Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Избыточное кодирование данных в информационных системах. Циклические коды.**

Студент: Дрозд А. И.

ФИТ 3 курс 2 группа

Преподаватель:

Нистюк Ольга Александровна

Минск 2024

**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.
3. Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента.

# **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). Для более глубокого изучения параметров и свойств ЦК, равно как и других корректирующих кодов, полезно ознакомиться с классическими книгами, например.

Рассматриваемые операции 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. Это следует из простых рассуждений: из равенства х^z − 1 = 0 получаем х^z = 1. Прибавив к левой и правой частям по единице, имеем х^z + 1 = 1 + 1 = 0. Таким образом, вместо двучлена х^z − 1 можно ввести х^z + 1 или 1 + х^z , из чего следует также, что х^z + х^z = х^z (1 + 1) = 0.

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. Показано на рисунке 1.1.



Рисунок 1.1 – Признак выбора порождающего полинома

Степень порождающего полинома определяет число проверочных символов: r = n – k. Из этого свойства следует простой способ формирования разрешенных кодовых слов ЦК − умножение информационного слова A(X) на порождающий полином G(X). Показан на рисунке 1.2.



Рисунок 1.2 – Простой способ формирования разрешенных кодовых слов ЦК

Порождающими могут быть только такие полиномы, которые являются делителями двучлена (бинома) Хz + 1 при нулевом остатке R(X) = 0. Предоставлено на рисунке 1.3.

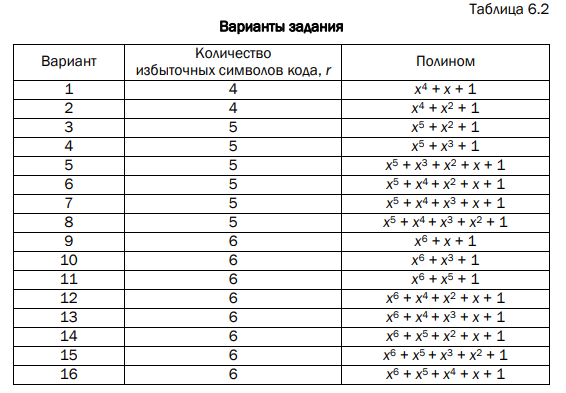


Рисунок 1.3 – Формула проверки порождающего полинома

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.

**Практическое задание**

Вариант 3



В соответствии с вариантом необходимо сгенерировать исходное сообщение длинной 31 бит определить r и n. Эти действия представлены на рисунке 2.1.



Рисунок 2.2 – Исходное сообщение, значения для r и n

Далее нам необходимо составить порождающую матрицу для нашего кода. Для этого необходимо записать порождающий полином в матрицу размером (n,k), дополнить нулями всю первую строку матрицы и каждую новую строку сдвигать на 1 бит вправо. Результат на рисунке 2.3.

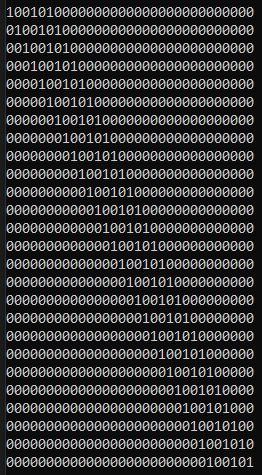


Рисунок 2.3 – Порождающая матрица

Далее нам необходимо сложить все строки по модулю 2 так, чтобы в левой подматрице образовалась диагональная матрица. После выполнения всех этих действий матрица примет канонический вид. Результат на рисунке 2.4.

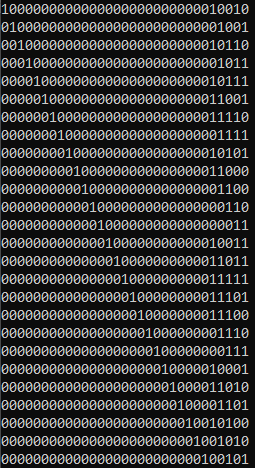


Рисунок 2.4 – Порождающая в каноническом виде матрица

Далее вычисляем проверочную матрицу путем извлечения правой подматрицы проверочных битов и добавления диагональной матрицы размером r\*r. Итог показан на рисунке 2.5.

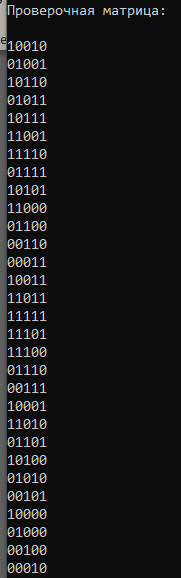


Рисунок 2.5 – Проверочная матрица

Необходимо сгенерировать одну и две ошибки. Для вычисления позиции ошибки необходимо выполнить операцию деления над исходным сообщением (с ошибкой) и порождающим полиномом. Остаток от деления будет соответствовать строке проверочной матрицы. Исправление сообщения с 1 ошибкой показано на рисунке 2.6.

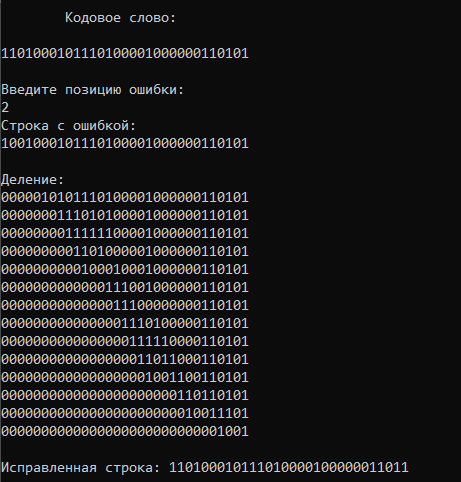


Рисунок 2.6 – Исправление сообщения с 1 ошибкой

С двумя ошибками производится такая же операция, только ошибки вычисляются путём сложения по модулю 2 двух строк, которые будут соответствовать позиции ошибки проверочной матрицы. Итог показан на рисунке 2.7.

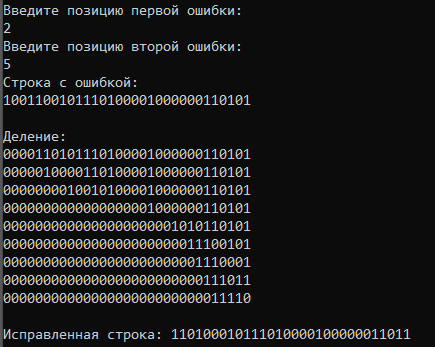


Рисунок 2.6 – Исправление сообщения с 2 ошибками

**Вывод:**

Циклические коды – это семейство помехоустойчивых кодов, одной из разновидностей которых являются коды Хемминга. Каждый вектор (кодовое слово), получаемый из исходного кодового вектора путем циклической перестановки его символов, также является разрешенным кодовым вектором. При простейшей циклической перестановке символы кодового слова перемещаются слева направо на одну позицию. Циклический код не обнаруживает только такие искаженные помехами кодовые комбинации, которые приводят к появлению на стороне приема других разрешенных комбинаций этого кода.

В этой лабораторной работе я ознакомился с понятием циклических кодов, разобрался в поиске ошибок и их исправлении. Также были изучены принципы построения матриц, необходимых для функционирования данного кода.