Код — это набор кодовых слов.

Эффект кода:

- длина $n \to$ большое минимальное расстояние;
- асимптотика, корреляция, иерархия.

Линейный код задаётся порождающей матрицей G:

$$\vec{c} = \vec{m} \cdot G.$$

Порождающая матрица линейного (n, k)-кода — матрица размером $k \times n$, строки которой являются базисными векторами линейного подпространства размерности k над GF(2).

Кодовые слова — линейные комбинации базисных векторов.

$$\vec{m} = (m_1, \ldots, m_k), \qquad \vec{c} = \vec{m} \cdot G.$$

Пусть проверочный вектор

$$\vec{h} = (h_1, \ldots, h_n).$$

Тогда для любого кодового слова $\vec{c}_i \in C$:

$$\vec{c}_i \cdot \vec{h} = 0,$$

то есть

$$c_1 h_1 + c_2 h_2 + \cdots + c_n h_n = 0.$$

Проверка ортогональности:

$$G \cdot \vec{h}^T = 0, \qquad (k \times n) \cdot (n \times 1) = (k \times 1).$$

Каждый кодовый вектор ортогонален проверочному вектору.

$$G \in \mathbb{F}_2^{k \times n}, \qquad \operatorname{rank}(G) = k.$$

Матрица G состоит из k линейно независимых строк (базис подпространства кода). Столбцы матрицы G задают ортогональное подпространство по отношению к проверочной матрице.

$$G \cdot \vec{h}^T = 0$$

(матрица умножения, показывающая ортогональность).

$$\vec{h} = (h_1, \ldots, h_n)$$

— проверочный вектор.

Пусть проверочная часть состоит из компонент $h_{k+1}, \ldots, h_n$.

Если

$$\vec{c} = (q_1, q_2, \ldots, q_k),$$

то условие проверки имеет вид:

$$\sum_{i=1}^{k} q_i x_i + \sum_{j=1}^{n-k} q_{k+j} h_{k+j} = 0.$$

Работа ведётся над полем GF(2) (определитель $\neq 0$ означает невырожденность матрицы).

Пусть $r = n - k$ — избыточность кода.

Тогда проверочная матрица

$$H \in \mathbb{F}_2^{(n-k)\times n}.$$

Связь между матрицами:

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

Систематический вид:

$$G_{k\times n} = \begin{bmatrix} I_k & P \end{bmatrix} \quad \text{или} \quad \begin{bmatrix} P & I_k \end{bmatrix}.$$

$$H = \begin{bmatrix} P^T & I_{n-k} \end{bmatrix}.$$

Пример порождающей матрицы:

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

(и другие систематические формы G и H).

$$H_{\text{sys}} = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}, \qquad d_{\min} = \min_{m \neq 0} \omega(m \cdot G),$$

где $\omega(\cdot)$ — вес Хэмминга.

$$\vec{c} = \vec{m} \cdot G.$$

Пример проверочной матрицы:

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

$$R = \frac{k}{n} = \frac{1}{2}, \qquad n - k < k.$$

Если $\vec{c} \cdot H^T = 0$ и $\omega(\vec{c}) = 3$, то

$$\vec{c} = (1, \ldots, 0, \ldots, 1, \ldots, 1, \ldots, 0).$$

Чтобы найти $d_{\min}$, необходимо найти минимальное число d линейно зависимых столбцов матрицы H.

Теорема. Минимальное расстояние линейного (n, k)-кода равно d тогда и только тогда, когда любой набор из $d-1$ столбцов матрицы H линейно независим, а некоторый набор из d столбцов — линейно зависим.

Теорема Синглтона. Минимальное расстояние кода (n, k) удовлетворяет неравенству

$$d \leq n - k + 1.$$

(Также известна теорема Грайсмера.)

Дуальный код — код, порождающая матрица которого является проверочной матрицей исходного кода (и наоборот):

$$G_1 \cdot H_1^T = 0, \qquad G_2 = H_1, \qquad H_2 = G_1.$$

Пример $(n, n-1)$-кода:

$$H = (1, 1, \ldots, 1).$$

Любое кодовое слово имеет чётный вес. Это код с проверкой на чётность — обнаруживает одиночную ошибку.

Строгий код, исправляющий и обнаруживающий ошибки.

Пусть

$$\vec{c} = \vec{m}, \qquad \vec{r} = \vec{c} + \vec{e}.$$

Тогда синдром:

$$\vec{r}H^T = (\vec{c} + \vec{e})H^T = \vec{c}H^T + \vec{e}H^T = \vec{e}H^T = \vec{h}_j.$$

$$\begin{bmatrix} 0 & \ldots & 0 & h_j & 0 & \ldots & 0 \end{bmatrix} = \vec{h}_j.$$

Параметры:

$$n = 2^m - 1, \qquad k = 2^m - 1 - m, \qquad r = m.$$

Код Хэмминга.

Для двоичного кода Хэмминга:

$$d = 3.$$

Код Хэмминга является совершенным кодом (исправляет одну ошибку и достигает границы Хэмминга).

Дуальный код кода Хэмминга также называется кодом Хэмминга в двойственном пространстве.

Расширенный код Хэмминга.

Расширенный код Хэмминга $(7, 4)$ даёт код $(8, 4)$ (код Расса–Хэмминга), в котором добавлен бит общей чётности.

Пример матрицы $(7, 4)$-кода:

$$\begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Код с минимальным расстоянием $d = 3$.