Задание 1: Расширенный код Хэмминга 8,4)

1. Исходная проверочная матрица для кода Хэмминга 7,4)

Выберем стандартную проверочную матрицу $H_{(7,4)}$ где столбцы — это все ненулевые двоичные числа от 1 до 7:

$$H_{(7,4)} = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

2. Построение проверочной матрицы для расширенного кода 8,4)

Чтобы получить расширенный код, нужно:

1. Добавить к $H_{(7,4)}$ слева столбец из всех нулей
2. Добавить снизу строку из всех единиц

Получаем матрицу $H_{(8,4)}$:

$$H_{(8,4)} = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

3. Приведение к систематическому виду $H_{sys} = [P^T|I]$

Выполнив преобразования:

- Поменять строки местами
- Прибавить 4-ю строку к 1-й и 2-й

$$H_{sys} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

4. Нахождение порождающей матрицы G

Порождающая матрица G размера $4 * 8$ удовлетворяет условию $G \cdot H^T = 0$.

Решив систему $H \cdot c^T = 0$, получаем следующий вид порождающей матрицы

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

**5. Минимальное расстояние кода d_{min}

Для линейных кодов минимальное расстояние равно минимальному весу ненулевого кодового слова. Также известно, что d_{min} равно минимальному числу линейно зависимых столбцов проверочной матрицы H . В матрице $H_{(8,4)}$ минимальное число линейно зависимых столбцов равно 4 например, столбцы $(1, 2, 3, 8)$. Следовательно, $d_{min} = 4$.

6. Таблица кодовых слов

№	ИС	КС биты	Вес	Расстояния до др. слов
0	0000	0000 0000	0	4,4,4,4,4,4,4,4,4,4,4,4,4,4,8
1	1000	1000 1110	4	4,4,4,4,4,4,4,4,4,4,4,4,4,8
2	0100	0100 1101	4	4,4,4,4,4,4,4,4,4,4,4,4,8
3	1100	1100 0011	4	4,4,4,4,4,4,4,4,4,4,8,4
4	0010	0010 1011	4	4,4,4,4,4,4,4,4,4,8,4
5	1010	1010 0101	4	4,4,4,4,4,4,4,4,8,4
6	0110	0110 0110	4	4,4,4,4,4,4,8,4,4
7	1110	1110 1000	4	4,4,4,4,8,4,4,4

№	ИС	КС биты	Вес	Расстояния до др. слов
8	0001	0001 0111	4	4,4,4,8,4,4,4
9	1001	1001 1001	4	4,4,8,4,4,4
10	0101	0101 1010	4	4,8,4,4,4
11	1101	1101 0100	4	8,4,4,4
12	0011	0011 1100	4	4,4,4
13	1011	1011 0010	4	4,4
14	0111	0111 0001	4	4
15	1111	1111 1111	8	-

Вывод: Все ненулевые кодовые слова имеют вес 4 кроме слова из одних единиц, весом 8. Следовательно, минимальное расстояние кода $d_{min} = 4$.

Задание 2: Дуальный код коду Хэмминга — симплексный код

Утверждение: Код, дуальный коду Хэмминга, является симплексным кодом, то есть расстояние между любыми двумя кодовыми словами одинаково и равно 2^{r-1} .

Доказательство:

1. **Параметры кодов:**
   - Исходный код Хэмминга имеет длину $n = 2^r - 1$ и размерность $k = 2^r - 1 - r$.
   - Дуальный код обозначим его $C^\perp$ будет иметь параметры: длина $n = 2^r - 1$, размерность $n - k = r$.
2. **Свойство линейности:** Так как код линейный, расстояние между двумя различными кодовыми словами c_1 и c_2 равно весу их разности: $d(c_1, c_2) = (wc_1 + c_2)$. Так как сумма двух кодовых слов также является кодовым словом в силу линейности), то для доказательства достаточно показать, что **вес любого ненулевого кодового слова** в дуальном коде постоянен и равен 2^{r-1} .
3. **Связь с порождающей матрицей:** Порождающая матрица дуального кода — это проверочная матрица H исходного кода Хэмминга размером $r \times 2^r - 1$. Столбцами H являются все возможные ненулевые двоичные векторы длины r . Любое кодовое слово $c \in C^\perp$ является линейной комбинацией строк H . То есть $c = m \cdot H$, где m — ненулевой информационный вектор длины r .
4. **Вычисление веса:** Значение j -го символа кодового слова c вычисляется как скалярное произведение информационного вектора m на j -й столбец матрицы H : $c_j = m \cdot h_j$ по модулю 2.
   - h_j пробегает все $2^r - 1$ ненулевых r-битных векторов.
   - Зафиксируем ненулевой вектор m . Рассмотрим линейную функцию $f_m(x) = m \cdot x$, где x — вектор из $\mathbb{F}_2^r$.
   - Множество всех 2^r векторов x включая нулевой) разбивается на две равные части: ровно половина из них 2^{r-1} штук) дают скалярное произведение 0, и ровно половина 2^{r-1} штук) дают скалярное произведение 1.
   - Столбцы h_j — это все ненулевые векторы. Следовательно, среди них ровно 2^{r-1} векторов дают $m \cdot h_j = 1, u2^{r-1} - 1$ векторов дают $m \cdot h_j = 0$. Добавим к рассмотрению формально нулевой столбец? В H его нет. Но так как нулевой вектор которого нет в H) дал бы 0, то количество единиц в кодовом слове c равно 2^{r-1} . Вес кодового слова $(wc) = 2^{r-1}$.
5. **Вывод:** Вес любого ненулевого кодового слова в дуальном к Хэммингу коде постоянен и равен 2^{r-1} . Следовательно, расстояние между любыми двумя различными кодовыми словами также равно 2^{r-1} . Это и есть определение симплексного кода.

Задание 3: Дуальный код к коду с проверкой на четность

Постановка: Пусть исходный код — это код с проверкой на четность длины n .

Решение:

1. **Характеристики исходного кода:**
   - Код с проверкой на четность длины n имеет размерность k = n - 1 . Обозначим его (n, n-1) .
   - Он состоит из всех векторов длины n , у которых сумма битов четна.
2. **Характеристики дуального кода:**
   - Параметры дуального кода: длина n остается той же, а размерность становится $n - k = n - n - 1) = 1.$

- Следовательно, дуальный код — это (n, 1) код с повторением.

3. **Порождающая и проверочная матрицы:**
   - Порождающая матрица G_{dual} дуального кода — это проверочная матрица H исходного кода.
   - Проверочная матрица исходного кода с проверкой на четность состоит из одной строки единиц: H = [1, 1, ..., 1] .
   - Следовательно, порождающая матрица дуального кода:

$$G_{\text{dual}} = [1 \quad 1 \quad 1 \quad \dots \quad 1]$$

   - Это матрица размера 1 times n .
4. **Количество кодовых слов:**
   - Размерность дуального кода $k_{\text{dual}} = 1$. Значит, количество кодовых слов равно $2^{k_{\text{dual}}} = 2^1 = 2$.
   - Это слова: $\mathbf{0} = (00..0)$ $\mathbf{1} = (11..1)$.
5. **Корректирующая способность:**
   - Минимальное расстояние кода d_{min} равно расстоянию между двумя единственными ненулевыми словами: $d_{min} = w(1) = n$.
   - Код может гарантированно исправлять t ошибок, где

$$t = \left\lfloor \frac{d_{min} - 1}{2} \right\rfloor = \left\lfloor \frac{n - 1}{2} \right\rfloor$$

Ответ:

- Характеристики дуального кода: (n, 1) .
- Количество кодовых слов: **2**.
- Код может гарантированно исправить $\lfloor \frac{n-1}{2} \rfloor$ ошибок.