МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ федеральное государственное автономное образовательное учреждение высшего образования
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ»

КАФЕДРА № 51

ОТЧЕТ
ЗАЩИЩЕН С ОЦЕНКОЙ

ПРЕПОДАВАТЕЛЬ

Ст.преподаватель		А.В. Афанасьева
должность, уч. степень, звание	подпись, дата	инициалы, фамилия

ОТЧЕТ О ЛАБОРАТОРНОЙ РАБОТЕ №1

Линейные блоковые коды

по дисциплине: ТЕОРИЯ КОДИРОВАНИЯ

РАБОТУ ВЫПОЛНИЛ

СТУДЕНТ ГР. №	5911		Е.А. Белов
		подпись, дата	инициалы, фамилия

Санкт-Петербург 2022

1. Цель работы

Разработать программный модуль, который строит случайный двоичный линейный блоковый код для заданных параметров (n, k).

2. Задание (Вариант 2)

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

3. Описание реализованного алгоритма

3.1 Линейный блоковый код

Входными параметрами для линейного блокового кода являются переменные n и k, где k является размером входного сообщения, а n – размер полученного кодового слова. Информация в коде представляется в виде двоичных векторов.

В реализованном алгоритме, сначала необходимо создать порождающую матрицу G, которая склеивается из единичной матрицы k×k и матрицы для дополнения размера k×(n-k). В разработанной программе матрица дополнения создается из случайной последовательности.

Множество кодовых слов получается в результате умножения каждого возможного сообщения на порождающую матрицу.

Для подсчета корректирующей способности кода t используется формула

$$t = \left\lfloor \frac{d_0 - 1}{2} \right\rfloor,$$

где d_0 является минимальным расстоянием кода, и равен минимальному весу не нулевого кодового слова.

3.2 Границы параметров кода

Граница Хэмминга. Все пространство двоичных последовательностей длины n имеет размер 2^n . Для некоторого кода длины n с расстоянием d рассматриваются сферы радиуса $t = \frac{d_0-1}{2}$, центрами которых являются кодовые слова.

В теории кодирования граница Хэмминга определяет пределы возможных значений параметров произвольного блокового кода. А именно, не существует q-ичного блокового кода C мощности $|C|$ и длины n с минимальным расстоянием d для которого не выполняется следующее неравенство:

$$|C| \le \frac{q^n}{\sum_{k=0}^{t} \binom{n}{k} (q-1)^k}$$

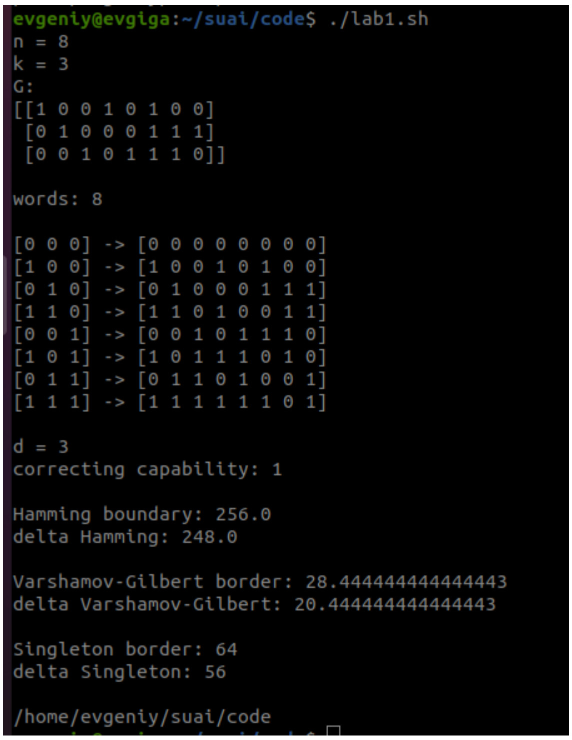
Нижняя граница, или граница *Варшамова-Гилберта*. В отличие от границы Хэмминга, где мы пытались найти максимально возможное число слов в коде (при заданных ограничениях n и d), при этом получая границу несуществования, в данном случае указывается процедура построения кода с заданными n и d, при этом делается попытка максимизировать число N слов в этом коде, что соответствует границе существования — код с таким N точно существует. В соответствии с границей Варшамова-Гилберта существует q-ичный блоковый код C мощности $|C|$ и длины n с минимальным расстоянием d для которого выполняется следующее неравенство:

$$|C| \ge \frac{q^n}{\sum_{k=0}^{d_0-1} \binom{n}{k} (q-1)^k}$$

Граница Синглтона. Устанавливает предел мощности кода C длины n и минимального расстояния Хэмминга d.

$$|C| \le q^{n-d_{min}+1}$$

4. Результат программы

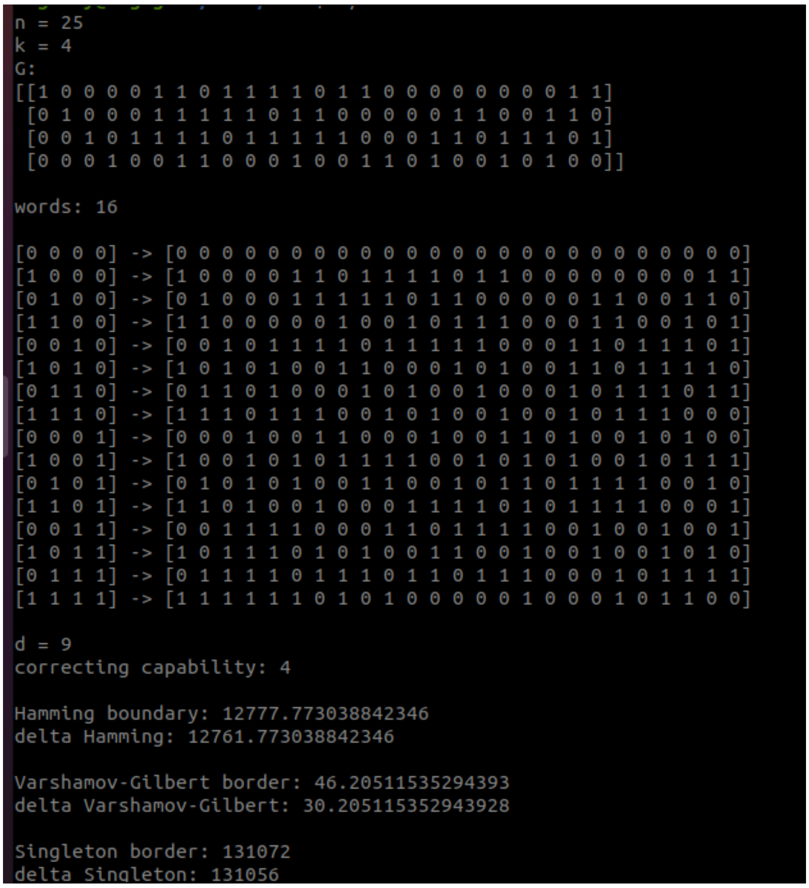


```
evgeniy@evgiga:~/suai/code$ ./lab1.sh
n = 8
k = 3
G:
[[1 0 0 1 0 1 0 0]
 [0 1 0 0 0 1 1 1]
 [0 0 1 0 1 1 1 0]]

words: 8

[0 0 0] -> [0 0 0 0 0 0 0 0]
[1 0 0] -> [1 0 0 1 0 1 0 0]
[0 1 0] -> [0 1 0 0 0 1 1 1]
[1 1 0] -> [1 1 0 1 0 0 1 1]
[0 0 1] -> [0 0 1 0 1 1 1 0]
[1 0 1] -> [1 0 1 1 1 0 1 0]
[0 1 1] -> [0 1 1 0 1 0 0 1]
[1 1 1] -> [1 1 1 1 1 1 0 1]

d = 3
correcting capability: 1

Hamming boundary: 256.0
delta Hamming: 248.0

Varshamov-Gilbert border: 28.444444444444443
delta Varshamov-Gilbert: 20.444444444444443

Singleton border: 64
delta Singleton: 56

/home/evgeniy/suai/code
```

Рис.1 Результат программы для k=3, n=8

```
n = 16
k = 3
G:
[[1 0 0 0 0 0 1 0 0 1 1 1 0 0 0 0]
 [0 1 0 1 1 1 0 0 1 0 1 1 0 1 0 1]
 [0 0 1 0 0 1 0 1 1 1 1 1 0 1 0 1]]

words: 8

[0 0 0] -> [0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0]
[1 0 0] -> [1 0 0 0 0 0 1 0 0 1 1 1 0 0 0 0]
[0 1 0] -> [0 1 0 1 1 1 0 0 1 0 1 1 0 1 0 1]
[1 1 0] -> [1 1 0 1 1 1 1 0 1 1 0 0 0 1 0 1]
[0 0 1] -> [0 0 1 0 0 1 0 1 1 1 1 1 0 1 0 1]
[1 0 1] -> [1 0 1 0 0 1 1 1 1 0 0 0 0 1 0 1]
[0 1 1] -> [0 1 1 1 1 0 0 1 0 1 0 0 0 0 0 0]
[1 1 1] -> [1 1 1 1 1 0 1 1 0 0 1 1 0 0 0 0]

d = 5
correcting capability: 2

Hamming boundary: 3855.0588235294117
delta Hamming: 3847.0588235294117

Varshamov-Gilbert border: 94.025824964132
delta Varshamov-Gilbert: 86.025824964132

Singleton border: 4096
delta Singleton: 4088
```

Рис.2 Результат программы для k=3, n=16



```
n = 25
k = 4
G:
[[1 0 0 0 0 1 1 0 1 1 1 1 0 1 1 0 0 0 0 0 0 0 0 1 1]
 [0 1 0 0 0 1 1 1 1 1 0 1 1 0 0 0 0 0 1 1 0 0 1 1 0]
 [0 0 1 0 1 1 1 1 0 1 1 1 1 1 0 0 0 1 1 0 1 1 1 0 1]
 [0 0 0 1 0 0 1 1 0 0 0 1 0 0 1 1 0 1 0 0 1 0 1 0 0]]

words: 16

[0 0 0 0] -> [0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0]
[1 0 0 0] -> [1 0 0 0 0 1 1 0 1 1 1 1 0 1 1 0 0 0 0 0 0 0 0 1 1]
[0 1 0 0] -> [0 1 0 0 0 1 1 1 1 1 0 1 1 0 0 0 0 0 1 1 0 0 1 1 0]
[1 1 0 0] -> [1 1 0 0 0 0 0 1 0 0 1 0 1 1 1 0 0 0 1 1 0 0 1 0 1]
[0 0 1 0] -> [0 0 1 0 1 1 1 1 0 1 1 1 1 1 0 0 0 1 1 0 1 1 1 0 1]
[1 0 1 0] -> [1 0 1 0 1 0 0 1 1 0 0 0 1 0 1 0 0 1 1 0 1 1 1 1 0]
[0 1 1 0] -> [0 1 1 0 1 0 0 0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0 1 1]
[1 1 1 0] -> [1 1 1 0 1 1 1 0 0 1 0 1 0 0 1 0 0 1 0 1 1 1 0 0 0]
[0 0 0 1] -> [0 0 0 1 0 0 1 1 0 0 0 1 0 0 1 1 0 1 0 0 1 0 1 0 0]
[1 0 0 1] -> [1 0 0 1 0 1 0 1 1 1 1 0 0 1 0 1 0 1 0 0 1 0 1 1 1]
[0 1 0 1] -> [0 1 0 1 0 1 0 0 1 1 0 0 1 0 1 1 0 1 1 1 1 0 0 1 0]
[1 1 0 1] -> [1 1 0 1 0 0 1 0 0 0 1 1 1 1 0 1 0 1 1 1 1 0 0 0 1]
[0 0 1 1] -> [0 0 1 1 1 1 0 0 0 1 1 0 1 1 1 1 0 0 1 0 0 1 0 0 1]
[1 0 1 1] -> [1 0 1 1 1 0 1 0 1 0 0 1 1 0 0 1 0 0 1 0 0 1 0 1 0]
[0 1 1 1] -> [0 1 1 1 1 0 1 1 1 0 1 1 0 1 1 1 0 0 0 1 0 1 1 1 1]
[1 1 1 1] -> [1 1 1 1 1 1 0 1 0 1 0 0 0 0 0 1 0 0 0 1 0 1 1 0 0]

d = 9
correcting capability: 4

Hamming boundary: 12777.773038842346
delta Hamming: 12761.773038842346

Varshamov-Gilbert border: 46.20511535294393
delta Varshamov-Gilbert: 30.205115352943928

Singleton border: 131072
delta Singleton: 131056
```

Рис.3 Результат программы для k=4, n=25

По результатам программы можно сделать вывод, что с увеличением параметра n, возрастает корректирующая способность.

Вывод

В ходе данной лабораторной работы была разработана программа, позволяющая строить случайный двоичный линейный блоковый код для заданных параметров (n, k). Для построенного кода были определены: количество кодовых слов, минимальное расстояние и корректирующая способность. Были изучены границы Хэмминга, Варшамова Гилберта и Синглтона.