УДК 621.391.23.019.3(04)

М. Ю. ЛОСЕВ, канд. техн. наук, *А. Н. РЫСОВАНЫЙ*

МЕТОДИКА ОЦЕНКИ РАСПОЗНАЮЩЕЙ СПОСОБНОСТИ ЦИКЛИЧЕСКИХ КОДОВ НА ПРИМЕРЕ КОДОВ ХЭММИНГА

В современных ЭВМ для контроля информации широкое распространение получили коды Хэмминга с кодовым расстоянием $d=3$ или $d=4$. Двоичный код Хэмминга, имеющий минимальное кодовое расстояние, равное 3, обеспечивает исправление одиночных ошибок, а код с $d=4$ исправляет одиночные ошибки и обнаруживает двойные.

Обнаружение ошибок более высокой кратности осуществляется с некоторой вероятностью $P(j)$*. Рассмотрим методику определения вероятности распознавания ошибок.

Для оценки обнаруживающей способности корректирующих кодов важное значение имеет понятие веса Хэмминга $W(V)$.

Весом Хэмминга $W(V)$ вектора V называется число ненулевых компонентов этого вектора. Кодовое расстояние между векторами V_i и $V_j (i \neq j)$ равно числу компонент, которыми они отличаются друг от друга. При искажении информации данный вектор V_j может перейти в подмножество разрешенных векторов $\bigcup_{j=i} V_i$, и ошибка не будет обнаружена. В этом случае кратность необнаруживаемой ошибки будет равна кодовому расстоянию между

* Питерсон У., Уэлдон Э. Коды, исправляющие ошибки. М., 1976. 596 с.

векторами (кодовыми комбинациями). Поэтому для вычисления вероятности необнаружения ошибки данной кратности с помощью кодов Хэмминга необходимо определить количество возможных расстояний в векторном пространстве и число кодовых комбинаций. Тогда вероятность пропуска ошибки данной кратности можно вычислить по формуле $Q_j = C_j/2^{n-k}$, где $n-k$ — число информационных разрядов в n-разрядном коде; C_j — количество кодовых расстояний кратности j.

Утверждение 1. Число вариантов кодового расстояния любой возможной величины для всех комбинаций систематического кода одинаково и аналогично распределению весов в разрешенных кодовых комбинациях.

Доказательство. Кодовое расстояние определяется весом комбинации, полученной в результате суммирования по модулю 2 двух или более других разрешенных комбинаций. Для систематического кода, к которому относится и код Хэмминга, такая сумма дает разрешенную кодовую комбинацию. Поэтому полученная в результате суммирования комбинация с весом d означает, с одной стороны, наличие разрешенной комбинации с весом d, с другой стороны, d — кодовое расстояние между ними. Что и требовалось доказать. Таким образом, в результате суммирования одной комбинации со всеми другими разрешенными получаем одновременно набор кодовых расстояний и разрешенных кодовых комбинаций.

Утверждение 2. Суммарное кодовое расстояние одной комбинации от всех других разрешенных комбинаций одинаково и определяется в соответствии с выражением $D_\Sigma = 2^{m-1}$, где m — число информационных разрядов.

Доказательство. Если все разрешенные комбинации выписать в таблицу, состоящую из 2^m строк и n столбцов (таблица всех разрешенных комбинаций), то в каждом столбце будет 2^{m-1} единиц. Поскольку всего разрядов n, приведенное утверждение можно считать доказанным.

Для всех систематических кодов значение D_Σ одинаково. Различие состоит в разном распределении кодовых расстояний.

Утверждение 3. Распределение кодового расстояния каждой из 2^{m-1} ненулевых комбинаций определяется компонентами вектора D, образованного путем перемножения матрицы W на вектор-столбец, все элементы которого равны 1. Матрица W есть результат произведения матрицы U размером $m \times (2^{m-1})$, включающей все ненулевые m-разрядные векторы, на порожденную матрицу G

$$D = W \cdot \begin{vmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{vmatrix} = U \cdot G \cdot \begin{vmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{vmatrix}.$$

Доказательство. Произведение $U \cdot G$ представляет собой матрицу, все строки которой являются разрешенными кодовыми комбинациями. Произведение матрицы W на столбец, состоящий из единиц, даст в результате вес вектора, отображающего данную строку. Следовательно, компоненты вектора D характеризуют вес разрешенных кодовых комбинаций. С учетом утверждения 1 можно сказать, что компоненты вектора D будут характеризовать распределение кодового расстояния. Что и требовалось доказать.

Пример. Пусть $m=3$ и заданы матрицы U и G:

$$U = \begin{vmatrix} 100 \\ 010 \\ 110 \\ 001 \\ 101 \\ 011 \\ 111 \end{vmatrix}; \quad G = \begin{vmatrix} 110100 \\ 011010 \\ 111001 \end{vmatrix}.$$

Матрица W будет иметь вид

$$W = U \cdot G = \begin{vmatrix} 110100 \\ 011010 \\ 101110 \\ 111001 \\ 001101 \\ 100011 \\ 010111 \end{vmatrix}.$$

Умножив полученную матрицу на вектор-столбец, получим матрицу D.

$$D = W \cdot \begin{vmatrix} 1 \\ 1 \\ \vdots \\ 1 \\ 1 \end{vmatrix} = \begin{vmatrix} 3 \\ 3 \\ 4 \\ 4 \\ 3 \\ 3 \\ 4 \end{vmatrix},$$

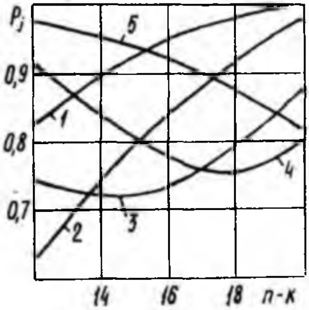

Рис. 1

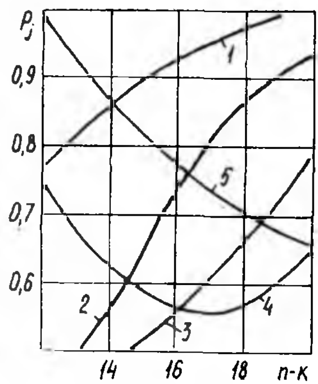

Рис. 2

в которой представлено распределение кодовых расстояний. В данном примере имеются комбинации с кодовым расстоянием (весом), равным 3, и три комбинации с кодовым расстоянием (весом) 4. На рис. 1, 2 представлены зависимости вероятности обнаружения ошибки заданной кратности i от количества информационных разрядов $W=3$ (рис. 1), $W=4$ (рис. 2), где *1* — $i=6$; *2* — $i=8$; *3* — $i=10$; *4* — $i=12$; *5* — $i=14$. Анализ изображенных зависимостей показывает, что характер изменения вероятностей обнаружения ошибок для различных кодовых расстояний один и тот же. Однако при использовании кодов с кодовым расстоянием 3 данная характеристика лучше (выше), чем у кодов с кодовым расстоянием 4. Это объясняется тем, что во втором случае увеличивается число разрешенных комбинаций. Наличие экстремальных точек объясняется тем, что с ростом кратности ошибки данная вероятность становится соизмеримой с разрядностью искаженного слова.

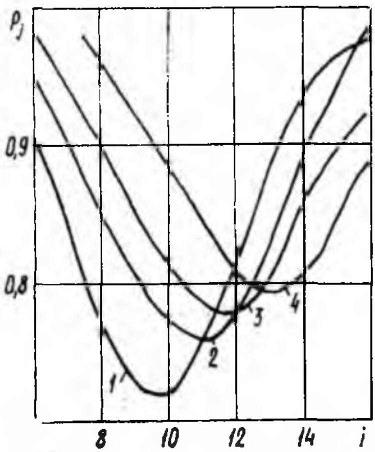

Рис. 3

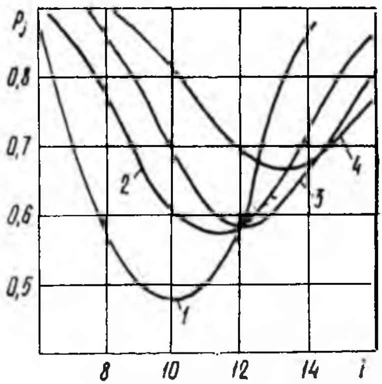

Рис. 4.

На рис. 3, 4 приведены зависимости вероятности обнаружения ошибок четной кратности при различном количестве информационных разрядов m и кодовым расстоянием *3* (рис. 3), *4* (рис. 4), где *1* — $m=14$; *2* — $m=16$; *3* — $m=18$; *4* — $m=20$. Анализ зависимости показывает, что коды Хэмминга с высокой вероятностью обнаруживают ошибки малой и большой кратности, т. е. на краях интервала кода. Это объясняется тем, что количество таких векторов минимально.

В процессе контроля с помощью кода Хэмминга с минимальным весом *3* при возникновении ошибки возможны два случая. В контрольном разряде осуществляется проверка на четность всего кодового слова. Если результат равен единице, то предполагается, что произошла ошибка и результат проверки кодом Хэмминга определяет номер искаженного разряда. Если результат проверки на четность 0, а проверка кодом Хэмминга «говорит», что имеется ошибка, то полагается, что обнаружена неисправимая ошибка.

Код Хэмминга с минимальным весом *4* обеспечивает распознавание ошибок, относящихся к двум подмножествам: подмножеству четных и подмножеству нечетных ошибок. Если ошибка нечетной кратности $i \geqslant 3$, то коррекция контролируемого слова будет осуществляться неверно, т. е. будут исправляться не те разряды.

Как показывают исследования, применение кода Хэмминга для распознавания многократных ошибок с минимальным кодовым расстоянием 4 эквивалентно наличию в контрольном слове двух контрольных точек, осуществляющих контроль по модулю 2.

Поступила в редколлегию 14.09.89