Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра информационных систем и технологий

Отчет

по дисциплине «Защита информации и надежность информационных систем»

Студент: Шедько Е.А.

ФИТ 3 курс 3 группа

Преподаватель: Берников В.О.

Лабораторная работа №6

**Тема «Избыточное кодирование данных в информационных системах. Циклические коды»**

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

**Задачи:**

* 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.
* Разработать приложение для кодирования/декодирования двоичной информации циклическим кодом.
* 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).

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:



здесь Bj(X) = Xn – кодовое слово; Aj(X) = Xk – информационное слово.

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.

Возможные порождающие полиномы для различных длин k информационного слова, найденные с помощью ЭВМ, сведены в обширные таблицы.

Можно добавить, что для k = 4 существуют только два порождающих полинома: х 3 + х + 1 (1011), и х 3 + х 2 + 1 (1101). Напомним, что эти полиномы относятся к двойственным: обратная запись (справа налево) одного в бинарной форме дает другой.

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.

**Результат выполнения программы**

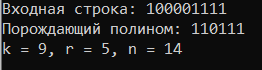
****

Рис. 1 – Ввод сообщения

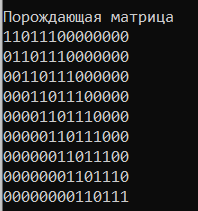


Рис. 2 –Генерация порождающей матрицы

Как показано на рисунках, сразу вводится информационное сообщение, далее вычисляются необходимые данные и генерируется порождающая матрица для дальнейшей работы.

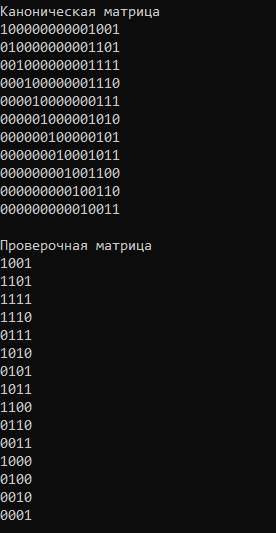


Рис. 2 — Каноническая порождающая и каноническая проверочная матрицы

Затем генерируются каноническая порождающая матрица и каноническая проверочная матрица.

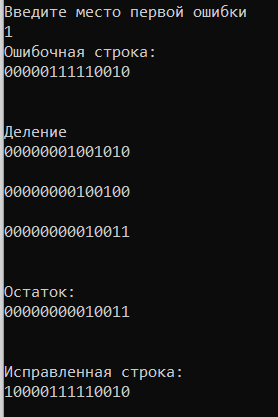


Рис. 3 — Вычисление кодового слова, генерация ошибок и их исправление

Далее вычисляется кодовое слово, генерируются и исправляются ошибки.

**Вывод:** в ходе лабораторной работы были приобретены практические навыки кодирования/декодирования двоичных данных при использовании циклических кодов (ЦК).