Теория кодирования

Гошин Егор Вячеславович, к.т.н., доцент
кафедры суперкомпьютеров и общей информатики

Предел корректирующей способности кода

Рассмотрим код длины n и размерности k, исправляющий ошибки до кратности t включительно.

Рассмотрим минимальное количество **различных** синдромов этого кода.

Синдромы

Синдромов для кодовых слов:	1
Синдромов для однократных ошибок:	…
Синдромов для двукратных ошибок:	…

Синдромы

Синдромов для кодовых слов: 1

Синдромов для однократных ошибок: n

Синдромов для двукратных ошибок: C_n^2

…

Синдромов для t-кратных ошибок: C_n^t

Итого различных синдромов: $1 + n + \ldots + C_n^t$

Максимальное число различных синдромов

Общее число синдромов ограничено сверху числом разрядов под эти синдромы: n-k

$$1 + n + \ \ldots + C_n^t \leq 2^{n-k}$$

или

$$|C| \leq \frac{2^n}{1 + n + \ \ldots + C_n^t}$$

Это выражение называется границей Хэмминга.

Как формировать матрицу кода?

Предположим, задача заключается в формировании кода с $n = 15$, $k = 6$, $d = 5$.

$$n - k = 15 - 6 = 9$$

Это означает, что необходимо найти 15 ненулевых векторов длины 9 таких, что любые $d - 1 = 4$ из них линейно независимы.

Первые 9 формируются легко – можно взять единичную матрицу.

$$H = \begin{bmatrix} I_9 \\ 111100000 \\ 100011100 \\ 101000011 \\ ??? \\ ??? \\ ??? \end{bmatrix}$$

Совершенные коды

Код длины n с нечётным кодовым расстоянием $d = 2t + 1$ называется совершенным кодом, если C обеспечивает равенство в границе Хэмминга:

$$|C| = \frac{2^n}{1 + n + \ \dots + C_n^t}$$

Число таких кодов **очень** ограниченно.

Так, очевидно, к таким кодам относятся тривиальные коды:

$(n, 1, n)$ – коды повторения,

$(n, n, 0)$ – просто двоичные коды, без избыточности

Нетривиальные совершенные коды

Тривиальные совершенные коды нас не очень интересуют. Они либо бесполезны с точки зрения исправления ошибок, либо слишком неэффективны.

Рассмотрим два класса совершенных кодов.

1. $(7,4,3)$: $\quad 2^4 = \frac{2^7}{1+7}$ $\qquad (15,11,3)$: $\quad 2^{11} = \frac{2^{15}}{1+15}$

2. $(23,12,7)$: $\qquad \frac{2^{23}}{1+23+253+1771} = \frac{2^{23}}{2048} = \frac{2^{23}}{2^{11}} = 2^{12}$

Коды Хэмминга

Рассмотрим коды длины $n = 2^r - 1$, предназначенные для исправления однократных ошибок.

Для этого они должны удовлетворять требованию

$$2^{\mathrm{k}} = \frac{2^n}{1+n}$$

После преобразований:

$$|\mathrm{C}| = \frac{2^n}{1+n} = \frac{2^{2^r-1}}{1+2^r-1} = \frac{2^{2^r-1}}{1+2^r-1} = 2^{2^r-1-r}$$

Таким образом, код Хэмминга имеет свойства: $(2^r - 1, 2^r - r - 1, 3)$.

Код Хэмминга

Сформируем матрицу кода Хэмминга. И начнём в этот раз с проверочной матрицы.

Поскольку код Хэмминга имеет свойства: $(2^r - 1, 2^r - r - 1,3)$, проверочная матрица должна состоять из $2^r - 1$ строк и r столбцов.

Поскольку при этом матрица H не должна содержать нулевых строк и все строки должны быть различными, она содержит **все** двоичные слова длины r.

Матрицы кода Хэмминга

$$H = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \qquad G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

Код Хэмминга

Код Хэмминга – совершенный код предназначенный для исправления одинарных ошибок.

Синдромы двойных ошибок для кода Хэмминга будут отличаться от нуля (код может быть использован для обнаружения двойных), но будут совпадать между собой и совпадать с синдромами для одинарных ошибок.

Таким образом, код Хэмминга можно использовать либо **для исправления одинарных ошибок**, либо **для обнаружения двойных**, но ***не одновременно!***

Пример кода Хэмминга

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

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

Передача с одиночной ошибкой

$$u = \begin{bmatrix} 1 & 0 & 0 & 1 \end{bmatrix}$$

$$v = uG = \begin{bmatrix} 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 0 \end{bmatrix}$$

Исходное сообщение:	$\begin{bmatrix} 1 & 0 & 0 & 1 \end{bmatrix}$
Отправлено:	$\begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 0 \end{bmatrix}$
В ходе передачи возникла ошибка	
Принято:	$\begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \end{bmatrix}$
Декодирование без исправления:	$\begin{bmatrix} 1 & 0 & 1 & 1 \end{bmatrix}$

Обнаружение одиночной ошибки

Исходное сообщение: $\begin{bmatrix}1 & 0 & 0 & 1\end{bmatrix}$

Отправлено: $\begin{bmatrix}1 & 0 & 0 & 1 & 1 & 0 & 0\end{bmatrix}$

В ходе передачи возникла ошибка

Принято: $\begin{bmatrix}1 & 0 & 1 & 1 & 1 & 0 & 0\end{bmatrix}$

$$vH = \begin{bmatrix}1 & 0 & 1 & 1 & 1 & 0 & 0\end{bmatrix}\begin{bmatrix}1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1\end{bmatrix} = \begin{bmatrix}1 & 0 & 1\end{bmatrix}$$

Синдром: $\begin{bmatrix}1 & 0 & 1\end{bmatrix}$

В принятом сообщении есть ошибка

Исправление одиночной ошибки

Исходное сообщение: $\begin{bmatrix}1 & 0 & 0 & 1\end{bmatrix}$

Отправлено: $\begin{bmatrix}1 & 0 & 0 & 1 & 1 & 0 & 0\end{bmatrix}$

В ходе передачи возникла ошибка

Принято: $\begin{bmatrix}1 & 0 & 1 & 1 & 1 & 0 & 0\end{bmatrix}$

Синдром: $\begin{bmatrix}1 & 0 & 1\end{bmatrix}$

В принятом сообщении есть ошибка

$\begin{bmatrix}1 & 0 & 1\end{bmatrix}$ – 3-я строка матрицы H'

Ошибка: $\begin{bmatrix}0 & 0 & 1 & 0 & 0 & 0 & 0\end{bmatrix}$

Исправленное сообщение: $\begin{bmatrix}1 & 0 & 0 & 1 & 1 & 0 & 0\end{bmatrix}$

Декодированное сообщение: $\begin{bmatrix}1 & 0 & 0 & 1\end{bmatrix}$

Передача с двойной ошибкой

$$u = \begin{bmatrix} 1 & 0 & 0 & 1 \end{bmatrix}$$

$$v = uG = \begin{bmatrix} 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 0 \end{bmatrix}$$

Исходное сообщение:	$\begin{bmatrix} 1 & 0 & 0 & 1 \end{bmatrix}$
Отправлено:	$\begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 0 \end{bmatrix}$
В ходе передачи возникла ошибка	
Принято:	$\begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$
Декодирование без исправления:	$\begin{bmatrix} 1 & 1 & 0 & 1 \end{bmatrix}$

Обнаружение двойной ошибки

Исходное сообщение: $\begin{bmatrix}1 & 0 & 0 & 1\end{bmatrix}$

Отправлено: $\begin{bmatrix}1 & 0 & 0 & 1 & 1 & 0 & 0\end{bmatrix}$

В ходе передачи возникла ошибка

Принято: $\begin{bmatrix}1 & 1 & 0 & 1 & 1 & 1 & 0\end{bmatrix}$

$$vH = \begin{bmatrix}1 & 1 & 0 & 1 & 1 & 1 & 0\end{bmatrix}\begin{bmatrix}1 & 1 & 1\\ 1 & 1 & 0\\ 1 & 0 & 1\\ 0 & 1 & 1\\ 1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{bmatrix} = \begin{bmatrix}1 & 0 & 0\end{bmatrix}$$

Синдром: $\begin{bmatrix}1 & 0 & 0\end{bmatrix}$

В принятом сообщении есть ошибка

Исправление двойной ошибки

Исходное сообщение:	$[1 \quad 0 \quad 0 \quad 1]$
Отправлено:	$[1 \quad 0 \quad 0 \quad 1 \quad 1 \quad 0 \quad 0]$
В ходе передачи возникла ошибка	
Принято:	$[1 \quad 1 \quad 0 \quad 1 \quad 1 \quad 1 \quad 0]$
Синдром:	$[1 \quad 0 \quad 0]$

В принятом сообщении есть ошибка

$[1 \quad 0 \quad 0]$ – 5-я строка матрицы H

Ошибка:	$[0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 0 \quad 0]$
Исправленное сообщение:	$[1 \quad 1 \quad 0 \quad 1 \quad 0 \quad 1 \quad 0]$
Декодированное сообщение:	$[1 \quad 1 \quad 0 \quad 1]$

Расширенный код Хэмминга

Можно расширить код Хэмминга одним разрядом для получения **расширенного кода Хэмминга**.

Расширенным кодом Хэмминга называется код с проверочной и порождающей матрицами вида:

$$H^* = \begin{bmatrix} H & j \\ 0 & 1 \end{bmatrix}, \qquad G^* = \begin{bmatrix} G & b \end{bmatrix}$$

где j – вектор из единиц, b – вектор такой, что вес каждой строки G^* – чётный.

Расширенный код Хэмминга

Расширенный код Хэмминга – совершенный код предназначенный для исправления одинарных ошибок.

Синдромы двойных ошибок для расширенного кода Хэмминга будут отличаться от нуля (код может быть использован для обнаружения двойных) и отличаться от синдромов для одинарных ошибок, при этом совпадать между собой.

Таким образом, расширенный код Хэмминга можно использовать **для исправления одинарных ошибок** и **для обнаружения двойных *одновременно!***

Расширенный код Хэмминга $(8,4,4)$

$$G^* = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

$$H^* = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Передача с одиночной ошибкой

$$u = \begin{bmatrix} 1 & 0 & 0 & 1 \end{bmatrix}$$

$$v = uG^* = \begin{bmatrix} 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

Исходное сообщение: $\begin{bmatrix} 1 & 0 & 0 & 1 \end{bmatrix}$

Отправлено: $\begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$

В ходе передачи возникла ошибка

Принято: $\begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$

Декодирование без исправления: $\begin{bmatrix} 1 & 0 & 1 & 1 \end{bmatrix}$

Обнаружение одиночной ошибки

Исходное сообщение: $[1 \quad 0 \quad 0 \quad 1]$

Отправлено: $[1 \quad 0 \quad 0 \quad 1 \quad 1 \quad 0 \quad 0 \quad 1]$

В ходе передачи возникла ошибка

Принято: $[1 \quad 0 \quad 1 \quad 1 \quad 1 \quad 0 \quad 0 \quad 1]$

$$vH^* = [1 \quad 0 \quad 1 \quad 1 \quad 1 \quad 0 \quad 0 \quad 1]\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix} = [1 \quad 0 \quad 1 \quad 1]$$

Синдром: $[1 \quad 0 \quad 1 \quad 1]$

В принятом сообщении есть ошибка

Исправление одиночной ошибки

Исходное сообщение: $\begin{bmatrix} 1 & 0 & 0 & 1 \end{bmatrix}$

Отправлено: $\begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$

В ходе передачи возникла ошибка

Принято: $\begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$

Синдром: $\begin{bmatrix} 1 & 0 & 1 & 1 \end{bmatrix}$

В принятом сообщении есть ошибка

$\begin{bmatrix} 1 & 0 & 1 & 1 \end{bmatrix}$ – 3-я строка матрицы H'

Ошибка: $\begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$

Исправленное сообщение: $\begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$

Декодированное сообщение: $\begin{bmatrix} 1 & 0 & 0 & 1 \end{bmatrix}$

Передача с двойной ошибкой

$$u = \begin{bmatrix} 1 & 0 & 0 & 1 \end{bmatrix}$$

$$v = uG^* = \begin{bmatrix} 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

Исходное сообщение: $\begin{bmatrix} 1 & 0 & 0 & 1 \end{bmatrix}$

Отправлено: $\begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$

В ходе передачи возникла ошибка

Принято: $\begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}$

Декодирование без исправления: $\begin{bmatrix} 1 & 1 & 0 & 1 \end{bmatrix}$

Обнаружение двойной ошибки

Исходное сообщение: $\begin{bmatrix}1 & 0 & 0 & 1\end{bmatrix}$

Отправлено: $\begin{bmatrix}1 & 0 & 0 & 1 & 1 & 0 & 0 & 1\end{bmatrix}$

В ходе передачи возникла ошибка

Принято: $\begin{bmatrix}1 & 1 & 0 & 1 & 1 & 1 & 0 & 1\end{bmatrix}$

$$vH^* = \begin{bmatrix}1 & 1 & 0 & 1 & 1 & 1 & 0 & 1\end{bmatrix}\begin{bmatrix}1 & 1 & 1 & 1\\ 1 & 1 & 0 & 1\\ 1 & 0 & 1 & 1\\ 0 & 1 & 1 & 1\\ 1 & 0 & 0 & 1\\ 0 & 1 & 0 & 1\\ 0 & 0 & 1 & 1\\ 0 & 0 & 0 & 1\end{bmatrix} = \begin{bmatrix}1 & 0 & 0 & 0\end{bmatrix}$$

Синдром: $\begin{bmatrix}1 & 0 & 0 & 0\end{bmatrix}$

В принятом сообщении есть ошибка

Исправление двойной ошибки

Исходное сообщение: $\begin{bmatrix}1 & 0 & 0 & 1\end{bmatrix}$

Отправлено: $\begin{bmatrix}1 & 0 & 0 & 1 & 1 & 0 & 0 & 1\end{bmatrix}$

В ходе передачи возникла ошибка

Принято: $\begin{bmatrix}1 & 1 & 0 & 1 & 1 & 1 & 0 & 1\end{bmatrix}$

Синдром: $\begin{bmatrix}1 & 0 & 0 & 0\end{bmatrix}$

В принятом сообщении есть ошибка

$\begin{bmatrix}1 & 0 & 0 & 0\end{bmatrix}$ – такого синдрома в матрице H нет

Ошибка не может быть исправлена