БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

кафедра РЭС

реферат на тему:

**«Циклические коды. Коды БЧХ»**

МИНСК, 2009

**Циклические коды**

Циклическим кодом называется линейный блоковый (n,k)-код, который характеризуется свойством цикличности, т.е. сдвиг влево на один шаг любого разрешенного кодового слова дает также разрешенное кодовое слово, принадлежащее этому же коду и у которого, множество кодовых слов представляется совокупностью многочленов степени (n-1) и менее, делящихся на некоторый многочлен g(x) степени r = n-k, являющийся сомножителем двучлена xn+1.

Многочлен g(x) называется порождающим.

Как следует из определения, в циклическом коде кодовые слова представляются в виде многочленов
где n - длина кода;

- коэффициенты из поля GF(q).

Если код построен над полем GF(2), то коэффициенты принимают значения 0 или 1 и код называется двоичным.
Пример. Если кодовое слово циклического кода
 то соответствующий ему многочлен

Например, если код построен над полем GF(q)=GF(23), которое является расширением GF(2) по модулю неприводимого многочлена f(z)=z3+z+1, а элементы этого поля имеют вид, представленный в таблице 1,

|  |
| --- |
| Таблица 1 |
| 0 | 000 | 0 | 3 | 011 | Z+1 |
| 0 | 001 | 1 | 4 | 110 | Z2+Z |
| 1 | 010 | Z | 5 | 111 | Z2+Z+1 |
| 2 | 100 | Z2 | 6 | 101 | Z2+1 |

то коэффициенты принимают значения элементов этого поля и поэтому они сами отображаются в виде многочленов следующего вида
где m - степень многочлена, по которому получено расширение поля GF(2);\ ai - коэффициенты, принимающие значение элементов GF(2), т.е. 0 и 1. Такой код называется q-ным.

Длина циклического кода называется примитивной и сам код называется примитивным, если его длина n=qm-1 на GF(q).

Если длина кода меньше длины примитивного кода, то код называется укороченным или непримитивным.

Как следует из определения общее свойство кодовых слов циклического кода - это их делимость без остатка на некоторый многочлен g(x), называемый порождающим.

Результатом деления двучлена xn+1 на многочлен g(x) является проверочный многочлен h(x).

При декодировании циклических кодов используются многочлен ошибок e(x) и синдромный многочлен S(x).

Многочлен ошибок степени не более (n-1) определяется из выражения где - многочлены, отображающие соответственно принятое (с ошибкой) и переданное кодовые слова.

Ненулевые коэффициенты в е(x) занимают позиции, которые соответствуют ошибкам.

Пример.

Синдромный многочлен, используемый при декодировании циклического кода, определяется как остаток от деления принятого кодового слова на порождающий многочлен, т.е.

или

Следовательно, синдромный многочлен зависит непосредственно от многочлена ошибок е(х).Это положение используется при построении таблицы синдромов, применяемой в процессе декодирования. Эта таблица содержит список многочленов ошибок и список соответствующих синдромов, определяемых из выражения (см. таблицу 2).



|  |
| --- |
| Таблица 2 |
| (x) | S(x) |
| 1 | Rg(x)[1] |
| X | Rg(x)[x] |
| X2 | Rg(x)[x2] |
|  |  |
|  |  |
|  |  |
| X+1 | Rg(x)[x+1] |
| X2+1 | Rg(x)[x2+1] |
|  |  |
|  |  |
|  |  |

В процессе декодирования по принятому кодовому слову вычисляется синдром, затем в таблице находится соответствующий многочлен е(х), суммирование которого с принятым кодовым словом дает исправленное кодовое слово, т.е. Перечисленные многочлены можно складывать, умножать и делить, используя известные правила алгебры, но с приведением результата по mod 2, а затем по mod xn+1, если степень результата превышает степень (n-1).

Примеры.

|  |  |
| --- | --- |
|  |  |

Допустим, что длина кода n=7, то результат приводим по mod x7+1.

При построении и декодировании циклических кодов в результате деления многочленов обычно необходимо иметь не частное, а остаток от деления.
Поэтому рекомендуется более простой способ деления, используя не многочлены, а только его коэффициенты (вариант 2 в примере).

Пример.

1.

2.


### **Матричное задание кодов**

Циклический код может быть задан порождающей и проверочной матрицами. Для их построения достаточно знать порождающий g(x) и проверочный h(x) многочлены. Для несистематического циклического кода матрицы строятся циклическим сдвигом порождающего и проверочного многочленов, т.е. путем их умножения на x и

При построении матрицы H(n,k) старший коэффициент многочлена h(x) располагается справа.

Пример. Для циклического (7,4)-кода с порождающим многочленом g(x)=x3+x+1 матрицы G(n,k) и H(n,k) имеют вид: где

Для систематического циклического кода матрица G(n,k) определяется из выражения где Ik - единичная матрица; Rk,r - прямоугольная матрица. Строки матрицы Rk,r определяются из выражений или где ai(x) - значение i-той строки матрицы Ik; i - номер строки матрицы Rk,r.

Пример. Матрица G(n,k) для (7,4)-кода на основе порождающего многочлена g(x)=x3+x+1, строится в следующей последовательности
или

Определяется R4,3, используя так как

Аналогичным способом определяется

В результате получаем или

Используя выражение получим тот же результат.
Строки матрицы G(n,k) можно определить непосредственно из выражения
где

Проверочная матрица в систематическом виде строится на основе матрицы G(n,k), а именно: где Ir - единичная матрица; - матрица из G(n,k) в транспонированном виде.

Пример. Для (7,4)-кода матрица H(n,k) будет иметь вид:

Одна из основных задач, стоящих перед разработчиками устройств защиты от ошибок при передаче дискретных сообщений по каналам связи является выбор порождающего многочлена g(x) для построения циклического кода, обеспечивающего требуемое минимальное кодовое расстояние для гарантийного обнаружения и исправления t-кратных ошибок.

Существуют специальные таблицы по выбору g(x) в зависимости от предъявляемых требований к корректирующим возможностям кода. Однако у каждого циклического кода имеются свои особенности формирования g(x). Поэтому при изучении конкретных циклических кодов будут рассматриваться соответствующие способы построения g(x).

**Коды БЧХ**

Одним из классов циклических кодов, способных исправлять многократные ошибки, являются коды БЧХ.

Примитивным кодом БЧХ, исправляющим tu ошибок, называется код длиной n=qm-1 над GF(q), для которого элементы являются корнями порождающего многочлена.

Здесь  - примитивный элемент GF(qm).

Порождающий многочлен определяется из выражения
где f1(x),f2(x)...- минимальные многочлены корней g(x).

Число проверочных элементов кода БЧХ удовлетворяет соотношению

Пример. Определить значение порождающего многочлена для построения примитивного кода БЧХ над GF(2) длины 31, исправляющего двух кратные ошибки (tu=2).

Исходя из определения кода БЧХ корнями многочлена g(x) являются: , где  - примитивный элемент GF(qm)=GF(25).

Порождающий многочлен определяется из выражения где f1(x), f2(x), f3(x), f4(x) - минимальные многочлены корней соответственно .

Примечание.

Минимальный многочлен элемента  поля GF(qm) определяется из выражения , где - наименьшее целое число, при котором .

Значения минимальных многочленов будут следующими:

Так как f1(x)= f2(x)= f4(x), то

На практике при определении значений порождающего многочлена пользуются специальной таблицей минимальных многочленов (см. таблицу 8 приложения), и выражением для порождающего многочлена При этом работа осуществляется в следующей последовательности.

По заданной длине кода n и кратности исправляемых ошибок tu определяют:
- из выражения n=2m-1 значение параметра m, который является максимальной степенью сомножителей g(x); - из выражения j=2tu-1 максимальный порядок минимального многочлена, входящего в число сомножителей g(x).

- пользуясь таблицей минимальных многочленов, определяется выражение для g(x) в зависимости от m и j. Для этого из колонки, соответствующей параметру m, выбираются многочлены с порядками от 1 до j, которые в результате перемножения дают значение g(x).

В выражении для g(x) содержаться минимальные многочлены только для нечетных степеней , так как обычно соответствующие им минимальные многочлены четных степеней  имеют аналогичные выражения.

Например, минимальные многочлены элементов соответствуют минимальному многочлену элемента 1, минимальные многочлены элементов соответствуют минимальному многочлену 3 и т.п.

Пример. Определить значение порождающего многочлена для построения примитивного кода БЧХ над GF(2) длины 31, обеспечивающего tu=3.

Определяем значения m и j.

Из таблицы минимальных многочленов в соответствии с m=5 и j=5 получаем

Заданные исходные данные: n и tu или k и tu для построения циклического кода часто приводят к выбору завышенного значения m и как следствие этого к неоправданному увеличению длины кода. Такое положение снижает эффективность полученного кода, так как часть информационных разрядов вообще не используется.

Пример. Требуется построить циклический код, исправляющий двух кратные ошибки, если длина информационной части кода k=40.

Согласно выражению для примитивного кода n=2m-1, ближайшая длина кода равна 63, для которой m=6, а r=mtu=12. Следовательно, код будет иметь n=63, k=51. Неиспользованных информационных разрядов будет 11(51-40).

Подобное несоответствие в ряде случаев можно устранить, применяя непримитивный код БЧХ.

Непримитивным кодом БЧХ, исправляющим tu ошибок, называется код длины n над GF(q), для которого элементы являются корнями порождающего многочлена.

Здесь i-непримитивный элемент GF(qm), а длина кода n равна порядку элемента i.

Примечание.

Порядком элемента i является наименьшее n, для которого .

Пример. Порядок элемента 3 поля GF(26) равен 21, так как .

Порождающий многочлен непримитивного кода БЧХ, по аналогии с примитивным кодом, определяется из выражения - минимальные многочлены элементов поля GF(qm), которые являются корнями g(x); i - степень непримитивного элемента .

Пример. Определить значение g(x) для построения непримитивного кода БЧХ над GF(2) длины n=20, исправляющего двух кратные ошибки.

Из таблицы непримитивных элементов GF(2m) (см. таблицу 7 приложения) выбираем поле, элемент  которого имеет порядок больший, но близкий к заданному n.

**Приложение**

**Таблица 1**

Разложение бинома хn+1 на неприводимые сомножители

|  |  |  |
| --- | --- | --- |
| **Степень бинома** | **Последовательности степеней корней неприводимых сомножителей** | **Неприводимые сомножители** |
| 7 | 1 2 43 6 5 | 1315 |
| 15 | 01 02 04 0803 06 12 0905 1007 14 13 11 | 023037007031 |
| 31 | 01 02 04 08 1603 06 12 24 1705 10 20 09 1807 14 28 25 1911 22 13 26 2115 30 29 27 23 | 045075067057073051 |
| 63 | 01 02 04 08 16 3203 06 12 24 48 3305 10 20 40 17 3407 14 28 56 49 3509 18 3611 22 44 25 50 3713 26 52 41 19 3815 30 60 57 51 3921 4223 46 29 58 53 4327 54 4531 62 61 59 55 47 | 103127147111015155133165007163013141 |

Примечание. В разложение всех биномов входит сомножитель 03 с корнем 00. Все сомножители представлены в восьмеричной форме.

**Таблица 2**

Элементы поля GF(16) как расширение GF(2) по примитивному многочлену (z)=z4+z+1

|  |  |  |
| --- | --- | --- |
| **В двоичном виде** | **В виде многочлена** | **В виде степени** |
| 0000 | 0 | 0 |
| 0001 | 1 | 0 |
| 0010 | z | 1 |
| 0100 | z2 | 2 |
| 1000 | z3 | 3 |
| 0011 | z+1 | 4 |
| 0110 | z2+z | 5 |
| 1100 | z3+z2 | 6 |
| 1011 | z3+z+1 | 7 |
| 0101 | z2+1 | 8 |
| 1010 | z3+z | 9 |
| 0111 | z2+z+1 | 10 |
| 1110 | z3+z2+z | 11 |
| 1111 | z3+z2+z+1 | 12 |
| 1101 | z3+z2+1 | 13 |
| 1001 | z3+1 | 14 |

**Таблица 3**

Элементы поля GF(16) как расширение GF(4) по примитивному многочлену f(z)=z2+z+2

|  |  |  |  |
| --- | --- | --- | --- |
| **В четвертичном виде** | **В десятичном виде** | **В виде многочлена** | **В виде степени** |
| 00 | 0 | 0 | 0 |
| 01 | 1 | 1 | 0 |
| 10 | 4 | z | 1 |
| 12 | 6 | z+2 | 2 |
| 32 | 14 | 3z+2 | 3 |
| 11 | 5 | z+1 | 4 |
| 02 | 2 | 2 | 5 |
| 20 | 8 | 2z | 6 |
| 23 | 11 | 2z+3 | 7 |
| 13 | 7 | z+3 | 8 |
| 22 | 10 | 2z+2 | 9 |
| 03 | 3 | 3 | 10 |
| 30 | 12 | 3z | 11 |
| 31 | 13 | 3z+1 | 12 |
| 21 | 9 | 2z+1 | 13 |
| 33 | 15 | 3z+3 | 14 |

**Таблица 4**

Элементы поля GF(4) как расширение GF(2) по примитивному многочлену f(z)=z2+z+1

|  |  |  |  |
| --- | --- | --- | --- |
| **В двоичном виде** | **В виде многочлена** | **В виде степени** | **В десятичном виде** |
| 00 | 0 | 0 | 0 |
| 01 | 1 | 0 | 1 |
| 10 | z | 1 | 2 |
| 11 | z+1 | 2 | 3 |

**Таблица 6**

Элементы поля GF(8) как расширение GF(2) по примитивному многочлену f(z)=z3+z+1

|  |  |  |
| --- | --- | --- |
| **В двоичном виде** | **В виде многочлена** | **В виде степени** |
| 000 | 0 | 0 |
| 001 | 1 | 0 |
| 010 | z | 1 |
| 100 | z2 | 2 |
| 011 | z+1 | 3 |
| 110 | z2+z | 4 |
| 111 | z2+z+1 | 5 |
| 101 | z2+1 | 6 |

**Таблица 7**

Непримитивные элементы поля GF(2m)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **¹** | **m** | **GF(2m)** | **** | **n** |
| 1 | 4 | GF(24) | 3 | 5 |
|  |  |  | 5 | 3 |
| 2 | 6 | GF(26) | 3 | 21 |
|  |  |  | 7 | 9 |
|  |  |  | 9 | 7 |
| 3 | 8 | GF(27) | 3 | 85 |
|  |  |  | 5 | 51 |
|  |  |  | 15 | 17 |
|  |  |  | 17 | 15 |
| 4 | 9 | GF(29) | 7 | 73 |
| 5 | 10 | GF(210) | 3 | 341 |
|  |  |  | 11 | 93 |
|  |  |  | 31 | 33 |
|  |  |  | 33 | 31 |
| 6 | 12 | GF(212) | 3 | 1365 |
|  |  |  | 5 | 819 |
|  |  |  | 7 | 585 |
|  |  |  | 9 | 455 |
|  |  |  | 13 | 315 |
|  |  |  | 15 | 273 |
|  |  |  | 21 | 195 |
|  |  |  | 45 | 91 |
|  |  |  | 63 | 65 |
|  |  |  | 65 | 63 |

**Таблица 8**

Минимальные неприводимые многочлены в поле GF(2m)

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 2tu-1 |  |  |  |  | m |  |  |  |  |
|  | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 1357911131517192123252729313335 | 7 | 1315 | 31370731 | 4575675773 | 103127147111015155 | 211217235367277325203 | 435567763551675747453727023545613543433477615435537771 | 10211131146112311423105511671541133316051027175117431617 1401 | 2011201724153771225720652157265335152773375320332443357324613041753023 |

Такими являются GF(26) и 3, порядок которого n=21.

Так как j=2tu-1=2(2-1=3, то выражение для g(x) будет иметь вид
где f3(x) и f9(x) - минимальные многочлены элементов 3 и 9 поля GF(26).

Значения этих многочленов следующие:

Выражения для f3(x) и f9(x) можно определить из таблицы минимальных многочленов, используя для этого параметр m выбранного поля GF(2m) и порядковые номера сомножителей g(x).

Для рассмотренного примера m=6, а порядковые номера равны 3 и 9. Поэтому
.

**ЛИТЕРАТУРА**

1. Лидовский В.И. Теория информации. - М., «Высшая школа», 2002г. – 120с.
2. Метрология и радиоизмерения в телекоммуникационных системах. Учебник для ВУЗов. / В.И.Нефедов, В.И.Халкин, Е.В.Федоров и др. – М.: Высшая школа, 2001 г. – 383с.
3. Цапенко М.П. Измерительные информационные системы. - . – М.: Энергоатом издат, 2005. - 440с.
4. Зюко А.Г. , Кловский Д.Д., Назаров М.В., Финк Л.М. Теория передачи сигналов. М: Радио и связь, 2001 г. –368 с.
5. Б. Скляр. Цифровая связь. Теоретические основы и практическое применение. Изд. 2-е, испр.: Пер. с англ. – М.: Издательский дом «Вильямс», 2003 г. – 1104 с.