ЛЕКЦИЯ 7. БЛОЧНЫЕ ЛИНЕЙНЫЕ КОДЫ

7.1. Математическое описание процессов кодирования и декодирования

7.2. Коды с проверкой на четность

7.3. Коды Хэмминга

7.1. Математическое описание процессов кодирования и декодирования

При формировании блочных кодов информационная последовательность разбивается на блоки из m информационных разрядов. К ним добавляется k проверочных разрядов. Блок после кодирования состоит из $n = m + k$ разрядов.

Блочным линейным кодом с маркировкой (n,m) называются последовательности кодовых комбигаций из n разрядов, характеризующиеся тем, что сумма двух разрешенных кодовых комбинаций является разрешенной кодовой комбинацией.

При задании кода обычно указывают, какие информационные разряды принимают участие в формировании каждого из k проверочных разрядов. Например, для кода с n=5, m=3 и k=2 каждый проверочный разряд b_i определяется суммированием по модулю 2 по правилу

$$b_1 = a_1 \oplus a_2; \quad b_2 = a_2 \oplus a_3,$$

где a_i - информационные разряды.

Комбинация такого кода записывается в виде a_1, a_2, a_3, b_1, b_2 или в обратном b_2, b_1, a_3, a_2, a_1

Для информационной последоваательности

$a = 110$

проверочные разряды

$b_1 = a_1 \oplus a_2 = 1 + 1 = 0,$

$b_2 = a_2 \oplus a_3 = 1 + 0 = 1.$

На выходе кодера будет сформирована кодовая комбинация

$F = 11001.$

В декодере рассчитывается синдром (опознаватель ошибок), элементы которого формируются путем суммирования по mod2 проверочного разряда и тех информационных, которые принимали участие в его формировании.

$s_1 = b_1 \oplus a_1 \oplus a_2 = 0 \oplus 1 \oplus 1 = 0,$

$s_2 = b_2 \oplus a_2 \oplus a_3 = 1 \oplus 1 \oplus 0 = 0.$

Если синдром равен нулю, то считается, что ошибок нет.

Пусть на вход декодера поступает блок

$F' = 1 0 0 0 1$ - ошибка во втором разряде.

$s_1 = b_1 \oplus a_1 \oplus a_2 = 0 \oplus 1 \oplus 0 = 1,$

$s_2 = b_2 \oplus a_2 \oplus a_3 = 1 \oplus 0 \oplus 0 = 1.$

Синдром не равен нулю $\Rightarrow$ ошибка обнарежена.

Таблица 7.1. Кодовые комбинации

№ п/п	a_1	a_2	a_3	b_1	b_2
1	1	0	0	1	0
2	0	1	0	1	1
3	0	0	1	0	1
4	1	1	0	0	1
5	0	I	I	I	0
6	1	0	1	1	1
7	1	1	1	0	0
8	0	0	0	0	0

	информационные символы	проверочные символы

Под линейно независимыми кодовыми комбинациями понимают такие, сумма по mod2 которых (в любом сочетании) не равняется нулю.

1. 1 0 0 1 0	1. 1 0 0 1 0	1. 1 0 0 1 0
2. 0 1 0 1 1	4. 1 1 0 0 1	4. 1 1 0 0 1
3. 0 0 1 0 1	5. 0 1 1 1 0	7. 1 1 1 0 0
(1)	(2)	(3)

Для первой группы:

1. 1 0 0 1 0	1. 1 0 0 1 0	2. 0 1 0 1 1	1. 1 0 0 1 0
$\oplus$	$\oplus$	$\oplus$	$\oplus$
2. 0 1 0 1 1	3. 0 0 1 0 1	3. 0 0 1 0 1	2. 0 1 0 1 1
------------------	----------------	------------------	$\oplus$
1 1 0 0 1	1 0 1 1 1	0 1 1 1 0	3. 0 0 1 0 1
			-----------
			1 1 1 0 0.
4.	6.	5.	7.

Порождающая матрица (n,m) в канонической форме

$G(n,m) = \left\| I_m, R_{m \times k} \right\|$,

где I_m - единичная матрица информационных разрядов размерности $m \times m$, $R_{m,k}$ - матрица проверочных разрядов, размерность которой $m \times k$.

Для примера – (5,3) кода каноническая форма порождающей матрицы имеет вид

$$G(5,3) = \begin{Vmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{Vmatrix}.$$

Процесс кодирования заключается в умножении информационной последовательности на порождающую матрицу

$F = a \cdot G(n,m)$.

Пример $a = 110$

$$G(5,3) = \begin{Vmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{Vmatrix}.$$

$$F = 110 \cdot \begin{Vmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{Vmatrix} = 11001.$$

Выделяется подматрица $R^T_{m x k}$ являющаяся транспонированной матрицей $R_{m x k}$:

если $R_{m x k} = \begin{vmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \end{vmatrix}$ то $R^T_{m x k} = \begin{vmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{vmatrix}$.

Для обнаружения или исправления ошибок строится проверочна матрица.

$$H = \left\| R^T_{m \times k}, I_{k \times k} \right\|,$$

$$H = \begin{vmatrix} 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{vmatrix}.$$

Проверочная матрица связана с порождающей соотношением

$$G(n, m) H^T = 0 .$$

Процесс декодирования математически описывают произведением вектора–строки принятой кодовой комбинации $F' = F + E$ (E - вектор ошибки) и транспонированной проверочной матрицы H

$S = F'H^T$,

где S – результат декодирования (синдром);

$(\bullet)^T$ - знак транспортирования.

На вход декодера поступает

$F' = 1\ 0\ 0\ 0\ 1$ - ошибка во втором разряде.

$$S = 1\ 0\ 0\ 0\ 1 \begin{Vmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{Vmatrix} = 11\,.$$

Синдром не равен нулю $\Rightarrow$ ошибка обнаружена.

7.2. Коды с проверкой на четность

В таком коде к кодовым комбинациям m-разрядного кода добавляется один дополнительный разряд (символ проверки на четность, называемый проверочным, или контрольным). Если число символов 1 исходной кодовой комбинации четное, то в дополнительном разряде формируют контрольный символ 0, а если число символов 1 нечетное, то в дополнительном разряде формируют символ 1. В результате общее число символов 1 в любой передаваемой кодовой комбинации всегда будет четным.

Правило формирования проверочного разряда:

$$b = a_1 \oplus a_2 \oplus \ldots \oplus a_m$$

Критерием правильности принятой комбинации является равенство нулю результата S суммирования по модулю 2 всех n символов кода, включая проверочный символ b. При наличии одиночной ошибки S принимает значение 1 :

$$S = b \oplus a_1 \oplus a_2 \oplus \ldots \oplus a_m = \begin{cases} 0 - \textit{ошибки нет} \\ 1 - \textit{однократная ошибка.} \end{cases}$$

7.3. Коды Хэмминга

Коды Хэмминга позволяют исправлять одиночную ошибку в блоке. Для каждого числа проверочных символов $k = 3,4,5,...$ существует классический код Хэмминга с маркировкой

$$(n,m) = (2^k - 1, 2^k - 1 - k),$$

т.е. — (7,4), (15, 11), (31, 26) ...

Пример. Код Хэмминга (7,4).

m=4: a_1, a_2, a_3, a_4, $k=3: b_1, b_2, b_3$.

Определим правило формирования проверочных разрядов:

$b_1 = a_1 \oplus a_2 \oplus a_3$;
$b_2 = a_2 \oplus a_3 \oplus a_4$;
$b_3 = a_1 \oplus a_2 \oplus a_4$.

Порождающая матрица в канонической форме

$G(7,4) = \|I_4, R_{4\times 3}\|$.

G(7,4) =

a_1	a_2	a_3	a_4	b_1	b_2	b_3
1	0	0	0	1	0	1
0	1	0	0	1	1	1
0	0	1	0	1	1	0
0	0	0	1	0	1	1

$$R_{4\times 3} = \begin{vmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{vmatrix}, \quad R^{T}_{4\times 3} = \begin{vmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{vmatrix}$$

Проверочная матрицу

$$H = \begin{vmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{vmatrix}.$$

Транспонированная проверочная матрица

$$H^{T} = \begin{vmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{vmatrix}.$$

Кодирование

$$F = a \cdot G(n,m)$$

Пусть $a = 1100$.

$$F = 1100 \cdot \begin{Vmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{Vmatrix} = 1100010.$$

Декодирование.

Для определения и исправления искаженного разряда используется матрица одиночных ошибок:

$$E = \left\| I_{n \times n}, H^T \right\|.$$

При определении синдрома в проверочной матрице находится комбинация синдрома. Искаженный разряд – это разряд в данной строке, в которой стоит «1». Искаженный разряд исправляем посредством сложения строки в матрице ошибок полученной комбинации.

Пример. Для кода (7,4) задана комбинация $F = 1100010$.
Составляется матрица одиночных ошибок

$$E = \begin{vmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & & 0 & 0 & 1 \end{vmatrix}$$

Принята комбинация $F' = 1110010$ - искажен третий разряд. Определяем синдром

$$S = 1110010 \begin{vmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{vmatrix} = 110 .$$

В проверочной матрице находим комбинацию 110.

$$E = \begin{array}{|ccccccc ccc|l}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & \xleftarrow{110} \\
\hline
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 &
\end{array}$$

Прибавляем третью строку единичной матрицы к полученной комбинации $F' = 1110010$.

$$\begin{array}{l} \;\;1110010 \\ \oplus \\ \;\;0010000 \\ \hline \;\;1100010 \end{array}$$

Сообщение исправлено.

Таблица 7.2. Методика построения кода Хэмминга (7,4)

№ разряда	№ разряда в двоичной системе	Места расположения информационных и проверочных разрядов
1	001	$b_1 = a_1 + a_2 + a_4$
2	010	$b_2 = a_1 + a_3 + a_4$
3	011	a_1
4	100	$b_3 = a_2 + a_3 + a_4$
5	101	a_2
6	110	a_3
7	111	a_4

На приемной стороне рассчитывается синдром

$s_1 = b_1 + a_1 + a_2 + a_4$,

$s_2 = b_2 + a_1 + a_3 + a_4$,

$s_3 = b_3 + a_2 + a_3 + a_4$.

При этом синдром укажет номер искаженного разряда.

Пример. На вход кодера поступает информационная последовательность $a = 1011$.

	a_1	a_2	a_3	a_4
$a =$	1	0	1	1

$b_1 = a_1 + a_2 + a_4 = 1 + 0 + 1 = 0$,

$b_2 = a_1 + a_3 + a_4 = 1 + 1 + 1 = 1$,

$b_3 = a_2 + a_3 + a_4 = 0 + 1 + 1 = 0$.

Тогда на выходе кодера

	b_1	b_2	a_1	b_3	a_2	a_3	a_4
$F =$	0	1	1	0	0	1	1

Пусть на вход декодера поступает блок (искажен 5-й разряд (a_2))

	b_1	b_2	a_1	b_3	a_2	a_3	a_4
$F'=$	0	1	1	0	1	1	1

$$s_1 = b_1 + a_1 + a_2 + a_4 = 0+1+1+1=1,$$

$$s_2 = b_2 + a_1 + a_3 + a_4 = 1+1+1+1=0,$$

$$s_3 = b_3 + a_2 + a_3 + a_4 = 0+1+1+1=1.$$

Синдром 101 соответствует 5-му разряду

№ разряда	№ разряда в двоичной системе
1	0 0 1
2	0 1 0
3	0 1 1
4	1 0 0
5	1 0 1
6	1 1 0
7	1 1 1
	$s_3 s_2 s_1$

Заменяем 5-й разряд на противоположный и получаем исправленное сообщение

	b_1	b_2	a_1	b_3	a_2	a_3	a_4
$F =$	0	1	1	0	0	1	1

2-й способ получения синдрома

Складываются номера разрядов, в которых находятся «1» в полученной кодовой комбинации

	b_1	b_2	a_1	b_3	a_2	a_3	a_4
$F' =$	0	1	1	0	1	1	1

Это номера: 2 (010), 3 (011), 5 (101), 6 (110) и 7 (111)

0 1 0
0 1 1
1 0 1
1 1 0
1 1 1
------
1 0 1 - синдром