Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Защита информации и надёжность информационных систем

Студент: Скалкович С.Л

ФИТ 3 курс 2 группа

Преподаватель: Нистюк О.А.

**Лабораторная работа №5**

**Циклические коды**

Цель: приобретение практических навыков кодирования/ декодирования двоичных данных при использовании циклических кодов (ЦК).

Задачи:

1. Закрепить теоретические знания по алгебраическому описанию и использованию ЦК для повышения надежности передачи и хранения в памяти компьютера двоичных данных, для контроля интегральности файлов информации.

2. Разработать приложение для кодирования/декодирования двоичной информации циклическим кодом.

**1. Теоретические сведения**

Циклические коды − это семейство помехоустойчивых кодов, одной из разновидностей которых являются коды Хемминга.

Основные свойства ЦК:

• относятся к классу линейных, систематических;

• сумма по модулю 2 двух разрешенных кодовых комбинаций дает также разрешенную кодовую комбинацию;

• каждый вектор (кодовое слово), получаемый из исходного кодового вектора путем циклической перестановки его символов, также является разрешенным кодовым вектором; к примеру, если кодовое слово имеет следующий вид: 1101100, то разрешенной кодовой комбинацией будет и такая: 0110110;

• при простейшей циклической перестановке символы кодового слова перемещаются слева направо на одну позицию, как в приведенном примере;

• поскольку к числу разрешенных кодовых комбинаций ЦК относится нулевая комбинация 000...00, то минимальное кодовое расстояние dmin для ЦК определяется минимальным весом разрешенной кодовой комбинации;

• циклический код не обнаруживает только такие искаженные помехами кодовые комбинации, которые приводят к появлению на стороне приема других разрешенных комбинаций этого кода;

• в основе описания и использования ЦК лежит полином или многочлен некоторой переменной (обычно Х).

Операции кодирования и декодирования циклических кодов сводятся к известным процедурам умножения и деления двоичных чисел, либо соответствующих этим числам полиномов. Действия с кодовыми словами производятся по правилам арифметики по модулю 2. Следует помнить, что вычитание равносильно сложению.

Порождающие полиномы циклических кодов. Характеризуя ЦК в общем случае, обычно отмечают следующее: ЦК составляют множество многочленов {Вj(X)} степени r (r − число проверочных символов в кодовом слове), кратных порождающему (образующему) полиному G(Х) степени r, который должен быть делителем бинома Xn + 1, т. е. остаток после деления бинома на G(X) должен быть нулевым.

Формирование разрешенных кодовых комбинаций ЦК Bj(X) основано на предварительном выборе порождающего (генераторного или образующего) полинома G(X), который обладает важным отличительным признаком: все комбинации Bj(X) делятся на порождающий полином G(X) без остатка:

*Bj(X) / G(X) = Aj(X).*

Степень порождающего полинома определяет число проверочных символов: r = n – k. Из этого свойства следует простой способ формирования разрешeнных кодовых слов ЦК − умножение информационного слова A(X) на порождающий полином G(X).

Порождающими могут быть только такие полиномы, которые являются делителями двучлена (бинома) Хz + 1 при нулевом остатке: R(X) = 0.

Таким образом, в основе построения ЦК лежит операция деления передаваемой кодовой комбинации на порождающий неприводимый полином степени r. Остаток R(X) от деления используется при формировании проверочных разрядов. При декодировании принятой n-разрядной кодовой комбинации (Yn) опять производится ее деление на порождающий (производящий, образующий) полином.

Синдромом ошибки в этих кодах является наличие остатка от деления принятой кодовой комбинации на порождающий полином. Если синдром равен нулю, то считается, что ошибок нет. В противном случае с помощью полученного синдрома можно определить номер разряда принятой кодовой комбинации, в котором произошла ошибка, и исправить ее примерно по той же схеме, которую мы использовали для кода Хемминга.

При этом следует обратить внимание на важную деталь: умножение полинома на х приводит к сдвигу членов полинома на один разряд влево, а при умножении на хr – на r разрядов влево с заменой r младших разрядов полинома на нули. Деление же полинома на х приводит к соответствующему сдвигу членов полинома вправо с уменьшением показателей членов на 1. Такой сдвиг требует дописать справа r проверочных символов к исходной кодовой комбинации Аi(Х) после умножения ее на хr.

Декодирование принятого сообщения по синдрому. Основная операция: принятое кодовое слово (Yn) нужно поделить на порождающий полином, который использовался при кодировании. Если Yn принадлежит коду, т. е. слово не искажено помехами, то остаток от деления (синдром) будет нулевым. Декодирование ненулевого синдрома имеет целью определение ошибочного бита в принятом сообщении или, иначе говоря, определение вектора Еn.

1. **Практическая часть**

В соответствии с вариантом №12 необходимо принимать следующие параметры, представленные на рисунке 1:

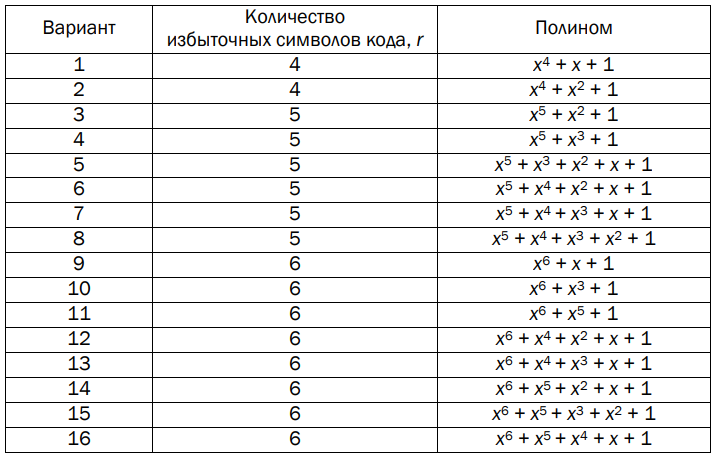


Рисунок 1 – Варианты заданий

**Вариант 12**

Количество избыточных символов r = 6, полином Xn = x6 + x4 + x2 +x+ 1.

Переводим полином в двоичный вид: Xk = 1010111,

Избыточная часть X­r = X6.

Xn = 01011001100100101011010100

Сначала требуется построить порождающую матрицу G (рисунок 2):

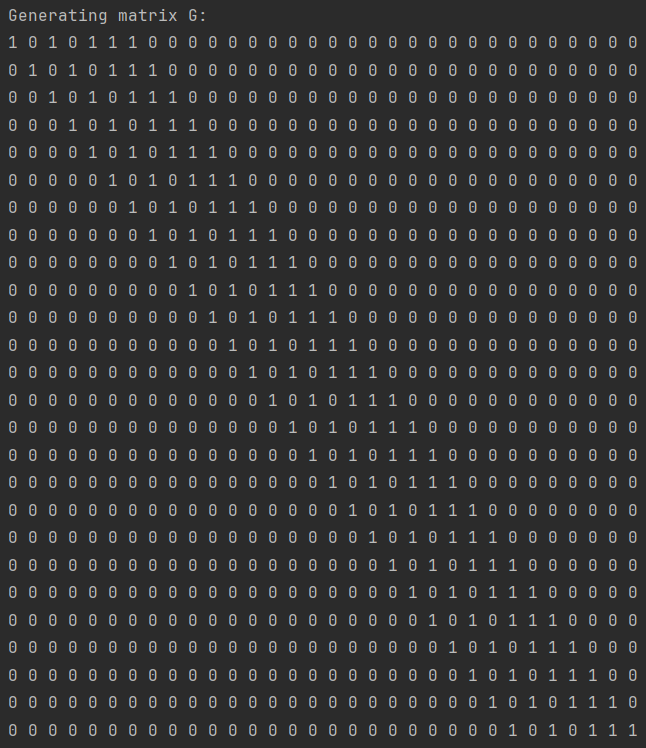


Рисунок 2 – Порождающая матрица

И привести ее в канонический вид (рисунок 3):



Рисунок 3 – Порождающая матрица в каноническом виде

Из полученной матрицы выделяем 6 последних столбцов для формирования проверочной матрицы (рисунок 4):

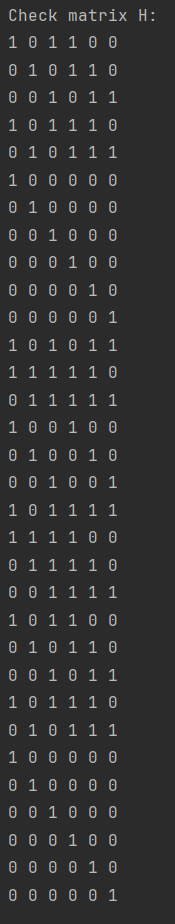


Рисунок 4 – Проверочная матрица

Далее транспонируем проверочную матрицу для приведения её в канонический вид (рисунок 5):

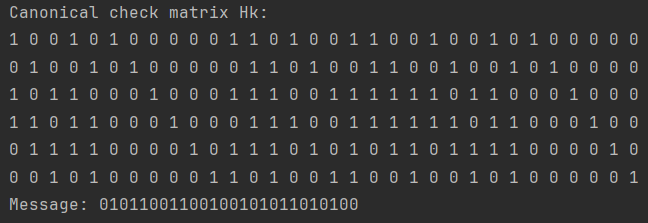


Рисунок 5 – Каноническая проверочная матрица

Данная матрица будет использоваться для определения позиции ошибки с помощью синдрома.

Для получения синдрома полученное сообщение (рисунок 6) делится на порождающий полином.

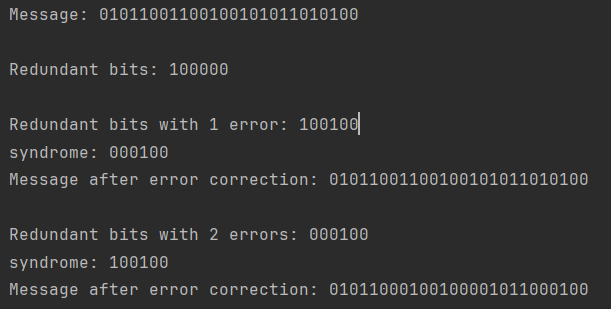


Рисунок 6 – Нахождение и исправление ошибок в сообщениях

При 1 ошибке допущенной в 14 бите сообщения, мы получили синдром 000100 который соответствует 14 столбцу проверочной матрицы, соответственно ошибка найдена и исправлена верно, при ошибке в 2 битах, синдром не соответствует ни одному столбцу проверочной матрицы соответственно ошибка не может быть определенна.

**Вывод**

В ходе выполнения лабораторной работы были получены теоретические сведения о циклических кодах и использованы при выполнении практического задания. А также получили навыки кодирования/декодирования двоичных данных при использовании циклических кодов. Были изучены принципы деления, умножения, сложения и вычитания полиномов.