И. М. БОЯРИНОВ

О ПОРОГОВОМ ДЕКОДИРОВАНИИ ЦИКЛИЧЕСКИХ КОДОВ ХЭММИНГА

При применении корректирующих кодов в информационных системах важной задачей является построение простых методов и устройств, исправляющих ошибки. Одним из методов, особенно удобных для технической реализации, является пороговое декодирование. В статье рассматривается метод порогового декодирования циклических кодов Хэмминга. Циклический $(2^m-1,\ 2^m-m-1)$-код Хэмминга m-го порядка [1] определяется как нулевое пространство матрицы

$$H=(1,\ \alpha,\ \alpha^2,\ \cdots,\ \alpha^{2^m-2}), \tag{1}$$

где α — примитивный элемент поля $GF(2^m)$. Если степени α представить в виде векторов столбцов из 0 и 1, то среди столбцов матрицы H появится каждый ненулевой столбец длины m. Скалярное произведение любой линейной комбинации $(h_0,\ h_1\cdots,h_{n-1})$ строк матрицы H и кодового вектора $a=(a_0,\ a_1,\ \cdots,\ a_{n-1})$ задает контрольное соотношение, называемое проверкой на четность,

$$\sum_{j=0}^{n-1} a_j h_j=0 \pmod 2, \tag{2}$$

выполняющееся для каждого кодового вектора. Системой ортогональных (разделенных) проверок [2], [3] называется такое множество контрольных соотношений (2), которое удовлетворяет следующим условиям:

1) в каждую проверку входит один и тот же символ, например a_j;

2) любой символ $a_i,\ i\neq j$ входит не более чем в одно соотношение.

Блоковый $(n,\ k)$-код может быть полностью ортогонализован, если можно построить $d-1$ проверок, ортогональных относительно каждого информационного символа (d — минимальный вес кодового слова).

Теорема 1. $(2^m-1,\ 2^m-m-1)$-коды Хэмминга не могут быть полностью ортогонализованы при $m>2$.

Доказательство проведем индукцией по m. Пусть $m=3$. Проверяем непосредственно, что для $(7, 4)$-кода нельзя построить двух ортогональных нетривиальных проверок относительно первого символа.

Пусть теперь для кода Хэмминга k-го порядка не существует двух ортогональных проверок относительно первого символа. Проверочная матрица H_{k+1} кода, $(k+1)$ порядка, получается из проверочной матрицы H_k кода k-го порядка добавлением 2^k столбцов и строки такой, что во все столбцы матрицы H_k добавляется по нулевому символу.

Любой линейной комбинации строк матрицы H_{k+1}, задающей проверку относительно первого символа, можно однозначно поставить в соответствие некоторую линейную комбинацию строк матрицы H_k отбрасыванием символов, не входящих в матрицу H_k. Поэтому любая проверка кода $(k+1)$ порядка относительно первого символа будет содержать все символы соответствующей ей проверки кода k-го порядка. Следовательно, для кода Хэмминга $(k+1)$-порядка не существует двух ортогональных проверок относительно первого, а в силу циклических свойств кода, и любого другого символа. Теорема доказана. Из теоремы 1 следует, что мажоритарное декодирование кодов Хэмминга в один шаг не удается. Рассмотрим метод составления специальных проверок, вообще говоря неортогональных, позволяющий осуществить пороговое декодирование кодов Хэмминга. Справедлива следующая теорема.

Теорема 2. Существует система m-проверок кода Хэмминга m-го порядка, которая удовлетворяет следующим условиям:

1) в каждую проверку входит один и тот же символ, например x_j;

2) любой символ x_i $i\neq j$ входит хотя бы в одну, но не более чем в $m-1$ проверок.

Доказательство. Произвольную проверку

$$\sum_{j=0}^{n-1} x_j h_j = 0 \pmod 2$$

кодового слова $a=(x_0, x_1, \cdots, x_{n-1})$, содержащую первый символ x_0, можно представить в виде

$$x_0 = \sum_{j=0}^{n-1} x_j h_j \pmod 2. \qquad (3)$$

Будем говорить, что в этом случае вектор $h=(h_0, h_1, \cdots, h_{n-1})$ определяет проверку (3) относительно первого символа. Построим систе-

му m-проверок, удовлетворяющих условиям теоремы. Первая строка проверочной матрицы H_m кода m-го порядка определяет первую проверку относительно первого символа. Сумма первой и второй строк определяет вторую проверку относительно первого символа и т. д. Наконец, сумма первой и m-строки определяет m-проверку. Построенная система проверок удовлетворяет условиям теоремы. Действительно, первый и только первый символ входит во все m проверок, так как первый и только первый столбец матрицы H_m имеет первый символ, равный единице, а все остальные символы равны нулю. Любой другой символ α_j входит хотя бы в одну проверку, так как матрица H_m не содержит нулевого столбца. Теорема доказана.

Используя теорему 2, для кода Хэмминга m-го порядка предлагается декодирующая схема, содержащая $n = 2^m - 1$ разрядов регистра сдвига (буферное запоминающее устройство), m сумматоров по модулю 2, один пороговый элемент и позволяющая исправить одну ошибку. Процедура декодирования выглядит следующим образом. На вход порогового элемента подаются результаты m-проверок относительно первого символа. Если результаты всех m-проверок совпадают (достигается порог m), берем это значение в качестве первого символа. На этом декодирование прекращается — все остальные символы верные. Если порог m не достигается, считаем первый символ неискаженным, производим циклический сдвиг сообщения в регистре и повторяем процедуру относительно второго символа и т. д. Следует отметить, что по сравнению с известными [1] предлагаемая схема декодирования имеет примерно такую же сложность оборудования, но дает значительный выигрыш во времени обработки информации.

Всякий код с минимальным расстоянием d может исправлять любую комбинацию из $d - 1$ или меньшего числа стираний. Предложенная декодирующая схема для кода Хэмминга с минимальным расстоянием $d = 3$ позволяет исправить любую комбинацию из 2 или меньшего числа стираний.

Процедура декодирования выглядит следующим образом. Пусть произошло стирание двух символов: α_l, α_j. На вход порогового элемента подаются результаты m-проверок относительно символа α_l, причем в качестве значения символа α_j берется 0. Если результаты всех проверок совпадают (достигается порог m), берем это значение в качестве символа α_l и, кроме того, считаем $\alpha_j = 0$. Если порог m не достигается, заменяем значение символа α_j на единицу, а в качестве значения символа α_l берем значение, даваемое m-проверками (порог достигается). На этом декодирование прекращается. Если произошло стирание одного символа α_l, то, подавая на вход порогового элемента результаты m-проверок относительно символа α_l, мы сразу получаем его истинное значение на выходе порогового элемента.

Приведем без доказательства ввиду простоты следующее утверждение.

Любой циклический (n, k)-код может исправить пачку стираний длины $n-k$ или меньше. Метод порогового декодирования приводит к очень простой схеме декодирования, состоящей всего из одной проверки относительно первого символа. Например, в построенной системе m-проверок для кода Хэмминга достаточно взять первую проверку. Применим рассмотренный метод к исправлению пачек ошибок длины 2 или меньше. В качестве кода может быть использован циклический код Хэмминга, исправляющий одну ошибку и обнаруживающий две ошибки. Он совпадает с нулевым пространством матрицы

$$H = \begin{pmatrix} 1, & \alpha, & \alpha^2, & \cdots, & \alpha^{2^m-2} \\ 1, & 1, & 1, & \cdots, & 1 \end{pmatrix},$$

где α — примитивный элемент поля $GF(2^m)$. Предложенная декодирующая схема должна содержать в этом случае, кроме указанных элементов, еще один сумматор по модулю 2 для проверки на четность по всем символам и несколько логических элементов.

Процедура декодирования выглядит следующим образом.

Производится проверка на четность по всем символам. Если результат проверки равен 1 — произошла одиночная ошибка. Исправление ошибки производится изложенным выше методом. Если результат проверки равен 0 — имеет место пачка ошибок длины 2 или ошибок не произошло. Ошибок не произошло в том, и только в том, случае, если порог m достигается и значение порога совпадает со значением первого символа. В противном случае имеет место пачка ошибок длины 2. В этом случае заменяем значение второго символа на противоположный и подаем снова результаты всех m-проверок на пороговый элемент. Если порог m достигается и его значение противоположно значению первого символа — произошли ошибки в первом и втором символе. Исправив их, прекращаем декодирование. В противном случае производим циклический сдвиг сообщений в регистре и повторяем процедуру относительно второго символа. Заменяем значение третьего символа на противоположный. Если порог m достигается и его значение противоположно значению второго символа, произошла пачка ошибок $\alpha_1\ \alpha_2$. Исправив их, прекращаем декодирование. В противном случае считаем второй символ неискаженным. Производим циклический сдвиг в регистре и повторяем процедуру и т. д.

Следует отметить, что схема, позволяющая декодировать пачки ошибок длины 2, отличаясь от известных [1] простотой и меньшим количеством оборудования, дает одновременно выигрыш в скорости обработки информации.

Автор считает своим приятным долгом выразить благодарность Р. Р. Варшамову за полезные советы в процессе работы над статьей.

Ի. Մ. ԲՈՑԱՐԻՆՈՎ

ՀԵՄԻՆԳԻ ՑԻԿԼԻԿ ԿՈԴԵՐԻ ՍԱՀՄԱՆԱՅԻՆ ԱՊԱԿՈԴԱՎՈՐՄԱՆ ՄԱՍԻՆ

Ա մ փ ո փ ո ւ մ

Ապացուցվում է Հեմինգի կոդերի լրիվ օրթոգոնալացման անհնարինությունը։ Առաջադրվում է առանձին սխալի ուղղումը թույլատրող սահմանային ապակոդավորման մոդիֆիկացված մեթոդ։ Մեթոդը կիրառվում է երկու երկարության առանձին խմբերի և երկու սիմվոլների ջնջման ուղղելուն։

ЛИТЕРАТУРА

1. *У. Питерсон.* Коды, исправляющие ошибки. М., Изд. „Мир", 1964.
2. *Дж. Месси.* Пороговое декодирование, М., Изд. „Мир", 1966.
3. *В. Д. Колесник, Е. Т. Мирончиков.* Некоторые циклические коды и схема декодирования по большинству проверок. Проблемы передачи информации, 1965, 1, 2, 3—17.