Кафедра информационных технологий и безопасности

Кан О.А.

**Лабораторная работа № 4**

по дисциплине

«Информационные основы защиты информации»

Специальность: 6В06301 – «Системы информационной безопасности»

Караганда 2023

**Лабораторная работа № 4**

**Тема:** Корректирующие коды. Код Хемминга.

**Цель работы:** Ознакомление с принципами построения корректирующих кодов на примере кода Хемминга.

**Краткие сведения из теории**

При построении корректирующих кодов важной характеристикой является кодовое расстояние. Кодовое расстояние - это то минимальное число элементов, в которых одна кодовая комбинация отличается от другой. Для определения кодового расстояния достаточно сравнить две кодовые комбинации по модулю 2 (операция XOR) и подсчитать число единиц в полученной комбинации. Например, сложив по модулю 2 две комбинации

10110101101 XOR 11001010101 = 01111111000

получим, что кодовое расстояние между ними d=7.

Рассмотрим построение корректирующего кода Хемминга.

При построении уравнений проверки для кода Хемминга все номера разрядов кода записывают в двоичном виде:

a1=0001, a2=0010, a3=0011 и т.д.

**Первое проверочное уравнение** составляют как сумму по модулю 2 всех разрядов, в номерах которых в младшем разряде (2^0) стоит единица:

r1=a1⊕a3⊕a5⊕a7⊕...

**Второе уравнение** составляют как сумму по модулю 2 всех разрядов, в номерах которых стоит единица на втором месте (2^1):

r2=a2⊕a3⊕a6⊕a7...

**Третье уравнение** составляют как сумму по модулю 2 всех разрядов, в номерах которых стоит единица на третьем месте (2^2):

r3=a4⊕a5⊕a6⊕a7...

Уравнения кодирования для определения проверочных разрядов находят приравниванием проверочных уравнений нулю при отсутствии ошибок.

a1=a3⊕a5⊕a7...

a2=a3⊕a6⊕a7...

a4=a5⊕a6⊕a7...

............................

Проверочные разряды a1,a2,a4 размещается внутри кодовой комбинации на местах, соответствующих их номеру.

**Пример.** Организовать передачу кодовой комбинации 1100 с использованием кода Хемминга. Число проверочных разрядов n- k=3. В коде Хемминга они разместятся на первом a1, втором a2, на четвертом a4 местах.

Кодовая комбинация примет вид a1a21a4100.

Определим:

a1=a3⊕a5⊕a7=1⊕1⊕0=0

a2=a3⊕a6⊕a7=1⊕0⊕0=1

a4=a5⊕a6⊕a7=1⊕0⊕0=1

Следовательно, будет передана комбинация 0111100, в которой a1, a2, a4-проверочные разряды.

Если при передаче информации произошла одиночная ошибка и принята комбинация вида 0101100, то декодирование дает следующие результаты:

r1=a1⊕a3⊕a5⊕a7=0⊕0⊕1⊕0=1

r2=a2⊕a3⊕a6⊕a7=1⊕0⊕0⊕0=1

r3=a4⊕a5⊕a6⊕a7=1⊕1⊕0⊕0=0

Получим R=r1 r2 r3---1\*2^0+a\*2^1+0\*2^2=3.

Отсюда номер искаженного разряда равен 3. Следовательно “0” третьего разряда надо изменить на “1”.

Рассмотрим код Хемминга для числа информационных разрядов k=8. Для обнаружения и исправления одиночных ошибок имеем

d=2\*t1+1=3

Верхняя граничная оценка Хемминга для числа проверочных разрядов (n-k) при t=1.

n-klog2(n+1), т.к. n>k, то подставим

n=9, получим n-k>={log210}=4

отсюда n=12, r=n-k=4. X=a1a2a3a4a5a6a7a8a9a10a11a12

Составим уравнения проверки:



Найдем уравнения кодирования для определения проверочных разрядов

а1=a3+a5+a7+a9+a11

a2=a3+a6+a7+a10+a11

a4=a5+a6+a7+a12

a8=a9+a10+a11+a12

Проверочные разряды разместятся внутри передаваемого кода на местах a1,a2,a4,a8.

**Порядок выполнения работы**

1. Изучить теоретический материал.
2. Выполнить задания.
3. Ответить на контрольные вопросы.

**Задание 1**

1. Построить код Хемминга для десятичного числа Х = 237.
2. Декодировать код Хемминга Х=1110111.

**Задание 2**

1. Написать программу добавления проверочных разрядов к 8-ми разрядному двоичному коду, введенному в текстовое поле.
2. Предусмотреть возможность внесения изменений (замена 0 на 1, или 1 на 0) в кодовую комбинацию, расположенную в текстовом поле.
3. Добавить кнопку для проверки кодовой комбинации, расположенной в текстовом поле.
4. Выдать сообщение о результатах проверки на экран.

**Содержание отчета**

1. Титульный лист.
2. Результаты выполненных работ.
3. Листинг программы с комментариями.
4. Ответы на контрольные вопросы.

**Контрольные вопросы**

1. Для чего применяют корректирующие коды?
2. Как обнаруживают ошибки в коде Хемминга?
3. Как определяется кодовое расстояние?
4. Как строятся проверочные уравнения в коде Хемминга?
5. Где располагаются проверочные разряды в коде Хемминга?