

Повторение

Код - набор кодовых символов

Эффективный код:

- длинные (n) \Rightarrow большое минимальное расстояние
- сложности кодера и декодера

Линейные коды $\Rightarrow G \cdot m^*G = C$

Порождающая матрица линейного (n, k) кода - матрица размера $k * n$, строки - базисные вектора лин. пространства

Кодовые слова - лин. комбинации базисных векторов

$$\vec{m} = (m_1, \dots, m_k) \quad c = m * G$$

$$\vec{c} = (c_1, \dots, c_n)$$

$$\vec{h} = (h_1, \dots, h_n) - \text{проверка } c \text{ from } C \quad (c, h)$$

$$G * h^T = 0$$

$$(k * n) * (1 * n)^T = (k * n) * (n * 1) = (k * 1)$$

Размерность линейного пространства проверок

$$H : G * H^T = 0$$

G матрица размера $k * n$

k - лин. нез. строк

$\text{rank } G = k \Rightarrow$ в матрице G **k лин. нез. столбцов**

индексы лин. нез. столбцов образуют **информационную совокупность**

индексы лин. завис. столбцов образуют **проверочную совокупность**

$$G * h^T = (g_{11} \ g_{12} \ g_{1k} \ g_{1k+1} \ g_{1n})$$

$$(g_{21} \ g_{22} \ g_{2k} \ g_{1k+1} \ g_{2n}) * (x_1 \ x_k \ h_k \ h_{k+1} \ h_n)$$

$$(g_{k1} \ g_{k2} \ g_{kk} \ g_{1k+1} \ g_{kn})$$

[1, k] столбцы - информационная совокупность

[k + 1, n] столбцы - проверочная совокупность

в h^T зафиксируем (h_{k+1}, \dots, h_n)

найдем (x_1, \dots, x_k) , чтобы $G * h^T = 0$

$$\vec{g}_i = (g_{1i} \ g_{2i} \ \dots \ g_{ki})$$

$$\vec{g}_1 * x_1 + \vec{g}_2 * x_2 + \dots + \vec{g}_n * h_n = 0$$

$$\vec{g}_1 * x_1 + \vec{g}_2 * x_2 \dots = -(\dots + \vec{g}_n * h_n)$$

$$(g_{11} \ g_{12} \ g_{1k})$$

$$(g_{21} \ g_{22} \ g_{2k}) * (x_1, \dots, x_k) = -(\dots + \vec{g}_n * h_n)$$

$$(g_{k1} \ g_{k2} \ g_{kk})$$

можно найти единственное решение в терминах (x_1, \dots, x_k)

$$H = (n - k) * n$$

$r = n - k$ - избыточность кода

Систематический вид

эквивалентное представление $G_{k*n} = [I_{k*k} \ P]$ - **систематический вид**

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

$$H = (P^T \ I_r)$$

исходная матрица

Лекция 2

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

переставим местами столбцы, получаем систематический вид

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

P транспонируется и получается первая часть матрицы H систематическая

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

обратное преобразование

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

$$d_{min} = \min w(m * G)$$

всего ненулевых двоичных кодовых слов $2^k - 1$

столбцы матрицы H линейно зависимы

чтобы найти мин расстояние надо найти минимальный набор линейно зависимых столбцов матрицы H

теорема 1

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

сколько в матрице H линейно независимых столбцов?

$$\text{rank } H = n - k$$

теорема 2

минимальное расстояние линейного (n, k) кода удовлетворяет неравенству $d \leq n - k + 1$

Дуальный код

дуальный код к данному коду - это код порождающая матрица, которого является проверочной матрицей данного кода

$$G_1 * H_2^T = 0$$

$$G_2 = H_1$$

$$H_2 = G_1$$

пример

($n, n - 1$)-код

$H = (1, \dots, 1)$ - размерность $(1, n)$

$$G = (I_{n-1} * (1 \dots 1))$$

$d_{min} = 2$ (в каждой строке две единицы)

это код с проверкой на четность: любое кодовое слово имеет четный вес, может обнаружить любые ошибки нечетного веса

Кода Хэмминга

строим код который исправляет любые одиночные ошибки

$$m c = m * G c + e w(e) = 1$$

$$\vec{e} = (0, 0, 1, 0, 0) - \text{ошибка}$$

$$(c + e) * H^T = c * H^T + e * H^T = e * H^T = h_j$$

$$k = n - r = 2^r - 1 - r$$

$$n = 2^r - 1$$

семейство таких кодов называют кодами Хэмминга

Симплексный код

двоичные коды Хэмминга оптимальны в том смысле, что не существует кодов (даже нелинейных) с большим числом код слов с расстоянием $d = 3$ при такой же длине

$$G = H_{\text{хэм}}$$

для дуальных кодов кодам Хэмминга $d = 2^{r-1}$ - **симплексный код**

Расширенный код Хэмминга

в H добавляется нулевой столбец вначале и строка из всех единиц снизу

если код Хэмминга был (n, k) , то расширенный код будет $(n + 1, k)$

$$n = 2^{r-1}$$

$$r = 2^{r-1} - k$$

дуальный код к расширенным кодам Хэмминга - **код Рида-Маллера 1го порядка**