2. Konspekt lekcii “Principy postroenija linejnyh blochnyh kodov (na primere koda Hemminga 7,4)”

Линейные блочные коды

Конечное множество β разрешенных комбинаций линейного блочного кода образует так называемую конечную группу порядка 2^k, где $к$ – число информационных символов в кодовой комбинации, 2^k – количество элементов, образующих группу.

Группой в высшей алгебре называется множество объектов или элементов, для которых определена некоторая операция f, позволяющая любой паре элементов a и b однозначно сопоставить третий элемент c, обязательно принадлежащий той же группе. Такой операцией может быть, например, сложение (и, в частности по mod2) $a+b=c$, или умножение (в частности, тоже по mod2) $ab=c$. Соответственно группа называется аддитивной или мультипликативной.

Для элементов группы должны выполняться следующие условия:

1. Замкнутость: $f(a, b)=c$.

В частности, в группе, где определяется операция сложения, $a+b=c$, а в группе, где определяется операция умножения, $f(ab)=c$, где a,b,c обязательно принадлежат одной и той же группе.

2. Ассоциативность: $F[f(a, b), c]=F[a, f(b, c)]$.

В частности, в группе, со сложением $(a+b)+c=a+(b+c)$, а в группе с умножением $(ab)c=a(bc)$.

3. Существование нейтрального элемента, то есть такого, участие которого в операции не изменяет ее результат.

В группе со сложением это нулевой элемент, для которого $a+0=0+a=a$, а в группе с умножением это единичный элемент, для которого $1\cdot a=a\cdot 1=a$.

4. Существование обратного элемента, то есть такого, операция с участием которого приводит к нейтральному элементу: в группе со сложением к нулевому элементу, $a+a=0$ по mod2, а в группе с умножением –

к единичному элементу, 1·1=1; (– 1)·(–1)=1. То есть обратным элементом в обоих случаях является сам элемент.

Кроме того, группа может удовлетворять условию коммутативности: $a+b=b+a$; $ab=ba$. Такие группы называются коммутативными (абелевыми). Это условие не является обязательным.

Далее везде используются операции только по mod2. Заметим: из формулы $a+a=0$ следует, что $a=-a$, то есть операции сложения и вычитания по mod2 совпадают.

Рассмотрим безызбыточный, или (κ, κ), код. Этот код полностью описывается порождающей матрицей, содержащей κ строк и κ столбцов:

$$J_k = \underbrace{\left\|\begin{matrix} 1 & 0 & 0 & & & & 0 \\ 0 & 1 & 0 & & & & 0 \\ 0 & 0 & 1 & & & & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & 0 & & & 1 \end{matrix}\right\|}_{k \text{ столбцов}} \Bigg\} k \text{ строк}$$

Здесь каждая строка содержит только одну единицу. Суммируя по модулю 2 строки между собой во всех возможных сочетаниях, получим все 2^k кодовых слов безызбыточного кода. Аналогично (m, k) код полностью описывается своей порождающей матрицей

$$J_{m,k} = \left\|\begin{matrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & b_{11} & b_{12} & \ldots & b_{1r} \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & b_{21} & b_{22} & \ldots & b_{2r} \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & b_{31} & b_{32} & \ldots & b_{3r} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & b_{k1} & b_{k2} & \ldots & b_{kr} \end{matrix}\right\} k \text{ строк}$$

$$\underbrace{\qquad\qquad\qquad}_{k \text{ столбцов}} \quad \underbrace{\qquad\qquad}_{r \text{ столбцов}}$$

Эта матрица состоит из порождающей матрицы J_k и приписанной к ней справа проверочной части, содержащей r столбцов. Очевидно, для кода с заданным кодовым расстоянием $d_{\min}$ вес каждой строки проверочной части, приписанной к матрице J_k, должен быть не менее $d_{\min} - 1$, поскольку строка единичной матрицы уже имеет вес, равный 1. Сложение двух любых строк

матрицы J_k дает вес, равный 2, значит, сумма двух любых приписанных строк проверочной части должен иметь вес не менее $d_{\min} - 2$. Для кодов малой значности, используя эти соображения, можно путем перебора возможных значений символов проверочной части b_{ij} найти код с хорошими корректирующими свойствами. В частности такие коды с $d_{\min} = 3$ (код $(7, 4)$) и $d_{\min} = 4$ (код $(15, 11)$) были найдены Хэммингом и поэтому называются кодами Хэмминга. Например, код $(7, 4)$ с $d_{\min} = 3$ имеет порождающую матрицу

$$J_{7,4} = \begin{Vmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{Vmatrix}$$

Нетрудно убедиться, что проверочная часть этой порождающей матрицы удовлетворяет сформулированным выше требованиям: вес каждой ее строки – не менее 2, вес суммы двух любых строк – не менее $d_{\min} - 2 = 1$.

Как показано в теории кодирования, зная порождающую матрицу, можно построить другую матрицу – проверочную, имеющую r строк:

$$M_{m,k} = \underbrace{\begin{Vmatrix} b_{11} & b_{21} & b_{31} & \dots & \dots & \dots & b_{k1} \\ b_{12} & b_{22} & b_{32} & \dots & \dots & \dots & b_{k2} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ b_{1r} & b_{2r} & b_{3r} & \dots & \dots & \dots & b_{kr} \end{Vmatrix}}_{k \text{ столбцов}} \quad \underbrace{\begin{Vmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 1 \end{Vmatrix}}_{m-k=r \text{ столбцов}} \quad r \text{ строк}$$

Первые k столбцов этой матрицы суть строки проверочной части порождающей матрицы, остальные r столбцов представляют собой единичную матрицу. В декодере решаются так называемые tпроверочные уравнения. В них входят суммы (по mod2) тех разрядов принимаемого кодового слова, в которых в строке проверочной матрицы записана единица. Эти суммы должны быть равны 0, то есть осуществляется проверка на четность. Например, для кода (7, 4) получаем проверочную матрицу

$$M_{7,4} = \begin{array}{c} \begin{array}{ccccccc} a_1 & a_2 & a_3 & a_4 & b_1 & b_2 & b_3 \end{array} \\ \left\| \begin{array}{ccccccc} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{array} \right\| \end{array}$$

и проверочные уравнения:

$$a_1 + a_2 + a_3 + b_1 = 0$$

$$a_2 + a_3 + a_4 + b_2 = 0$$

$$a_1 + a_2 + a_4 + b_3 = 0.$$