Министерство образования и науки Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г.ЧЕРНЫШЕВСКОГО»

Кафедра дискретной математики
и информационных технологий

Полиномиальное кодирование

АВТОРЕФЕРАТ БАКАЛАВРСКОЙ (МАГИСТЕРСКОЙ, ДИПЛОМНОЙ) РАБОТЫ

Студентки 4 курса 421 группы
направления 09.03.01 «Информатика и вычислительная техника»
факультета компьютерных наук и информационных технологий
Кирдиной Ульяны Сергеевны

Научный руководитель
к. ф.-м.н., доцент каф ДМиИТ _____ И.П. Мангушева
дата, подпись

Заведующий кафедрой
к. ф.-м.н., доцент _____ Л. Б. Тяпаев
дата, подпись

Саратов 2016 год

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Целью выпускной квалификационной работы является рассмотрение одного из методов помехоустойчивого кодирования, а именно, метода полиномиального кодирования и декодирования двоичных сообщений. Для достижения цели, поставленной в дипломной работе, необходимо было решить следующие задачи.

1 Изучить теоретический материал, касающийся метода полиномиального кодирования и его использования для обнаружения и корректировки искажений при передаче по каналу связи с помехами.

2 Продемонстрировать работу метода на примерах.

3 Разработать и реализовать алгоритмы построения кода двоичного сообщения, обнаружения ошибки в коде на выходе канала связи и корректировки кода для случая, когда это возможно.

4 Описать область применения полиномиальных кодов;

5 Рассмотреть задачу нахождения порождающих многочленов;

6 Реализовать метод полиномиального кодирования и декодирования двоичных сообщений.

Структурно работа состоит из введения, теоретической части, практической части, заключения, списка использованных источников и трех приложений.

1 Основные понятия

Группой называется система [G, ·, 1, $^{-1}$] со следующими свойствами:

1. x*(y*z) = (x*y)*z для всех x, y, z ∈ G;

2. 1*x = x*1 = x для всех x ∈ G;

3. $x*x^{-1} = x^{-1}*x = 1$ для всех x ∈ G

Кольцом называется алгебраическая система R= [R, +, *] с двумя бинарными операциями + и *, которые удовлетворяют следующим условиям [1].

1. + определят на R структуру абелевой группы: $a*b=b*a$ для любых $a,b\in G$;

2. * определяет на R структуру моноида;

3.справедливы законы дистрибутивности: $a(b+c)=ab+ac,\quad (a+b)c=ac+bc$ для любых $a,b,c\in R$.

Кольцо называется коммутативным, если a*b=b*a для всех a, b ∈ R.

Моноидом называется полугруппа с нейтральным элементом e, что $ex=xe=x$

Полем называется коммутативное кольцо, содержащее не менее двух элементов, в котором все ненулевые элементы образуют группу по умножению. К этому классу принадлежат поля целых чисел Z_n по модулю простого числа n. Для построения кодов используются поля степени двойки Z_2.

Двоичным (m, n) - кодом называется пара, состоящая из схемы кодирования E : $2^m \to 2^n$ и схемы декодирования D: $2^n \to 2^m$, где 2^n - множество всех двоичных последовательностей длины n.

Систематический код - это код, в котором каждой кодовой последовательности однозначно сопоставляется входная последовательность [2].

2 Помехоустойчивое кодирование

При передаче информации по каналам связи возможны ошибки вследствие помех и искажений сигналов. Для обнаружения и исправления возникающих ошибок используются помехоустойчивые коды.

Помехоустойчивость - способность системы осуществлять прием информации в условиях наличия помех в линии связи и искажений во внутри аппаратных трактов. Помехоустойчивость обеспечивает надежность и достоверность передаваемой информации (данных).

Помехоустойчивое кодирование – один из эффективных методов повышения достоверности и надежности передачи данных. Этот метод позволяет за счет внесения дополнительной избыточности в кодовые комбинации передаваемых сообщений обеспечить возможность обнаружения и исправления одиночных, кратных и групповых ошибок [8].

2.1 Блочные коды

Блочный код заменяет каждый блок из m символов некоторым более длинным блоком из n символов, который после передачи подлежит декодированию. Из соображений простоты и надежности большинство систем связи конструируется для передачи двоичных последовательностей. Блочный (m, n) – код определяется двумя функциями: $E: 2^m \rightarrow 2^n$, $D: 2^n \rightarrow 2^m$, $m \leq n$.

Одним из ключевых понятий теории кодирования принадлежит понятие расстояния между двоичными словами. Расстояние d(a, b) между двумя словами $a = (a_1,\ldots,a_n)$ и $b=(b_1,\ldots,b_n)$ равно числу позиций, в которых $a_i \neq b_i$. Если слова отличаются в точно одной позиции, то расстояние равно единице.

Весом w(a) слова $a=(a_1,..,a_n)$ называется число единиц среди его координат. Тогда **расстоянием** d(a, b) между двоичными словами одинаковой длины называется вес их суммы, то есть d(a, b) = w(a+b) [2].

Теорема 1. Для того чтобы код давал возможность обнаруживать все ошибки в $\leq$ k позициях, необходимо и достаточно, чтобы наименьшее расстояние между двумя кодовыми словами было k+1.

Теорема 2. Для того чтобы код давал возможность исправлять все ошибки в $\leq$ k позициях, необходимо и достаточно, чтобы наименьшее расстояние между двумя кодовыми словами было 2k+1.

2.2 Групповые коды

Блочный код называется групповым, если его кодовые слова образуют группу. Иногда групповые коды являются блоковыми кодами, имеющими практическое значение. Групповые коды также называют линейными или кодами с обобщенными проверками на четность [2].

Теорема 3. Если код является групповым, то наименьшее расстояние между двумя кодовыми словами равно наименьшему весу ненулевого кодового слова [2].

3 Полиномиальное кодирование

Полиномом степени ≤ m от неизвестной x над коммутативным кольцом R называется выражение вида:

$$a_0 + a_1 x + \ldots + a_m x^m = \sum_{k=0}^{m} a_k x^k, \quad a_k \in R$$

Элементы a_k называются коэффициентами полинома, они могут быть нулевыми.

Полином иногда обозначается символически a(x). При таком обозначении имеется в виду, что полином рассматривается как функция из R в R.

Вес многочлена - это количество ненулевых слагаемых в многочлене.

Два стандартных полинома называются равными, если у них одинаковая каноническая форма.

Полиномиальные коды – это специальный класс групповых кодов. При кодировании сообщения отождествляются с многочленами, а само кодирование заключается в умножении на фиксированный многочлен [4]. Для блочных (m, n) – кодов в каждом блоке имеется k = n – m контрольных символов. Пусть a_0, …. , a_{m-1} – символы сообщения a. Будем рассматривать двоичный алфавит, его нужно отождествить с Z_2. Тогда слова сообщения можно отождествить с многочленами степени ≤ m – 1 над Z_2:

$$a \leftrightarrow a_0 + a_1 x + \ldots + a_{m-1} x^{m-1}. \qquad (5)$$

Пусть F – некоторое конечное поле. Фиксируем многочлен степени k:

$$g(x) = g_0 + g_1 x + \ldots + g_k x^k \in F[x],\ g_0 \neq 0,\ g_k \neq 0. \qquad (6)$$

Если $g_0=0$, то все кодовые слова будут начинаться с нуля, и первый символ не будет нести никакой информации, если же $g_k=0$, то последний символ не будет нести информации.

Полиномиальный код с кодирующим многочленом g (x) кодирует слово сообщения **a** вида (6) следующим многочленом:

$$b(x) = b_0 + b_1 x + \ldots + b_{n-1} x^{n-1} = a(x)\, g(x)\ [6].$$

Теорема 4. Минимальное расстояние между двумя кодовыми словами полиномиального кода с кодирующим многочленом g(x) совпадает с минимумом весов многочленов a(x)g(x).

Теорема 5. Если многочлен с коэффициентами в Z_2 делится на 1+x, то он имеет четное число ненулевых коэффициентов.

Декодирование при полиномиальном кодировании осуществляется путем деления кодового полинома b(x) на порождающий полином g(x). Если остаток от деления на g(x) равен 0, то значит, что ошибки отсутствуют в процессе передачи кодовой комбинации. Частное от деления является искомым полиномом a(x).

3.1 Возможности полиномиальных кодов

Теорема 7. Если g(x) не является делителем ни одного многочлена вида x^k-1 при k<n, то для (m, n) – кода, порожденного g(x), минимальное расстояние между словами не меньше трех [1].

Доказательство. Множество кодовых слов имеет вид a(x) g(x), deg a(x)<m. Так как код является групповым, то минимальное расстояние между кодовыми словами совпадает с минимальным весом кодового слова. Если существует кодовое слово веса 2, то g(x) делит многочлен вида $e(x)= x^i+x^j= x^i(1+x^{j-1})$. Так как $g_0=1$, g(x) делит $1+ x^{j-1}$, поэтому не существует кодовых слов весом 2. Также не может существовать кодовое слово веса 1, иначе g(x) должен был бы делить x^i.

Многочлен g(x) степени k над Z_2 называется **примитивным**, если $g(x) \mid (x^m - 1)$ для $m = 2^k – 1$, но ни для какого меньшего значения m.

Примитивные многочлены строятся путем перебора. Некоторые примитивные многочлены приведены в таблице 1.

Таблица 1 - Примитивные многочлены

m		m	
3	$1+X+X^3$	14	$1+X+X^6+X^{10}+X^{14}$
4	$1+X+X^4$	15	$1+X+X^{15}$
5	$1+X^2+X^5$	16	$1+X+X^3+X^{12}+X^{16}$
6	$1+X+X^6$	17	$1+X^3+X^{17}$
7	$1+X^3+X^7$	18	$1+X^7+X^{18}$
8	$1+X^2+X^3+X^4+X^8$	19	$1+X+X^2+X^5+X^{19}$
9	$1+X^4+X^9$	20	$1+X^3+X^{20}$
10	$1+X^3+X^{10}$	21	$1+X^2+X^{21}$
11	$1+X^2+X^{11}$	22	$1+X+X^{22}$
12	$1+X+X^4+X^6+X^{12}$	23	$1+X^5+X^{23}$
13	$1+X+X^3+X^4+X^{13}$	24	$1+X+X^2+X^7+X^{24}$

Теорема 6. Рассмотрим полиномиальный (m, n)- код, порожденный многочленом g(x). «Строка ошибок» $e=e_0e_1\ldots e_{n-1}$ останется необнаруженной в том и только том случае, если соответствующий многочлен ошибок делится на g(x).

Доказательство. Строка ошибок остается необнаруженной только в том случае, если она является кодовым словом, это доказывает требуемое.

Обнаружение ошибок производится с помощью алгоритма деления с остатком: нужно поделить многочлен, отвечающий принятому слову, на g(x); если остаток степени <deg g оказывается ненулевым, то при передаче произошло искажение.

Лемма (алгоритм Евклида). Пусть $a(x), b(x)$ - многочлены в $F[x], b(x)\neq 0$. Тогда существует неполное частное $q(x)\in F[x]$ и остаток $r(x)\in F[x]$ со свойствами: либо $r(x)=0$, либо $\deg r(x)<\deg b(x)$ и

$$a(x)=b(x)\,q(x)+r(x),\ \deg r(x)<\deg b(x)$$

Частное *q(x)* и остаток *r(x)* можно вычислить с помощью следующего алгоритма.

Положим $a(x)=\sum_{k=1}^{m}a_k x^k$ и $b(x)=\sum_{k=0}^{n}b_k x^k$, где $b_n\neq 0$. Рассмотрим два случая.

Случай 1. Если $m<n$, *полагаем* $q(x)=0$ и $r(x)=a(x)$.

Случай 2. Если $m \geq n,$ положим

$$a_1(x) = a(x) - b_n^{-1} a_m x^{m-n} b(x) = a(x) - q_1(x) b(x).$$

Степень этого многочлена не больше $m-1$, ибо старшие коэффициенты у $a(x)$ и $q_1(x)b(x)$ совпадают и равны $b_n^{-1} a_m b_n = a_m$. После не более чем $m-n+1$ таких шагов степень остатка окажется меньше m.

Экспонентой многочлена g называется наименьшее положительное целое число e, для которого $g(x) \mid (x^e - 1)$. В частности, $g \in Z_2[x]$ примитивен, если его степень равна k, а экспонента $e = 2^k - 1$.

Теорема 7. Пусть кодирующий многочлен полиномиального (m, n) – кода имеет вид g(x) = (1 + x)*h(x), где экспонента емногочлена h(x) больше n. Тогда можно обнаружить любую комбинацию из двух простых или двойных ошибок.

При простом умножении на *g(x)* входные символы перемешиваются и заменяются их линейными комбинациями, поэтому на самом деле используется другая процедура кодирования. А именно, многочлен a(x) кодируется многочленом $b(x)=x^{n-m}a(x) - r(x)=q(x)g(x)$, где *r(x)*- остаток от деления $x^{n-m}\ a(x)$ на *g(x)*, а *q(x)* - неполное частное.

При таком методе кодирования кодовые слова состоят из всех многочленов, делящихся на $g(x)$. Вектор коэффициентов $b_{n-k},..., b_n$ совпадает с входным вектором $a_0,.., a_{m-1}$.

3.2 Понятие о кодах Боуза - Чоудхури - Хоккенгема

В 1960 году независимо Боуз, Чоудхури и Хоккенгем открыли один класс эффективных полиномиальных кодов с исправлением многократных ошибок. Эти коды получили название кодов Боуза-Чоудхури-Хоккенгема или БЧХ-кодов. В таких кодах число контрольных символов зависит от числа ошибок, которое нужно обнаружить или исправить.

Алфавит БЧХ - кода отождествляется с некоторым конечным полем GF (q). Из-за использования двоичных устройств q обычно является степенью

двойки. Кодирующий многочлен g(x) имеет коэффициенты в этом поле, а кодовые слова состоят из всех кратных многочлена g(x) [1].

Можно построить БЧХ - код, у которого минимальное расстояние между словами $\geq d$, т.е. для любого наперед заданного d.

Кодирующий многочлен g(x) для БЧХ-кода, длина кодовых слов которого n, строится так: находится примитивный многочлен минимальной степени q такой, что $n \leq 2^q - 1$ или $q \geq \log_2(n+1)$. Пусть α — корень этого многочлена, тогда рассмотрим кодирующий многочлен g(x) = НОК $(m_1(x),..., m_{d-1}(x))$, где $m_1(x),..., m_{d-1}(x)$ - многочлены минимальной степени, имеющие корни соответственно $\alpha, \alpha^2,..., \alpha^{d-1}$.

Построенный кодирующий многочлен производит код с минимальным расстоянием между кодовыми словами, не меньшим d, и длиной кодовых слов n [4].

ЗАКЛЮЧЕНИЕ

В ходе работы были решены следующие задачи:

1. Изучен теоретический материал, касающийся метода полиномиального кодирования и его использования для обнаружения и корректировки искажений при передаче по каналу связи с помехами.
2. Продемонстрирована работа метода на примерах.
3. Разработаны алгоритмы построения кода двоичного сообщения, обнаружения ошибки в коде на выходе канала связи и корректировки кода для случая, когда это возможно.
4. Реализован метод полиномиального кодирования и декодирования двоичных сообщений.

В ходе работы сделан вывод, что полиномиальные коды могут исправлять однократные, двойные и многократные ошибки.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Биркгоф Г., Барти Т. Современная прикладная алгебра, Мир, 1976

2 Дж. Кларк, мл.Дж.Кейн. Кодирование с исправлением ошибок в системах цифровой связи, 1987

3 Мангушева И.П. Курс лекций по дискретной математике. Часть I. Элементы теории множеств и отношений. Функции алгебры логики. Функции к-значной логики. : учеб. пособие. Саратов: Издат. центр «Наука».

4 Лидовский В. В. Теория информации, Москва, 2004

5 Планета информатики. Кодирование информации. [Электронный ресурс]:[сайт].
URL: http://www.inf1.info/book/export/html/202
Дата обращения 18.05.16

6 НОУ ИНТУИТ. Полиномиальные коды. [Электронный ресурс]:[сайт].
URL: http://www.intuit.ru/studies/courses/2256/140/lecture/3920?page=3
Дата обращения 20.05.16

7 Прикладная математика. Алгоритм Евклида. [Электронный ресурс]:[сайт].
URL : http://www.pm298.ru/mnog2.php
Дата обращения 10.05.16

8 Золотарёв В. В., Овечкин Г.В. Помехоустойчивое кодирование. Горячая линия - Телеком, 2004