Цель работы:

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

Ход работы:

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.

1. *Построение кода*

Линейные блоковые коды позволяют представить информационные и кодовые слова в виде двоичных векторов, что позволяет описать процессы кодирования и декодирования с помощью аппарата линейной алгебры, с учетом того, что компонентами вводимых векторов и матриц являются символы «0» и «1».

Линейным двоичным (n, k) - кодом будем называть k-мерное подпространство n-мерного пространства двоичных последовательностей.

Один из способов задания кода основан на построении порождающей матрицы $G = [\ I \mid C\ ]$, где I – единичная матрица размера $k \times k$, а C – матрица дополнения размера $k \times (n - k)$. В ходе данной лабораторной работы, в соответствии с вариантом задания матрица дополнения генерировалась случайным образом.

Порождающая матрица:

1	0	0	0	1	0	0
0	1	0	0	1	0	1
0	0	1	0	1	0	0
0	0	0	1	1	1	1

Рисунок 1. Пример порождающей матрицы для k = 4 и n = 7.

Генерация кодовых слов производилась путем умножения всех сообщений из множества *M* (множество возможных сообщений) на порождающую матрицу.

Множество кодовых слов:

0	0	0	0	0	0	0
0	0	0	1	1	1	1
0	0	1	0	1	0	0
0	0	1	1	0	1	1
0	1	0	0	1	0	1
0	1	0	1	0	1	0
0	1	1	0	0	0	1
0	1	1	1	1	1	0
1	0	0	0	1	0	0
1	0	0	1	0	1	1
1	0	1	0	0	0	0
1	0	1	1	1	1	1
1	1	0	0	0	0	1
1	1	0	1	1	1	0
1	1	1	0	1	0	1
1	1	1	1	0	1	0

Рисунок 2. Пример кодовых слов для k = 4 и n = 7.

Расстояние Хэмминга d_H (x, y) между двумя векторами *x* и *y* определяется как число позиций, в которых эти векторы различаются. Однако в общем случае код содержит не два слова, а гораздо больше, и эти слова могут находиться на различном расстоянии друг от друга. За меру, характеризующую код в целом, принимают минимальное кодовое расстояние.

$$d_0 = \min_{i \neq j} d(a_i, a_j). \qquad (1)$$

Лемма 2.1. Минимальное расстояние линейного кода равно его минимальному весу: $d_0 = W_0$. В программной реализации был вычислен минимальный вес вектора, являющегося кодовым словом.

Код с минимальным расстоянием d_0 может исправить любую комбинацию из t ошибок, где t – корректирующая способность кода, равная:

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

2. *Границы параметров кода.*

2.1 Граница Хэмминга.

Верхняя граница N, или граница Хэмминга, строится следующим образом. Все пространство двоичных последовательностей длины n имеет размер 2^n. Для некоторого кода длины n с расстоянием d рассматриваются сферы радиуса $t = (d-1)/2$, 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:

$$|C| \leq \frac{q^n}{\sum_{i=0}^{t} C_i^n \, (q-1)^k} \tag{3}$$

2.2. Граница Варшамова-Гилберта.

Нижняя граница, или граница Варшамова-Гилберта, строится следующим образом. 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:

$$|C| \geq \frac{q^n}{\sum_{i=0}^{d_{min}-1} C_i^n (q-1)^k} \tag{4}$$

Данное неравенство не отрицает существование кодов с мощностью меньшей, чем эта граница, таким образом граница Варшамова-Гилберта утверждает лишь факт существования кода с данной мощностью.

2.3. Граница Синглтона.

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

$$|C| \leq q^{n-d_{min}+1} \tag{5}$$

3. Примеры работы программы

```
Введите длину информационного слова k = 4
Введите длину кодового слова  n = 7
Порождающая матрица:
     1     0     0     0     1     1     1
     0     1     0     0     0     0     1
     0     0     1     0     1     1     1
     0     0     0     1     1     1     0

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

Количество кодовых слов 16
Минимальное расстояние кода: 2
Корректирующая способность: 0
Граница Хэмминга: 128
   16 < 128
   Отклонение = 112
Граница Варшамова-Гилберта: 16
   16 <= 16
   Отклонение = 0
Граница Синглтона:64
   16 <= 64
   Отклонение = 48
```

Рисунок 3. Пример работы программы для кода (4, 7).

Отклонение от границы Варшамова-Гилберта равно 0, соответственно между кодовыми словами большое расстояние. Также мощность кода меньше границы Хэмминга, меньше границы Синглтона, соответственно данный код является “плохим”.

```
Введите длину информационного слова k = 3
Введите длину кодового слова  n = 6
Порождающая матрица:
     1     0     0     0     1     1
     0     1     0     1     0     0
     0     0     1     1     0     0

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

Количество кодовых слов 8
Минимальное расстояние кода: 2
Корректирующая способность: 0
Граница Хэмминга: 64
   8 < 64
   Отклонение = 56
Граница Варшамова-Гилберта: 10
   8 <= 10
   Отклонение = 2
Граница Синглтона:32
   8 <= 32
   Отклонение = 24
```

Рисунок 4. Пример работы программы для кода (3, 6).

Мощность кода меньше границы Варшамова-Гилберта, меньше границы Хэмминга, меньше границы Синглтона, соответственно данный код является “плохим”.

```
Введите длину информационного слова k =3
Введите длину кодового слова  n =5
Порождающая матрица:
     1     0     0     1     1
     0     1     0     1     0
     0     0     1     1     0

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

Количество кодовых слов 8
Минимальное расстояние кода: 2
Корректирующая способность: 0
Граница Хэмминга: 32
   8 < 32
   Отклонение = 24
Граница Варшамова-Гилберта: 6
   8 > 6
   Отклонение = 2
Граница Синглтона:16
   8 <= 16
   Отклонение = 8
```

Рисунок 5. Пример работы программы для кода (3,5).

Мощность кода больше границы Варшамова-Гилберта, меньше границы Хэмминга, меньше границы Синглтона, соответственно данный код лучше, чем код в двух предыдущих примерах.

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. Для каждой из границ было посчитано отклонение мощности кода.