Домашнее задание 1

Кокорин Илья, M3439

Вариант № 64

1 Начальные условия

Проверочная матрица $H = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \end{pmatrix}$

2 Определить скорость кода

$r = 4$ (количество строк проверночной матрицы)

$n = 10$ (количество столбцов проверочной и порождающей матриц)

$r = n - k \Rightarrow k = n - r = 10 - 4 = 6$ (количество строк порождающей матрицы)

Скорость кода $R = \frac{k}{n} = \frac{6}{10} = 0.6$ бит/символ

3 Определить минимальное расстояние кода

По теореме 2.4 минимальное расстояние линейного (n, k)-кода равно d в том и только в том случае, когда любые $d - 1$ столбцов проверочной матрицы линейно независимы и существует набор из d линейно зависимых столбцов.

Любые два столбца проверочной матрицы H линейно независимы, так как все столбцы матрицы H различны (в F_2 это эквивалентно линейной независимости двух векторов).

Заметим также, что первый, второй и четвертый столбцы матрицы H линейно зависимы

$$\begin{matrix} 0 \\ 1 \\ 0 \\ 1 \end{matrix} + \begin{matrix} 0 \\ 0 \\ 1 \\ 0 \end{matrix} + \begin{matrix} 0 \\ 1 \\ 1 \\ 1 \end{matrix} = \begin{matrix} 0 \\ 0 \\ 0 \\ 0 \end{matrix}$$

Поэтому d = 3

4 Построить порождающую матрицу

Приведём матрицу H тривиальными преобразованиями (сменой строк и заменой строки её линейной комбинацией с другими строками) к виду $(P^T I_r)$

Исходная матрица:

$$\begin{matrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \end{matrix}$$

Меняем 3 и 4 строки местами

$$\begin{matrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \end{matrix}$$

Заменяем вторую строку на линейную комбинацию второй и четвёртой

$$\begin{matrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \end{matrix}$$

Заменяем первую строку на линейную комбинацию первой и четвёртой

$$\begin{matrix} 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \end{matrix}$$

Заменим вторую строку на линейную комбинацию второй и третьей.

$$\begin{matrix} 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \end{matrix}$$

Заменим первую строку на линейную комбинацию первой и третьей

$$\begin{matrix} 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \end{matrix}$$

Заменим четвёртую строку на линейную комбинацию первой и четвёртой

$$\begin{matrix} 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \end{matrix}$$

Заменим четвёртую строку на линейную комбинацию второй и четвёртой

$$\begin{matrix} 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{matrix}$$

Тогда

$$P^T = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 \end{pmatrix}$$

Тогда $P = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \end{pmatrix}$

Тогда $G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}$

Проведём проверку:

```
g = [
        [1, 0, 0, 0, 0, 0, 1, 0, 1, 1],
        [0, 1, 0, 0, 0, 0, 1, 1, 0, 1],
        [0, 0, 1, 0, 0, 0, 0, 1, 0, 1],
        [0, 0, 0, 1, 0, 0, 0, 1, 1, 0],
        [0, 0, 0, 0, 1, 0, 1, 1, 0, 0],
        [0, 0, 0, 0, 0, 1, 1, 1, 1, 0]
]
```

```
def transpose(matrix):
        n = len(matrix)
        m = len(matrix[0])
        transposed = [[None for _ in range(n)] for _ in range(m)]

        for i in range(n):
                for j in range(m):
                        transposed[j][i] = matrix[i][j]
        return transposed


h = [
        [0, 0, 0, 0, 1, 0, 0, 1, 1, 1],
        [1, 0, 1, 1, 1, 0, 1, 0, 1, 1],
        [0, 1, 0, 1, 0, 0, 1, 1, 0, 1],
        [1, 0, 0, 1, 0, 1, 0, 0, 1, 0]
]

h_t = transpose(h)

n = len(g)
m = len(g[0])
assert m == len(h_t)
k = len(h_t[0])


result = [[0 for _ in range(k)] for _ in range(n)]

for i in range(n):
        for j in range(k):
                for z in range(m):
                        result[i][j] += g[i][z] * h_t[z][j]
                        result[i][j] %= 2

print(result)
# [[0, 0, 0, 0], [0, 0, 0, 0], [0, 0, 0, 0],
  [0, 0, 0, 0], [0, 0, 0, 0], [0, 0, 0, 0]]
```

Проверка показывает, что $G \cdot H^T = 0$

5 Закодировать произвольное сообщение

Пусть

$m = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$

Тогда $c = m \cdot G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}$

Тогда $c = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}$