Лабораторная работа №1

ЛИНЕЙНЫЕ БЛОКОВЫЕ КОДЫ

1. Цель работы

Разработать программный модуль, который строит случайный двоичный линейный блоковый код для заданных параметров (n, k). Для построенного кода оценить расстояние. Указать, на сколько полученные параметры далеки от границ существования (Хемминга, Варшамова-Гилберта, Синглтона).

Требования к программе:

1) Для построенного кода возвращается порождающая матрица, количество слов в коде и его корректирующая способность.
2) Возвратить отклонения расстояния кода от всех границ.

Требования к отчету: Отчет должен содержать описание реализованного алгоритма, формулы и примеры вычисления границ и параметров, примеры работы программы.

2. Ход работы

2.1. Построение кода

Блочный код длиной n символов, состоящий из 2^k кодовых слов, называется линейным (n, k)-кодом при условии, что все его 2^k кодовых слов образуют k-мерное подпространство векторного пространства n-последовательностей двоичного поля GF(2).

Будем строить код на основе сгенерированной порождающей матрицы G, такой что:

$$G = [\ I_{k\times k} \mid C_{k\times r}\ ],$$

где I – единичная матрица, C – случайно сгенерированная матрица, $r = n - k$.

Затем генерируем все возможные двоичные векторы длины k и умножаем на порождающую матрицу G. Таким образом формируется множество всех 2^k кодовых слов.

2.2. Минимальное расстояние кода и корректирующая способность

Минимальное расстояние d линейного кода является минимальным из всех расстояний Хемминга всех пар кодовых слов. Вес вектора w — расстояние Хемминга между этим вектором и нулевым вектором, иными словами — число ненулевых компонент вектора.

Минимальное расстояние кода будем искать с помощью перебора по всем построенным словам:

$$\mathrm{d} = \min\left(\mathrm{w}(\overline{\mathrm{c}})\right)$$

Зная минимальное расстояние кода d, можно оценить корректирующую способность кода t. Корректирующая способность определяет, какое максимальное число ошибок в одном кодовом слове код может гарантированно исправить:

$$t = \left\lfloor \frac{d-1}{2} \right\rfloor$$

2.3. Границы Хемминга, Варшамова-Гилберта, Синглтона

Граница Хемминга (граница плотной упаковки).

Граница Хэмминга определяет пределы возможных значений параметров произвольного блокового кода. А именно, не существует блокового кода, для которого не выполняется неравенство (для двоичного случая имеет вид):

$$2^n \geq 2^k \sum_{i=0}^{t} C_n^i$$

Граница Варшамова-Гилберта (нижняя граница – существования). Для двоичного случая имеет вид:

$$2^k \sum_{i=0}^{d-1} C_n^i \geq 2^n$$

Граница Синглтона (верхняя граница):

$$k \leq n - d + 1$$

2.4. Примеры вычисления границ и параметров

Рассмотрим пример построения кода с параметрами: $k = 3, n = 7$
Число кодовых слов будет равно $|C| = 2^k = 2^3 = 8$

Пусть порождающая матрица G имеет вид:

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{bmatrix}$$

Множество двоичных векторов:
{000, 001, 010, 011, 100, 101, 110, 111}.
Умножим их на порождающую матрицу и получим множество кодовых слов:
C = {0000000, 0010110, 0101001, 1001101, 0111111, 1011011, 1100100, 1110010}

Минимальное расстояние $d = 3$
Корректирующая способность: $t = \left\lfloor \frac{d-1}{2} \right\rfloor = 1$
Граница Хемминга: *выполняется*

$$2^7 \geq 2^3 \cdot 8; \quad 128 \geq 64$$

Граница Варшамова-Гилберта: *выполняется*

$$128 \cdot 29 \geq 8$$

Граница Синглтона: *выполняется*

$$3 \leq 7 - 3 + 1; \quad 3 \leq 5$$

Все границы соблюдены, а это значит, что построенный код, хоть и не является совершенным, но при этом является хорошим.

2.5. Примеры работы программы

Пример 1.

Входные данные:

```
Введите n = 7
Введите k = 3
```

Результаты работы программы:

```
Количество кодовых слов: 8
```

```
Порождающая матрица G:
    1   0   0   1   0   1   0
    0   1   0   1   1   1   1
    0   0   1   1   1   1   0

Множество кодовых слов:
    0   0   0   0   0   0   0
    0   0   1   1   1   1   0
    0   1   0   1   1   1   1
    0   1   1   0   0   0   1
    1   0   0   1   0   1   0
    1   0   1   0   1   0   0
    1   1   0   0   1   0   1
    1   1   1   1   0   1   1
```

```
Минимальное расстояние кода: 3
Корректирующая способность: 1
```

```
Сравнение с границами:
Граница Хэмминга:
Выполняется
   8 <= 128
   Отклонение = 120

Граница Варшамова-Гилберта:
Выполняется
   8 >= 5
   Отклонение = 3

Граница Синглтона:
Выполняется
   3 <= 5
   Отклонение = 2
```

Все границы соблюдены, что говорит о том, что построенный код, хоть и не является совершенным, но при этом является хорошим.

Пример 2.

Входные данные:

```
Введите n = 8
Введите k = 2
```

Результаты работы программы:

```
Количество кодовых слов: 4

Порождающая матрица G:
    1    0    1    0    0    1    1    0
    0    1    0    0    1    0    0    0

Множество кодовых слов:
    0    0    0    0    0    0    0    0
    0    1    0    0    1    0    0    0
    1    0    1    0    0    1    1    0
    1    1    1    0    1    1    1    0

Минимальное расстояние кода: 2
Корректирующая способность: 0

Сравнение с границами:
Граница Хэмминга:
Выполняется
   4 <= 256
   Отклонение = 252

Граница Варшамова-Гилберта:
Не выполняется
   4 < 29
   Отклонение = 25

Граница Синглтона:
Выполняется
   2 <= 7
   Отклонение = 5
```

Граница Варшамова-Гилберта не выполняется, что говорит о том, что построенный код не является хорошим. Это значит, что при заданных параметрах существует код большей мощности.

3. Выводы

В ходе выполнения лабораторной работы разработали программу, позволяющую строить двоичные линейные блоковые коды по заданным параметрам n и k. Кроме того, для построенного кода определили количество кодовых слов, минимальное расстояние d и корректирующую способность.

Были изучены понятия границы Хэмминга, Варшамова-Гилберта и Синглтона и проверено соответствие кода этим границам. Для каждой из границ было посчитано отклонение мощности кода.