Коды Хемминга и их построение

5 января 2023 г. 1:33

Коды Хемминга

Коды Хемминга это линейные коды, которые обеспечивают минимально возможное количество проверочных символов для минимального кодового расстояния $d = 3$. Рассмотрим метод построения порождающей и проверочной матрицы для систематического кода Хемминга над полем $GF(2)$.

Пусть порождающая матрица кода $\mathbf{G}$ представляется в левой канонической форме:

$$\mathbf{G} = [\mathbf{I}_k|\mathbf{G}_2], \tag{17}$$

где $\mathbf{I}_k$ – единичная подматрица размером $k \times k$ и $\mathbf{G}_2$ – подматрица размером $r \times k$.

Проверочная матрица $\mathbf{H}$ может быть записана как:

$$\mathbf{H} = [\mathbf{H}_1|\mathbf{H}_2], \tag{18}$$

где $\mathbf{H}_1$ – подматрица размером $r \times k$, $\mathbf{H}_2$ – подматрица размером $r \times r$.

$$\mathbf{0} = \mathbf{G} \cdot \mathbf{H}^T = [\mathbf{I}_k|\mathbf{G}_2] \begin{bmatrix} \mathbf{H}_1^T \\ \mathbf{H}_2^T \end{bmatrix} = \mathbf{H}_1^T + \mathbf{G}_2 \cdot \mathbf{H}_2^T. \tag{19}$$

Пусть проверочная матрица $\mathbf{H}$ представлена в правой канонической форме, то есть $\mathbf{H}_2^T$ – единичная подматрица. Тогда,

$$\mathbf{0} = \mathbf{H}_1^T + \mathbf{G}_2 \cdot \mathbf{H}_2^T = \mathbf{H}_1^T + \mathbf{G}_2. \tag{20}$$

С учетом работы в поле $GF(2)$, из (20) следует:

$$\mathbf{G}_2 = \mathbf{H}_1^T. \tag{21}$$

$0 = H_1^T + G_2 \Rightarrow G_2 = -H_1^T$

где минус?

Считаем по модулю 2: вычесть 1 всё равно, что прибавить 1

т.к. $GF(2)$

- Матрица $\mathbf{H}$ не должна содержать нулевых столбцов.
- Из Теоремы 2 следует, что для построения линейного кода с расстоянием $d = 3$ любые два столбца $\mathbf{H}$ должны быть линейно независимы. В случае $GF(2)$ это означает, что любые два столбца $\mathbf{H}$ должны быть различными (это возможно, когда $n = k + r \leq 2^r - 1$). При этом, матрица $\mathbf{H}$ должна быть записана в правой канонической форме, то есть содержать единичную подматрицу в правой части.

Построение кода Хемминга

Input.
Длина кодового слова n.
Длина информационной последовательности k.

Step 1.
$r := n - k$.
Сформировать $\mathbf{H}_1$ размером $r \times k$ из k различных столбцов, каждый из которых содержит больше одной единицы.

Step 2.
Сформировать $\mathbf{H}_2$ как единичную матрицу $r \times r$.
$\mathbf{H} := [\mathbf{H}_1|\mathbf{H}_2]$.

Step 3.
Сформировать $\mathbf{G}_1$ как единичную матрицу $k \times k$.
$\mathbf{G} := [\mathbf{G}_1|\mathbf{H}_1^T]$.

Пример. $n = 7$, $k = 4$. Скорость кода $R = \frac{k}{n} = \frac{4}{7}$.

$$\mathbf{H}_1 = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix},$$

$$\mathbf{H} = [\mathbf{H}_1|\mathbf{H}_2] = \left[\begin{array}{cccc|ccc} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{array}\right]$$

$$\mathbf{G} = [\mathbf{G}_1|\mathbf{H}_1^T] = \left[\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{array}\right]$$

$$\left[\begin{array}{cccc|ccc} 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right]$$