Лекция 2

Оформила: Балакшина А.Д. 5030102/20101

21 февраля 2026 г.

Код - это набор кодовых слов.
Эффективный код:

- длинный (n), то есть большое минимальное расстояние
- - сложности кодера и декодера

Чтобы уменьшить сложность можно рассмотреть линейные коды, где для нахождения КС нужно только умножить ИС на порождающую матрицу.

1 Какова размерность линейного пространства проверок H?

$$G \cdot H^T = 0$$

$G_{k \times n}$ - k линейно-независимых строк
Ранг = k
В матрице G существует k линейно-независимых столбцов
Зафиксируем лин.-незав. столбцы. Их индексы образуют **информационную совокупность**. Остальные индексы столбцов образуют **проверочную совокупность**. Соответствующие символы называются информационными/проверочными.
Примем, что первые k столбцов - информационные.

$$G \cdot h^T = \begin{pmatrix} g_{1,1} & g_{1,2} & \dots & g_{1,k} & g_{1,k+1} & \dots & g_{1,n} \\ g_{2,1} & g_{2,2} & \dots & g_{2,k} & g_{2,k+1} & \dots & g_{2,n} \\ \dots & & & & & & \\ g_{k,1} & g_{k,2} & \dots & g_{k,k} & g_{k,k+1} & \dots & g_{k,n} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ \dots \\ x_k \\ h_{k+1} \\ \dots \\ h_n \end{pmatrix}$$

На позициях $h_{k+1}, ..., h_n$ - зафиксируем
Хотим найти $x_1, ..., x_k$ такие, чтобы равенство выполнялось

$$\vec{g_i} = \begin{pmatrix} g_{1,i} \\ g_{2,i} \\ \dots \\ g_{k,i} \end{pmatrix}$$

$$\vec{g_1} \cdot x_1 + \vec{g_2} \cdot x_2 + ... + \vec{g_k} \cdot x_k + \vec{g_{k+1}} \cdot h_{k+1} + ...\vec{g_n} \cdot h_n = \vec{0}$$

$$\vec{g_1} \cdot x_1 + \vec{g_2} \cdot x_2 + ... + \vec{g_k} \cdot x_k = -(\vec{g_{k+1}} \cdot h_{k+1} + ...\vec{g_n} \cdot h_n)$$

$$\begin{pmatrix} g_{1,1} & g_{1,2} & \dots & g_{1,k} \\ g_{2,1} & g_{2,2} & \dots & g_{2,k} \\ \dots & & & \\ g_{k,1} & g_{k,2} & \dots & g_{k,k} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ \dots \\ x_k \end{pmatrix} = -(\vec{g_{k+1}} \cdot h_{k+1} + ...\vec{g_n} \cdot h_n)$$

У матрицы слева столбцы линейно-независимы (т.к. ранг k). Тогда $det \neq 0$ и можем найти единственное решение. Существует 2^{n-k} способов задать вектор $(h_{k+1}, ..., h_n)$. Для каждого находим свою последовательность x. Тогда размерность пространства H: $(n-k)n$
Избыточность кода: $r = n - k$

2 Как найти матрицу проверок по порождающей и наоборот?

Пусть есть G. Можем применять к ней операции, в результате будут получаться разные коды, но они будут **эквивалентными**.
Например, **систематический вид**: $G_{kn} = \begin{bmatrix} I_{kk} & P \end{bmatrix}$

$$c = m \cdot G = (m\ m \cdot P)$$

На первых k позициях будут информационные символы.

Для систематического вида матрица $H = (P^T\ I_{rr})$

3 Как найти минимальное расстояние быстрее?

$d_{min} = min_{m \neq 0} \omega(m \cdot G)$ Чтобы найти минимальное расстояние по этой формуле, нужно перебрать $2^k - 1$ кодовых слов.
Пусть есть (n, k), $R > \frac{1}{2}$. Тогда $n - k < k$.

$$\omega(C) = 3$$

$$c = (1...0...1...1...0)$$

Столбцы H - линейно зависимы. Тогда слово с минимальным весом - слово с минимальным количеством единиц. **Чтобы найти минимальное расстояние кода, нужно найти минимальный набор линейно зависимых столбцов матрицы H**.

Теорема: Мин. расстояние линейного (n, k)-кода равно d в том и только в том случае, когда любые d-1 столбец проверочной матрицы линейно независимы и существует набор из d линейно зависимых столбцов.

Сколько в матрице H лин.-независ. столбцов? **n-k**
Теорема: граница Синглтона: мин. расстояние линейного (n, k) кода удовлетворяет нер-ву $d <= n - k + 1$.

4 Дуальный код

Дуальный код - код, порождающая матрица которого является проверочной матрицей данного кода.

5 Код с проверкой на чётность

(n, n-1) - код $H = (1, ..., 1)$

$$G = \begin{pmatrix} I_{n-1n-1} & \text{единич. столбец} \end{pmatrix}$$

Все кодовые слова имеют чётный вес. Моежт обнаружить любые ошибки нечётного веса.

6 Код, который исправляет любые одиночные ошибки

$$m, c = m \cdot G, c + e, \omega(e) = 1$$

$$(c + e) \cdot H^T = c \cdot H^T + e \cdot H^T = e \cdot H^T = \vec{h_j}$$

Значит, ошибка произошла на позиции j.
Можно так построить матрицу H, чтобы этот столбец сразу задавал позицию - **коды Хэмминга**.(7, 4)

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

Двоичные коды Хэмминга оптимальны в том смысле, что не существ. кодов (даже нелинейных) с большим числом кодовых слов с расстоянием 3 при такой же длине.

В строках матрицы H всегда одинаковое число единиц - $r-1$.

В дуальном коде к коду Хэмминга $d = 2^{r-1}$. Это **симплексный код**.

Расширенный код Хэмминга: добавляем слева нулевой столбец, и вниз - единичную строку.

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

(8, 4)

$n = 2^{r-1}$

Дуальный код к расширенному коду Хэмминга - **код Рида-Маллера первого порядка**