Расширенные коды Хемминга и их построение

5 января 2023 г. 1:33

- Расширенные коды Хемминга обеспечивают минимально возможное количество проверочных символов для минимального кодового расстояния $d = 4$.
- Увеличение минимального расстояние кода достигается путем замены одного информационного символа исходного кода Хемминга на проверочный символ.
- Поэтому проверочная матрица такого кода должна иметь на одну строку больше, чем в коде Хемминга.

- В соответствии с теоремой 2 в проверочной матрице расширенного кода Хемминга любые три столбца должны быть линейно независимые.
- В случае кода над полем $GF(2)$ это означает, что
  - любые два столбца матрицы $\mathbf{H}$ должны быть различны;
  - матрица $\mathbf{H}$ не должна содержать нулевого столбца;
  - любые два столбца в сумме не должны давать третий.

Обозначим через $\mathbf{H}^3$ проверочную матрицу кода Хемминга с минимальным расстоянием $d = 3$. Тогда матрица

$$\mathbf{H}^4 = \left[\begin{array}{ccccc} 1 & 1 & 1 & \dots & 1 \\ \hline & & & & \\ & & \mathbf{H}^3 & & \\ & & & & \end{array}\right] \qquad (22)$$

удовлетворяет приведенным выше требованиям для кода с минимальным расстоянием $d = 4$.

- Во-первых, матрица $\mathbf{H}^4$ не содержит двух одинаковых столбцов и не содержит нулевой столбец, поскольку в матрице $\mathbf{H}^3$ нет нулевых столбцов и все столбцы разные.
- Во-вторых, сумма по модулю 2 любых двух столбцов не равна никакому третьему столбцу, так как сумма двух столбцов будет содержать 0 в первом разряде, тогда как все столбцы в $\mathbf{H}^4$ в первом разряде равны 1.

- Для формирования порождающей матрицы расширенного кода Хемминга проверочную матрицу $\mathbf{H}^4$ необходимо представить в правой канонической форме.
- Так как строки матрицы $\mathbf{H}^4$ являют базисным векторами линейного пространства, то каждый базисный вектор можно заменить другим базисным вектором, который является линейного комбинацией исходных базисных векторов.
- В случае кодов над полем $GF(2)$ можно менять любую строку матрицы $\mathbf{H}^4$ на сумму двух или более строк по модулю 2 до тех пор, пока матрица $\mathbf{H}^4$ не примет правую каноническую форму.
- Затем, аналогично коду Хемминга можно построить порождающую матрицу.

Пример---

Требуется построить проверочную и порождающую матрицу расширенного кода Хемминга с длиной кодового слова $n = 7$ и информационной последовательностью длины $k = 3$. В соответствии с шагом 1 алгоритма формируется подматрица

$$\mathbf{H}_1^3 = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix},$$

затем в соответствии с шагом 2 формируется единичная матрица $\mathbf{H}_2^3$ размером 3×3, и формируется проверочная матрица в виде

$$\mathbf{H}^3 = [\mathbf{H}_1^3 | \mathbf{H}_2^3] = \left[\begin{array}{cccc|ccc} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{array}\right].$$

В соответствии с шагом 3 формируется проверочная матрица расширенного кода как

$$\mathbf{H}_4 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Затем сумма всех строк $\mathbf{H}_4$ по модулю 2 записывается в первую строку:

$$\mathbf{H}_4 = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Для формирования правой канонической формы первая строка матрицы $\mathbf{H}_4$ складывается со второй, результат сложения записывается во вторую строку. Затем первая строка складывается с третьей, результат сложения записывается в третью строку. В итоге матрица $\mathbf{H}_4$ представляется как

$$\mathbf{H}_4 = [\mathbf{H}_1^4 | \mathbf{H}_2^4] = \left[\begin{array}{ccc|cccc} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{array}\right].$$

В соответствии с шагом 4 формируется единичная подматрица $\mathbf{G}_1^4$ размером 3×3 и порождающая матрица в виде

$$\mathbf{G} = [\mathbf{G}_1^4 | (\mathbf{H}_1^4)^T] = \left[\begin{array}{ccc|cccc} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{array}\right].$$
