Лабораторная работа N 3

КОРРЕКТИРУЮЩИЕ КОДЫ ХЕММИНГА

ЦЕЛЬ РАБОТЫ. Изучение принципов помехоустойчивого кодирования, ознакомление с классификацией корректирующих кодов и основными их характеристиками, с методами кодирования и декодирования на примере кода Хемминга и циклического кода (9, 5).

1. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПОДГОТОВКЕ К ЛАБОРАТОРНОЙ РАБОТЕ

Для выполнения лабораторной работы студенты должны предварительно изучить раздел 1 настоящего методического руководства и получить у преподавателя допуск к работе.

1.1 Принципы помехоустойчивого кодирования.

В реальных условиях приём двоичных символов всегда происходит с ошибками, когда вместо символа "1" принимается символ "0" и наоборот. Ошибки могут возникать из-за помех, действующих в канале связи (особенно помех импульсного характера), изменения за время передачи характеристик канала (например, замирания), снижения уровня передачи, нестабильности амплитудно- и фазочастотных характеристик канала и т.п.

Общепринятым критерием оценки качества передачи в дискретных каналах является нормированная на знак или символ допустимая вероятность ошибки для данного вида сообщений. Так, допустимая вероятность ошибки при телеграфной связи может составлять 10^{-3} (на знак), а при передаче данных - не более 10^{-6} (на символ). Для обеспечения таких значений вероятностей одного улучшения только качественных показателей канала связи может оказаться недостаточным. Поэтому основной мерой является применение специальных методов повышения качества приёма передаваемой информации. Эти методы можно разбить на две группы.

К первой группе относятся методы увеличения помехоустойчивости приёма единичных элементов (символов) дискретной информации, связанные с выбором уровня сигнала, отношения сигнал-помеха (энергетические характеристики), ширины полосы канала, методов приёма и т.д.

Ко второй группе относятся методы обнаружения и исправления ошибок, основанные на искусственном введении избыточности в передаваемое сообщение. Увеличить избыточность передаваемого сигнала можно различными способами. Так как объём сигнала

$$V = P \cdot \Delta F \cdot T, \qquad (3.1)$$

где P - мощность сигнала, Вт; ΔF - ширина спектра сигнала, Гц;
T - время передачи сигнала, сек, то его увеличение возможно за счёт увеличения P, ΔF и T.

Практические возможности увеличения избыточности за счёт мощности и ширины спектра сигнала в системах передачи дискретной информации по стандартным каналам резко ограничены. Поэтому для повышения качества

приёма, как правило, идут по пути увеличения времени передачи и используют следующие основные способы:

1) многократная передача кодовых комбинаций (метод повторения);
2) одновременная передача кодовой комбинации по нескольким параллельно работающим каналам;
3) помехоустойчивое (корректирующее) кодирование, т.е. использование кодов, исправляющих ошибки.

Иногда применяют комбинации этих способов.

Многократное повторение (ℓ раз) кодовой комбинации является самым простым способом повышения достоверности приёма и легко реализуется, особенно в низкоскоростных системах передачи для каналов с быстро меняющимися параметрами. Метод многократного повторения исследовался в лабораторной работе N1 на примере кода МТК-2 с мажоритарным декодированием [1].

Способу многократного повторения аналогичен способ передачи одной и той же информации по нескольким параллельным каналам связи. В этом случае необходимо иметь не менее трёх каналов связи (например, с частотным разнесением), несущие частоты которых нужно выбирать таким образом, чтобы ошибки в каналах были независимы. Достоинством таких систем являются надёжность и малое время задержки в получении информации. Основным недостатком многоканальных систем так же, как и систем с повторением, является нерациональное использование избыточности.

Наиболее целесообразно избыточность используется при применении помехоустойчивых (корректирующих) кодов.

При помехоустойчивом кодировании чаще всего считают, что избыточность источника сообщений на входе кодера равна $\chi = 0$. Это обусловлено тем, что очень многие дискретные источники (например, цифровая информация на выходе ЭВМ) обладают малой избыточностью. Если избыточность первичных источников сообщений существенна, то в этих случаях по возможности стремятся ее уменьшить путём эффективного кодирования, применяя, например, коды Шеннона-Фано или Хафмена. Эти вопросы исследовались в лабораторной работе N2 на примере кода Хафмена [2]. Затем методами помехоустойчивого кодирования можно внести такую избыточность в сигнал, которая позволит достаточно простыми средствами улучшить качество приёма. Таким образом, эффективное кодирование вполне может сочетаться с помехоустойчивым.

В обычном равномерном непомехоустойчивом коде число разрядов n в кодовых комбинациях определяется числом сообщений и основанием кода.

Коды, у которых все кодовые комбинации разрешены к передаче, называются простыми или равнодоступными и являются полностью безизбыточными. Безизбыточные первичные коды обладают большой "чувствительностью" к помехам.

Внесение избыточности при использовании помехоустойчивых кодов обязательно связано с увеличением n - числа разрядов (длины) кодовой комбинации. Таким образом, всё множество $N = 2^n$ комбинаций можно разбить на два подмножества: подмножество разрешённых комбинаций, т.е. обладающих определёнными признаками, и подмножество запрещённых комбинаций, этими признаками не обладающих.

Помехоустойчивый код отличается от обычного тем, что в канал передаются не все кодовые комбинации N , которые можно сформировать из имеющегося числа разрядов n , а только их часть N_K, которая составляет подмножество разрешённых комбинаций.

Если при приёме выясняется, что кодовая комбинация принадлежит к запрещённым, то это свидетельствует о наличии ошибок в комбинации, т.е. таким образом решается задача обнаружения ошибок. При этом принятая комбинация не декодируется (не принимается решение о переданном сообщении). В связи с этим помехоустойчивые коды называют корректирующими кодами. Корректирующие свойства избыточных кодов зависят от правила их построения, определяющего структуру кода, и параметров кода (длительности символов, числа разрядов, избыточности и т.п.).

Первые работы по корректирующим кодам принадлежат Хеммингу, который ввёл понятие минимального кодового расстояния d_{min} и предложил код, позволяющий однозначно указать ту позицию в кодовой комбинации, где произошла ошибка. К "k" информационным элементам в коде Хемминга добавляется "r" проверочных элементов для автоматического определения местоположения ошибочного символа. Коды Хемминга будут рассмотрены подробнее далее.

1.2. Классификация помехоустойчивых корректирующих кодов.

На рис. 3.1 приведена упрощённая классификация помехоустойчивых кодов. Остановимся кратко на основных особенностях различных классов кодов. Помехоустойчивые (корректирующие) коды делятся на блочные и непрерывные.

Блочными называются коды, в которых информационный поток символов разбивается на отрезки и каждый из них преобразуется в определённую последовательность (блок) кодовых символов. В блочных кодах кодирование при передаче (формирование проверочных элементов) и декодирование при приёме (обнаружение и исправление ошибок) выполняются в пределах каждой кодовой комбинации (блока) в отдельности по соответствующим алгоритмам.

Непрерывные или рекуррентные коды образуют последовательность символов, не разделяемую на отдельные кодовые комбинации. Кодирование и декодирование непрерывно совершаются над последовательностью элементов без деления их на блоки. Формирование проверочных символов ведётся по рекуррентным (возвратным) правилам, поэтому непрерывные коды часто называют рекуррентными или цепными.

В простейшем цепном коде каждый проверочный элемент формируется путём сложения по модулю 2 соседних или отстоящих друг от друга на определённое число позиций информационных элементов. В канал связи передаётся последовательность импульсов, в которой за каждым информационным следует проверочный. Подобную чередующуюся последовательность разрядов имеет, например, корреляционный манчестерский код [3].

К непрерывным кодам относятся и свёрточные коды, в которых каждый информационный символ, поступающий на вход кодирующего устройства, вызывает появление на его выходе ряда проверочных элементов, образованных суммированием по модулю 2 данного символа и " k-1 " предыдущих информационных символов. Рекуррентные коды позволяют исправлять групповые ошибки (" пачки ") в каналах связи.

Блочные коды делятся на равномерные и неравномерные. В равномерных кодах, в отличие от неравномерных, все кодовые комбинации содержат одинаковое число n - символов (разрядов) с постоянной длительностью τ_0 импульсов символов кода. Равномерные коды в основном и применяются в системах связи, так как это упрощает технику передачи и приёма.

Рис.3.1.

Классическими примерами неравномерного кода являются код Морзе, широко применяемый в телеграфии, и код Хафмена, применяемый для компрессии информации (факсимильная связь, ЭВМ).

Никаких специальных мер по исправлению и обнаружению ошибок в коде Морзе не предусматривается в связи с большой избыточностью самого передаваемого текста. В этом смысле код Морзе не относится к классу корректирующих кодов.

Почти все блочные корректирующие коды принадлежат к разделимым кодам, в которых кодовые комбинации состоят из двух частей: информационной и проверочной. Их символы всегда занимают одни и те же позиции, т.е. располагаются на определённых местах. Как правило, в таких кодах, все кодовые комбинации которых содержат n символов, первые k символов являются информационными, а за ними располагаются (n - k) проверочных символов. В соответствии с этим разделимые коды получили условное обозначение – (n , k) - коды.

В неразделимых кодах деление на информационные и проверочные символы отсутствует. К таким кодам относятся, в частности, коды с постоянным весом, так называемые равновесные коды. Например, Международным Консультативным Комитетом по телеграфии и телефонии (МККТТ) рекомендован для использования телеграфный код № 3 - семиразрядный код с постоянным весом, т.е. с числом единиц в каждой кодовой комбинации, равным 3 (W = 3).

Систематические коды образуют наиболее обширную группу (n, k)- разделимых кодов. Особенностью этих кодов является то, что проверочные (корректирующие) символы образуются с помощью линейных операций над информационными. Кроме того, любая разрешённая кодовая комбинация может быть получена в результате линейной операции над набором *к* линейно независимых кодовых комбинаций. В частности, суммирование по модулю 2 двух и более разрешённых комбинаций также дает разрешённую кодовую комбинацию. Поскольку теоретической основой получения таких комбинаций является математический аппарат линейной алгебры, то коды и называют линейными, а учи-

тывая, что проверочные символы формируются по определённой системе (правилам), блочные равномерные разделимые линейные коды получили название систематических. Использование аппарата линейной алгебры, в которой важное значение имеет понятие "группа", породило и другое название этих кодов - групповые.

Эти коды получили наибольшее применение в системах передачи дискретной информации.

Несистематические (нелинейные) коды указанными выше свойствами не обладают и применяются значительно реже в специальных случаях. Примером нелинейного кода является уже упоминавшийся неразделимый, равновесный код. Эти коды обычно используются в несимметричных каналах связи, в которых вероятность перехода $1 \rightarrow 0$ значительно больше вероятности перехода $0 \rightarrow 1$ или наоборот. В таких каналах очень маловероятно, чтобы в одном блоке были переходы обоих видов, и поэтому почти все ошибки приводят к изменению веса блока, и, следовательно, обнаруживаются.

Другим примером несистематического кода является код с контрольным суммированием - итеративный код. В этом коде проверочные разряды формируются в результате суммирования значений разрядов как в данной кодовой комбинации, так и одноимённых разрядов в ряде соседних с ней комбинаций, образующих совместный блок. Итеративные коды позволяют получить так называемые мощные коды, т.е. коды с длинными блоками и большим кодовым расстоянием при сравнительно простой процедуре декодирования. Итеративные коды могут строиться как комбинационные посредством произведения двух или более систематических кодов.

К комбинационным кодам можно отнести также антифединговые коды,, предназначенные для обнаружения и исправления ошибок в каналах с замираниями (федингом) сигналов. Для таких каналов с группированием ошибок применяют метод перемежения символов или декорреляции ошибок. Он заключается в том, что символы, входящие в одну кодовую комбинацию, передаются не непосредственно друг за другом, а перемежаются символами других кодовых комбинаций исходного систематического или любого другого кода. Если интервал между символами, входящими в одну кодовую комбинацию, сделать длиннее "памяти" (интервала корелляции) канала с замираниями, то в пределах длительности одной исходной кодовой комбинации группирования ошибок не будет. На приёме после обратной "расфасовки" в кодовых комбинациях можно производить декодирование с обнаружением и исправлением ошибок.

В систематических кодах различают два метода формирования проверочной группы символов: поэлементный и в целом.

Наиболее известны среди систематических кодов коды Хемминга, которые исторически были найдены раньше многих других кодов и сыграли большую роль в развитии теории корректирующих кодов. В этих кодах используется принцип проверки на чётность определённого ряда информационных символов. Проверочная группа из r символов формируется поэлементно по соответствующему алгоритму. Коды Хемминга, имеющие $d_{min} = 3$, позволяют исправить одну ошибку (раздел 1.4).

Расширенные коды Хемминга строятся в результате дополнения кодов с $d_{min} = 3$ общей проверкой каждой из кодовых комбинаций на чётность, т.е. ещё одним проверочным символом. Это позволяет увеличить минимальное кодовое расстояние до $d_{min} = 4$.

Циклические коды также относятся к классу линейных систематических кодов и обладают всеми их свойствами. Коды названы циклическими потому, что циклический сдвиг любой разрешённой кодовой комбинации также является разрешённой комбинацией. Теория построения циклических кодов базируется на разделах высшей алгебры, изучающей свойства двоичных многочленов. Особую роль в этой теории играют так называемые неприводимые многочлены, т.е. полиномы, которые не могут быть представлены в виде произведения многочленов низших степеней. В связи с этим циклические коды относят к разновидности полиномиальных кодов.

Среди циклических кодов особое место занимает класс кодов, предложенных Боузом и Рой-Чоудхури и независимо от них Хоквингемом [4]. Коды Боуза-Чоудхури-Хоквингема получили сокращённое наименование БЧХ - коды и отличаются специальным выбором порождающего (образующего) циклический код полинома, что приводит к простой процедуре декодирования.

В циклических кодах " r " проверочных символов, добавляемых к исходным " k " информационным, могут быть получены сразу, т.е. в целом, в результате умножения исходной подлежащей передаче кодовой комбинации Q(x) простого кода на одночлен x^r и добавлением к этому произведению остатка R(x), полученного в результате деления произведения на порождающий полином P(x).

Отметим, что коды Хемминга также можно получить по алгоритмам формирования циклических кодов [4].

Проблема помехоустойчивого кодирования представляет собой обширную область теоретических и прикладных исследований. Основными задачами при этом являются следующие: отыскание кодов, эффективно исправляющих ошибки требуемого вида; нахождение методов кодирования и декодирования и простых способов их реализации.

Наиболее разработаны эти задачи применительно к систематическим кодам. Такие коды успешно применяются в вычислительной технике, различных автоматизированных цифровых устройствах и цифровых системах передачи информации.

1.3. Основные характеристики корректирующих кодов.

В настоящее время наибольшее внимание с точки зрения технических приложений уделяется двоичным блочным корректирующим кодам. При использовании блочных кодов цифровая информация передаётся в виде отдельных кодовых комбинаций (блоков) равной длины. Кодирование и декодирование каждого блока осуществляется независимо друг от друга.

Почти все блочные коды относятся к разделимым кодам, кодовые комбинации которых состоят из двух частей: информационной и проверочной. При общем числе n символов в блоке число информационных символов равно k, а число проверочных символов

$$r = n - k. \qquad (3.2)$$

К основным характеристикам корректирующих кодов относятся:

- число разрешённых и запрещённых кодовых комбинаций;
- избыточность кода;
- минимальное кодовое расстояние;
- число обнаруживаемых или исправляемых ошибок;
- корректирующие возможности кодов.

Число разрешённых и запрещённых кодовых комбинаций.

Для блочных двоичных кодов, с числом символов в блоках равным n, общее число возможных кодовых комбинаций определяется значением

$$N_0 = 2^n \ . \qquad (3.3)$$

Число разрешённых кодовых комбинаций при наличии k информационных разрядов в первичном коде равно

$$N_k = 2^k \ . \qquad (3.4)$$

Очевидно, что число запрещённых комбинаций равно:

$$N_З = N_0 - N_k = 2^n - 2^k \ , \qquad (3.5)$$

а с учётом (3.2) отношение будет:

$$N_0 / N_k = 2^n / 2^k = 2^{n-k} = 2^r \ , \qquad (3.6)$$

где r -число избыточных (проверочных) разрядов в блочном коде.

Избыточность корректирующего кода.

Избыточностью корректирующего кода называют величину

$$\chi = \frac{r}{n} = \frac{n-k}{n} = 1 - \frac{k}{n} \ , \qquad (3.7)$$

откуда следует

$$B_k = \frac{k}{n} = 1 - \chi \ . \qquad (3.8)$$

Эта величина показывает, какую часть общего числа символов кодовой комбинации составляют информационные символы. В теории кодирования величину B_k называют относительной скоростью кода. Если производительность источника информации равна H символов в секунду, то скорость передачи после кодирования этой информации окажется равной

$$B = H \cdot \frac{k}{n} \ , \qquad (3.9)$$

поскольку в закодированной последовательности из каждых n символов только к символов являются информационными.

Если число ошибок, которые нужно обнаружить или исправить, значительно, то необходимо иметь код с большим числом проверочных символов. Чтобы при этом скорость передачи оставалась достаточно высокой, необходимо в каждом кодовом блоке одновременно увеличивать как общее число символов, так и число информационных символов. При этом длительность кодовых блоков будет существенно возрастать, что приведёт к задержке информации при передаче и приёме. Чем сложнее кодирование, тем длительнее временная задержка информации.

Минимальное кодовое расстояние - $d_{min.}$

Для того, чтобы можно было обнаружить и исправлять ошибки, разрешённая комбинация должна как можно больше отличаться от запрещённой. Если ошибки в канале связи действуют независимо, то вероятность преобразования одной кодовой комбинации в другую будет тем меньше, чем большим числом символов они различаются.

Если интерпретировать кодовые комбинации как точки в пространстве, то отличие выражается в близости этих точек, т.е. в расстоянии между ними.

Количество разрядов (символов), которыми отличаются две кодовые комбинации, можно принять за кодовое расстояние между ними. Для определения

этого расстояния нужно сложить две кодовые комбинации по модулю 2 и подсчитать число единиц в полученной сумме. Например, две кодовые комбинации $x_i = 01011$ и $x_j = 10010$ имеют расстояние $d(x_i,x_j)$, равное 3, так как

$$\begin{array}{l} x_i = 01011 \quad \rightarrow \quad W = 3 \\ \oplus \\ \underline{x_j = 10010 \quad \rightarrow \quad W = 2} \end{array}$$

$$x_i \oplus x_j = 11001 \quad \rightarrow \quad d(x_i,x_j) = 3 \ . \qquad (3.10)$$

(Здесь под операцией "⊕" понимается сложение по mod2).

Заметим, что кодовое расстояние $d(x_i, x_0)$ между комбинацией x_i и нулевой $x_0 = 00..0$ называют весом W комбинации x_i, т.е. вес x_i равен числу "1" в ней.

Расстояние между различными комбинациями некоторого конкретного кода могут существенно отличаться. Так, в частности, в безизбыточном первичном натуральном коде (n = k) это расстояние для различных комбинаций может изменяться от единицы до величины n, равной значности кода. Особую важность для характеристики корректирующих свойств кода имеет минимальное кодовое расстояние d_{min}, определяемое при попарном сравнении всех кодовых комбинаций, которое называют расстоянием Хемминга.

В безизбыточном коде все комбинации являются разрешёнными, и, следовательно, его минимальное кодовое расстояние равно единице - $d_{min} = 1$. Поэтому достаточно исказиться одному символу, чтобы вместо переданной комбинации была принята другая разрешённая комбинация. Чтобы код обладал корректирующими свойствами, необходимо ввести в него некоторую избыточность, которая обеспечивала бы минимальное расстояние между любыми двумя разрешёнными комбинациями не менее двух - $d_{min} \geq 2$.

Минимальное кодовое расстояние является важнейшей характеристикой помехоустойчивых кодов, указывающей на гарантируемое число обнаруживаемых или исправляемых заданным кодом ошибок.

Число обнаруживаемых или исправляемых ошибок.

При применении двоичных кодов учитывают только дискретные искажения, при которых единица переходит в нуль ($1 \rightarrow 0$) или нуль переходит в единицу ($0 \rightarrow 1$). Переход $1 \rightarrow 0$ или $0 \rightarrow 1$ только в одном элементе кодовой комбинации называют единичной ошибкой (единичным искажением). В общем случае под кратностью ошибки подразумевают число позиций кодовой комбинации, на которых под действием помехи одни символы оказались заменёнными на другие. Возможны двукратные (g = 2) и многократные (g > 2) искажения элементов в кодовой комбинации в пределах $0 \leq g \leq n$.

Минимальное кодовое расстояние является основным параметром, характеризующим корректирующие способности данного кода. Если код используется только для обнаружения ошибок кратностью g_0, то необходимо и достаточно, чтобы минимальное кодовое расстояние было равно

$$d_{min} \geq g_0 + 1 \ . \qquad (3.11)$$

В этом случае никакая комбинация из g_0 ошибок не может перевести одну разрешённую кодовую комбинацию в другую разрешённую. Таким образом, условие обнаружения всех ошибок кратностью g_0 можно записать в виде:

$$g_0 \leq d_{min} - 1 \ . \qquad (3.12)$$

Чтобы можно было исправить все ошибки кратностью $g_и$ и менее, необходимо иметь минимальное расстояние, удовлетворяющее условию:

$$d_{min} \geq 2 \cdot g_u + 1 . \qquad (3.13)$$

В этом случае любая кодовая комбинация с числом ошибок $g_и$ отличается от каждой разрешённой комбинации не менее чем в $g_и + 1$ позициях. Если условие (3.13) не выполнено, возможен случай, когда ошибки кратности g исказят переданную комбинацию так, что она станет ближе к одной из разрешённых комбинаций, чем к переданной или даже перейдёт в другую разрешённую комбинацию. В соответствии с этим, условие исправления всех ошибок кратностью не более $g_и$ можно записать в виде:

$$g_u \leq (d_{min} - 1) / 2 . \qquad (3.14)$$

Из (3.11) и (3.13) следует, что если код исправляет все ошибки кратностью $g_и$, то число ошибок, которые он может обнаружить, равно $g_0 = 2 \cdot g_и$. Следует отметить, что соотношения (3.11) и (3.13) устанавливают лишь гарантированное минимальное число обнаруживаемых или исправляемых ошибок при заданном d_{min} и не ограничивают возможность обнаружения ошибок большей кратности. Например, простейший код с проверкой на чётность с $d_{min} = 2$ позволяет обнаруживать не только одиночные ошибки, но и любое нечётное число ошибок в пределах $g_0 < n$.

Корректирующие возможности кодов.

Вопрос о минимально необходимой избыточности, при которой код обладает нужными корректирующими свойствами, является одним из важнейших в теории кодирования. Этот вопрос до сих пор не получил полного решения. В настоящее время получен лишь ряд верхних и нижних оценок (границ), которые устанавливают связь между максимально возможным минимальным расстоянием корректирующего кода и его избыточностью [4].

Так, граница Плоткина даёт верхнюю границу кодового расстояния d_{min} при заданном числе разрядов n в кодовой комбинации и числе информационных разрядов k, и для двоичных кодов:

$$d_{min} \leq \frac{n \cdot 2^{k-1}}{2^k - 1} \qquad (3.15)$$

или $$r \geq 2 \cdot (d_{min} - 1) - log_2\ d_{min} \qquad (3.16)$$

при $n \geq 2 \cdot d_{min} - 1$.

Верхняя граница Хемминга устанавливает максимально возможное число разрешённых кодовых комбинаций (2^k) любого помехоустойчивого кода при заданных значениях *n* и d_{min}:

$$2^k \leq 2^n \ / \ \sum_{i=0}^{\frac{d_{min}-1}{2}} C_n^i , \qquad (3.17)$$

где C^i_n - число сочетаний из n элементов по i элементам.
Отсюда можно получить выражение для оценки числа проверочных символов:

$$r \geq log_2 (\sum_{i=0}^{\frac{d_{min}-1}{2}} C_n^i) . \qquad (3.18)$$

Для значений (d_{min} / n) $\leq$ 0.3 разница между границей Хемминга и границей Плоткина сравнительно невелика.

Граница Варшамова-Гильберта для больших значений n определяет нижнюю границу для числа проверочных разрядов, необходимого для обеспечения заданного кодового расстояния:

$$r \geq log_2 (\sum_{i=0}^{d-2} C_{n-1}^{i}) . \qquad (3.19)$$

Отметим, что для некоторых частных случаев Хемминг получил простые соотношения, позволяющие определить необходимое число проверочных символов [5, 6] :

$r \geq log_2 (n + 1)$ для $d_{min} = 3$,

$r \geq log_2 (2 \cdot n)$ для $d_{min} = 4$.

Блочные коды с $d_{min} = 3$ и 4 в литературе обычно называют кодами Хемминга.

Все приведённые выше оценки дают представление о верхней границе числа d_{min} при фиксированных значениях n и k или оценку снизу числа проверочных символов r при заданных k и d_{min}.

Существующие методы построения избыточных кодов решают в основном задачу нахождения такого алгоритма кодирования и декодирования, который позволял бы наиболее просто построить и реализовать код с заданным значением d_{min}. Поэтому различные корректирующие коды при одинаковых d_{min} сравниваются по сложности кодирующего и декодирующего устройств. Этот критерий является в ряде случаев определяющим при выборе того или иного кода.

1.4. Корректирующие коды Хемминга.

Построение кодов Хемминга базируется на принципе проверки на чётность веса W (числа единичных символов) в информационной группе кодового блока.

Поясним идею проверки на чётность на примере простейшего корректирующего кода, который так и называется кодом с проверкой на чётность или кодом с проверкой по паритету (равенству).

В таком коде к кодовым комбинациям безизбыточного первичного двоичного k - разрядного кода добавляется один дополнительный разряд (символ проверки на чётность, называемый проверочным, или контрольным). Если число символов “1” исходной кодовой комбинации чётное, то в дополнительном разряде формируют контрольный символ 0, а если число символов “1” нечётное, то в дополнительном разряде формируют символ 1. В результате общее число символов “1” в любой передаваемой кодовой комбинации всегда будет чётным.

Таким образом, правило формирования проверочного символа сводится к следующему:

$$r_1 = i_1 \oplus i_2 \oplus ... \oplus i_k ,$$

где i - соответствующий информационный символ (0 или 1), k - общее их число а под операцией "⊕" здесь и далее понимается сложение по mod2. Очевидно, что добавление дополнительного разряда увеличивает общее число возможных комбинаций вдвое по сравнению с числом комбинаций исходного первичного кода, а условие чётности разделяет все комбинации на разрешённые и неразрешённые. Код с проверкой на чётность позволяет обнаруживать одиночную ошибку при приёме кодовой комбинации, так как такая ошибка нарушает условие чётности, переводя разрешённую комбинацию в запрещённую.

Критерием правильности принятой комбинации является равенство нулю результата S суммирования по mod 2 всех n символов кода, включая проверочный символ r_1. При наличии одиночной ошибки S принимает значение 1:

$$S = \underbrace{r_1 \oplus i_1 \oplus i_2 \oplus \ldots \oplus i_k}_{n} = \begin{cases} 0 & - \text{ ошибки нет} \\ 1 & - \text{ однократная ошибка.} \end{cases}$$

Этот код является (k +1, k) - кодом, или (n, n -1) - кодом. Минимальное расстояние кода равно двум ($d_{min} = 2$), и, следовательно, никакие ошибки не могут быть исправлены. Простой код с проверкой на чётность может использоваться только для обнаружения (но не исправления) однократных ошибок.

Увеличивая число дополнительных проверочных разрядов и формируя по определённым правилам проверочные символы r, равные 0 или 1, можно усилить корректирующие свойства кода так, чтобы он позволял не только обнаруживать, но и исправлять ошибки. На этом и основано построение кодов Хемминга.

Коды Хемминга. Рассмотрим эти коды, позволяющие исправлять одиночную ошибку, с помощью непосредственного описания. Для каждого числа проверочных символов r = 3,4,5**...** существует классический код Хемминга с маркировкой

$$(n,k) = (2^r - 1,\ 2^r - 1 - r), \qquad (3.20)$$

т.е. - (7,4), (15,11), (31,26) **...**

При других значениях числа информационных символов k получаются так называемые усечённые (укороченные) коды Хемминга. Так, для международного телеграфного кода МТК-2 , имеющего 5 информационных символов, потребуется использование корректирующего кода (9,5), являющегося усечённым от классического кода Хемминга (15,11), так как число символов в этом коде уменьшается (укорачивается) на 6. Для примера рассмотрим классический код Хемминга (7,4), который можно сформировать и описать с помощью кодера, представленного на рис.3.2. В простейшем варианте при заданных четырёх (k=4) информационных символах (i_1, i_2, i_3, i_4) будем полагать, что они сгруппированы в начале кодового слова, хотя это и не обязательно. Дополним эти информационные символы тремя проверочными символами (r = 3), задавая их следующими равенствами проверки на чётность, которые определяются соответствующими алгоритмами [3,5]:

$$r_1 = i_1 \oplus i_2 \oplus i_3;$$
$$r_2 = i_2 \oplus i_3 \oplus i_4;$$
$$r_3 = i_1 \oplus i_2 \oplus i_4,$$

где знак $\oplus$ означает сложение по модулю 2.

В соответствии с этим алгоритмом определения значений проверочных символов r_i ниже выписаны все возможные 16 кодовых слов (7,4) - кода Хемминга.

На рис. 3.3 приведена схема декодера для (7,4) - кода Хемминга, на вход которого поступает кодовое слово

$$V = (i_1', i_2', i_3', i_4', r_1', r_2', r_3')$$

Апостроф означает, что любой символ слова может быть искажён помехой в канале передачи.

В декодере в режиме исправления ошибок строится последовательность:

$$s_1 = r_1' \oplus i_1' \oplus i_2' \oplus i_3';$$
$$s_2 = r_2' \oplus i_2' \oplus i_3' \oplus i_4';$$
$$s_3 = r_3' \oplus i_1' \oplus i_2' \oplus i_4'.$$

Трёхсимвольная последовательность (s_1, s_2, s_3) называется синдромом. Термин "синдром" используется и в медицине, где он обозначает сочетание признаков, характерных для определённого заболевания. В данном случае синдром S = (s_1, s_2, s_3) представляет собой сочетание результатов проверки на чётность соответствующих символов кодовой группы и характеризует определённую конфигурацию ошибок (шумовой вектор).

Кодовые слова (7,4) - кода Хемминга.

к = 4				r = 3		
i_1	i_2	i_3	i_4	r_1	r_2	r_3
0	0	0	0	0	0	0
0	0	0	1	0	1	1
0	0	1	0	1	1	0
0	0	1	1	1	0	1
0	1	0	0	1	1	1
0	1	0	1	1	0	0
0	1	1	0	0	0	1
0	1	1	1	0	1	0
1	0	0	0	1	0	1
1	0	0	1	1	1	0
1	0	1	0	0	1	1
1	0	1	1	0	0	0
1	1	0	0	0	1	0
1	1	0	1	0	0	1
1	1	1	0	1	0	0
1	1	1	0	1	1	1

Число возможных синдромов определяется выражением

$$S = 2^r. \qquad (3.21)$$

При числе проверочных символов r = 3 имеется восемь возможных синдромов ($2^3 = 8$). Нулевой синдром (000) указывает на то, что ошибки при приёме отсутствуют или не обнаружены. Всякому ненулевому синдрому соответствует определённая конфигурация ошибок, которая и исправляется. Классические коды Хемминга (3.20) имеют число синдромов, точно равное их необходимому числу, позволяют исправить все однократные ошибки в любом информативном и проверочном символах и включают один нулевой синдром. Такие коды называются плотноупакованными.

Усечённые коды являются неплотноупакованными, так как число синдромов у них превышает необходимое. Так, в коде (9,5) при четырёх проверочных символах число синдромов будет равно 2^4 =16, в то время как необходимо всего 10. Лишние 6 синдромов свидетельствуют о неполной упаковке кода (9,5).

Для рассматриваемого кода (7,4) в таблице 1 представлены ненулевые синдромы и соответствующие конфигурации ошибок.

Таблица 1

Синдром	001	010	011	100	101	110	111
Конфигурация ошибок	0000001	0000010	0001000	0000100	1000000	0010000	0100000
Ошибка в символе	r_3	r_2	i_4	r_1	i_1	i_3	i_2

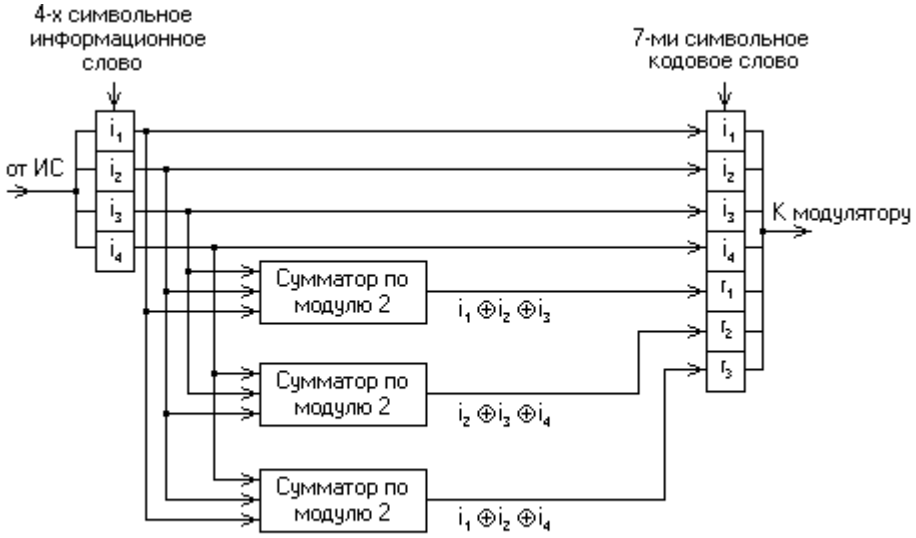

Рис.3.2. Кодер для простого (7,4) - кода Хемминга

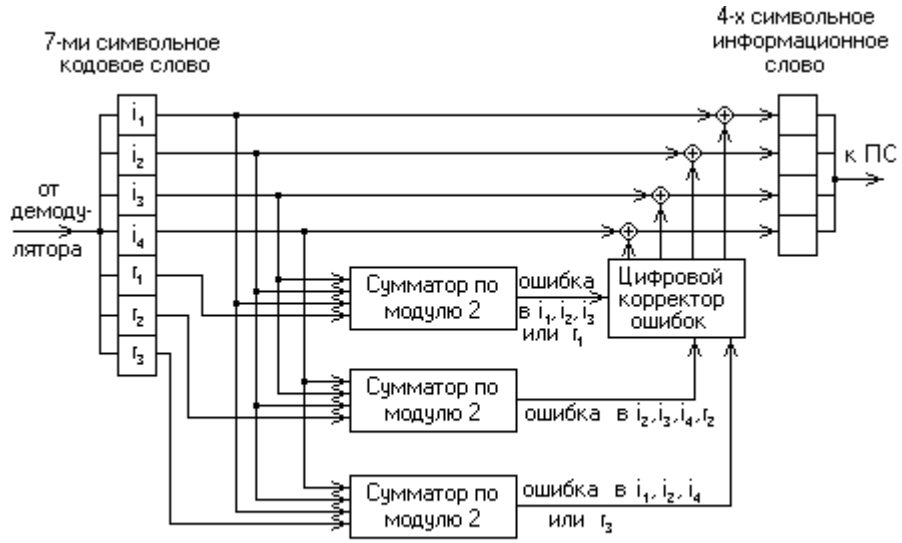

Рис.3.3. Декодер для простого (7,4) - кода Хемминга

Таким образом, код (7,4) позволяет исправить все одиночные ошибки. Простая проверка показывает, что каждая из ошибок имеет свой единственный синдром. При этом возможно создание такого цифрового корректора ошибок (дешифратора синдрома), который по соответствующему синдрому исправляет соответствующий символ в принятой кодовой группе. После внесения исправления проверочные символы r_i можно на выход декодера (рис.3.3) не выводить. Две или более ошибки превышают возможности корректирующего кода Хемминга, и декодер будет ошибаться. Это означает, что он будет вносить неправильные исправления и выдавать искажённые информационные символы.

Идея построения подобного корректирующего кода, естественно, не меняется при перестановке позиций символов в кодовых словах. Все такие варианты также называются (7,4) - кодами Хемминга.

2. ПОРЯДОК ВЫПОЛНЕНИЯ ЛАБОРАТОРНОЙ РАБОТЫ

В лабораторной работе исследуется усечённый код Хемминга (9,5). Длина кодового слова n = 9 разрядов, информационная часть содержит k = 5 разрядов, количество проверочных разрядов r = 4. Соответствующие алгоритмы проверки на чётность рассматриваемого кода имеют вид:

$$\begin{aligned} \mathbf{r_1} &= \mathbf{i_2} \oplus \mathbf{i_3}, \\ \mathbf{r_2} &= \mathbf{i_1} \oplus \mathbf{i_3} \oplus \mathbf{i_4}, \\ \mathbf{r_3} &= \mathbf{i_2} \oplus \mathbf{i_4} \oplus \mathbf{i_5}, \\ \mathbf{r_4} &= \mathbf{i_1} \oplus \mathbf{i_2} \oplus \mathbf{i_5}, \end{aligned} \qquad (3.22)$$

а алгоритм вычисления символов синдрома:

$$\begin{aligned} \mathbf{S_1} &= \mathbf{i_2} \oplus \mathbf{i_3} \oplus \mathbf{r_1}, \\ \mathbf{S_2} &= \mathbf{i_1} \oplus \mathbf{i_3} \oplus \mathbf{i_4} \oplus \mathbf{r_2}, \\ \mathbf{S_3} &= \mathbf{i_2} \oplus \mathbf{i_4} \oplus \mathbf{i_5} \oplus \mathbf{r_3}, \\ \mathbf{S_4} &= \mathbf{i_1} \oplus \mathbf{i_2} \oplus \mathbf{i_5} \oplus \mathbf{r_4}, \end{aligned} \qquad (3.23)$$

Данный код имеет минимальное кодовое расстояние d_{min}= 3 , следовательно, теоретически он исправляет все однократные ошибки. Все одно– и двухкратные ошибки обнаруживаются.

Для выполнения лабораторной работы необходимо выбрать соответствующую позицию в основном меню и нажать клавишу < ENTER >, которую в дальнейшем необходимо нажимать при переходе от пункта к пункту.

1.) Начинать выполнение лабораторной работы следует при появлении в нижней строке экрана указания:

"Введите кодируемые символы>".

2.) В ответ на это указание необходимо ввести от одного до пяти алфавитно-цифровых символов, допустимых для кода МТК-2. Число введённых символов должно быть равно числу членов бригады. Они автоматически закодируются безизбыточным кодом МТК-2, кодовые слова которого печатаются на экране. Нажатие клавиши <ESC> означает отказ от выполнения работы.

3.) Кодовые слова безизбыточного кода МТК-2 необходимо закодировать корректирующим кодом (9,5), руководствуясь алгоритмом (3.22), приведённым в [4]. Информационный вектор i, очевидно, представляет собой кодовое слово кода МТК-2. Полученные векторы *x* кода (9,5) (кодовые слова) необходимо ввести, набрав их на клавиатуре.

4.) В кодовые слова *x* кода (9,5) автоматически вносятся однократные ошибки, в результате чего формируются некоторые векторы *y*, не совпадающие с соответствующими векторами *x*.

Необходимо, пользуясь алгоритмом (3.23), определить синдром S и ввести его символы с клавиатуры. В соответствии с вычисленным вектором S в таблице декодирования автоматически отыскиваются шумовые векторы z и отображаются на экране. Необходимо проанализировать их и убедиться в том, что ненулевая позиция в этих векторах соответствует искажённым разрядам в векторах *y*, т.е. соотношение $x = z \oplus y$ справедливо.

5.) Далее, в кодовые слова *x* кода (9,5) автоматически вносятся двухкратные ошибки, т.е. вновь формируются векторы *y*, не равные соответствующим векторам *x*. Необходимо повторить действия предыдущего пункта. При анализе шумовых векторов z необходимо учитывать, что таблица декодирования исследуемого в лабораторной работе кода содержит только синдромы, соответствующие однократным ошибкам z_i. Поэтому возможны две ситуации:

а) вычисленному синдрому S_i в таблице не соответствует никакой шумовой вектор z_i. В этом случае на экране будут напечатаны символы (*******).

б) вычисленному синдрому S_i в таблице соответствует некоторый вектор z_i. В этом случае необходимо убедиться в том, что он неправильно отображает реальную конфигурацию ошибок.

Рассмотрим пример, поясняющий ход выполняемых операций. Пусть выбрана и введена буква "Ф", ей соответствует кодовое слово кода МТК-2 **i** = 10110. Таким образом, на экране отобразится следующая информация:

Символ	Код МТК-2
Ф	10110

В результате применения алгоритмов (3.22) получим вектор *x* корректирующего кода (9,5), который и необходимо ввести.

Таким образом, получим вектор x = (101101111), и изображение на экране примет вид:

Символ	Код МТК-2	Код (9,5)
Ф	10110	101101111

Далее, в вектор *x* вносится однократная ошибка, т.е получается вектор *y*, не совпадающий с *x*, например: y = (101001111), и на экране будет следующее изображение:

Символ	Код МТК-2	Код (9,5)	Искажения
Ф	10110	101101111	101001111

Декодируем вектор *y*, пользуясь алгоритмом (3.23), т.е. определяем синдром S, который необходимо ввести. Вычисленный синдром S = 0110.
Полученный синдром вводится в приведённую выше таблицу, которая примет вид:

Символ	Код МТК-2	Код (9,5)	Искажения	Синдром
Ф	10110	101101111	101001111	0110

Вычисленному синдрому соответствует шумовой вектор Z = (000100000), т.е. ошибка произошла в шестом разряде (при счёте разрядов справа - налево) исходного вектора *x*. На экране появится следующее изображение:

Символ|Код МТК-2 | Код (9,5) |Искажения |Синдром |Шумовой вектор
Ф | 10110 |101101111 |101001111 | 0110 | 000100000

Далее, в вектор *x* вносится двухкратная ошибка, т.е. опять получается вектор y, не совпадающий с *x*, например: y = (100001111). На экране будет предъявлена следующая таблица:

Символ | Код МТК-2 | Код (9,5) | Искажения |

Ф | 10110 |101101111 |100001111 |

Вновь декодируем вектор *y*, пользуясь алгоритмом (3.23), т.е. определяем синдром S, который небходимо ввести.
Полученный синдром:

Символ | Код МТК-2 | Код (9,5) | Искажения | Синдром

Ф | 10110 |101101111 | 100001111 | 1010

Таким образом, в результате декодирования получен ненулевой синдром. Однако в таблице декодирования ему может не соответствовать никакой шумовой вектор, поэтому изображение на экране примет вид:

Символ | Код МТК-2 | Код (9,5) | Искажения | Синдром |Шумовой вектор
Ф | 10110 | 101101111| 100001111 | 1010 | ********

Код (9,5) с $d_{min} = 3$ не справляется с исправлением двукратной ошибки.

На этом выполнение лабораторной работы заканчивается. Представление отчёта не требуется. Факт выполнения бригадой лабораторной работы, включая количество попыток по пунктам фиксируется в специальном файле на диске.

3. КОНТРОЛЬНЫЕ ВОПРОСЫ И ЗАДАЧИ

1. Перечислить и пояснить методы повышения качества приёма передаваемой информации.
2. Какие способы повышения избыточности находят применение в настоящее время?
3. Рассмотрите преимущества и недостатки метода многократного повторения.
4. Какие коды называются равнодоступными?
5. В чём заключается сущность помехоустойчивого кодирования?
6. Какие задачи решают помехоустойчивые коды?
7. Какой код называется кодом с проверкой по паритету?
8. В чём заключается сложность выбора корректирующего кода для реальных каналов связи?
9. Какие коды называются блочными?
10. Какие коды называются непрерывными?
11. Приведите примеры равномерных и неравномерных кодов.
12. Какова особенность неразделимых кодов? Приведите пример неразделимого кода.
13. Какие коды называются систематическими? Каковы их основные свойства?
14. Перечислите основные классы систематических кодов.
15. Перечислите основные характеристики корректирующих кодов.
16. Что такое минимальное кодовое расстояние?
17. Укажите количественную связь между минимальным кодовым расстоянием и корректирующей способностью кода.

18. Что определяет верхние границы для кодового расстояния?
19. Что определяет нижние границы для кодового расстояния?
20. Определите границы Плоткина и Хемминга для кодов (6,3) и (7,4), имеющих $d_{min} = 3$.
21. Определите границу Варшамова-Гильберта для этих же кодов.
22. Дайте определение синдрома ошибок.
23. Сформируйте алгоритм декодирования систематических кодов, основанный на таблицах декодирования.
24. Закодируйте целые числа от 5 до 8 кодом Хемминга (7,4), пользуясь уравнениями для проверок.
25. Закодируйте целые числа от 9 до 16 кодом Хемминга (7,4), пользуясь порождающей матрицей.
26. Дайте определение шумового вектора.
27. Определите шумовой вектор для конфигурации из одной ошибки в пятой позиции кода (9,5).
28. Определите шумовой вектор для конфигурации из двух ошибок в пятой и седьмой позициях кода (9,5).
29. Чему равны скорость и избыточность кода (9,5)?
30. Сколько всего синдромов ошибок может содержать таблица декодирования кода (9,5)?

Библиографический список

1. Г.И. Никитин. Первичные коды: Метод. указ., ЛИАП, Л., 1984, 28 с.
2. Г.И. Никитин. Эффективные коды: Метод. указ., ЛИАП, Л., 1987, 28 с.
3. А.К. Журавлев, Г.И. Никитин. Радиотехнические системы передачи информации: Учеб.пособие /ЛИАП, Л., 1984, 86 с.
4. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки: Пер. с англ. М.: Мир, 1976, 600 с.
5. Кларк Д., Кейн Д. Кодирование с исправлением ошибок в системах цифровой связи: Пер. с англ. М.: Радио и Связь,1987, 300 с.
6. Пенин П.Е.,Филиппов Л.Н. Радиотехнические системы передачи информации. М.: Радио и Связь, 1984, 256 с.
7. Блейхут Р. Теория и практика кодов, контролирующих ошибки. Пер. с англ. М.: Мир, 1986, 576 с.

Содержание

1. Методические указания к лабораторной работе 1
1.1 Принципы помехоустойчивого кодирования 1
1.2 Классификация помехоустойчивых корректирующих кодов 3
1.3 Основные характеристики корректирующих кодов 6
1.4 Корректирующие коды Хемминга 10
2. Порядок выполнения лабораторной работы 14
3. Контрольные вопросы и задачи 16
Библиографический список 17

Графика и компьютерная вёрстка
Романова М.Я. 2002 г.