

## 1 Общие слова о линейных кодах

Пусть задано подмножество  $\mathfrak{K} \subset V_n$  множества двоичных векторов длины  $n$ , называемое кодом и пусть задана матрица  $H$ .

**Определение:**  $(n, k)$ -кодом называется код со словами длиной  $n$  в каждом из которых содержится  $k$  информационных символов.

**Определение:** Линейным называется код, каждый вектор которого удовлетворяет уравнению  $Hc^t = 0$ . Матрица  $H$  называется проверочной матрицей кода  $\mathfrak{K}$ .

**Определение:** Код называется групповым, если множество его слов образует группу.

Очевидно, что каждый линейный код является групповым (более того, множество его слов образует подпространство в пространстве  $V_n$ ).

**Примеры:**

1. Рассмотрим код с повторением.  $\mathfrak{K} = \{(c_1, c_2, \dots, c_n) | c_1 = c_i, i = 1 \dots n\}$   
Его проверочной матрицей будет

$$H = \begin{pmatrix} 1 & 1 & 0 & \dots & 0 \\ 1 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & \dots & 1 \end{pmatrix}$$

2. Код с проверкой на четность.  $\mathfrak{K} = \{(c_1, c_2, \dots, c_n) | c_n = \sum_{i=1}^{n-1} c_i\}$  Проверочная матрица:

$$H = (1, 1, \dots, 1)$$

**Определение:** Будем говорить что проверочная матрица записана в каноническом виде если  $H = (A | -I)$ , где  $I$  – единичная матрица

В случае когда проверочная матрица записана в каноническом виде очень просто отделить информационные и проверочные символы: первые  $k$  – информационные, остальные – проверочные.

Пусть  $u = (\alpha_1, \alpha_2, \dots, \alpha_k)$  – исходное информационное слово. Тогда

$$c^t = \begin{pmatrix} I \\ -A \end{pmatrix} u^t$$

Транспонировав равенство получим  $c = uG$ , где  $G = (I | -A^t)$ . Матрица  $G$  называется порождающей матрицей. Из полученного результата сразу вытекает следующий результат Матрицы  $G$  и  $H$  связаны соотношением  $HG^t = 0$ .

На самом деле матрица  $G$  иметь такой вид не обязана. Это справедливо для кодов с матрицей  $H$  в каноническом виде, то есть для систематических кодов.

Есть более общий способ получить матрицу  $G$ .

Посмотрим на равенство  $Hc^t = 0$  как на однородную систему линейных уравнений. Посмотрим базис решений этой системы, пусть это будут  $\{e_1, e_2, \dots, e_k\}$ . Тогда любой вектор  $c$  мы сможем записать как линейную комбинацию этих векторов  $c = \sum_{i=1}^k \alpha_i e_i$ , где  $\alpha_i \in \mathbb{Z}_2$ . Далее запишем найденные решения в строки матрицы  $G$ . Таким образом получим порождающую матрицу.

Заметим, что раз строки матрицы  $G$  есть ничто иное как решение уравнения  $Hc^t = 0$ , то получаем следующую теорему:

**Теорема:** Матрицы  $H$  и  $G$  связаны соотношением  $HG^t = 0$ .

## 2 Как определять и корректировать ошибки

Перед тем как идти дальше следует сделать несколько замечаний. Во-первых, имея информационное слово длины  $k$  мы не можем просто так выбрать кодирующую матрицу  $G$ .

Чтобы декодировать принятое сообщение  $c$ , формально, нам нужно найти его прообраз, а это ничто иное как решение системы уравнений  $uG = c$ . Это значит что  $\text{rank } G = k$ . Аналогично,  $\text{rank } H = n - k$ .

**Теорема:** Пусть код  $\mathfrak{K}$  имеет минимальное расстояние  $\geq d \Leftrightarrow$  любые  $d - 1$  столбцов матрицы  $H$  линейно независимы.

**Доказательство:**  $\square \Rightarrow$  Заметим что минимальное расстояние линейного кода равно минимальному весу его ненулевого слова.

Пусть  $w(\mathfrak{K}) = d$ , и пусть  $c = (\alpha_1, \alpha_2, \dots, \alpha_n) \in \mathfrak{K}$  – кодовое слово и  $H = (h_1, h_2, \dots, h_n)$  – проверочная матрица кода ( $h_i$  – столбцы  $H$ ). Из соотношения  $Hc^t = 0$  имеем  $\alpha_1 h_1 + \alpha_2 h_2 + \dots + \alpha_n h_n = 0$ . Пусть  $w(c) = d$ . Тогда существует ровно  $d$  линейно зависимых столбцов проверочной матрицы.

Пусть теперь известно что  $t$  столбцов матрицы  $H$  линейно независимы, то есть справедливо равенство

$$\varepsilon_{i_1} h_{i_1} + \varepsilon_{i_2} h_{i_2} + \dots + \varepsilon_{i_t} h_{i_t} = 0.$$

Это значит что существует вектор  $x$  такой что на позициях  $i_j, j = 1 \dots t$  у него стоят 1, а на других 0.

Значит для такого вектора  $x$  справедливо равенство  $Hx^t = 0$ , тогда, с учетом того что  $w(\mathfrak{K}) = d$ , получаем  $t \geq d$ . Следовательно любые  $d - 1$  столбцов матрицы  $H$  линейно независимы.

$\Leftarrow$  Обратно, пусть любые  $d - 1$  столбцов  $H$  – линейно независимы, тогда если  $c \in \mathfrak{K}$ , то  $w(c) \geq d$ . ■