ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 19 МАТЕМАТИКИ Выпуск 3
2012

Н. Б. Буторина, **Ю. Б. Буркатовская** (Томск, ТГУ, ТПУ). **Оценка числа слагаемых, представляющих одиночные кодовые слова равновесного кода, в специальном представлении множества всех кодовых слов.**

При обеспечении самопроверяемости дискретных устройств требуется разрабатывать самотестируемые детекторы кодов. Самотестируемость означает, что в рамках рассматриваемого класса неисправностей для каждой из неисправностей существует тестовый набор среди множества всех кодовых слов детектора.

Для компактного представления всех кодовых слов ранее была предложена специальная формула $A(X)$ разложения кодовых слов (m,n)-кода; $D_p^q(X^r)$ — это дизъюнкция конъюнкций, представляющих все равновесные (q,p)-кодовые слова, $p<n$, $q\leqslant p$, $X^r\subset X$, $X=\{x_1,x_2,\ldots,x_n\}$. Будем считать, что $n=2m$. Разделим множество X на два подмножества X^1, X^2, где $X^1=\{x_1,x_2,\ldots,x_g\}$, $X^2=\{x_{g+1},x_{g+2},\ldots,x_n\}$.

Теорема 1. $D_p^q(X)=\sum_{i=E_1}^{E_2}D_g^i(X^1)D_{n-g}^{q-i}(X^2)$, *где* $E_1=\max\{0,g+q-p\}$, $E_2=\min\{g,q\}$.

Первоначальное множество переменных X мощности n разбивается на два подмножества X^1 и X^2, $|X^1|=g=\lceil n/2\rceil$, $|X^2|=s=n-g$, и к $D_n^m(X)$ применяется теорема 1. Если $g>2$ и $s>2$, то теорема 1 используется еще раз для каждого коэффициента разложения $D_g^i(X^1)$, $D_s^{q-i}(X^2)$, $E_1\leqslant i\leqslant E_2$, и т.д. В результате получаем формулу A, задающую все кодовые слова (m,n)-кода.

Число l достигаемых кодовых слов может быть меньше числа всевозможных кодовых слов C_n^m. Важно, чтобы свойство самотестируемости обеспечивалось именно на поступающих на входы детектора кодовых словах. Для решения этой задачи множество всех кодовых слов представляется суммой таких подмножеств кодовых слов, что каждое подмножество задается выражением

$$D_2^{q_1}(X^1)\ldots D_2^{q_a}(X^a)D_1^{p_1}(X^{a+1})\ldots D_1^{p_b}(X^h). \qquad (1)$$

В работе, представленной данным сообщением, дана оценка числа всех слагаемых в разложении и слагаемых вида (1), представляющих одно кодовое слово. Полученные оценки позволят доказать, что для любого l подобное разложение возможно.

Чтобы слагаемое вида (1) представляло одно кодовое слово, необходимо, чтобы все q_i в $D_2^{q_i}(X^i)$ были равны либо 0, либо 2.

Введем следующие обозначения для формулы (1): a — количество $D_2^{q_i}(X^i)$, b — количество $D_1^{p_i}(X^{a+i})$, a_0 — число q_i, равных 0, a_1 — число q_i, равных 1, a_2 — число q_i, равных 2, b_0 — число p_j, равных 0, b_1 — число p_j, равных 1.

Теорема 2. *Количество* V *всех слагаемых вида* (1) *в формуле* A *равно*

$$V=\sum_{b_1=0}^{b}C_b^{b_1}\sum_{a_2=E_1}^{E_2}C_a^{a_2}C_{a-a_2}^{m-b_1-2a_2},$$

где $E_1 = \max\{0, m - b_1 - a\}$, $E_2 = \lfloor (m - b_1)/2 \rfloor$.

Теорема 3. *Количество* W *слагаемых вида* (1) *в формуле* A, *представляющих одно кодовое слово, равно*

$$W = \sum_{a_2 = U_1}^{U_2} C_a^{a_2} C_b^{m-2a_2}, \text{ где } U_1 = \lceil (m - b)/2 \rceil, \quad U_2 = \lfloor m/2 \rfloor.$$

На основе формулы A для любого подмножества кодовых слов мощности l строится самотестируемый детектор.