадежного элемента. Этот элемент инвертируется, и следовательно, если в начальный момент в комбинации было $\frac{d_0}{2}$ искаженных элементов, то последовательность на выходе сумматора будет иметь $\frac{d_0}{2} - 1$ искаженных элементов. С вы-

хода сумматора комбинация поступает в декодер Д, который известными методами исправляет $\frac{d_0}{2} - 1$ оставшихся ошибок, и исправленная комбинация с выхода декодера Д через схему ИЛИ поступает на выход устройства.

Другим методом декодирования, занимающим промежуточное положение между поэлементным приемом и приемом в целом, является декодирование по наиболее надежным элементам (метод Бородина). Процедура декодирования в этом случае характеризуется тем, что решение о переданной кодовой комбинации принимается не по всем n

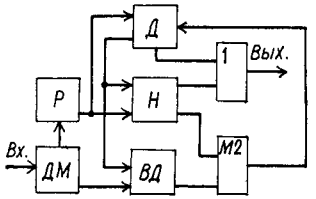


Рис. 7.1

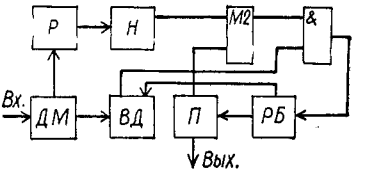


Рис. 7.2

элементам, а по n_1 наиболее надежным элементам. Поскольку в любой кодовой комбинации можно стереть, по крайней мере, $(d_0 - 1)$ элементов, для того чтобы сохранить возможность различать кодовые комбинации, то число наиболее надежных элементов должно лежать в пределах

$$k \leqslant n_1 \leqslant n - d_0 + 1.$$

С учетом сказанного процедура декодирования начинается с выделения k наиболее надежных элементов в принятой кодовой комбинации. Эти элементы сравниваются с одноименными элементами 2^k эталонных комбинаций. Процесс декодирования заканчивается, если окажется, что эти элементы однозначно определяют одну из комбинаций кода. Если же отобранные элементы совпадают с элементами двух или более кодовых комбинаций, то к ним добавляется еще один наиболее надежный среди оставшихся $(n - k)$ элементов и процесс сравнения повторяется. Описанные операции продолжаются до тех пор, пока не окажется, что отобранные элементы отличаются от какой-то одной комбинации в числе позиций, меньшем, чем от всех остальных. В этом случае могут быть исправлены все ошибки вплоть до $(d_0 - 1)$-кратных при условии, что $(n - d_0 + 1)$ правильно принятых элементов имеют меру похожести, большую, чем неправильно принятые.

На рис. 7.2 изображена структурная схема декодера, осуществляющего прием по наиболее надежным элементам. Эти элементы определяются вероятностным детектором ВД, сигналы с выхода которого на схеме И опрашивают результат сравнения надежных элементов с одноименными элементами эталонных комбинаций, поступающих из блока памяти II. Решающий блок РБ продолжает процесс декодирования, формируя сигнал на ВД для добавления дополнительного наиболее надежного элемента, или заканчивает декодирование.

В этом случае сигнал с РБ поступает в блок памяти II, считывая наиболее похожую кодовую комбинацию на выход устройства.

Отметим, что сложность технической реализации метода приема по наиболее надежным символам не намного уступает идеальному декодированию в целом, так как в основе метода сохраняется принцип сопоставлений с полным набором эталонных кодовых комбинаций.

В заключение приведем без доказательства выражение, которое вытекает из теоремы Финка [31] и устанавливает соотношение между вероятностями приема кодовой комбинации с ошибками для различных методов приема

$$P_1 \geqslant P_2 \geqslant P_3 \geqslant P_4, \qquad (7.1)$$

где P_1 — вероятность того, что при поэлементном приеме кодовая комбинация принята с ошибкой ($P_{ош}$); P_2 — вероятность того, что при поэлементном приеме с исправлением максимально возможного числа ошибок произошла неисправимая ошибка; P_3 — вероятность приема кодовой комбинации с ошибкой при идеальном декодировании в целом; P_4 — вероятность того, что при поэлементном приеме с обнаружением ошибок произошла необнаруженная ошибка.

Соотношение (7.1) переходит в равенство только при коде без избыточности. Дополнительно следует отметить, что вероятности P_2 и P_4 являются нижней и верхней границей оценки помехоустойчивости для заданного кода и канала связи при идеальном декодировании в целом.

7.3. Оптимизация обработки избыточных кодов в каналах со стиранием

Определение двоичного симметричного стирающего канала ДССтК. На рис 7.3 изображен график, иллюстрирующий статистические характеристики *ДССтК*, которые определяются тремя вероятностями: P — вероятностью трансфор-

мации элемента при отсутствии стираний; S — вероятностью стирания элемента; q — вероятностью правильного приема элемента при отсутствии стираний.
При этом всегда выполняется условие

$$P + q + S = 1.$$

На выходе двоичных приемников с симметричным интервалом стирания случайные величины отождествляются с элементом 0 только тогда, когда

$$y_j < -v,$$

а с элементом *1*, когда

$$y_j > v,$$

где v — порог стирания и распределение $f_0(y)$ является зеркальным отображением распределения $f_1(y)$ относительно нуля. Если окажется, что $-v < y_j < v$, то дополнительно вырабатывается символ Θ стирания, фиксирующий факт ненадежности данного элемента.

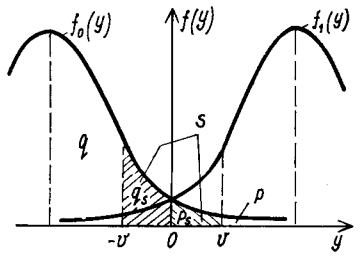


Рис. 7.3

Очевидно, что вероятность трансформации элемента P определяется формулой

$$P = \int_{-\infty}^{-v} f_1(y)\,dy = \int_{v}^{\infty} f_0(y)\,dy, \qquad (7.2)$$

а вероятность стирания

$$S = \int_{-v}^{v} f_0(y)\,dy = \int_{-v}^{v} f_1(y)\,dy. \qquad (7.3)$$

Из рис. 7.3 и выражений (7.2, 7.3) очевидно, что

$$\begin{aligned} S &= P_s + q_s; \\ P_0 &= P + P_s; \\ q_0 &= q + q_s, \end{aligned} \qquad (7.4)$$

где P_s — вероятность правильного стирания элемента; q_s — вероятность ложного стирания; P_0 — вероятность

искажения элемента; q_0 — вероятность правильного приема элемента. Стирания Θ, отмечающие ненадежные элементы принимаемой кодовой комбинации могут быть использованы для повышения помехоустойчивости приема так же, как используются апостериорные вероятности ошибки P_j в оптимальных и квазиоптимальных методах.

Известны три метода обработки избыточных кодов с использованием стираний.

В соответствии с первым методом кодовая комбинация стирается, если стерт хотя бы один элемент либо если кодом обнаружена ошибка. Этот метод относится к адаптивным методам приема, косвенно учитывающим качество используемого канала связи. Он позволяет обеспечить высокое значение достоверности, которое достигается за счет увеличения потери информации. Второй метод отличается от первого только тем, что избыточный код используется для исправления ошибок. Его эффективность невелика.

Третий метод используется для исправления стираний и обнаружения ошибок на нестертых позициях. Стирание кодовой комбинации осуществляется либо в том случае, когда число стертых элементов больше, чем $d_0 - 1$, либо когда код обнаруживает на нестертых позициях ошибки.

Покажем, что этот метод и некоторые его модификации расположены достаточно близко к оптимальным методам декодирования.

Исправление стираний. Математическое описание для ДССтК. Пусть кодовый метод используется для исправления стираний и обнаружения ошибок на нестертых позициях. Вероятность необнаружения декодером ошибки при стирании j элементов ($j = 1,2,3,\ldots,n$)в кодовой комбинации определяется из предположения, что для ее отождествления стираются все j одноименных элементов в сопоставляемых с принятой разрешенных комбинациях. При этом можно считать, что кодовые комбинации укорачиваются на число, равное числу стертых элементов. Число возможных комбинаций становится равным 2^{n-j}, а число разрешенных остается равным 2^k. Тогда доля кодовых комбинаций с необнаруженными ошибками будет

$$q_{\text{н. о}} = \begin{cases} 2^{-(n-k-j)} & \text{для } i+j \geqslant d_0; \\ 0 & \text{для } i+j < d_0, \end{cases}$$

где i — число ошибок на нестертых позициях. Вероятность необнаружения ошибок в общем виде определяется выражением

$$P_{\text{н.о}}(s, n) = \sum_{i=1}^{d_0-1} \sum_{j=d_0-i} 2^{-r+j} P(i, n) P_s(j, n) +$$
$$+ \sum_{i=d_0}^{n} \sum_{j=0}^{d_0-1} 2^{-r+j} P(i, n) P(i, n) P_s(j, n), \qquad (7.5)$$

где $P(i, n)$ — вероятность трансформации i элементов на нестертых позициях; $P_s(j, n)$ — вероятность стирания j элементов.

Для канала связи с независимыми ошибками выражение (7.5) приобретает следующий вид:

$$P_{\text{н.о}}(s, n) = \sum_{i=1}^{d_0-1} 2^{-r+d_0+i} C_n^i P^i C_{n-i}^{d_0-i} S^{d_0-i} (1-p-s)^{n-d_0} +$$
$$+ \sum_{i=d_0}^{n} \sum_{j=0}^{d_0-1} 2^{-r+j} C_n^i P^i C_{n-i}^j S^j (1-p-s)^{n-(i+j)}. \qquad (7.6)$$

Потери информации в данном методе обусловливаются теми ошибками, которые не были исправлены при помощи стираний, но были обнаружены кодовым способом. Вероятность обнаруженных ошибок определяется по формуле

$$P_{\text{о.о}}(s, n) = \sum_{i=1}^{d_0-1} \sum_{j=0}^{d_0-1-j} P(i, n) P_s(j, n) +$$
$$+ \sum_{i=1}^{d_0-1} \sum_{j=d_0-i} \frac{2^{r-j}-1}{2^{r-j}} P(i, n) P_s(j, n) +$$
$$+ \sum_{i=d_0}^{n} \sum_{j=0}^{d_0-1} \frac{2^{r-j}-1}{2^{r-j}} P(i, n), P_s(j, n) + \sum_{j=d_0}^{n} P_s(j, n). \qquad (7.7)$$

Для канала связи с независимыми ошибками выражение (7.7) приобретает вид

$$P_{\text{о.о}}(s, n) = \sum_{i=1}^{d_0-1} \sum_{j=0}^{d_0-1-i} C_n^i P^i C_{n-i}^j S^j (1-p-s) +$$
$$+ \sum_{i=1}^{d_0-1} \frac{2^{r-d_0+i}}{2^{r-d_0+i}} C_n^i P^i C_{n-i}^{d_0-i} S^{d_0} (1-p-s)^{n-d_0} +$$
$$+ \sum_{i=d_0}^{n} \sum_{j=0}^{d_0-1} \frac{2^{r-j}-1}{2^{r-j}} C_n^i P^i C_{n-i}^j (1-p-s)^{n-(i+j)} +$$
$$+ \sum_{j=d_0}^{n} C_n^j S^j (1-s)^{n-j}. \qquad (7.8)$$

При выполнении условий $p < s$ и $s \ll 1$ выражения (7.6) и (7.8) можно упростить, ограничившись членами, имеющими наибольший вес. В этом случае получим

$$P_{\text{н. о}}(s, n) \approx 2^{-r+d_0-1} n C_{n-1}^{d_0-1} P S^{d_0-1} (1-p-s)^{n-d_0}, \quad (7.9)$$

$$P_{\text{о.о}}(s, n) \approx np(1-p-s)^{n-1}. \quad (7.10)$$

Режим исправления стираний позволяет уменьшить потери информации при незначительном снижении достоверности по сравнению с режимом обнаружения ошибок циклическим кодом. Следовательно, при ДССтК режим исправления стираний по помехоустойчивости занимает промежуточное положение между режимами исправления и обнаружения ошибок избыточных кодов.

Исправление стираний в каналах связи с группирующимися ошибками. Приняв допущение о том, что законы группирования ошибок и стираний одинаковы и взяв за основу модель канала с группирующимися ошибками, описанную в [35], получим выражения для определения следующих вероятностных характеристик:

$$\begin{aligned} P(\geqslant i, n) &= P\left(\frac{n}{i}\right)^{1-\alpha}; \\ P_s(\geqslant j, n) &= S\left(\frac{n}{j}\right)^{1-\alpha}; \\ P(i, n) &= P(\geqslant i, n) - P[\geqslant (i+1), n]; \\ P_s(j, n) &= P(\geqslant j, n) - P[\geqslant (j+1), n]. \end{aligned} \quad (7.11)$$

Подставляя (7.11) в (7.5) и (7.7), получим формулы для определения вероятностей необнаружения и обнаружения ошибок в каналах связи с группирующимися ошибками.

Реализация метода исправления стираний. На рис. 3.7 представлена функциональная схема устройства исправления стираний [8].

Сложность рассмотренного в п.3.4 устройства в элементах памяти S может быть оценена при помощи выражения

$$S_1 = 3n + k,$$

а быстродействие, характеризуемое максимальным временем обработки сообщения,

$$\delta_1 = \frac{1}{t_{\text{об}}^{\max}} = \frac{1}{\tau(2^k+1)n},$$

где τ — длительность тактового интервала.

Так как в основу рассмотренного метода положен принцип сопоставлений, то это приводит к значительному снижению быстродействия устройства, что является его существенным недостатком.

7.4. Модифицированный метод исправления стираний

Недостаток рассмотренного в п.7.2 метода, состоящий в малом быстродействии, может быть устранен, если стирания использовать для формирования возможных векторов ошибок, их поочередного наложения на принятую кодовую комбинацию с последующей кодовой проверкой полученного результата [9].

На рис. 7.4 изображена функциональная схема соответствующего модифицированного устройства для исправления стираний. Работает устройство следующим образом.

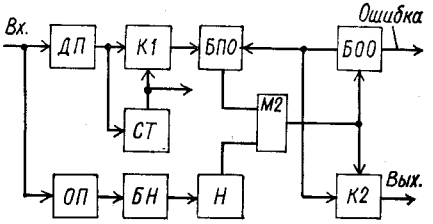


Рис. 7.4

Принятая кодовая комбинация одновременно поступает на входы однопороговой ОП и двухпороговой ДП схем. С выхода ОП кодовая комбинация через буферный накопитель БН вводится в основной накопитель Н. В результате анализа каждого принимаемого элемента кодовой комбинации на выходе ДП появляется сигнал стирания в том случае, если принятый элемент не может быть отождествлен ни с единицей, ни с нулем. Стирания через открытый ключ К1 подаются в блок формирования полиномов ошибок БПО и подсчитываются счетчиком СТ. Устройство рассчитано на исправление $t = d_0 - 1$ стираний, поэтому емкость СТ равна t. При появлении стираний в количестве $\eta > t$ импульс переноса с выхода СТ закрывает К1 и может использоваться для стирания кодовой комбинации. После приема n элементов комбинации избыточного (n, κ)-кода последняя из Н подается на вход сумматора по модулю два, на другой вход которого из БПО одновременно поступает нулевой полином ошибок. С выхода сумматора элементы принятой комбинации подаются в блок обнаружения ошибок БОО. На выход устройства элементы комбинации не поступают, так как ключ К2 закрыт. При необнаружении ошибок БОО выдает сигнал в БПО и на управляющий

вход К2, открывая его. Блок, восприняв сигнал необнаружения ошибок, в очередном цикле формирует полином ошибок, аналогичный предыдущему, т. е. нулевой. Кодовая комбинация второй раз поступает из Н через сумматор и открытый ключ К2 непосредственно на выход устройства. Если при первом цикле проверки БОО обнаруживает ошибку, то комбинация из Н выдается на проверку второй раз и при этом БПО формирует полином одиночной ошибки для ДССтК, который на сумматоре осуществляет первую попытку исправления принятой комбинации. Скорректированная комбинация проверяется в БОО, который при необнаружении ошибки выдает сигнал в БПО и на управляющий вход К2, открывая его.

Блок БПО формирует полином одиночной ошибки, аналогичный предыдущему, и исправленная комбинация в очередном цикле работы через К2 поступает на выход устройства. Если БОО обнаружит ошибку в первом варианте скорректированной комбинаций, то проверки продолжаются. При этом БПО формирует очередной полином ошибки и т. д. до первого необнаружения ошибки в какомлибо из вариантов скорректированной комбинации, после чего в очередном цикле исправленная комбинация поступает на выход. Если ошибка будет обнаружена во всех циклах проверки, включая и последний, при котором комбинация корректируется полиномом t-кратной ошибки, то БОО фиксирует наличие в принятой комбинации неисправляемой ошибки, о чем выдает сигнал на выход. В результате могут исправляться ошибки до t-кратных включительно в том случае, когда они произошли на стертых позициях.

Быстродействие рассмотренного устройства определяэтся выражением

$$\delta_2 = \frac{1}{n\tau\left(\sum_{i=0}^{t} C_i^i + 1\right)},$$

что в μ_1 раз больше, чем в случае (7.3)

$$\mu_1 = \frac{\delta_2}{\delta_1} = \frac{2^k + 1}{\sum_{i=0}^{t} C_i^i + 1}.$$

Если $K = 50$ и $t = 4$, то $\mu_3 = 6 \cdot 10^{13}$.

Однако повышение быстродействия достигается за счет увеличения сложности, которая оценивается выражением

$$S_2 \approx n\left(\sum_{i=0}^{t} C_t^i + 1\right) + 2n + r,$$

где первый член определяет сложность БПО; $2n$ характеризует сложность БН и Н; r определяет сложность БОО. Следовательно, можно записать, что $S_2 > S_1$ в μ_2 раз:

$$\mu_2 = \frac{S_2}{S_1} = \frac{n\left(\sum_{i=0}^{t} C_t^i + 1\right) + 2n + r}{3n + k}.$$

Если $k = 50$; $n = 62$; $t = 4$, то $\mu_2 \cong 5$.

Метод исправления ошибок просмотром вариантов нежестких решений является перспективным для использования в ИС и позволяет улучшить характеристики почти любого алгоритма декодирования блочных кодов за счет снижения быстродействия [3].

7.5. Исправление стираний в кодах с повторением

Исправление стираний в кодах с повторением позволяет значительно повысить помехоустойчивость достаточно простыми средствами [12].

Математическое описание. Если имеет место двукратное повторение сообщения, закодированного избыточным (n, k)-кодом, то при обнаружении ошибки в первой посылке целесообразно ее запоминание $(\vec{Y}_1)$. При приеме второй посылки $(\vec{Y}_2)$ фиксируются соответствующие ей стирания $\vec{\Theta}$ и определяется результат сложения по модулю два $(\vec{\Omega})$ одноименных элементов $\vec{Y}_1$ и $\vec{Y}_2$. Результат логического перемножения $\vec{\Theta}$ и $\vec{\Omega}$

$$\vec{e} = \vec{\Theta}\,\vec{\Omega}$$

с большей вероятностью указывает на искаженные элементы второй посылки, которые инвертируются в соответствии с $\vec{e}$. Скорректированная комбинация

$$\vec{X} = \vec{Y}_2 \oplus \vec{e}$$

подвергается кодовой проверке и при отсутствии ошибок выдается для дальнейшей обработки.

На рис. 7.5 изображена временна́я диаграмма, иллюстрирующая процедуру исправления одиночной ошибки во второй посылке.

Неверная коррекция элементов во второй посылке будет происходить в тех случаях, когда одноименным несовпадающим элементам будет соответствовать ложное стирание. Когда суммарное количество таких коррекций совместно с искажениями на нестертых позициях второй посылки превысит обнаруживающую способность кода ($\sigma = d_0 - 1$), будет иметь место необнаруживаемая ошибка.

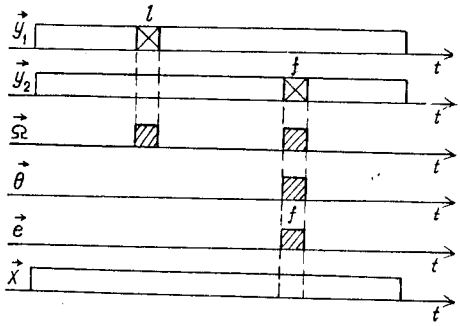


Рис. 7.5

Вероятность необнаруженных ошибок может быть вычислена по формуле

$$P_{\text{н.о}} = (s, n) \cong \frac{1}{2^r} \sum_{i=d_0}^{n} C_n^i P_0^i (1 - P_0)^{n-i} + \frac{1}{2^r} \sum_{i=1}^{d_0-1} \sum_{j=d_0-i}^{n} C_n^i \times$$
$$\times P_0^i q_s^j (1 - P_0)^{n-i} C_{n-i}^j P^j (1 - P)^{n-(i+j)}.$$

Приближенное выражение получим, если выделим составляющие, имеющие наибольший вес

$$P_{\text{н.о}}(s, n) \approx \frac{1}{2^r} C_n^{d_0} P_0^{d_0} + \frac{C_{n-1}^{d_0-1}}{2^r} n P_0 q_s P^{d_0-1}. \qquad (7.12)$$

Вероятность обнаруженных ошибок, характеризующая потери информации при приеме 2-й посылки, может быть вычислена по формуле

$$P_{\text{о.о}}(s, n) = \sum_{i=1}^{d_0-1} \sum_{j=0}^{d_0-1-i} C_n^i C_{n-i}^j P_0^i q_s^j P^j (1 - P_0)^{n-i} (1 - P)^{n-(i+j)}$$

или приближенно

$$P_{\text{о.о}}(s, n) \approx n P_0 q_s. \qquad (7.13)$$

Техническая реализация. На рис. 7.6 приведена функциональная схема устройства исправления стираний для кодов с повторением. Работает устройство следующим образом.

Принятая кодовая комбинация поступает на входы однопороговой ОП и двухпороговой ДП схем. С выхода однопороговой ОП схемы комбинация в виде последовательности нулей и единиц через ключ К и схему *1* ИЛИ записывается в накопитель Н, а через схему *2* ИЛИ вводится в блок БОО обнаружения ошибок.

В случае обнаружения ошибки блок БОО разрешает выдачу комбинаций из накопителя Н получателю. Комби-

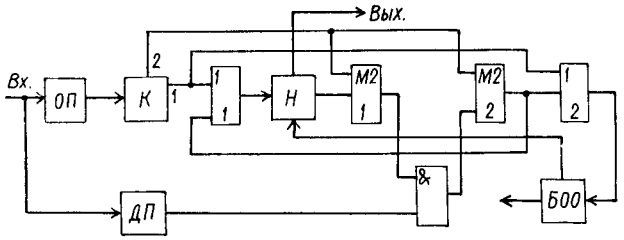


Рис. 7.6

нация из накопителя Н поступает на выход устройства. В случае обнаружения ошибок осуществляется повторный прием сообщения. При этом информационный вход ключа К переключается с выхода *1* на выход *2*. Принятая комбинация второй посылки с выхода *2* ключа К через сумматор *2* по модулю два и схему *1* ИЛИ, осуществляя последовательный сдвиг 1-й посылки на один из входов сумматора *1*, записывается в накопитель Н, а через схему *2* ИЛИ поступает в блок БОО. Если ошибка не обнаружилась, информация из накопителя Н выдается получателю. Для уменьшения числа потерь, возникающих в случае искажения обеих посылок, устройство обеспечивает исправление ошибки при повторении комбинации. Для этого на сумматоре *1* по модулю два происходит поразрядное сравнение обеих комбинаций при одновременном выявлении двухпороговой схемой ДП ненадежных элементов стираний 2-й посылки. Результат стирания поступает на один из входов схемы И, на другой вход которой выдаются сигналы стирания, формируемые двухпороговой схемой ДП. Инвертирование элементов комбинаций 2-й посылки на сумматоре 2

будет происходить в том случае, когда на обеих входах схемы И одновременно появляется сигнал несовпадения двух посылок, формируемый сумматором *1*, и сигнал стирания, выявленный двухпороговой ДП схемой. В абсолютном большинстве случаев это будет соответствовать исправлению искаженной комбинации. Исправленная комбинация 2-й посылки записывается в накопитель Н и в случае необнаружения ошибок блоком БОО выдается получателю.

Сложность рассмотренного устройства оценивается выражением

$$S_3 \approx 2n - k,$$

т.е. оно проще устройства 7.3 на величину

$$\gamma = S_2 - S_3 = n\left(\sum_{i=0}^{t} C_i^i + 2\right).$$

Таким образом, исправление ошибок в избыточных кодах на основе анализа ограниченной совокупности нежестких решений определено как одно из перспективных направлений квазиоптимальных методов приема и обработки сообщений с избыточностью.

В этом случае избыточный код используется только для обнаружения ошибок и эффективность метода приближается к эффективности декодирования двоичных кодов, по методу максимального правдоподобия, что позволяет улучшить характеристики почти любого алгоритма декодирования блочных кодов за счет дополнительных затрат времени на вычисления.

Достаточно эффективны методы исправления стираний и для кодов с повторением.

8. АЛГЕБРАИЧЕСКИЕ МЕТОДЫ ПОСТРОЕНИЯ СВЕРТОЧНЫХ КОДОВ (СК)

8.1. Определение сверточных кодов

Впервые алгебраические конструктивные методы синтеза СК были развиты в [13]. Такие же коды, но несколько позже, были найдены Д. Л. Месси, Д. Д. Кастелло и Й. Юстесеном [20].

Сверточные коды в теоретическом плане являются обобщением блочных, однако наличие функциональной зависи-

мости проверочных элементов от информации, содержащейся не только в данном блоке, но и в других, определяет новое качество и свойство СК [22]: простоту технической реализации при исправлении ошибок; снижение требований к процедуре циклового фазирования; возможность получения как угодно малой вероятности ошибки при конечной скорости передачи и исправления ошибки при скоростях передачи, близких к пропускной способности канала; хорошую совместимость процедуры декодирования СК по максимальному правдоподобию с многоуровневыми модемами, что приближает этот метод обработки по своим возможностям к приему в целом.

Все это позволяет не стремиться к увеличению длины блока и приближает декодирование СК к процессу непрерывной обработки информации, что хорошо согласуется с последовательной и непрерывной передачей больших массивов измерительных данных в ИС с объектами, рассредоточенными на больших расстояниях.

Дадим определение СК, используя терминологию [22].

Сверточный код можно разделить на элементарные блоки (ЭБ) длиной b, состоящие из кодовых символов X_{ij} (1, 2,...,b), где индексы обозначают соответственно номер ЭБ в кодовой последовательности и порядковый номер символа внутри ЭБ. СК используется для преобразования информационной последовательности Z, которая разбивается на ЭБ длиной $b - m$ символов, т. е.

$$Z = z_{i1};\ z_{i2},\ \ldots,$$
$$z_{ib-m};\ z_{i+1b-m};\ z_{i+2,\,1};\ \ldots\ .$$

При этом различают систематические и несистематические СК.

Систематическим сверточным $(b,\ b-m)_L$ -кодом называется отображение множества информационных последовательностей

$$Z = \{z_{ij}\}\ \ (j = 1.\ 2,\ \ldots,\ b-m)$$

на множество кодовых последовательностей $X = \{x_{ij}\}$, где X разделена на ЭБ длиной b символов и включает в себя неизменными символы информационной последовательности, т. е. $x_{ij} = z_{ij}$ для $j = 1, 2, \ldots, b-m$, а символы каждого из L соседних ЭБ связаны между собой с помощью m линейных проверочных соотношений

$$\sum_{\theta=0}^{L-1} \sum_{j=1}^{k} a_{\theta,\,j}^{(\xi)} x_{i-\theta},\ j = 0,\ \xi = 1,\ \ldots,\ m, \qquad (8\ 1)$$

коэффициенты $a^{(5)}_{\theta, j}$ взяты из того же поля, что и символы $x_{i, j}$, а знак $\sum$ означает суммирование в этом поле. Число символов в L ЭБ, символы которых связаны проверочными соотношениями (8.1), называется кодовым ограничением

$$n_{\text{А}} = Lb. \tag{8.2}$$

В несистематическом СК все b символов ЭБ являются линейными функциями соседних L символов информационной последовательности.

Оценка корректирующих возможностей СК осуществляется по трем критериям [22]:

минимальному расстоянию b на длине кодового ограничения $n_{\text{А}}$;

свободному расстоянию df;

профилю (графику) расстояния по длине порождающего многочлена.

Выбор критерия определяется типом декодера СК. Для алгебраического синдромного декодера, работающего на длине кодовых ограничений $n_{\text{А}}$, используют критерий по d. Декодер максимального правдоподобия имеет интервал задержки декодирования, значительно превышающий L, и на этом интервале достигается критерий $d\,f$. Выбор СК по профилю расстояния нужен при последовательном декодировании, потому что вероятность пика числа вычислений и среднее число вычислений на декодированный ЭБ уменьшаются при раннем выявлении ложного пути, а этот путь быстро обнаруживается как раз при последовательном увеличении минимального расстояния с увеличением длины генератора.

В целом свободное расстояние df является определяющим, так как от него зависят и два других критерия, поэтому конструктивные методы нахождения СК наиболее развиты к настоящему времени для критерия df [22].

Скорость кода, определяемая отношением числа информационных символов к длине блока, для сверточных кодов равна

$$R = \frac{Z}{(Z + L)\, b}. \tag{8.3}$$

Если $Z \gg L$, то $R = \frac{1}{b}$.

8.2. Приведение сверточных кодов к многократным циклическим кодам

Реализация линейных проверочных соотношений (8.1) осуществляется при помощи регистра сдвига на L разрядов и сумматоров по модулю два, соединенных в соответствии с (8.1).

Совокупность связей j-го сумматора с разрядами регистра описывается с помощью коэффициентов $\{\delta_{ie}\}$, $l = \overline{1, l}$; $j = \overline{1, b}$. Если j-й сумматор связан с l-м разрядом регистра, то $\delta_{jl} = 1$, в противном случае $\delta_{jl} = 0$. Тогда совокупность связей j-го сумматора с разрядами регистра представима в виде вектора

$$\delta_j = (\delta_{j1}, \delta_{j2}, \ldots, \sigma_{jl}), \quad j = 1, b, \tag{8.4}$$

который в иной форме может быть записан как многочлен $R_j(x)$. Двоичная форма записи вектора $\vec{\delta}_j$ является двоичной формой записи многочлена $R_j(x)$.

Вектор $\vec{x}$ выходного кодового слова сверточного кода можно разложить на b векторов $\vec{x}_1$, где $\vec{x}_j$ есть вектор выходного кодового слова j-го сумматора по модулю два, у которого связи с регистром определяются многочленом $R_j(x)$.

Исходя из этого вектор $\vec{x}$ запишется в виде

$$\vec{x} = (\vec{x}_1, \vec{x}_2, \ldots, \vec{x}_b). \tag{8 5}$$

Известно [14] представление образующей матрицы циклического кода в виде

$$G_{Z+S,\,Z} = \left\| \begin{array}{r} R(x) \\ x\,R(x) \\ x^2R(x) \\ \ldots\ldots\ldots \\ x^{z-1}R(x) \end{array} \right\|, \tag{8.6}$$

где $R(x)$ — образующий (порождающий) полином степени S циклического кода; $x^iR(x)$ — циклический сдвиг на i позиций влево образующего полинома $R(x)$.

Если $Z + S \leqslant n$ и $R(x)$ входит в разложение двучлена x^{n+1}, то имеет место циклический БЧХ-код с заданными корректирующими свойствами. При $Z + S > n$ полученный циклический код теряет свойства БЧХ-кода со всеми вытекающими отсюда последствиями.

Образующую матрицу многократного циклического кода можно представить как расположенные рядом образующие матрицы (8.6) циклических кодов, т. е. в виде

$$G_{bz+\sum_{j=1}^{b} s_j;\ z} = \| G_{z+s_1;\ z} | G_{z+s_2;\ z} | \ldots | G_{z+sb;\ z} \|, \quad (8.7)$$

где $G_{z+s_j;\ z}$ — образующая матрицы циклического кода, образованного полиномом $R(x)$, $j = \overline{1, b}$; S_j — величина, равная степени полинома $R_j(x)$.

Матрица (8.7) определяет выходной вектор $\bar{x}$ (8.5) сверточного кода и является циклической, образованной полиномом, который можно выписать по ее первой строке.

Несмотря на то что матрица (8.7) является циклической, сверточный код не сводится к циклическому коду. Действительно, в противном случае мы не имели бы возможности для произвольного значения Z закодированных сверточным кодом информационных символов при произвольном числе $b \geqslant 2$ сумматоров по модулю два получить величину минимального кодового расстояния df, большую 2. Однако для каждого конкретного значения Z можно образующую матрицу сверточного кода представить в виде образующей матрицы некоторого укороченного циклического кода, причем с изменением Z образующий полином такой матрицы изменяется, поскольку меняется число нулей, расположенных в образующем полиноме результирующей матрицы сверточного кода между полиномами $R_j(x)$. Этот факт изменения образующего полинома и позволяет получить в сверточном коде величину минимального кодового расстояния, большую 2. Необходимо найти минимальное число строк матрицы (8.7), выбранных подряд, по исследованию которых можно предпочесть по величине минимального кодового расстояния в таком укороченном коде один сверточный код другому. В произвольном случае поставленную задачу решить трудно.

Докажем в этой связи следующую теорему.

Теорема 1. Если сверточный код задан образующей матрицей (8.7) $G_{bz+\sum_{j=1}^{b} s_j;\ z}$, то нижняя граница для минимального кодового расстояния определяется величиной

$$df = 2b.$$

Доказательство. Пусть $R_1(x) = \ldots = R_b(x)$, тогда сверточный код вырождается в b-кратное повторение некоторого циклического кода. При произвольном значении Z найдется многочлен $M(x)$ такой, что вес результата произведения $R_1(x)\,M(x)$ будет равен 2, а величина минимального кодового расстояния сверточного кода будет $2b$, хотя многочлен $R_1(x)$ может быть образующим полиномом некоторого циклического (n_1, m_1) БЧХ-кода. Это произойдет в тех случаях, когда

$$M(x) = \frac{x^{Z+s_1}+1}{R_1(x)}.$$

Таким образом, теорема доказана.

Число информационных символов m_1 этого кода может быть больше величины L, т. е. больше увеличенной на единицу степени образующего полинома $R_1(x)$. Поэтому исследование L строк матрицы (8.7) в общем случае не позволяет определить минимальный вес кодовых слов. Если (n_1, m)-код имеет величину минимального кодового расстояния $d_1 > 2$, то, выделив в образующей матрице (8.7) L первых строк (при $m_1 > L$), найдем, что такой сверточный код имеет минимальное кодовое расстояние, равное $d_1 b$, а это не соответствует действительности.

Однако в дальнейшем будет показано, что если $R_1(x) \neq R_2(x) \neq \ldots \neq R_b(x)$ и если порождающий многочлен матрицы (8.7) получен определенным образом из образующего полинома $g(x)$ некоторого циклического (n, κ) БЧХ-кода, достаточно рассмотреть L первых строк матрицы (8.7) для сравнения различных кодов. При этом оказывается, что для лучших кодов величина минимального кодового расстояния больше величины $d_1 b$, полученной при исследовании L строк матрицы (8.7), порождающий многочлен которой содержит полиномы $R_1(x) = R_2(x) = R_b(x)$. Это дает возможность при сравнении моделированием на ЭВМ различных способов синтеза сверточных кодов ограничиваться числом строк матрицы (8.7), равным L.

Таким образом, представимость сверточных кодов в виде многократных циклических кодов позволяет свести задачу выбора порождающей последовательности сверточного кода к выбору b образующих полиномов циклических кодов. При этом необходимо выбрать полиномы так, чтобы для произвольной информационной последовательности вес кодового слова многократного циклического кода был не менее некоторой величины $\frac{\overline{df}}{\overline{df}}$, причем при заданных

значениях b и L величина df должна быть максимальной. Иными словами, необходимо подобрать полиномы таким образом, чтобы b циклических кодов совместно поддерживали вес любого закодированного многочлена не ниже некоторого максимального достижимого уровня. Поскольку циклические коды являются линейными, линейным является и многократный циклический код, т.е. линейная комбинация двух и более любых слов многократного циклического кода представляет собой кодовое слово этого же кода. Следовательно, соответствующим выбором и исследованием полиномов $R_j(x)$ многократного циклического кода можно целенаправленно, а не случайно синтезировать связи сумматоров по модулю два с разрядами x-регистра.

8.3. Синтез систематических сверточных кодов

В п. 8.1 дано определение систематических $(в, в-m)_L$-сверточных кодов и рассмотрены их свойства.

Покажем цикличность проверочной матрицы данного кода и найдем при $b=2$ и $m=1$ алгоритм синтеза связей второго сумматора по модулю два с L-разрядным регистром, обеспечивающий максимальную величину минимального кодового расстояния в кодовом слове при $Z \gg L$. Скорость такого кода $R < 0{,}5$ и стремится к величине 0,5 с ростом Z. Сопоставим связи второго сумматора по модулю два с разрядами регистра в соответствии с полиномом

$$R(x) = a_{L-1}x^{L-1} + a_{L-2}x^{L-2} + \ldots + a_1 x + a_0,$$

где $a_i = 1\,(i = \overline{1, L-2})$, если сумматор связан с $(i+1)$-м разрядом регистра, в противном случае $a_j = 0$.

Образующая матрица такого кода, подвергнутая линейным преобразованиям (перестановке столбцов), не изменяющим ранг матрицы, может быть приведена к каноническому коду

$$G^{*}_{(2Z+L-1);\,Z} = \|\overline{I}_Z;\ G_{(Z+L-1);\,Z}\| = \left\| \begin{matrix} R(x) \\ xR(x) \\ I_Z;\ x^2R(x) \\ \ldots\ldots\ldots \\ x^{Z-1}R(x) \end{matrix} \right\|, \quad (8.8)$$

где $\overline{J}_Z$ — матрица, в которой единицы расположены на побочной диагонали; $G_{(Z-L-1);\,Z}$ — дополнительная матрица $(Z+L-1)$ проверочных элементов; $x^iR(x)$ — циклический сдвиг влево на i столбцов полинома $R(x)$.

С помощью матрицы (8.8) для заданного в виде многочлена $M(x)$ степени $(Z-1)$ кодируемого сообщения можно найти вектор $\vec{x}$ кодового слова сверточного кода. Ранг матрицы (8.8) равен Z и растет с увеличением последнего.

По образующей матрице можно построить проверочную матрицу, представляющую в удобной форме правила построения проверочных символов в кодах с проверкой на четность. Включив в число информационных символов $L-1$ нулей, содержащихся в x-регистре перед введением информации, и $L-1$ нулей, подаваемых в регистр после введения Z информационных символов, проверочную матрицу можно представить в виде

$$B_{(2Z+3L-3);\,(Z+L-1)} = \left\| \begin{array}{l} x^{Z+L-2}R^*(x) \\ \cdots\cdots\cdots \\ x^2R^*(x) \\ xR^*(x);\ I_{(Z+L-1)} \\ 1R(x) \end{array} \right\| = \\ = \| B_{(Z+2L-2);\,(Z+L-1)};I_{(Z+L-1)} \|, \qquad (8.9)$$

где I_{Z+L-1} — единичная матрица; $B_{(Z+2L-2);\,(Z+h-1)}$ — дополнительная матрица; $R^*(x)$ — полином, обратный (двойственный) полиному $R(x)$.

Проверочная матрица (8.9) является циклической, поскольку при $Z=\infty$ сдвиг вправо на единицу компонент любой строки снова дает строку, принадлежащую этой же матрице.

Отметим, что систематические сверточные коды с циклической проверочной матрицей не обеспечивают максимально достижимой величины минимального кодового расстояния, но зато позволяют в кодовом слове выделить в явном виде информационные и проверочные символы, что важно в некоторых приложениях.

Известно [28], что величина $\bar{d}f$ на единицу больше числа выбранных произвольно столбцов, которые можно вычеркнуть в матрице (8.9), не изменяя ее ранга.

Однако в такой общей постановке количество вычислений, необходимое для нахождения полинома $R(x)$, очень велико, или нет гарантии получить максимально возможную величину $\bar{d}f$, если $R(x)$ выбрано случайным образом, как это делалось в известных методиках [22].

Необходимо на основании обнаруженной связи между циклическими и сверточными кодами разработать алгоритм выбора полиномов для синтеза систематических

СК на основании известных полиномов циклических кодов. При этом ставится задача получения кодов с максимальной величиной минимального кодового расстояния при заданных ограничениях на емкость памяти и при условии минимального перебора возможных полиномов.

В связи с этим исследуется возможность такого видоизменения образующего полинома $g(x)$ некоторого циклического (n, κ) -БЧХ-кода, при котором полином $g(x)$ приводится к порождающему многочлену $f(x)$ сверточного кода.

Максимальная величина минимального кодового расстояния в выходном слове среди различных сверточных кодов может быть найдена, если ранг матрицы (8.9) $Z = L$ или если матрица (8.9) содержит $Z = L$ информационных символов.

Следовательно, необходимо исследовать матрицу (8.9), имеющую $(3L - 1)$ столбцов и L строк. Порождающий многочлен такой матрицы имеет степень $(2L - 1)$ и содержит в двоичном представлении $(L - 1)$ нулей между двумя единицами старших разрядов, т. е.

$$F(x) = a_{2L-1}x^{2L-1} + a_{L-1}x^{L-1} + a_{L-2}x^{L-2} + \ldots + a_1x + a_0. \tag{8.10}$$

Покажем, что порождающий многочлен $F(x)$ СК может быть получен методом обобщенной диффузной реконструкции образующего полинома $g(x)$ первообразного циклического кода. Для этого докажем следующую теорему.

Теорема 8.2. Если $g(x)$ — образующий полином циклического (n, κ)-кода, $h(x) = (1 + x^n) / g(x)$ — образующий полином дуального циклического кода, а d_g и d_h — минимальные кодовые расстояния этих кодов, то может быть найден систематический $(2,1)$ L = СК, удовлетворяющий следующим соотношениям:

$$df \geqslant \min_{L>n-k} \{d_g,\ 2d_h\}; \tag{8.11}$$

Доказательство. Преобразуем образующий полином $g(x)$ первообразного циклического кода к виду

$$F(x) = x^{r+\nu} + x^{n-k} + g(x), \tag{8.12}$$

где $\nu = (2L - 1) - r$—число нулей, которое дополнительно вводятся между двумя старшими разрядами $g(x)$; $f_{L-1}(x) = g(x) + x^{n-k}$ — порождающий многочлен образованного $(2,1)_L$-СК.

Произведем оценку веса последовательности X, порождаемой $(2,1)_L$-СК, при вводе информационной последовательности Z:

$$X = F(x)\,Z(x) = x^{r+\nu}\,Z(x) + x^{n-k}Z(x) + g(x)\,Z(x). \quad (8.13)$$

Можно записать, что

$$W[F(x)\,Z(x)] = W[x^{r+\nu}Z(x)] + W[x^{n-k}Z(x) + g(x)\,Z(x)],$$

где $W[Z(x)]$ — вес многочлена $Z(x)$.
Так как

$$W[x^{r+\nu}Z(x)] = W[x^{r+\nu}Z(x)] = W[Z(x)],$$

а

$$W[g(x)\,Z(x)] = dg$$

в тех случаях, когда максимальная степень $Z(x)$ не превышает $(k-1)$, то

$$W[x^{n-k}Z(x) + g(x)\,Z(x)] \geqslant dg - W[Z(x)] \quad (8.14)$$

и, следовательно,

$$W[F(x)\,Z(x)] \geqslant dg. \quad (8.15)$$

Когда $Z(x) = h(x)$, то из (8.13) получим

$$W[g(x)\,h(x)] = 2, W[x^{n-k}h(x) + g(x)\,h(x)] = W[h(x)]$$

и

$$W[F(x)\,h(x)] \geqslant 2d_h. \quad (8\ 16)$$

Полагаем в общем случае, что $Z(x) = S(x)$, причем степень многочлена $S(x)$ превышает $(k-1)$. Тогда возможны два варианта: многочлен $S(x)$ не содержит в качестве сомножителя полином $h(x)$; многочлен $S(x)$ содержит в качестве сомножителя полином $h(x)$.

Для первого варианта получим, что

$$W[g(x)\ S(x)] = dg$$

на основании свойств циклических (n, k)-БЧХ-кодов и

$$W[x^{n-k}S(x) + g(x)\,S(x)] \geqslant dg - W[S(x)]$$

аналогично (8.14). Следовательно,

$$W[F(x)\,S(x)] \geqslant dg. \quad (8.17)$$

Во втором варианте представим $S(x) = S'(x)\,h(x)$. Тогда

$$W[x^{r+\nu}S'(x)\,h(x)] = d_h \quad (8.18)$$

из свойств дуальных циклических кодов, а

$$W[x^{n-k}S'(x)h(x)+g(x)S'(x)h(x)]=d_h,$$

так как

$$x^{n-k}S'(x)h(x)+g(x)S'(x)=h(x)S'(x)[x^{n-k}+g(x)],$$

причем

$$S'(x)[x^{n-k}+g(x)]=S^*(x)$$

есть многочлен, не содержащий в качестве сомножителя $h(x)$, и, следовательно, по аналогии с (8.18).

$$W[h(x)S^*(x)]=d_h. \tag{8.19}$$

В результате из (8.18) и (8.19) получим

$$W[F(x)S(x)]=2d_h. \tag{8.20}$$

Обобщая (8.15 — 8.20), получим (8.11). При этом всегда вследствие обобщенной диффузной реконструкции (ν-раздражения) выполняется неравенство

$$L \leqslant n-\kappa.$$

Таким образом, теорема доказана.

Полученные результаты теоремы (8.2) определяют методику синтеза квазиоптимальных систематических $(2,1)_L$-СК в классе первообразных циклических БЧХ-кодов.

Известно, что минимальные кодовые расстояния dg и d_h являются функциями образующего полинома $g(x) \in \bar{G}$:

$$d_g=F_1[g(x)], \quad d_h=F_2[g(x)],$$

где $\bar{G}$ — множество образующих полиномов циклических кодов из разложения двучлена x^n+1.

Тогда максимальное значение минимального кодового расстояния $(2,1)_L$-СК получим на основании выражения

$$d_f^{\max}=\max_{g(x)\in\bar{G}}\min\{F_1[g(x)],\ 2F_2[g(x)]\}. \tag{8.21}$$

Экспериментальные проверки показывают, что (8.21) имеет место в области значений

$$dg \approx 2d_h, \tag{8.22}$$

что реализуется при относительной скорости первообразного циклического кода $R \approx 0{,}33$ и соответствует числу информационных символов кода

$$k > \left[\frac{1}{3}(n+1)\right]. \tag{8.23}$$

Из возможных образующих полиномов $g(x)$ циклического (n, κ)-кода следует использовать для синтеза только те, которые содержат между двумя самыми старшими разрядами максимальное число нулей, так как это минимизирует емкость памяти кодера при обеспечении заданных корректирующих возможностей кода. Основываясь на доказанном, покажем пример синтеза систематического $(2,1)_L$-СК.

Пример 8.1. Циклический (15,5)-БЧХ-код задан образующим полиномом $g(x) = x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1 \sim 10100110111$ и имеет минимальное кодовое расстояние $d = 7$.

Определяем число разрядов x-регистра $L = 9$ по конфигурации полинома $g(x)$ и находим число нулей для обеспечения ν-раздражения

$$\nu = (2L - 1) - r = 17 - 10 = 7.$$

Следовательно, порождающая последовательность СК будет

$$F(x) = 100000000100110111,$$

где порождающая последовательность подканала проверочных символов

$$f_{L-1}(x) \sim 100110111.$$

Так как дуальный код, определяемый полиномом $h(x)\frac{x^{15}+1}{g(x)}$, имеет минимальное кодовое расстояние $d_h = 4$, то минимальное кодовое расстояние СК будет не менее

$$d_f = \min\{dg,\ 2d_n\} = 7.$$

Для сравнения укажем [22], что систематический $(2,1)_L$-СК, полученный методом наращивания, имеет $d = 6$ и преимущества разработанного конструктивного метода синтеза систематических СК увеличиваются с возрастанием L.

8.4. Методы синтеза несистематических сверточных кодов с относительной скоростью $R = \frac{1}{b}$

Метод обобщенной диффузной реконструкции. Несистематические $(b,1)_L$-сверточные коды задаются образующей матрицей

$$G_b(Z + L - 1);\ Z = \|\, G^{(1)}(Z + L - 1);\ Z \,|\, G^{(2)}(Z + L - 1);$$
$$Z \,|\, \ldots \,|\, G^{(b)}(Z + L - 1);\ Z \,\|. \qquad (8.24)$$

Ограничим образующую матрицу (8.24) L строками и b $(2L-1)$ столбцами. Тогда порождающий многочлен $F(x)$ такой циклической матрицы можно выписать по ее первой строке. Он имеет степень не более $[(b-1)(2L-1)+L-1]$ и содержит по $L-1$ нулю между каждой парой входящих в него образующих полиномов $B_j(x)$, степень каждого из которых также не превышает величины $L-1$.

Результаты, полученные в предыдущем параграфе, можно распространить на синтез связей $b \geqslant 2$ сумматоров по модулю два с разрядами x-регистра, при которых достигается максимальная (или близкая к ней) величина минимального кодового расстояния сверточного кода.

Докажем для этого следующую теорему.

Теорема 8.3. Пусть $g(x)$ — образующий полином циклического (n, κ)-кода, $h(x)$ — образующий полином дуального циклического кода, а d_g и d_h — соответственно минимальные кодовые расстояния этих кодов. Тогда существует несистематический $(b, 1)_L$-СК, удовлетворяющий соотношениям

$$d_f \geqslant \min\{d_g, b, d_h\}; \qquad (8.25)$$

$$L \leqslant \sup\{(r+1)/b\}.$$

Доказательство. Пусть $b=2$. Методом обобщенной диффузной реконструкции преобразуем порождающий полином $g(x)$ первообразного циклического (n, k)-кода к виду

$$F(x) = g(x)\,x^{L-1} + [g'(x) + g(x)],$$

где $L \leqslant \sup\{(r+1)/2\}$ — объем памяти одного подканала синтезируемого кода; $f^{(1)}_{L-1} = g'(x)\,x^{L-1}$ — порождающий многочлен первого подканала $(2,1)_L$-СК; $f^{(2)}_{L-1} = g'(x) + g(x)$ — порождающий многочлен второго подканала $(2,1)_L$-СК.

Произведем оценку веса последовательности X, порождаемой $(2,1)_L$-СК, при вводе информационной последовательности Z:

$$X = F(x)\,Z(x) = g'(x)\,x^{L-1}\,Z(x) + g'(x)\,Z(x) + g(x)\,Z(x).$$

Веса многочленов определяются следующим образом:

$$W[F(x)\,Z(x)] = W[g'(x)\,x^{L-1}Z(x)] + W[g'(x)\,Z(x) + g(x)\,Z(x)],$$

причем

$$W[g'(x)\,x^{L-1}Z(x)] = W[Z(x)\,g'(x)],$$

$$W[g'(x)\,Z(x) + g(x)\,Z(x)] \geqslant dg - W[g'(x)\,Z(x)].$$

Следовательно, когда максимальная степень $Z(x)$ не превышает $(k-1)$,

$$W[F(x)\,Z(x)] \geqslant dg. \tag{8.26}$$

В тех случаях, когда $Z(x) = h(x)$, будем иметь

$$W[g'(x)\,x^{L-1}h(x)] = d_h;$$

$$W[g'(x)\,h(x) + g(x)\,h(x)] = d_h,$$

так как $g(x)\,h(x) = x^n + 1$ и, следовательно,

$$W[F(x)\,h(x)] = 2d_h. \tag{8.27}$$

Полагаем в общем случае, что $Z(x) = S(x)$, причем степень многочлена $S(x)$ превышает $(\kappa = 1)$. Тогда по аналогии с теоремой 8.2 рассмотрим два варианта.

Когда многочлен $S(x)$ не содержит в качестве сомножителя $h(x)$, получим

$$W[g(x)\,S(x)] = d_g$$

из свойств циклических (n, κ) -БЧХ-кодов.
Этот вес может быть уменьшен на величину, превышающую

$$W[g'(x)\,S(x)] = W[g'(x)\,x^{L-1}S(x)],$$

и одновременно увеличивается на величину $W[g'(x)\,x^{L-1} \times \times S(x)]$, следовательно

$$W[F(x)\,S(x)] \geqslant d_g. \tag{8.28}$$

Если многочлен $S(x)$ содержит сомножитель $h(x)$, т.е. $S(x) = S'(x)\,h(x)$, то из свойств дуальных циклических кодов получим, что

$$W[g'(x)\,S'(x)\,h(x)\,x^{L-1}] = d_h, \tag{8.29}$$

а так как

$$g'(x)\,S'(x)\,h(x) + g(x)\,S'(x)\,h(x) = S'(x)\,h(x) \times \times [g'(x) + g(x)],$$

причем $S'(x)\,[g'(x) + g(x)] = S^*(x)$ — многочлен, не содержащий в качестве сомножителя $g(x)$, то, следовательно,

$$W[h(x)\,S^*(x)] = d_h. \tag{8.30}$$

В результате из (8.29) и (8 30) получим

$$W[F(x)S(x)] = 2d_h.$$

Обобщая (8.26) — (8.30) и распространяя на $b > 2$, будем иметь первую часть (8.25).

Вторая часть утверждения (8.25) следует из возможности дробного значения величины $(r + 1)$ и наличия некоторого количества нулей в местах деления последовательности, соответствующей образующему полиному первообразного циклического кода. Таким образом, теорема доказана.

Методика синтеза квазиоптимальных несистематических $(b, 1)_L$-СК основана на тех же положениях (8.21), (8.22) и (8.23), что и систематических кодов. Покажем это на примере.

Пример 8.2. Циклический (31,11)-БЧХ-код задан образующим полиномом $g(x) = x^{20} + x^{19} + x^{18} + x^{15} + x^{14} + x^{13} + x^9 + x^7 + x^4 + x^3 + 1 \sim 11100111000101001100 1$ и имеет минимальное кодовое расстояние $d_g = 11$.

Слева от центра можно выделить полином

$$R_1(x) = x^7 + x^6 + x^5 + x^2 + x + 1 \sim 11100111,$$

а справа от центра — полином

$$R_2(x) = x^9 + x^7 + x^4 + x^3 + 1 — 1010011001.$$

Так как дуальный код, определяемый полиномом $h(x)$, имеет минимальное кодовое расстояние $d_h = 6$, что обусловлено его свойствами, то минимальное кодовое расстояние СК будет не менее

$$df = \min\{d_g 2d_h\} = 11.$$

При этом, чем большее количество нулей сосредоточено в области деления последовательности, соответствующей образующему полиному первообразного циклического кода, тем при меньшем кодовом ограничении n_A синтезируется СК с заданными корректирующими возможностями.

Так, для циклического (63,24)-БЧХ-кода синтезирован $(2,1)_{18}$-СК, обладающий минимальным кодовым расстоянием $d_f \geqslant 15$. Для сравнения укажем, что в [22] получен $(2,1)_{20}$-СК с такими же корректирующими возможностями, что на 10 % хуже по объему требуемой памяти.

При $b > 2$ полином $g(x)$ обобщенной диффузной реконструкцией «раздвигается» на b участков, соответствующих полиномам $R_j(x)$, $j = \overline{1, b}$. При этом требования к поли-

номам $g(x)$ и $h(x)$ изменяются. Циклический (n, k)-код, из которого выбираются полиномы $g(x)$, должен иметь величину k, близкую к величине $\frac{n+1}{b+1}$ и $k \geqslant L$, а дуальный циклический $(n, n-k)$-код, образуемый полиномом $h(x) = (x^n + 1)/g(x)$, должен иметь величину минимального кодового расстояния d_h такую, чтобы выполнялось условие

$$d_g \approx b d_h. \tag{8.31}$$

Покажем выполнение этих условий на следующем примере.

Пример 8.3. Синтезировать несистематический $(3,1)_L$-СК, квазиоптимальный в классе циклических кодов, определяемых двучленом $(x^{31} + 1)$.

Определяем число информационных элементов кода

$$k \geqslant \frac{n+1}{b+1}, \quad k = 10.$$

Минимальное кодовое расстояние циклического (31,10)-кода $d_g = 12$, дуального (31,21)-кода $d_h = 5$, а образующий полином $g(x)$ имеет следующий вид:

$$g(x) = x^{21} + x^{20} + x^{19} + x^{17} + x^{14} + x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \sim 11101001101011011111111.$$

Обобщенной диффузной реконструкцией «раздвижением» определяем порождающие многочлены трех подканалов:

$$R_1(x) = x^4 + x^3 + x^2 + 1;$$
$$R_2(x) = x^6 + x^5 + x^3 + x + 1;$$
$$R_3(x) = x^6 + x^5 + x^4 + x^3 + x^2 + 1.$$

Минимальное кодовое расстояние синтезированного кода из (8.25) будет $d_f \geqslant 12$.

Итак, в общем виде алгоритм выбора полиномов $R_i(x)$, $(i = \overline{1.\ b})$ степени $L - 1$ состоит в следующем:

1) определении степени полинома $g(x)$, которая должна быть не менее bL;

2) нахождении циклического (n, k)-БЧХ-кода (начиная поиск с кодов, имеющих наименьшее значение длины блока n), порождаемого полиномом $g(x)$ степени $n - k \geqslant bL$ и имеющего минимальное кодовое расстояние d_g; причем необходимо, чтобы полином $h(x) = \frac{x^n + 1}{g(x)}$ сте-

пени k порождал дуальный $(n, n-k)$-БЧХ-код с минимальным кодовым расстоянием $d_h \approx d_g/b$;

3) определении минимального кодового расстояния d_f синтезируемого СК в соответствии с (8.25);

4) обобщенной диффузной реконструкции «раздвижении» образующих полиномов таким образом, чтобы среди них можно было выбрать полиномы $R_j(x)$, обладающие минимально достижимой величиной L, если величина d_f удовлетворяет поставленным условиям;

5) переходе к (n_1, κ_1)-БЧХ-коду, где $n_1 > n$, если величина L оказалась меньше требуемой, а величину минимального кодового расстояния d_f необходимо увеличить, и в повторении пунктов 1—4 алгоритма.

Примечания:

1. Следует учитывать тот факт, что математическое ожидание веса произведения $R_j(x)\, h(x)$ оказывается больше величины bd_h, что позволяет производить поиск СК и среди полиномов (n, κ_1) -кода, где $\kappa_1 < \kappa$.

2. Существенное влияние на достижимую величину d_f оказывает способ «раздвижения» образующего полинома $g(x)$. Можно рекомендовать «раздвигать» образующий полином $g(x)$ так, чтобы степени полиномов $R_j(x)$ имели наименьшее отличие. Данная рекомендация соответствует интуитивному представлению и проверена экспериментально.

Метод последовательного направленного анализа образующих полиномов первообразных циклических кодов. Рассмотрим еще один алгебраический метод синтеза сверточных кодов с заданными корректирующими свойствами, дополняющий ранее изложенный.

Введем следующие обозначения: $R_j(x) = g_j(x)$ — полином, в соответствии с которым синтезируются связи j-го сумматора по модулю два с x-регистром. Он одновременно является образующим полиномом некоторого циклического (n, k)-БЧХ-кода; $h_j(x)$ — образующий полином дуального кода, удовлетворяющий условию $h_j(x)\, g_i(x) = x^n + 1$; d_{gj} — величина минимального кодового расстояния в циклическом (n, k)-БЧХ-коде, образованном $g_i(x)$; d_{hj} — величина минимального кодового расстояния в дуальном циклическом (n, k)-коде, образованном полиномом $h_j(x)$; f_{jl} — вес результата произведения полиномов $g_l(x)\, h_l(x) \times (j = \overline{1, b},\ i = \overline{1, b})$; $H^*_{j,i}, \ldots, l, (j, i, \ldots, l \in 1, b)$— многочлен, равный произведению всех неповторяющихся неприводимых полиномов, входящих в разложения $h_j(x)$,

$h_i(x), \ldots, h_l(x)$, $(j \neq i \neq \ldots \neq l)$, dj, $i, \ldots, l$ — вес многочлена $H^*_{j,i}, \ldots, l$; fr, $м$ — вес результата произведения полинома $gr(x)$ на H^*_j, $i, \ldots, l$, $(r = \overline{1, b})$, $(\mu = \overline{1, M})$, где M — множество различных многочленов $Hj, i, \ldots, l$.

Алгоритм выбора полиномов $R_j(x)$ состоит в том, что выбираются b образующих полиномов $g_i(x)$, $(j = \overline{1, b})$ циклического (n, k)-БЧХ-кода, имеющего величину $k \leqslant L$. Следовательно, при кодировании сверточным кодом, образованным полиномами $g_i(x)$ некоторого сообщения, содержащего числа информационных символов не более k, вес кодового слова СК d_{f_1}, будет не менее

$$d_{f_1} \geqslant \sum_i d_{gj}. \tag{8.32}$$

Если число информационных символов равно $k+1$, то при их распределении в соответствии с конфигурацией полинома $h_j(x)$ вес произведения $h_j(x)g_i(x) = x^n + 1$ окажется равным 2, а произведений $h_j(x)g_i(x)$, $(j = i)$ — величинам f_{ji}. Вес кодового слова СК $d_{f_{2j}}$ будет равен

$$d_{f_{2i}} = 2 + \sum_{j=1,\, j\neq 1}^{b} fj, \; i(i = \overline{1, b}). \tag{8.33}$$

В дальнейшем находятся величины

$$d_{f_{3\mu}} \sum_r fr, \; \mu, \; (\mu = 1, M) \tag{8.34}$$

при распределении информационных символов согласно конфигурации многочленов $H^*j, i, \ldots, l$, степень которых не должна превосходить $L - 1$, что следует из определения образующей матрицы (8.24) СК. Это ограничение определяет значение M.

Величина минимального кодового расстояния d_f в сверточном коде, синтезированном описанным способом, равна минимальной из величин dfv, $(v = \overline{1, 3})$, полученных согласно (8.32) — (8.34):

$$d_f = \min\{d_{f_1}, \; d_{f_{2j}}, \; (j = \overline{1, b}), \; d_{f_{3\mu}}(\mu = \overline{1, M})\}. \tag{8.35}$$

Рассмотрим пример синтеза СК с соответствии с разработанным методом.

Пример 8. 4. Пусть задано $b = 3$ и $L \leqslant 22$. Выбираем (31,10)-код, обладающий $d_g = 12$. Этот код [35] может быть образован любым из 14 возможных полиномов.

Выберем:

$$g_1(x) = R_1(x) = g_1g_2g_3g_4g_5;$$
$$g_2(x) = R_2(x) = g_1g_2g_5g_6g_7;$$
$$g_3(x) = R_3(x) = g_1g_3g_4g_6g_7,$$

где

$$g_1 = x + 1 \sim 11;$$
$$g_2 = x^5 + x + 1 \sim 100101;$$
$$g_3 = x^5 + x^3 + 1 \sim 101001;$$
$$g_4 = x^5 + x^3 + x^2 + x + 1 \sim 101111;$$
$$g_5 = x^5 + x^4 + x^2 + x + 1 \sim 110111;$$
$$g_6 = x^5 + x^4 + x^3 + x + 1 \sim 111011;$$
$$g_7 = x^5 + x^4 + x^3 + x^2 + 1 \sim 111101.$$

Причем $g_1g_2g_3g_4g_5g_6g_7 = x^{31} + 1$.
Найдем, что $d_{f_1} = \sum_j d_{gj} = 36$.

Определим полиномы $h_j(x)$:
$h_1(x) = g_6g_7$; $h_2(x) = g_3g_4$; $h_3(x) = g_2g_5$.

Вычислим веса $f_{j,i}$ произведений $g_j(x)\,h_i(x)$:

$$f_{1,1} = 2;\ f_{2.1} = 18;\ f_{3.1} = 18;$$
$$f_{1,2} = 18;\ f_{2.2} = 2;\ f_{3.2} = 20;$$
$$f_{1,3} = 20;\ f_{2.3} = 22;\ f_{3.3} = 2,$$

что позволяет найти величины

$$d_{f21} = \sum_{j=1}^{3} f_{j,1} = 38;\ d_{f22} = \sum_{j=1}^{3} f_{j,2} = 40;\ d_{f23} = \sum_{j=1}^{3} f_{j,3} = 44.$$

Определяем многочлены H^*j, i, ..., l:

$$H^*_{1,2} = g_6g_7g_3g_4;\ H^*_{1,3} = g_6g_7g_2g_5;\ H^*_{2,3} = g_3g_4g_2g_5,$$

каждый из которых имеет 20-ю степень, что вызывает необходимость вычисления произведений полиномов $g_r(x) \times$ $\times H^x_j$, i, ..., l и определения их веса:

$$f_{1.1.2} = 14;\ f_{2.1.2} = 18;\ f_{3.1.2} = 22;$$
$$f_{1.1.3} = 10;\ f_{2.1.3} = 22;\ f_{3.1.3} = 18;$$
$$f_{1.2.3} = 22;\ f_{2.3.3} = 10;\ f_{3.2.3} = 14,$$

что позволяет найти величины:

$$d_{f31} = \sum_{r=1}^{3} f_{r,1,2} = 54;\ d_{f32} = \sum_{r=1}^{3} f_{r,1,3} = 50;$$
$$d_{f33} = \sum_{r=1}^{3} f_{r,2,3} = 46.$$

Очередной многочлен $H^*_{j,\,i,\,\ldots\,,l}$ имеет вид $H^*_{1,2,3} = g_6g_7g_3g_4g_2g_5$, т. е. является многочленом 30-й степени, превышающей $L = 22$, что позволяет окончить вычисления величин $f_{r,\,\mu}$.

На основании (8.35) найдем, что синтезированный СК обладает минимальным кодовым расстоянием $d_f = 36$.

Наиболее оптимальным поиском полиномов является поиск на основе сочетания первого и второго алгоритмов синтеза СК.

8.5. Синтез сверточных кодов с относительной скоростью $R \neq 1/b$

Распространим алгебраический подход, плодотворно использованный при синтезе сверточных кодов с относительной скоростью $R = 1/b$, на конструирование СК с относительной скоростью $R = \frac{u}{b}$, где u — целое число, меньшее b.

Известен метод I-укорочения, состоящий в исключении части проверочных символов исходного кода путем вычеркивания некоторых столбцов проверочной части образующей матрицы. Эта операция приводит к изменению относительной скорости кода R в широком диапазоне (в сторону увеличения). Однако одновременно уменьшается и минимальное кодовое расстояние d исходного кода. Показано, что если вычеркивается q произвольных столбцов, то нижняя граница для минимального кодового расстояния d' полученного кода определяется выражением

$$d' \geqslant d - q.$$

Только для двоичных циклических кодов максимальной длины решена задача I-укорочения, обеспечивающая получение максимальной величины d' при заданной скорости R. Это достигается за счет исключения подпространств различной размерности из порождающей матрицы исходного кода. Тогда параметры полученного кода определяются следующими соотношениями:

$$n' = 2^k - 1 - \sum_{l} (2^l - 1),$$

$$d' = 2^{k-1} - \sum_{l} 2^{l-1},$$

где $l = 1,2,3 \ldots$ — размерность подпространств

Таким образом, для сверточных кодов задача состоит в определении подпространств, исключение которых из образующей матрицы СК приводило бы к наименьшему изменению минимального кодового расстояния d_f СК при заданной относительной скорости R.

Пусть циклический (n, k) -код задан образующей матрицей

$$G_{n,k} = \| I_k,\ G_{n-k,k} \|, \tag{8.36}$$

где $G_{n-k,k}$ — проверочная подматрица кода.

Матрицу (8.36) можно получить не только известным способом построения циклических кодов, но и методом формирования систематических сверточных кодов, если проверочные символы получать на выходе сумматоров по модулю два, связи которых с X-регистром организованы в соответствии с многочленами, отображающими столбцы проверочной подматрицы в (8.36).

Столбцы подматрицы $G_{n-k,n}$ представляют собой один или более многочленов $R_j(x)$, $(j = \overline{1, n-k})$, циклически сдвинутых один относительно другого на некоторое число позиций.

Эти многочлены определяют синтез связей и алгоритм оптимального I-укорочения СК, а именно многочлены различной конфигурации порождают проверочные подматрицы СК, а фазовые положения одинаковых многочленов определяют подпространства, которые необходимо исключить и сохранить в проверочной подматрице СК, порождаемой данным многочленом.

Сверточный код, полученный в результате осуществления указанных процедур, обладает относительной скоростью передачи R и минимальным кодовым расстоянием d_j, которые соответствуют аналогичным характеристикам первообразного циклического (n, k) -кода.

Покажем справедливость изложенных положений на примере.

Пример 8.5. Пусть задан циклический (15,11)-код, образованный полиномом $q(x) = x^4 + x + 1 \sim 10011$ с $d = 3$ и $R = \frac{11}{15}$.

Необходимо найти систематический СК с такими же характеристиками.

Определим образующую матрицу циклического (15,11)-кода :

$$G_{15,11} = \left\| \begin{array}{ccccccccccc|cccc} 0&0&0&0&0&0&0&0&0&0&1 & 0&0&1&1 \\ 0&0&0&0&0&0&0&0&0&1&0 & 0&1&1&0 \\ 0&0&0&0&0&0&0&0&1&0&0 & 1&1&0&0 \\ 0&0&0&0&0&0&0&1&0&0&0 & 1&0&1&1 \\ 0&0&0&0&0&0&1&0&0&0&0 & 0&1&0&1 \\ 0&0&0&0&0&1&0&0&0&0&0 & 1&0&1&0 \\ 0&0&0&0&1&0&0&0&0&0&0 & 0&1&1&1 \\ 0&0&0&1&0&0&0&0&0&0&0 & 1&1&1&0 \\ 0&0&1&0&0&0&0&0&0&0&0 & 1&1&1&1 \\ 0&1&0&0&0&0&0&0&0&0&0 & 1&1&0&1 \\ 1&0&0&0&0&0&0&0&0&0&0 & 1&0&0&1 \end{array} \right\|. \qquad (8.37)$$

Столбцы проверочной подматрицы соответствуют многочлену

$$R(x) = x^8 + x^7 + x^6 + x^5 + x + 1 \sim 111101011$$

с четырьмя смежными фазовыми положениями, определяемыми нулевыми членами многочлена

$$R'(x) = x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x + 1 \sim 11111110000.$$

Следовательно, связи второго сумматора по модулю два СК устанавливаются в соответствии с распределением единиц $R(x)$, а коммутация проверочных символов определяется конфигурацией многочлена $R'(x)$.

Образующая матрица СК после процедуры I-укорочения и выполнения элементарных преобразований приводится к виду (8.37), показывая, что полученный СК имеет такое же минимальное кодовое расстояние, как и исходный циклический (n, κ)-код.

Распределение информационных (α) и проверочных (β) символов СК, выполненное с учетом $R'(x)$, имеет вид

$$\underbrace{\alpha_1\alpha_2\alpha_3\alpha_4\alpha_5\alpha_6\alpha_7\alpha_8\beta_1\alpha_9\beta_2\alpha_{10}\beta_3\alpha_{11}\beta_4\alpha_{12}\alpha_{13}}_{1\ 1\ 1\ 1\ 1\ 1\ 1\ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 1}.$$

Относительная скорость передачи СК $R = \frac{11}{15}$.

Систематический СК с относительной скоростью $R \neq 1/b$ может быть преобразован в несистематический с увеличением минимального кодового расстояния d_f по методике (8.4).

Итак, алгоритм выбора полиномов для синтеза сверточных кодов, обладающих скоростью $R \neq 1/b$, и алгоритм работы коммутатора СК состоит в следующем:

нахождение циклического (n, κ)-БЧХ-кода, обладающего заданной скоростью R и числом информационных символов $\kappa = L$, где L определяет минимально допустимое (по условиям задачи) значение длины кодовых ограничений;

построение канонической формы образующей матрицы выбранного циклического (n, κ) -кода;

нахождение образующих полиномов, в соответствии с которыми синтезируются связи сумматоров с разрядами регистра, по дополнительной проверочной подматрице канонической матрицы (n, k) -кода;

определение алгоритма коммутации выходов сумматоров, обеспечивающего получение максимальной величины минимального кодового расстояния, по фаховому положению многочленов одинаковой конфигурации, отображающих столбцы проверочной подматрицы циклического (n,κ)-кода;

определение для несистематических кодов многочлена $R_1(x)$ согласно методу последовательного направленного анализа образующих полиномов первообразных циклических кодов с целью получения максимальной величины минимального кодового расстояния.

8.6. Оценка сверточных кодов

Разработанные методы алгебраического синтеза сверточных кодов позволяют строить СК с максимальной (или близкой к максимальной) величиной минимального кодового расстояния.

В табл. 8.1 приведены сравнительные характеристики некоторых СК, полученные на основе разработанных методов (1), и более поздних разработок (2) [20,22].

Таблица 8.1

№ пп	Первообразный циклический код	Сверточный код	d_g	d_h	d_f		L	
					1	2	1	2
1	(15,5)	систематический	7	4	7	—	9	—
2	(15,5)	несистематические	7	4	$\geqslant 7$	$\geqslant 7$	6	6
3	(31,11)		11	6	$\geqslant 11$	$\geqslant 11$	10	11
4	(63,24)		15	8	$\geqslant 15$	$\geqslant 15$	18	20

Анализ показывает, что найденные коды обладают в ряд случаев лучшими характеристиками, чем аналогичные коды, полученные позже.

Для оценки минимального кодового расстояния d_f СК используются нижние и верхние границы, аналогичные границам для блоковых методов кодирования.

Известна [22] нижняя граница (1) свободного расстояния Костелло (рис. 8.1)

$$d_f \geqslant Lb \frac{-R}{\ln (2e^{-R} - 1)} - 0_1(1), \quad 0 < R < \ln 2, \qquad (8.38)$$

где величина $O(1) \to 0$ при $L \to \infty$. Эта граница действительна лишь для полного ансамбля (несистематических) СК. Верхняя (2) уточненная граница [22] определяется выражением

$$df \leqslant [(L-4)b/2] + 4b. \qquad (8.39)$$

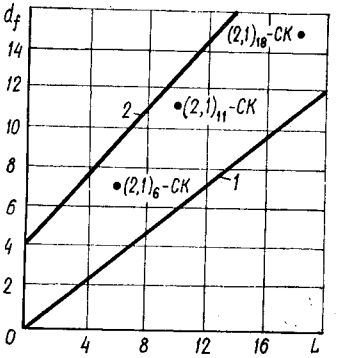


Рис. 8.1

Точками показано местоположение синтезированных СК для $b = 2$ и $R = 0{,}5$.

Эффективность применения разработанных конструктивных методов синтеза сверточных кодов можно оценить в теоретическом плане при сравнении с СК, полученными случайным образом.

Известно, что средняя вероятность ошибочно декодировать блок из Z информационных символов методом последовательного декодирования определяется неравенством

$$P(\varepsilon) \leqslant Z e^{-LbE(R)}, \qquad (8.40)$$

где $E(R)$ — функция надежности данного метода кодирования — декодирования.

Очевидно, величина $\bar{P}(\varepsilon)$ определяет среднее значение совокупности положительных чисел $\{P_i\}$, где P_i — вероятность ошибки для i-го кода рассматриваемого класса, поскольку в любой совокупности положительных чисел лишь $1/\eta$ доля этих чисел может превысить их среднее значение более чем в η раз. Следовательно, не менее чем у 90 % всех кодов ансамбля вероятность ошибки $P(\varepsilon)$ не превышает $10\,\bar{P}(\varepsilon)$, у 99 % кодов $P(\varepsilon)$ не превышает $100\,\bar{P}(\varepsilon)$ и т. д. Если обозначить через $P(S)$ вероятность (риск)

выбора «плохого» кода, то не менее чем у $[1—P(S)] \cdot 100\ \%$ всех кодов ансамбля вероятность ошибки $P(\varepsilon)$ не превышает $P(\varepsilon) / P(S)$. Для требуемых значений вероятностей $P^*(\varepsilon)$ и $P^*(S)$ при случайном выборе СК необходимо дополнительное увеличение кодового ограничения за счет увеличения L. В этом случае можно записать:

$$P^*(\varepsilon) = P(\varepsilon)\, P^*(S) = Z \exp\{-L'bE(R)\}, \qquad (8.41)$$

где $L' = Lx$ — увеличенное значение памяти СК, а X — коэффициент пропорциональности.

Из (8.40) и (8.41) определяем

$$x = 1 - \ln P(S)/LbE(R). \qquad (8.42)$$

Например, если $P(\varepsilon) = 10^{-10}$ и $P^*(S) = 10^{-5}$, то $x = 1{,}44$, т. е. объем памяти кодера и декодера должен быть увеличен на 44 %.

Таким образом, использование алгебраических конструктивных методов построения сверточных кодов в практическом плане эквивалентно или увеличению корректирующих возможностей СК при заданной длине кодовых ограничений, или уменьшению сложности и стоимости технической реализации при заданной помехоустойчивости.

В теоретическом плане развитие алгебраического подхода в анализе и синтезе СК важно тем, что позволяет проникнуть вглубь внутренней структуры сверточных кодов, выявить связи с весьма плодотворными методами синтеза циклических БЧХ-кодов, использовать теоретическую основу и логику алгебраической теории для установления новых закономерностей и принципов построения СК.

9. СИСТЕМЫ ПЕРЕДАЧИ ДИСКРЕТНОЙ ИНФОРМАЦИИ С РЕШАЮЩЕЙ ОБРАТНОЙ СВЯЗЬЮ

9.1. Классификация систем с решающей обратной связью

Повышение достоверности передачи информации, помимо использования кодов с исправлением ошибок, может быть достигнуто за счет введения дополнительного обратного канала для организации обратной связи. В этом случае используются коды с обнаружением ошибок, за счет

чего при неизменном коде резко возрастает кратность гарантийно обнаруживаемых ошибок, а следовательно и достоверность. В системах без обратной связи при использовании корректирующих кодов обычно ориентируются на некоторые средние статистические данные о канале. Обратная же связь дает возможность путем проведения постоянного анализа ошибок устанавливать фактическое состояние канала во время передачи и вводить избыточность, позволяющую достигнуть требуемой достоверности. При хорошем состоянии канала такой подход снижает общую избыточность. Особенно эффективным введение обратной связи оказывается тогда, когда помехи в обоих направлениях коррелированы или когда влияние помех в канале обратной связи значительно слабее, чем в канале прямой связи.

В соответствии с алгоритмами обмена информацией различают:

системы односторонней направленности;

системы автоматизированного управления с решающей обратной связью (РОС);

системы автоматизированного управления с информационной обратной связью (ИОС).

Рассмотрим более подробно системы с РОС, как наиболее перспективные и широко применяемые.

В зависимости от алгоритма обмена информацией системы РОС делятся на следующие классы (35):

1. Системы с ожиданием сигнала обратной связи (РОС—ОЖ). Основная особенность этих систем в том, что передатчик, передав n-элементную комбинацию, или ожидает сигнал обратной связи (РОС — ОЖ), или повторяет ранее переданную комбинацию (РОС—ОЖ). Передача следующего сообщения возможна только после приема подтверждения по ранее переданной комбинации.

2. Системы с накоплением правильно принятых комбинаций (РОС—НК). В этих системах ρ комбинаций корректирующего кода объединяются в блок. Этот блок передается и на приемной стороне все комбинации проверяются на отсутствие ошибок. Безошибочные комбинации записываются в накопитель, а комбинации с ошибками стираются. Если хотя бы одна из различных комбинаций будет принята, то посылается запрос и повторяется весь блок, а в приемнике из этого блока отбираются комбинации, не принятые при первой передаче. Переспросы производятся до тех пор, пока не будут приняты все комбинации блока. После приема всех ρ комбинаций посылается сигнал

подтверждения. Получив его, передатчик передает следующий блок комбинации.

3. Системы с адресным переспросом (РОС—АП). Эти системы во многом аналогичны системам с накоплением, но в отличие от последних приемник в РОС-АП формирует сложный сигнал переспроса, в котором указываются условные номера адреса не принятых приемником комбинаций. Поэтому передатчик повторяет не весь блок, как в системе с накоплением, а лишь непринятые комбинации.

4. Системы с последовательной передачей кодовых комбинаций. Эти системы осуществляют блокировку приемника на время приема h комбинаций после обнаружения ошибки с последующим повторением при переспросе h заблокированных комбинаций (РОС — ПП).

5. Системы с многоступенчатым переспросом (РОС—ПМ). В этих системах предусматривается как переспрос комбинаций, так и переспрос блоков комбинаций, т.е. имеются несколько ступеней переспроса. Однако в этом случае используются специальные методы кодирования (итерированные, каскадные и другие коды).

9.2. Системы одностороннего действия с ожиданием сигнала обратной связи

Алгоритм функционирования системы. На рис. 9.1 приведены структурная схема и временная диаграмма функционирования системы с ожиданием сигнала обратной связи.

Датчик информации ДИ пункта А формирует сообщение, которое кодируется избыточным (n, k) -кодом в кодирующем устройстве КУ и выдается в канал связи. Одновременно сообщение запоминается в накопителе Н. В пункте В комбинация (n, κ) -кода декодируется. При необнаружении ошибок декодированное сообщение выдается в приемник информации ПИ и формирователь сигнала обратной связи ФС передает в пункт А подтверждение u о правильном приеме. При обнаружении ошибок декодированное сообщение стирается и в ПИ не выдается, а ФС формирует запрос W на повторную передачу сообщения, принятого с ошибкой.

Дешифратор ДШ пункта А, выделив запрос W, выдает сигнал в Н, обеспечивая повторную передачу сообщения. При выделении сигнала подтверждения u ранее запомненное сообщение стирается и датчик инфор-

мации ДИ формирует очередное сообщение, которое передается аналогично ранее рассмотренному.

Определим основные характеристики системы в предположении использования идеального канала обратной связи, т.е. канала, ошибками в котором можно пренебречь по сравнению с ошибками в основном канале связи. Такое допущение во многих случаях является вполне обоснованным, например, в космических системах связи, соединяющих наземную станцию с подвижными космическими объектами.

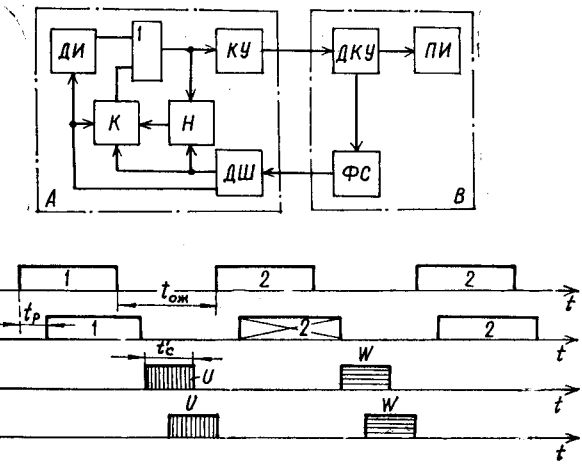


Рис. 9.1

В качестве основных характеристик систем будем считать:

относительную скорость передачи R;

среднее время доведения информации $\bar{t}_д$;

вероятность необнаружения ошибок $P_{н.о}$;

вероятность потери сообщения $P_п$.

Относительная скорость передачи. Исходными данными для определения относительной скорости передачи являются параметры избыточного (n, k) -кода и вероятность потери $P_п$ сообщения при его однократной передаче, которая может быть определена известными методами.

Если число передаваемых собщений N, причем в общем случае $N \to \infty$, то число однократно потерянных соответственно повторенных сообщений будет

$$N_1 = NP_п,$$

число двухкратно потерянных и дополнительно повторенных сообщений определяется как

$$N_2 = N_1 P_{\text{п}} = N P_{\text{п}}^2,$$

а число i-кратно потерянным и соответствующее число раз повторенных сообщений будет

$$N_i = N P_{\text{п}}^i.$$

Таким образом, вместе с повторениями будет иметь место

$$N_{\Sigma} = N \sum_{i=0}^{m-1} P_{\text{п}}^i \tag{9.1}$$

передач сообщений, где m — максимальное число повторений. Относительная скорость передачи в общем виде определяется выражением

$$R = \frac{K_{\Sigma}}{n_{\Sigma}}, \tag{9.2}$$

где $K_{\Sigma} = kN$ — общее число переданных информационных элементов; K_{Σ} — общее число элементов, которое могло быть передано за N_{Σ} передач сообщений.

Из диаграммы рис. 9.1 следует, что за одну передачу формируется n элементов комбинации (n, κ) -кода и за время ожидания $t_{\text{ож}}$ могло быть передано

$$n_1 = \frac{t_{\text{ож}}}{V}$$

элементов, где V — относительная скорость модуляции; $t_{\text{ож}} = 2t_{\text{р}} + t_{\text{с}} + t_{\text{об}}$, $t_{\text{р}}$ — время распространения сигнала по каналу связи; $t_{\text{с}}$ — длительность сигналов обратной связи; $t_{\text{об}}$ — время логической обработки сигналов.

При использовании полудуплексных каналов связи $t_{\text{ож}}$ увеличивается на величину времени коммутации каналов связи $2t_{\text{к}}$, где $t_{\text{к}} = 150$ мс.

Можно положить, что $n_1 = \mu n$, где μ — коэффициент, определяющий соотношение времени ожидания $t_{\text{ож}}$ и времени передачи сообщения. Тогда общее число элементов

$$n_{\Sigma} = (1 + \mu) n N_{\Sigma},$$

а относительная скорость передачи

$$R_1 = \frac{k}{n(1+\mu)\sum_{i=0}^{m} P_{\text{п}}^i}.$$

Для системы с неограниченным числом переспросов, т. е. когда $m \to \infty$,

$$\sum_{t=0}^{\infty} P_{\text{п}}^{t} = \frac{1}{1 - P_{\text{п}}}, \tag{9.3}$$

как бесконечная сумма убывающей геометрической прогрессии. В этом случае относительная скорость передачи определяется выражением

$$R_1 = \frac{k(1 - P_{1\text{п}})}{n(1 + \mu)},$$

где $\frac{k}{n(1+\mu)}$ — определяет постоянную информационную избыточность; $(1 - P_{\text{п}})$ — определяет переменную информационную избыточность системы. Если число передач ограничивается величиной m, то

$$\sum_{t=0}^{m-1} P_{\text{п}}^{t} = \frac{1 - P_{\text{п}}^{m}}{1 - P_{\text{п}}}, \tag{9.4}$$

и относительная скорость передачи

$$R_1 = \frac{k}{n(1+\mu)} \cdot \frac{1 - P_{\text{п}}}{1 - P_{\text{п}}^{m}}. \tag{9.5}$$

Среднее время доведения информации $\bar{t}_{\text{д}}$. Зная вероятность потери сообщения при одном повторении $P_{\text{п}}$, можно определить вероятность доведения информации с первой передачи

$$P_1 = 1 - P_{\text{п}}.$$

Время доведения в этом случае (без учета $t_{\text{р}}$ и $t_{\text{об}}$)

$$t_1 = \mu t + t,$$

где

$$t = \frac{n}{V}.$$

Вероятность доведения информации со второй передачи определяется как

$$P_2 = P_{\text{п}}(1 - P_{\text{п}}),$$

а время доведения

$$t_2 = 2t_1 = 2(\mu t + t).$$

Вероятность доведения информации с i-й передачи и соответствующее время доведения

$$P_i = P_{\text{п}}^{i-1}(1 - P_{\text{п}}),\ t_i = it_1 = (\mu t + t)\, i.$$

Тогда среднее время $\bar{t}_{\text{д}}$ определится как

$$\bar{t}_{\text{д}} = \sum_{i=1}^{m} P_i t_i = t(1 - P_{\text{п}}) \sum_{i=1}^{m} P_{\text{п}}^{i-1}(1 + \mu)\, i. \qquad (9.6)$$

Вероятностные характеристики системы. Вероятность ошибочного приема комбинации для системы с ожиданием при m -кратной передаче (т.е. вероятность выдачи в ПИ сообщения с необнаруженной ошибкой) [12]

$$P_{\text{н. о}}^{\text{с}} = \frac{P_{\text{н. о}}}{1 - P_{\text{п}}}(1 - P_{\text{п}}^{m}), \qquad (9.7)$$

где $P_{\text{н. о}}$ — вероятность ошибок, не обнаруживаемых используемым (n, k)-кодом.

Так как в реальных системах $P_{\text{п}} \ll 1$, то

$$P_{\text{н. о}}^{\text{с}} \approx P_{\text{н. о}}. \qquad (9.8)$$

Вероятность потери информации при m-кратной передаче сообщения определяется выражением

$$P_{\text{п}\,(m)}^{\text{с}} = P_{\text{п}}^{m}, \qquad (9.9)$$

что следует из теоремы о совместном выполнении случайных независимых событий.

Выражение (9.9) позволяет определить необходимое число передач сообщений m для обеспечения вероятности потери сообщений в системе, не превышающей заданную,

$$m = \left\lceil \frac{\lg P_{\text{п}}(m)_{\text{з}}}{\lg P_{\text{п}}} \right\rceil. \qquad (9.10)$$

Более подробное описание других систем приводится в [12].

9.3. Определение оптимальных характеристик кода в режиме обнаружения ошибок

При известных значениях параметров канала связи P_0 и α [35] для определения оптимальных параметров кода выбран критерий максимума скорости передачи при заданном значении вероятности необнаруженной ошибки $P_{\text{н. о}} \leqslant P_{\text{н. о}}^{\text{д}}$. Относительная скорость передачи опре-

деляется как параметрами кода, так и свойствами канала связи и в общем виде может быть представлена произведением двух функций:

$$R = F(r, n) f(n), \qquad (9.11)$$

где $F(r, n)$ зависит только от кода и представляет собой предельное значение R, когда ошибки в канале не возникают; $f(n)$ — вероятность безошибочного приема некоторых последовательностей, длины которых зависят от n. Для рассматриваемой системы РОС—ОЖ [12]

$$F(r, n) = \frac{n-r}{n}; \quad f(n) = \frac{1-P_{\text{п}}}{\mu(1-P_{\text{п}})+1}. \qquad (9.12)$$

Оптимальная длина кода, обеспечивающая наибольшую скорость передачи при заданной вероятности необнаруживаемых ошибок, соответствует экстремуму (9.11) и определяется как корень уравнения [15]

$$F'(n, r) f(n) + f'(n) F(n, r) = 0. \qquad (9.13)$$

Решение этого уравнения можно получить графически. Для этого строятся две кривые $\frac{F(n, r)}{F'(n, r)}$ и $\frac{f(n)}{f'(n)}$ как функции n и точка пересечения их определяет оптимальное значение n. Для алгоритма с ожиданием и канала с независимыми ошибками

$$\frac{F(n, r)}{F'(n, r)} = \frac{n(n-r)}{r} \quad \text{и} \quad \frac{f(n)}{f'(n)} = -\left(\frac{1}{P_0} - n\right) \times$$

$$\times [(\mu + 1) - \mu \cdot nP_0].$$

Тогда для $P_0 = 10^{-3}$ и $P_{\text{н. о}} \leqslant P^3_{\text{н. о}} = 10^{-6}$ при $\mu = 1$ $n_{\text{опт}} \approx 200$ (см. рис. 9.2).

Однако детальное исследование статистических последовательностей ошибок в реальных каналах связи показывает, что ошибки являются зависимыми и обладают тенденцией к группированию, т.е. между ними существует определенная связь — корреляция. При этом вероятность ошибки в сообщении $P\ (\geqslant 1, n)$ при групповом характере ошибок падает незначительно даже в случае применения кодов, обнаруживающих большое число ошибок в кодовых комбинациях. Границы минимального расстояния Плотника, Хэмминга и Варшамова-Гилберта таковы, что в этом случае число избыточных символов $r = (n - \kappa)$ должно составлять не менее 15 % для $n = 500$ и 40—45 % для $n = 100$.

На рис. 9.3. показаны графики $R = \varphi(n)$ для тропосферного телефонного канала ($\alpha = 0{,}44$; $P_0 = 10^{-3}$) и кабельного коммутируемого канала ($\alpha = 0{,}34$; $P_0 = 10^{-3}$) при скорости модуляции $V = 1200$ бод, при граничной допустимой вероятности необнаруженной ошибки $P^3_{\text{н. о}} \leqslant \leqslant 10^{-9}$. Для расчетов рассматривались двоичные коды

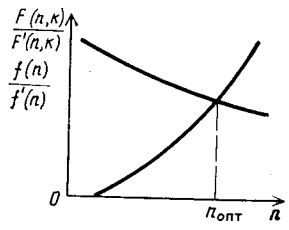


Рис. 9.2

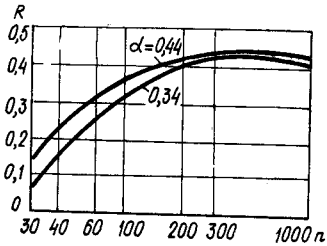


Рис. 9.3

Боуза — Чоудхури — Хоквингема (БЧХ) $n = 31{,}63$, 127, 255, 511 и 1023. Расчет вероятности необнаруженной ошибки производился по формуле

$$P_{\text{н. о}}(n) \cong \frac{1}{2^{n-k}} \left(\frac{n}{d_0}\right)^{1-\alpha} P_0. \qquad (9.14)$$

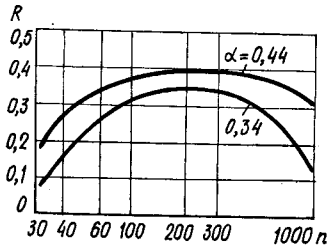


Рис. 9.4

Следует заметить, что оптимальная длина кодов для систем с решающей обратной связью различна для различных типов каналов, поэтому при разработке аппаратуры передачи данных целесообразно предусматривать изменение скорости передачи с учетом изменения качества канала связи и сохранения требуемой граничной допустимой вероятности необнаруживаемой ошибки.

На рис. 9.4 приведены графики $R = \varphi(n)$, рассчитанные для канала с $P_0 = 10^{-2}$ и различных значений α. Из рисунков видно, что оптимальная длина кодов для таких каналов лежит в пределах $n = 200$—300 и зависит от параметра α.

Уменьшение скорости передачи при малых значениях n ($n < 100$) обусловливается увеличением постоянной из-

быточности (структурой кода), а при больших значениях n ($n > 200$) скорость падает из-за увеличения переменной избыточности, вызванной частым появлением ошибок и повторной передачей искаженных комбинаций.

9.4. Выбор оптимального режима декодирования избыточных кодов

Выше была изложена методика выбора характеристик избыточного кода n и κ при использовании режима обнаружения ошибок. Обычно в системах с обратной связью требуемая достоверность обеспечивается при использовании кодов только с обнаружением ошибок. Тогда исправление ошибок не имеет смысла, тем более, что оно потребует, вообще говоря, существенного усложнения декодирующего устройства, а следовательно, снижения его надежности. Если, однако, при фиксированном модеме вероятность ошибочного приема символа велика, то это приводит к большой вероятности поражения кодового блока хотя бы одной ошибкой, а следовательно, и к частым переспросам, снижающим скорость передачи до недопустимой величины. При этом оптимальная длина блока, определенная в п.9.3, оказывается очень малой [35]. В связи с этим для передачи больших массивов информации ($n \geqslant 1000$) представляют интерес методы, основанные на применении избыточного кода в режиме обнаружения и частичного исправления ошибок кратности t и менее. Такая задача оптимизации сводится к выбору оптимальных в смысле некоторого критерия характеристик кода n, κ, и t [35].

Пусть система РОС оценивается параметрами $P_{\text{н. о}}(n)$ и R, а в качестве критерия оптимальности выбран критерий максимума скорости передачи. Оптимальными значениями n, κ и t будут такие, при которых

$$R(n,\ k,\ t) = R_{\max}, \tag{9.15}$$

$$P_{\text{н. о}}(n) \leqslant P^{\text{з}}_{\text{н. о}}. \tag{9.16}$$

При определении оптимальных характеристик кода следует учесть, что в зависимости от статистики ошибок дискретного канала связи применение частичного исправления может или увеличивать или снижать скорость передачи РОС.

Найдем в общем виде условие целесообразности частичного исправления ошибок в системах РОС. Так как скорость передачи системы РОС, при которой обеспечивается

граничное условие (9.16), а корректирующий код используется в режиме обнаружения ошибок $R_0 = R_1 R_2$, то в режиме частичного исправления ошибок при обеспечении условия (9.16) скорость передачи будет равна

$$R_{\text{и. о}} = (R_1 - \Delta R_1)(R_2 + \Delta R_2), \tag{9.17}$$

где R_1 — сомножитель, определяемый постоянной избыточностью кода и не зависящий от параметров канала связи; R_2 — сомножитель, определяемый каналом связи.

Частичное исправление ошибок следует считать эффективным и целесообразным, если $R_{\text{и. о}} - R > 0$. Это условие будет выполняться, если $R_1 \Delta R_2 - R_2 \Delta R_1 - \Delta R_1 \Delta R_2 > 0$ или

$$\Delta R_2 > \frac{\Delta R_1 R_2}{R_1 + \Delta R_2}. \tag{9.18}$$

Рассмотрим процедуру частичного исправления ошибок кратности t и обнаружения кратности σ на примере кодов БЧХ, используемых в системах с обратной связью.

Предположим, что при приеме кодового вектора v произошло $\nu \leqslant t$ ошибок в позициях $x_1, x_2, \ldots, x_\nu$, которым соответствуют ненулевые значения вектора ошибок e.

Первый шаг при декодировании состоит в вычислении синдрома по принятому вектору v, т.е. [14]

$$S = vH^{\text{т}}, \tag{9.19}$$

где $H^{\text{т}}$ — транспонированная проверочная матрица (n, k)-кода.

Если выполняется условие $\lambda \leqslant t$, то задача исправления ошибок в принятом кодовом векторе v заключается в определении местоположения ненулевых значений истинного вектора ошибок e_u. Истинным вектором ошибок e_u будет тот, который, будучи сопоставлен с принятым кодовым вектором v, обратит выражение (9.19) в нуль. Иными словами, истинным вектором ошибок считается вектор e_u, который обеспечивает выполнение условия

$$S_u = (v + e_u) H^{\text{т}} = 0. \tag{9.20}$$

Таким образом, второй этап декодирования заключается

в последовательном вычислении синдромов S_i, т. е.

$$\left.\begin{aligned} S_1 &= (v + e_1) H^{\mathrm{T}}; \\ S_2 &= (v + e_2) H^{\mathrm{T}}; \\ &\cdots\cdots\cdots \\ S_i &= (v + e_i) H^{\mathrm{T}}; \\ &\cdots\cdots\cdots \\ S_N &= (v + e_N) H^{\mathrm{T}} \end{aligned}\right\}, \tag{9.21}$$

где

$$N = n + C_n^2 + C_n^3 + \cdots + C_n^t.$$

Как только в результате очередной проверки синдром S окажется нулевым, принимается решение о том, что с принятым кодовым словом v сопоставлен истинный вектор ошибок e_u и результат декодирования посылается на выход декодера.

Следует заметить, что очередность подстановки векторов определяется вероятностью их появления, т.е. из всех образцов векторов ошибок первыми выбираются те, которые имеют наибольшую вероятность. Этими векторами могут быть, например, векторы минимального веса.

Произведем оценку эффективности частичного исправления ошибок для системы передачи информации с ожиданием решающего сигнала РОС—ОЖ. Как и в предыдущих параграфах, критерием оценки эффективности выбрана скорость передачи R при фиксированной достоверности $P_{\text{н. о}} \leqslant \leqslant P^3_{\text{н. о}}$.

Так как в режиме одновременного исправления и обнаружения ошибок при сохранении параметров (n, k)-кода [35]

$$P'_{\text{н. о}}(n) \approx \frac{\sum_{t=0}^{t} C_n^t}{2^{n-k}} P(\geqslant d_0 - t,\ n) \geqslant P_{\text{н. о}}(n), \tag{9.22}$$

то для обеспечения $P'_{\text{н. о}} \cong P_{\text{н. о}} \leqslant P^3_{\text{н. о}}$ возникает необходимость увеличения длины комбинации избыточного кода за счет увеличения дополнительной избыточности n'.

Найдем выражение для определения максимально возможного приращения длины кодовой комбинации n^1, при котором еще выполняется условие (9.18), а скорость передачи определяется с помощью выражения

$$R = \frac{k}{n(1+\mu)} [0 - P_{\text{о. о}}(n)]. \tag{9.23}$$

Если $\mu = 1$, то для определения n' можно записать

$$\frac{k}{2(n+n')}[1 - P_{\text{о. о}}(\geqslant t,\ n)] = \frac{k}{2n}[1 - P_{\text{о. о}}(0,\ n)], \quad (9.24)$$

где n' — приращение дополнительной избыточности для сохранения условия $P'_{\text{н. о}} \leqslant P^{3}_{\text{н. о}}$. Тогда, решая это равенство относительно n', можно найти выражение для $n'_{\text{доп}}$:

$$n'_{\text{доп}} = \frac{n[P_{\text{о. о}}(0,\ n) - P_{\text{о. о}}(\geqslant t,\ n)]}{1 - P_{\text{о. о}}(0,\ n)}. \quad (9.25)$$

Для каналов с независимым распределением ошибок это выражение можно записать в виде.

$$n'_{\text{доп}} = n\frac{1 - (1 - P_0)^n - \sum_{i=t+1}^{d_0 - t} C_n^i P_0^i (1 - P_0)^{n-i}}{(1 - P_0)^n}. \quad (9.26)$$

Для каналов с группирующимися ошибками, характеризуемых показателем группирования α,

$$n'_{\text{доп}} \approx \frac{n\left[n^{1-\alpha}P_0 - \left(\frac{n}{t}\right)^{1-\alpha}P_0\right]}{1 - n^{1-\alpha}P_0}. \quad (9.27)$$

Величина $n'_{\text{доп}}$ показывает предел, до которого еще есть смысл увеличивать дополнительную постоянную избыточность (кратность исправляемых ошибок t), выигрывая при этом в скорости передачи системы РОС—ОЖ. Дальнейшее увеличение избыточности не приводит к увеличению средней скорости передачи, а лишь необоснованно увеличивает сложность, и, следовательно, снижает надежность оборудования.

На рис. 9.5 показаны графики зависимости скорости передачи системы РОС—ОЖ от длины комбинации n при кратности исправляемых ошибок $t = 1$ для телефонного коммутируемого канала (*а*) и тропосферного телефонного канала (*б*) с различными средними частостями появления ошибок P_0. Пунктиром показаны кривые для $t = 0$.

Выигрыш в скорости передачи системы РОС—ОЖ можно оценить с помощью выражения

$$\theta(t \geqslant 1,\ n) = \frac{R(t \geqslant 1,\ n) - R(t = 0,\ n)}{R(t = 0,\ n)} \cdot 100\ \%. \quad (9.28)$$

Подставляя значения $R\ (t \geqslant 1, n)$ и $R\ (t = 0, n)$ в выражение (9.28), выигрыш в скорости передачи системы РОС-ОЖ, работающей в режиме частичного исправления

ошибок, по сравнению с системой, только обнаруживающей ошибки, будет (%)

$$\theta(t \geqslant 1,\ n) = \left\{\frac{n}{n+n'}\left[1 + \frac{\Delta P\ (t \geqslant 1,\ n)}{1 - P_{0.\,0}(t = 0,\ n)}\right] - 1\right\} 100, \tag{9 29}$$

где $\Delta P\ (t \geqslant 1, n) = P_{0.0}(t \geqslant 1,\ n) - P_{0.0}(t = 0, n)$ — увеличение вероятности приема сообщения за счет исправления ошибок.

Выигрыш в скорости передачи будет иметь место в случае выполнения неравенства

$$\frac{n}{n+n'}\left[1 + \frac{\Delta P\ (t \geqslant 1,\ n)}{1 - P_{0.\,0}\ (t = 0,\ n)}\right] > 1. \tag{9.30}$$

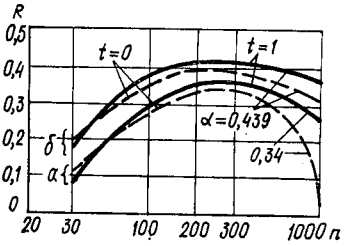


Рис. 9.5

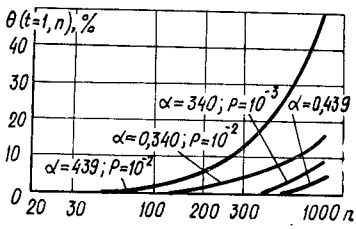


Рис. 9.6

В противном случае система передачи неэффективно использует исправление части ошибок с обнаружением остальных и увеличение сложности оборудования не оправдывает данный алгоритм декодирования.

На рис. 9.6 изображен график зависимости выигрыша $\Theta\ (t = 1, n)$ системы РОС—ОЖ, работающей в режиме исправления однократных и обнаружения многократных ошибок для кабельного и тропосферного телефонных каналов связи с различными частостями появления ошибок. Рассматривая график, надо отметить следующее. Если использование режима одновременного исправления и обнаружения ошибок в каналах достаточно высокого качества ($P_0 < \geqslant 10^{-3}$) определяется исходя из компромиссного решения вопроса увеличения скорости за счет усложнения оборудования, то с ухудшением канала ($P_0 \approx 10^{-2}$) вопрос применения систем передачи информации с РОС в режиме одновременного исправления и обнаружения ошибок

не вызывает сомнений. Действительно, при передаче данных кодов ($n \geqslant 500$) увеличение постоянной избыточности полностью компенсируется снижением переменной избыточности, вызванной частным поражением ошибками применяемых кодовых комбинаций (увеличением $P_{о.о}(n)$).

9.5. Увеличение относительной скорости передачи посредством представления поэтапной кодированной информации

Сочетание алгоритма многоступенчатого переспроса с идеей поэтапного кодирования и декодирования информации [35, 6] позволяет достичь увеличения относительной скорости передачи в системах передачи дискретной информации с решающей обратной связью. Определим достигаемый эффект на примере системы РОС—ОЖ.

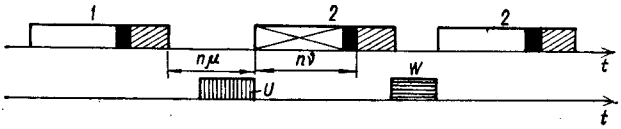


Рис. 9.7

Системы с ожиданием и поэтапным формированием сигнала решающей обратной связи РОС—ОЖ/ПЭ. На рис. 9.7 приведена временная диаграмма, поясняющая алгоритм функционирования данной системы. Из диаграммы следует, что сообщение кодируется избыточным кодом, содержащим две группы проверочных элементов — r_1 и r_2. На приемной стороне кодовая комбинация проверяется на отсутствие ошибок в два этапа: первый раз — после окончания приема $(\kappa + r_1)$ элементов комбинации, второй раз — по окончании приема $n = (\kappa + r_1 + r_2)$ элементов комбинации. Если при проверках ошибки не обнаруживаются, то формируется подтверждение u о правильном приеме и осуществляется передача очередного сообщения. При искажении кодовой комбинации ошибки в абсолютном большинстве случаев обнаруживаются после приема $(\kappa_1 + r_1)$ элементов сообщение *2* и переспрос W формируется раньше на время $t = \frac{r_2}{V}$. В некоторых редких случаях ошибки обнаруживаются не на первом, а на втором этапе приема n элементов. Тогда переспрос формируется аналогично подтверждению.

Выражение для определения относительной скорости передачи рассмотренной системы выводится по методике, изложенной в п. 9.2 и имеет вид

$$R_1' = \frac{k}{n(1+\mu)\left[1+\frac{\nu+\mu}{1+\mu}P_n\frac{1-P_n^{m-1}}{1-P_n}\right]}, \qquad (9.31)$$

где ν — коэффициент, определяющий долю элементов первого этапа декодирования $\nu = \frac{k+r_1}{n}$.

Для обеспечения наглядности сравнительного анализа преобразуем выражение (9.5) к виду

$$R_1 = \frac{k}{(n(1-\mu))\left[1+P_n\frac{1-P_n^{m-1}}{1-P_n}\right]}. \qquad (9.32)$$

Выражения (9.31) и (9.32) отличаются только сомножителем в знаменателе $\frac{\nu+\mu}{1+\mu}$, причем для того, чтобы выполнилось неравенство

$$R_1' > R_1,$$

необходимо соблюдение условий

$$\frac{\nu+\mu}{1+\mu} < 1, \text{ т. е. } \nu < 1.$$

Следует отметить, что поэтапная обработка информации в ИС с решающей обратной связью приводит также к уменьшению среднего времени доведения информации.

Таким образом, система передачи информации с решающей обратной связью позволяет обеспечить требуемое значение достоверности информации при меньшем значении общей избыточности передаваемых сообщений. При этом качество каналов связи накладывает ограничения и определяет оптимальную длину блоков сообщений и режим декодирования, обеспечивающие наибольшее значение относительной скорости передачи.

Дополнительное увеличение относительной скорости передачи достигается за счет использования поэтапных методов принятия решений при реализации процедур кодирования и декодирования передаваемых сообщений.

10. СЕЛЕКЦИЯ ИНФОРМАЦИИ В ИС

10.1. Виды ошибок в ИС

В информационных системах помимо ошибок, обусловленных искажением отдельных элементов кодовых комбинаций, имеют место ошибки, связанные со сдвигом кодовых комбинаций на временной оси. Первопричиной этого типа ошибок являются искажения отдельных элементов кодовых комбинаций, не обнаруженные кодовыми методами, но приводящие к специфическим вторичным эффектам, что заставляет их выделять в самостоятельные группы:

ошибка типа «сбой фазирования по циклам»;

вставки и выпадения информации.

Методы борьбы с перечисленными группами ошибок различны и требуют самостоятельного рассмотрения, но общим для них является использование принципа селекции (выделения) информации.

10.2. Фазирование информации по циклам

Фазирование по циклам предусматривает определение местоположения кодовых комбинаций на временной оси. При этом для кодовых комбинаций постоянной длины достаточно определить начало или конец каждой из них, а для кодовых комбинаций переменной длины обязательным является определение начала и конца каждой комбинации. Данная операция является обязательной для последующего правильного декодирования кодовых комбинаций как с исправлением, так и обнаружением ошибок кодовыми методами. Неправильное определение начала и конца кодовых комбинаций называется сбоем циклового фазирования.

Фазирование по циклам может осуществляться при помощи:

префиксных кодов;

кодов с запятой;

самосинхронизирующихся кодов.

Префиксные коды. Префиксные коды предполагают передачу перед каждой кодовой комбинацией специальной m-элементной последовательности — префикса (маркера) (рис. 10.1,*а*).

Эти коды требуют дополнительной избыточности и, следовательно, снижают относительную скорость пере-

дачи. Если относительная скорость передачи, определяемая избыточным (n, κ)-кодом,

$$R_1 = \frac{k}{n},$$

то относительная скорость передачи префиксного кода

$$R_2 = \frac{k}{n+m} \text{ и } R_2 < R_1$$

В некоторых случаях для обеспечения требуемых характеристик циклового фазирования используют сложный (составной) префикс, включающий в себя несколько

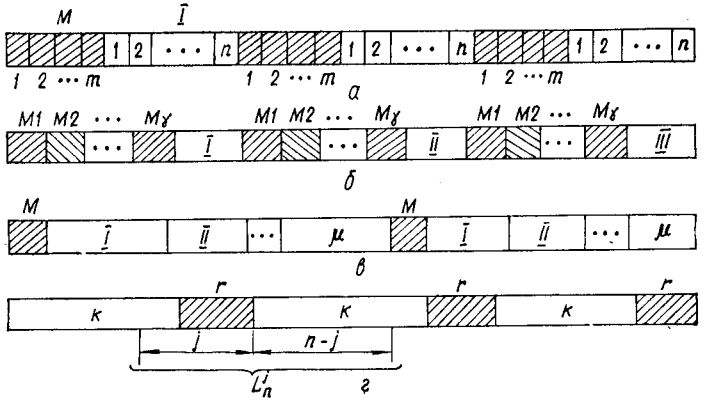


Рис. 10.1

маркеров $M1$, M2,..., $M\gamma$ (рис. 10.1, *б*). В этом случае относительная скорость передачи

$$R_3 = \frac{k}{n+\gamma m}, \text{ т. е. } R_3 < R_2 < R_1,$$

однако при этом увеличивается надежность установления фазирования по циклам, а следовательно, и селекция правильной информации. В общем случае характеристики системы циклового фазирования противоречивы и требуют оптимизации методами нелинейного программирования.

Покажем решение этой задачи для ДСК без памяти. Вероятность ложного выделения маркера определяется выражением

$$P_л = \frac{1}{2^m},$$

из чего следует, что с увеличением длины маркера уменьшается возможность установления ложного синхронизма.

Однако при этом увеличивается и вероятность потери маркера, что следует из

$$P_{n1} \approx mP_0,$$

где P_0 — вероятность искажения одного элемента маркера. Для сложного префикса, включающего γ маркеров, общая вероятность потери маркеров

$$P_n(\gamma) = (P_{n1})^\gamma = m^\gamma P_0^\gamma,$$

а вероятность ложного выделения маркера

$$P_л(\gamma) = \frac{\gamma}{2m}.$$

Таким образом, если заданы характеристики по надежности и точности установления синхронизма ($P_п^з$, $P_л^з$), то можно определить параметры сложного префикса m и γ из следующей системы нелинейных уравнений:

$$\begin{cases} P_л^з = \frac{\gamma}{2m}, \\ P_п^з = m^\gamma P_0^\gamma. \end{cases}$$

Коды с запятой. Код с запятой характеризуется передачей m-элементной последовательности перед группой μ кодовых комбинаций (рис. 10.1, *в*).

Относительная скорость передачи этих кодов характеризуется выражением

$$R_4 = \frac{k}{n + \frac{m}{\mu}}$$

и при $\mu = 1$ они вырождаются в префиксные коды.

Самосинхронизирующиеся коды. Самосинхронизирующиеся коды обладают свойством выделения каждой кодовой комбинации без наличия дополнительного канала (сигнала) фазирования. Для этого необходимо, чтобы никакой стык двух кодовых слов L_n^j не являлся разрешенным кодовым словом применяемого избыточного кода $j = 1 - (n - 1)$ (рис. 10.1, *г*).

В качестве примера использования самосинхронизирующегося кода можно указать на коды с повторением, описанные в 5.3 и обладающие высокой точностью установления синхронизма, так как длина синхросигнала определяется длиной одного повторения кодовой комбинации.

10.3. Вставки и выпадения информации

Вставки и выпадения информации имеют место в системах передачи дискретной информации, использующих канал обратной связи для подтверждения факта правильного приема или запроса на повторную передачу сообщений.

Если в системе РОС—ОЖ за счет ошибок в канале обратной связи произойдет трансформация сигнала подтверждения U в сигнал запроса W (рис. 10.2, *а*), то сообщение *1* будет передано дважды, т.е. на приемной стороне

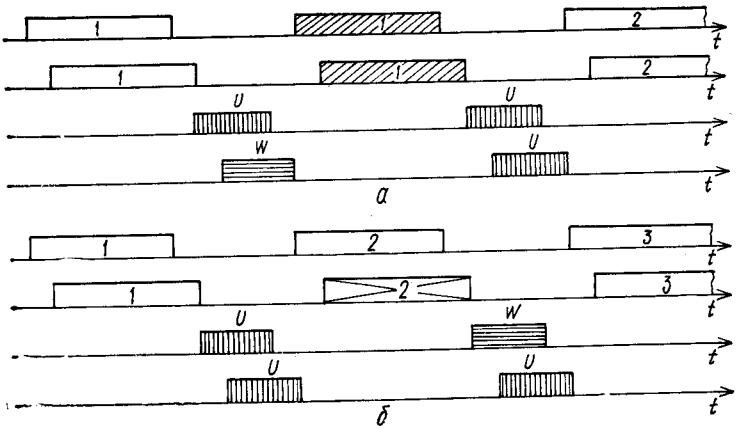


Рис. 10.2

будет иметь место вставка сообщения *1*. В этом случае произойдет сдвиг на временной оси всех сообщений и нарушение очередности их следования.

В том случае, когда при искажении сообщения *2* (рис. 10.2,*б*) сигнал запроса трансформируется в сигнал подтверждения U, имеет место выпадение сообщения *2*, сдвиг и нарушение очередности следования сообщений.

В системах РОС—ОЖ искажение и неприем сигнала обратной связи U приводит к многократной вставке передаваемого сообщения. Таким образом, можно сказать, что вставки и выпадения приводят к сдвигу информации. Негативные последствия вставок и выпадений сообщений могут быть разнообразны. Не вдаваясь в рассмотрение сущности этих последствий, перечислим основные:

нарушение алгоритма управления объектами;

уменьшение оперативности управления;

увеличение вероятности отказа в обработке сообщений как заявок системы массового обслуживания;

увеличение среднего времени обработки сообщений;

снижение относительной скорости передачи информации.

Поэтому обеспечению верности передачи сигналов обратной связи следует уделять соответствующее внимание. В тех случаях, когда обеспечение верности сопряжено с трудностями энергетического, конструктивного или иного характера, разумные требования можно установить, положив

$$P_{\text{сдв}} = P_{\text{вст}} + P_{\text{вып}} \leqslant \varepsilon P_{\text{н. о}},$$

где $P_{\text{н. о}}$ — вероятность необнаружения ошибок в основном передаваемом сообщении, слабо зависящая от достоверности сигналов обратной связи; ε — достаточно малый весовой коэффициент, сводящий вероятность вставок и выпадений к пренебрежимо малой величине.

Известно достаточно большое число методов передачи сигналов обратной связи, обеспечивающих заданные требования по верности этих сигналов. Основными из них являются [27]:

1) передача служебных сигналов по обособленным временным, частотным или другим каналам;

2) совместная передача служебных сигналов в основной информации;

3) смешанная передача.

Заданная достоверность служебных сигналов при этом обеспечивается, как правило, прямыми кодовыми методами, дополненными в определенных случаях косвенными — алгоритмическими методами. Из кодовых методов наибольшее распространение получили коды с повторением с мажоритарной обработкой на стороне приема служебного сигнала и рекуррентные коды — m-последовательности, псевдослучайные последовательности. Кодовым методам защиты информации от ошибок уделено достаточно внимания в предыдущих разделах, поэтому остановимся более подробно на косвенных методах защиты от вставок и выпадений информации.

Борьба со вставками и выпадениями информации в системах РОС—ОЖ. В системах передачи дискретной информации с ожиданием сигнала решающей обратной связи вставки информации могут быть исключены, если сравнивать каждое предыдущее правильно принятое сообщение с последующим. При совпадении сравниваемых сообще-

ний фиксируется вставка и принимаемое сообщение дальнейшей обработке на подвергается.

В системах РОС—ОЖ вставки информации возможны в пределах определенного времени

$$t_c^м = \frac{n}{V}(i-1),$$

где V — скорость модуляции; i — максимальное число повторений комбинации.

В течение этого времени и необходимо осуществлять селекцию аналогичных кодовых комбинаций.

На рис. 10.3 изображена структурная схема устройства для предотвращения вставок информации. Работает устройство следующим образом. Принятая кодовая комбинация через схему ИЛИ записывается в регистр записи РЗ, «выталкивая» нули в анализатор совпадений АС, и одновременно поступает через другой вход непосредственно в АС. Логика работы АС такова, что в случае несовпадения элементов сравниваемых комбинаций хотя бы в одном разряде происходит формирование сигнала, поступающего на управляющие входы вентиля считывания ВС и блока управления БУ и разрешающего перевод принятой кодовой комбинации из РЗ получателю П сообщений и перезапись ее в РЗ. Этот процесс осуществляется ускоренно для того, чтобы закончиться к моменту начала приема следующей комбинации. Одновременно БУ выдает сигнал, который включает датчик времени ДВ, отсчитывающий время селекции [12].

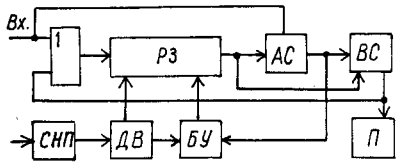


Рис. 10.3

Принятая последующая комбинация записывается в РЗ, «выталкивая» элементы предыдущей комбинации в АС, и одновременно поступает на другой вход АС. В случае полного совпадения элементов сравниваемых комбинаций сигнал разрешения на выходе АС отсутствует, кодовая комбинация из РЗ не считывается и получателю П не выдается. По окончании времени селекции $t_c^м$ ДВ выдает сигнал, устанавливающий РЗ в нулевое состояние. В этом случае очередная комбинация принимается как новая, выдается получателю и перезаписывается в РЗ. При этом вновь включается ДВ, регламентирующий интервал селекции для принятого сообщения.

Рассмотренный алгоритм исключения вставок может привести к потере информации. Произведем оценку этих потерь. Если положить, что все сообщения равновероятны $P_0 = \frac{1}{2^k}$ и безошибочно принимается j-е из i возможных повторений, то первые $(j-1)$ повторения очередного идентичного сообщения будут селектироваться. Вероятность потери сообщения в этом случае определяется выражением

$$P_{\text{п}_1} \approx P_{\text{с}}^2 (nP_0)^{i-j+1}.$$

Если же используется нумерация повторов с последующим определением номера в селекторе номера повторов

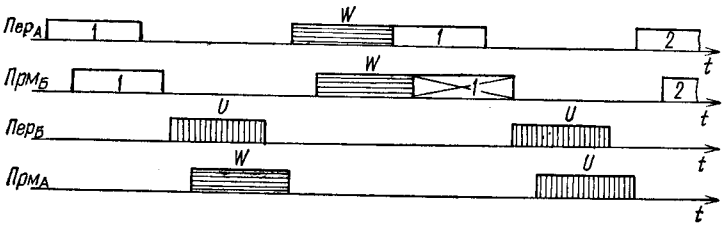


Рис. 10.4

СНП и перестраиваемый ДВ, на котором устанавливается время селекции

$$t_{\text{с}}^j = \frac{n}{V}(i-j)$$

в зависимости от номера j принятой комбинации, то это уменьшает потери информации, оцениваемые выражением

$$P_{\text{п}_2} \cong P_{\text{с}}^2 (nP_0)^i.$$

Рассмотренный метод требует увеличения сложности устройства обработки принимаемых сигналов. В некоторых случаях это нецелесообразно и существенного уменьшения вероятности вставки информации можно достигнуть путем передачи сигнала подтверждения переспроса. Для этого может использоваться непосредственно сигнал переспроса W, передаваемый перед повторяемым сообщением (рис.10.4). В этом случае трансформация сигнала подтверждения U в сигнал переспроса W не приводит к появлению вставки сообщения, так как выделение сигнала подтверждения переспроса W на приемной стороне указывает на повторение предыдущего сообщения, которое стирается.

Если при отсутствии сигнала подтверждения переспроса вероятность вставки информации определяется вероятностью трансформации сигнала подтверждения U в сигнал переспроса W

$$P_{\text{вст}_1} \cong P(W/U),$$

то введение сигнала подтверждения переспроса приводит к вставке информации только в том случае, если, кроме того, дополнительно имеет место трансформация сигнала подтверждения переспроса W в разрешенную комбинацию N избыточного (n, k)-кода

$$P_{\text{вст}_2} \cong P(W/U)\,P(N/W).$$

Вероятность выпадения информации в первом случае будет определяться выражением

$$P_{\text{вып}_1} \cong P_{\text{ош}} P(U/W),$$

где $P_{\text{ш}}$ — вероятность появления ошибок в кодовой комбинации; $P(U/W)$ — вероятность приема сигнала подтверждения U при условии, что был передан сигнал переспроса W.

Во втором случае выпадение будет иметь место, если в очередном цикле передачи дополнительно произойдет трансформация разрешенной комбинации N в комбинацию подтверждения переспроса W:

$$P_{\text{вып}_2} \cong P_{\text{ош}} P(U/W)\,P(W/N).$$

Обнаружение вставок и выпадений информации в системах РОС—ПП. В системах с последовательной передачей кодовых комбинаций обмен информацией, как правило, ведется по двум каналам одновременно в двух направлениях (рис.10.5).

Если приемник одной из станций обнаруживает ошибки в принимаемой комбинации (φ) или принимает запросную комбинацию ЗК длины n, то она стирается, а приемник блокируется на время приема h комбинаций. В этом случае передатчик данной станции посылает на противоположную станцию ЗК и затем повторяет h ранее переданных комбинаций (рис.10.5, *а*). Когда под действием ошибок в канале ЗК переходит в одну из разрешенных комбинаций, на станции, куда была послана ЗК$(h+1)$ комбинаций будет принято дважды, т. е. будет иметь место вставка из $(h+1)$ комбинаций. В то же время, как это видно из рис. 10.5, *в*, противоположной станцией не будет принято $h+1$ комбинаций, т. е. будет иметь место выпадение $h+1$ комбинаций из передаваемой последовательности. Описанный тип вста-

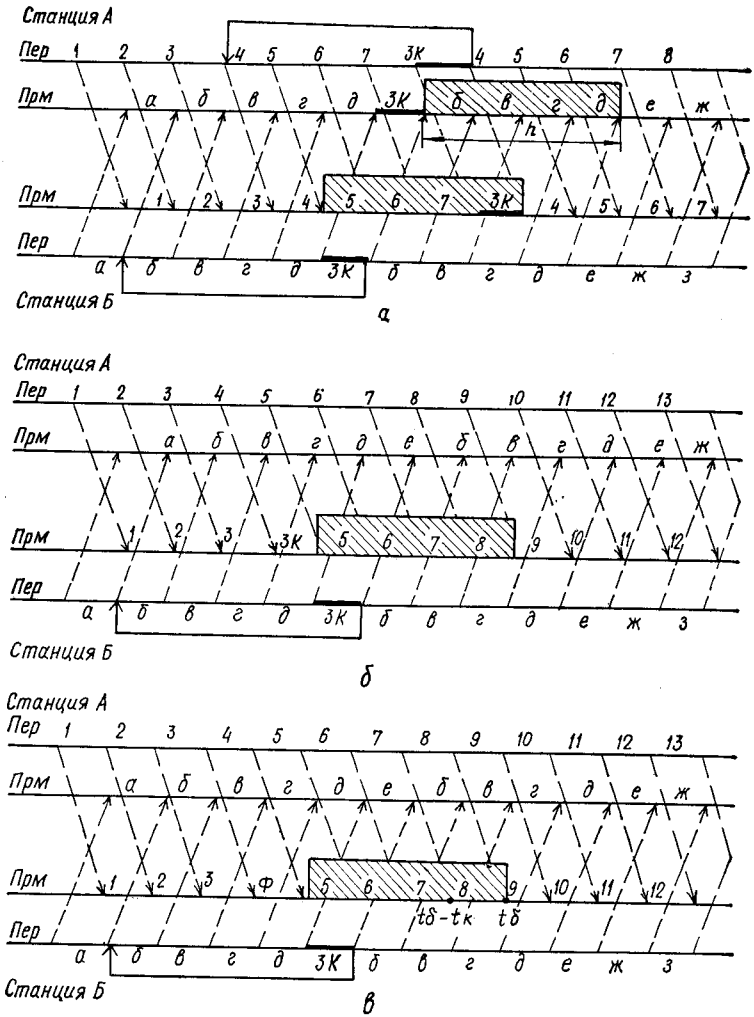


Рис. 10.5

вок и выпадений может быть обнаружен, если на станции обнаружения ошибки и формирования запроса на интервале $(t_\delta,\ t_\delta - t_k)$, где t_δ — время окончания блокировки, t_k — длительность кодовой комбинации, анализировать поступающую комбинацию. В случае неприема в указанный интервал комбинации запроса ЗК фиксируется вставка и выпадение сообщений.

Однако если на интервале $(t_\delta,\ t_\delta - t_k)$ разрешенная комбинация в свою очередь трансформируется в ЗК, то данным методом вставки и выпадения обнаружены не будут. Вероятность такого события может быть определена из выражения

$$P_{\text{сдв}_1} = P_{\text{ош}} P\,(N/W)\,P\,(W/N).$$

Возможно дальнейшее развитие описанного метода, повышающее его помехоустойчивость [12].

Для этого необходимо после обнаружения ошибки и формирования ЗК запоминать h комбинаций, попадающих под блокировку, с последующим их сравнением с соответствующими комбинациями, поступающими после выделения ЗК на интервале $(t_\delta,\ t_\delta - t_k)$. При несовпадении ν из h комбинаций, где $1 \leqslant \nu \leqslant h$, фиксируют выпадение $(2h + 1)$ комбинаций на станции обнаружения ошибки и вставку $(h + 1)$ комбинаций на противоположной станции. Для каналов с памятью сообщения, попавшие в зону блокировки и близлежащую зону, подвергаются усиленному воздействию помех и, соответственно, требуют более тщательной проверки на наличие или отсутствие ошибок. Это можно осуществить без каких-либо дополнительных кодовых или конструктивных затрат, если запоминаемые в период блокировки комбинации проверять дополнительно на наличие или отсутствие ошибок, сравнивать соответствующие безошибочные комбинации и при несовпадении фиксировать наличие ошибки в принятой комбинации.

Вероятность сдвига информации при использовании модифицированного метода определяется выражением

$$P_{\text{сдв}_2} \cong P_{\text{ош}} P\,(N/W)\,P\,(W/N)\,[P\,(N_i/N_i)]^\nu,$$

где член $[P\,(N_i/N_j)]^\nu$ учитывает одновременную трансформацию ν комбинаций в аналогичные ранее накопленные комбинации. Если положить $P\,(N/W) = P\,(W/N) = P\,(N_i/N_j) = 10^{-6}$; $P_{\text{ош}} = 10^{-2}$; $\nu = 2$, то $P_{\text{сдв}_1} = 10^{-14}$ и $P_{\text{сов}_2} = 10^{-26}$, т. е. модифицированный метод имеет значительно большую помехоустойчивость.

Возможны вставки и выпадения информации в системах РОС—ПП и в тех случаях, когда разрешенная комбинация трансформируется в запросную комбинацию ЗК при передаче в одном направлении, а запросная комбинация ЗК, в свою очередь, трансформируется в одну из разрешенных комбинаций при передаче в другом направлении (рис. 10.5, *б*). Тогда на станции приема ЗК будет иметь место выпадение $(h + 1)$ комбинаций, а на противополож-

ной станции — вставка $(h+1)$ комбинаций. Обнаружить данную ситуацию можно, если сравнивать h комбинаций, принятых до поступления ЗК с соответствующими h комбинациями, поступающими после приема ЗК. При несовпадении ν из h комбинаций, где $1 \leqslant \nu \leqslant h$, фиксируют недоверие к поступающей информации и продолжают ее прием. Анализируют на интервале $(t_\delta, t_\delta - t_k)$ кодовую комбинацию и, если она оказывается не ЗК, фиксируют на данной станции выпадение, а на противоположной станции вставку $(h+1)$ комбинаций. Выделение на интервале $(t_\delta, t_\delta - t_k)$ запросной комбинации ЗК свидетельствует о том, что имела место трансформация разрешенной комбинации в ЗК, что идентифицируется как обнаружение ошибки. При этом продолжают прием и анализируют поступающую информацию так, как это описано для случая, представленного на рис. 10.5, *в*.

Таким образом, специфическая категория ошибок в ИС характеризуется сдвигом кодовых комбинаций на временной оси, включает ошибки фазирования по циклам, а также вставки и выпадения информации, при этом методы борьбы с перечисленными группами ошибок различны, но общим для них является использование принципа селекции информации.

В общем случае характеристики системы циклового фазирования противоречивы и требуют оптимизации методами нелинейного программирования.

Модификация методов борьбы со вставками и выпадениями информации улучшает вероятностные характеристики систем передачи сообщений с решающей обратной связью.

Заключение

Рождение теории кодирования и декодирования связано с появлением работ В. А. Котельникова и К. Э. Шеннона. Советские и зарубежные ученые и инженеры продолжают создавать фундаментальные основы анализа и синтеза кодирования и декодирования в ИС. Развиваются математические моделирования процессов получения, преобразования, накопления и передачи инифомации в дискретных каналах ИС на основе использования идеальных и реальных моделей, теория эффективного, помехоустойчивого и оптимального кодирования.

Оптимальное кодирование все шире применяется в ИС, к которым можно отнести системы и сети связи, системы

передачи данных в АСУ, радионавигационные системы, вычислительные системы, всевозможные телемеханические системы измерения, контроля и управления.

Основные тенденции и перспективы развития кодеров и декодеров следующие:

дальнейшее уплотнение и повышение надежности каналов передачи информации;

применение широкополосных методов и устройств передачи информации;

широкое использование корректирующего кодирования и декодирования сигналов;

применение адаптации для оперативной коррекции характеристик каналов;

разработка методов принятия решений, оценки эффективности, качества и оптимальности с учетом надежности, быстродействия и всевозможных затрат;

применение статистического моделирования процессов передачи сообщений, внедрение функционально-модульного принципа построения ИС;

поиск новых методов и средств кодирования и декодирования информации на основе кодов Фибоначчи и «Золотой пропорции», устройств оптоэлектроники и т. д.

СПИСОК ЛИТЕРАТУРЫ

1. *Андрущенко А. Г.* и др. А.с. 657635 (СССР). Устройство для приема информации по двум параллельным каналам связи в СПД. — Опубл. в Б.И., 1979, № 14.
2. *Аксенов Б. Е., Александров А. М.* Об одном методе исследования потоков ошибок в каналах связи. — В кн.: Проблемы передачи информации. Вып. 4. М., 1968, т. 4, с. 79—83.
3. *Берлекэмп Э. Р.* Техника кодирования с исправлением ошибок. ТИИЭР, 1980, т. 68, № 5, с. 24—58.
4. *Бородин Л. Ф.* Введение в теорию помехоустойчивого кодирования. — М.: Сов. радио, 1968. — 408 с.
5. *Касаткин А. С., Кузьмин И. В.* Оценка эффективности автоматизированных систем контроля. — М.: Энергия, 1967. — 80 с.
6. *Ключко В. И.* А. с. 500595 (СССР). Способ передачи и приема поэтапно закодированных сообщений. — Опубл. в Б.И., 1976, № 3.
7. *Ключко В. И.* А.с. 520611 (СССР). Устройство для обнаружения ошибок в циклических кодах. — Опубл. в Б. И., 1976, № 25.
8. *Ключко В И.* А.с. 524316 (СССР). Устройство исправления стираний. — Опубл. в Б.И., 1976, № 29.
9. *Ключко В. И.* А.с. 540389 (СССР). Устройство для обнаружения и исправления ошибок. — Опубл. в Б. И., 1976, № 47.
10. *Ключко В. И.* А. с. 543174 (СССР). Декодирующее устройство для циклических мажоритарных кодов. — Опубл. в Б. И., 1977, № 2.
11. *Ключко В. И. и др.* А. с. 582564 (СССР). Декодирующее устройство. — Опубл. в Б.И., 1977, № 44.
12. *Ключко В. И.* Защита от ошибок при обмене информацией в АСУ. — М.: МО, 1980. — 256 с.
13. *Ключко В. И., Березняков Г. Е.* Коды с циклической проверочной матрицей. — В кн.: Приборы и системы автоматики. Х.: Изд-во Харьк. ун-та, 1972, вып. 24, с. 119—127.
14. *Колесник В. Д. Мирончиков Е. Т.* Декодирование циклических кодов. — М.: Связь, 1968. — 252 с.
15. *Коржик В. И., Финк Л. М.* Помехоустойчивое кодирование дискретных сообщений в каналах со случайной структурой. — М.: Связь, 1975. — 270 с.
16. *Кузьмин И. В.* Оценка эффективности и оптимизации АСКУ. — М.: Сов. радио, 1971. — 294 с.
17. *Кузьмин И. Б., Кедрус В. А.* Основы теории информации и кодирования. — К.: Вища шк. Головное изд-во, 1977. — 280 с.
18. *Мартынов Е. М.* Синхронизация в системах передачи дискретной информации. — М.: Связь, 1972. — 216 с.
19. *Мельников Ю. Н.* Достоверность информации в сложных системах.— М.: Сов. радио, 1973. — 192 с.

20. *Месси Д. Л., Кастелло Д. Д., Юстесен Й.* Веса многочленов и кодовые конструкции. — В кн.: Кибернетический сборник. М.: Мир, 1974, № 11, с. 24—47.
21. *Мизин И. А. Уринсон Л. С., Храмешин Г. К.* Передача информации в сетях с коммутацией сообщений. — М.: Связь, 1972. — 319 с.
22. *Нейфах А. Е.* Сверточные коды для передачи дискретной информации. — М.: Наука, 1979. — 222 с.
23. *Николаев Ю. И., Ключко В. И., Петухов В. Е.* А. с. 749350 (СССР). Устройство для приема кодов с повторением.— Опубл. в Б.И., 1980, № 27.
24. *Новопашный Г. Н.* Информационно-измерительные системы. — М.: Высш. шк., 1977. — 208 с.
25. *Новоселов О. Н., Фомин А. Ф.* Основы теории и расчета информационно-измерительных систем. — М.: Машиностроение, 1980. — 280 с.
26. *Орнатский П. П.* Теоретические основы информационно-измерительной техники. — К.: Вища шк., Головное изд-во. 1976. — 436 с.
27. *Передача* информации с обратной связью / Под ред. З. М. Каневского. — М.: Связь, 1976. — 352 с.
28. *Питерсон У., Уэлдон Э.* Коды, исправляющие ошибки. — М.: Мир, 1976. — 590 с.
29. *Самойленко С. И.* Помехоустойчивое кодирование. — М.: Наука, 1966. — 239 с.
30. *Справочник* по кодированию информации / Под ред. проф. Н.Т. Березюка. — Х.: Вища шк., Изд-во при Харьк. ун-те, 1978. — 252 с.
31. *Финк Л. М.* Теория передачи дискретных сообщений. — М.: Сов. радио. 1970. — 728 с.
32. *Цымбал В. П.* Теория информации и кодирование. — К.: Вища шк., Головное изд-во, 1982. — 304 с.
33. *Цымбал В. П., Клешко Г. Н., Лавинский Г. В.* Представление и поиск данных в информационной системе. — К.: КИНХ, 1973. — ... с.
34. *Четвериков В. Н.* Преобразование и передача информации в АСУ. — М.: Высш. шк., 1974. — 320 с.
35. *Элементы* теории передачи дискретной информации / Под ред. Л. П. Пуртова. — М.: Связь, 1972. — 232 с.

ОГЛАВЛЕНИЕ

Предисловие 3

1. Общие принципы построения информационных систем (ИС) 5

1.1. Структурная схема ИС 5
1.2. Математические модели источников ошибок 7
1.3. Форматизация сообщений в информационных системах . 11
1.4. Помехоустойчивое кодирование информации 15

2. Критерий оценки эффективности и качества ИС 18

2.1. Выбор критерия 18
2.2. Точность работы ИС 18
2.3. Время получения информации 22
2.4. Масса и объем аппаратуры ИС 23
2.5. Стоимость получения информации 24
2.6. Обобщенный функционально-статистический критерий оценки эффективности 25
2.7. Особенности оценки детерминированных вероятностных характеристик цифровых автоматических систем . . . 27

3. Линейные коды 30

3.1. Постановка задачи 30
3.2. Построение линейных кодов 30
3.3. Процедуры декодирования 32
3.4. Оценка сложности кодеров и декодеров линейных кодов . 34
3.5. Некоторые пути уменьшения сложности декодирующих устройств 36
3.6. Поэтапное кодирование и декодирование дискретной информации 41
3.7. Области применения поэтапных методов принятия решений 46

4. Циклические коды 52

4.1. Задание циклических кодов 52
4.2. Коды с постоянной четностью единиц 54
4.3. Помехоустойчивость циклических кодов 55
4.4. Алгоритм нахождения циклического кода, удовлетворяющего заданной достоверности 58
4.5. Принципы построения кодирующих и декодирующих устройств 61

4.6. Циклические коды, допускающие мажоритарное декодирование . . . 69
4.7. Поэтапное формирование и обработка циклических кодов . 73

5. Коды с повторением 81

5.1. Определение . . . 81
5.2. Обработка по критерию «два из двух» избыточных (n, k)-кодов . . . 83
5.3. Обработка избыточных (n, k)-кодов с повторением по критерию «один из двух» . . . 90
5.4. Исправление ошибок в избыточных (n, k)-кодах с повторением . . . 93

6. Мажоритарное декодирование кодов с повторением . . . 98

6.1. Адаптивное мажоритарное декодирование кодов с повторением . . . 98
6.2. Расширение области адаптивного мажоритарного декодирования кодов с повторением . . . 104
6.3. Мажоритарное декодирование избыточных (n, κ)-кодов с повторением . . . 112
6.4. Поэтапная обработка кодов с повторением . . . 114

7. Оптимальные и близкие к ним методы приема и обработки сообщений с избыточностью . . . 121

7.1. Общие положения . . . 121
7.2. Метод Вагнера и прием по наиболее надежным элементам 122
7.3. Оптимизация обработки избыточных кодов в каналах со стиранием . . . 124
7.4. Модифицированный метод исправления стираний . . . 129
7.5. Исправление стираний в кодах с повторением . . . 131

8. Алгебраические методы построения сверточных кодов (СК) . 134

8.1. Определение сверточных кодов . . . 134
8.2. Приведение сверточных кодов к многократным циклическим кодам . . . 137
8.3. Синтез систематических сверточных кодов . . . 140
8.4. Методы синтеза несистематических сверточных кодов с относительной скоростью $R = \frac{1}{b}$ . . . 145
8.5. Синтез сверточных кодов с относительной скоростью $R \neq \neq \frac{1}{b}$ . . . 153
8.6. Оценка сверточных кодов . . . 156

9. Системы передачи дискретной информации с решающей обратной связью . . . 158

9.1. Классификация систем с решающей обратной связью . 158
9.2. Системы одностороннего действия с ожиданием сигнала обратной связи . . . 160

9.3. Определение оптимальных характеристик кода в режиме обнаружения ошибок 164
9.4. Выбор оптимального режима декодирования избыточных кодов 167
9.5. Увеличение относительной скорости передачи посредством представления поэтапно кодированной информации . . . 172

10. Селекция информации в ИС 174

10.1. Виды ошибок в ИС 174
10.2. Фазирование информации по циклам 174
10.3. Вставки и выпадения информации 177
Заключение 184

Список литературы 186

Иван Васильевич Кузьмин
Владимир Игнатьевич Ключко
Валерий Антонович Литвин

КОДИРОВАНИЕ И ДЕКОДИРОВАНИЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Под редакцией
доктора технических наук
профессора *И. В. Кузьмина*

Редактор *Ж. Г. Давиденко*
Художественный редактор *С. П. Духленко*
Технический редактор *Л. Ф. Волкова*
Корректор *С. Я. Кахетелидзе*

Информ. бланк № 8922

Сдано в набор 27.02.85. Подп. в печать 11.06.85. БФ 02621. Формат 84×108/32. Бумага типогр. № 1. Лит. гарн. Выс. печать. Усл. печ. л. 10,08. Усл. кр.-отт. 10,34. Уч.-изд. л. 9,63. Тираж 1120 экз. Изд. № 6925. Зак. 5-1134. Цена 1р. 50к.

Головное издательство издательского объединения «Вища школа», 252054, Киев-54, ул. Гоголевская, 7

Отпечатано с матриц книжной фабрики им. М. В. Фрунзе в Харьковской городской типографии № 16, Харьков-3, ул. Университетская, 16. Зак. 1322.