~~II = пр...~~

Код - набор кодовых слов

Эффективные коды

- длинные (n) → большое мин. расстояние
- сложности кодера и декодера

Линейные коды → $G$ $\qquad m \cdot G = C$

Порожд. матрица линейного $(n,k)$-кода

матрица $k \times n$, строки - базисные в-ра линейн. п-ва

Кодовые слова - линейные комб-ии базис. векторов

$\vec{m} = (\underbrace{m_1, \dots, m_k}_{k})$ $\qquad \vec{c} = \vec{m} \cdot G$

$(\underbrace{c_1, \dots, c_n}_{n})$

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

$\vec{c} \in C$ $\qquad (\vec{c}, \vec{h}) = 0 = c_1 h_1 + c_2 h_2 + \dots c_n h_n = 0$

проверка

$G \cdot h^T = 0 \qquad k \times n \cdot (1 \cdot n)^T = k \times n \cdot n \times 1 = k \times 1$

Какова размерн-ть лин пр-ва проверки

$G : k \times n$ → $k$ лин. нез-х строк

$\mathrm{rank}\ G = k \Rightarrow$ в матр $G$ $\exists\, k$ лин нез-х столбцов

Индексы лн столбцов образуют инфор-ю совокуп-ть, остальные индексы образуют проверочную совокупность

$$G\cdot h^T = \left(\underbrace{\begin{matrix} g_{1,1} & g_{1,2} & \dots & g_{1,k} \\ g_{2,1} & g_{2,2} & \dots & g_{2,k} \\ \vdots & \vdots & & \\ g_{k,1} & g_{k,2} & \dots & g_{k,k} \end{matrix}}_{\text{информ}} \; \underbrace{\begin{matrix} g_{1,k+1} & \dots & g_{1,n} \\ g_{2,k+1} & \dots & g_{2,n} \\ & & \\ g_{k,k+1} & \dots & g_{k,n} \end{matrix}}_{\text{проверочн}}\right) \begin{pmatrix} x_1 \\ \vdots \\ x_k \\ h_{k+1} \\ \vdots \\ h_n \end{pmatrix}$$

$h_{k+1} \dots h_n$ – фиксируем

Находим $x_1 \dots x_k$ чтобы $Gh^T = 0$

$$\vec{g}_i = \begin{pmatrix} g_{1i} \\ g_{2i} \\ \vdots \\ g_{ki} \end{pmatrix}; \quad \vec{g}_1 x_1 + \vec{g}_2 x_2 + \dots + \vec{g}_k x_k + \vec{g}_{k+1} h_{k+1} + \dots$$

$$+ \vec{g}_n h_n = 0$$

$$\vec{g}_1 x_1 + \vec{g}_2 x_2 + \dots + \vec{g}_k x_k = -(\vec{g}_{k+1} h_{k+1} + \dots + \vec{g}_n h_n)$$

$$\underbrace{\begin{pmatrix} g_{11} & g_{12} & \dots & g_{1k} \\ \vdots & & & \\ g_{k1} & g_{k2} & \dots & g_{kk} \end{pmatrix}}_{\det \neq 0} \begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix} = -(\vec{g}_{k+1} h_{k+1} + \dots + \vec{g}_n h_n)$$

таким образом можем найти ед-ное решение $(x_1 \dots x_n)$

$2^{n-k}$ векторов $h_{k+1}, \dots, h_n$

Размерность $H$ и подпр-ва $n-k$

$r = n-k$ – избыточность кода

$G \cdot H^T = 0$

$G_{k\times n} = [I_{k\times k} \; P]$ – систематический вид

$$C = mG = (\underbrace{m}_{k} \;\; \underbrace{m \cdot P}_{r = n-k})$$

$$H = (P^T \; I_k)$$

Пример

$$G = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \xrightarrow{F} G_{sys} = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

$$H = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} \xleftarrow{F^{-1}} H_{sys} = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

$C = m \cdot G$

$$d_{min} = \min_{m \neq 0} \omega(m \cdot G)$$

$2^k - 1$ слов

$(n,k)$ код $\quad R = \frac{k}{n} > \frac{1}{2} \quad n-k < k$

$CH^T = 0$ столбцы $H$ лин. зависимы

Чтобы найти $d_{min}$ → найти мин набор л.з. столбцов матрицы $H$.

Теорема

Минимальное расстояние лин. $(n,k)$ кода в том и только том случае, когда $\forall$ $d-1$ столбец $H$ лин. нез. и $\exists$ набор из $d$ лин. з. столбцов

В $H$ $n-k$ лин. нез. столбцов

Теорема Граница Синглтона

Мин. расст-е лин $(n,k)$ кода удовл-т нер-ву $d \leq n-k+1$.

Дуальный код к данному коду — код, порождающая матрица которого является проверочной матрицей данного кода.

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

Примеры кодов

$(n, n-1)$ - код $\qquad H = (1 \dots 1)$

$G = \left( I_{n-1, n-1} \begin{matrix} 1 \\ \vdots \\ 1 \end{matrix} \right)$ Любое кодово слово имеет четный вес

Код с проверкой на четность обнар $\forall$ ошибки нечетного веса

Строим код, который испр $\forall$ единичные ошибки

$m,\ c = m \cdot G, \quad c + e^{k} \quad w(e) = 1$

$(c+e) \cdot H^T = \underset{0}{\underset{\shortparallel}{cH^T}} + eH^T = eH^T = e\, H^T = h_j^T$

$[0 \dots 0 1 0 \dots 0]$

$k = 2^r - 1 - r$

$n = 2^r - 1 \qquad n - k = 3$

$$\begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{array}$$
$$\begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

$2^{r-1}$ единиц в $H$

Семейство ~~кодов~~ кодов Хэмминга

Двоич. коды Хэмм. оптим-ы в том смысле, что не сущ-ет кодов (даже нелинейных) с большим числом кодовых слов с расстоянием $d = 3$ при такой же длине

Для дуальных кодов кодам Хэмминга $d = 2^{r-1}$

Симплексный код — код, дуальный коду Хэмминга

Расширенный код Хэмминга: добавл "0" столбец и строка "1"

$$\begin{matrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{matrix}$$

$(n, k)$ - код Хэмм $(7, 4)$

$(8, 4)$ - Расшир код Хэмм.

Дуальный код к расшир. $2^{n-r}$ $\quad 2^{n-1} - r$

коды Хэмминга — код Рида-Маллера I-го порядка