ГЕНЕРАЦИЯ СЛОВ СМЕЖНЫХ КЛАССОВ КОДА ХЭММИНГА

Махнист Л. П.

Брестский политехнический институт
224017, г. Брест, ул. Московская, 267

Аннотация. Предложен алгоритм формирования слов фиксированного веса смежных классов кода Хэмминга.

Ключевые слова: корректирующий код, код Хэмминга.

В работе предложен алгоритм генерирования всех двоичных последовательностей фиксированного веса заданного смежного класса кода Хэмминга [1]. Данный алгоритм предназначен для решения указанной задачи независимо от величины задаваемого веса, в отличие от алгоритмов, рассчитанных лишь для малых весов [2, 3]. В его основу положен алгоритм генерирования всех кодовых слов заданного веса расширенного кода Хэмминга, т.е. кода длины 2^m с добавлением общей проверки на четность.

Алгоритм формирования всех кодовых слов весов от 0 до некоторого заданного четного числа k ($0 \le k \le N$) расширенного кода Хэмминга H(m) длины $N = 2^m$.

<u>Исходные данные:</u>

- исходный вектор (00) веса 0 длины N = 2;
- $N = 2^m$;
- $0 \le k \le N$, $k \ne 2$, $N-2$;

<u>Выходные данные:</u>

- множество всех кодовых слов весов от 0 до некоторого заданного четного числа $k \le N$ расширенного кода Хэмминга H(m) длины $N=2^m$;

<u>Обозначения:</u>

A(i) - множество всех векторов кода H(i), вес которых не превосходит заданное число k ($1 \le i \le m$);

j - вес элемента (вектора) $\overline{a}$ множества A(i) (j - четно, $j \le k$, $j \ne 2$, $2^i - 2$, $i \ge 2$);

<u>Алгоритм:</u>

1. i:=1, A(i):={(00)};

2. i:=i+1, если i>m, то перейти к п.8; A(i):= {∅};

3. Если A(i-1) не пусто, то взять элемент $\overline{a}$ множества A(i-1), в противном случае перейти к п.2; A(i-1):= A(i-1) \ {$\overline{a}$};

4. Определить вес j вектора $\overline{a}$; если j=0, то перейти к п.5, в противном случае к п.6;

5. Построить все вспомогательные векторы $\bar{c}$ веса p_0 длины 2^{i-1}, которые содержат p_0 единиц в позициях, в которых вектор $\bar{a}$ содержит нули, где:

- p_0 изменяется от 0 до U=min {2(k div 4), 2^{i-1}} с шагом 2; перейти к п.7;

6. Построить вспомогательные векторы $\bar{c}$ веса p_0+p_1 длины 2^{i-1}, которые содержат p_0 единиц в позициях, где вектор $\bar{a}$ содержит нули, и p_1 единиц в позициях, где вектор $\bar{a}$ содержит единицы. При этом:

- p_0 изменяется от 0 до V=min {(k-j) div 2, 2^{i-1}-j} с шагом 1;

- p_1 изменяется от 0 до j с шагом 2, если p_0 - четно;

- p_1 изменяется от 1 до j-1 с шагом 2, если p_0 - нечетно;

7. Добавить в множество A(i) все элементы, которые образуются с помощью вектора $\bar{a}$ множества A(i-1) и любого из вспомогательных векторов $\bar{c}$ длины 2^{i-1} по следующему правилу: $(\bar{c}|\bar{c}\ \text{xor}\ \bar{a})$, где операция "xor" - побитовая исключающая "или"; перейти к п.3;

8. End.

Замечание.

1. Вектор, сформированный по правилу п.7, имеет вес $j+2p_0$.

2. Количество векторов, полученных по вектору $\bar{a}$ длины $n=2^{i-1}$ веса j можно определить по формуле:

$\sum_{p=0}^{U div 2} C_n^{2p}$, если j=0 (во введенных выше обозначениях $p_0=2p$);

$\sum_{p_0=0}^{V}(C_{n-j}^{p_0}\sum_{p_1} C_j^{p_1})$, где внутреннее суммирование производится по параметру p_1 от 0 до j с шагом 2, если p_0 – четно, и от 1 до j-1 с шагом 2, если p_0 – нечетно ($j\neq 0$).

3. В алгоритме для формирования множества A(m) можно использовать только два множества на каждом шаге алгоритма.

Пример. В основу данного алгоритма положено следующее свойство кодовых слов расширенного кода Хэмминга: кодовое слово длины 2^m дает возможность получить кодовые слова в два раза большей длины. Например, слово $\bar{a}$=0000. Составляются все векторы $\bar{c}$ четного веса этой длины: $\bar{c}$=0000; 1100; 1010; 1001; 0110; 0101; 0011; 1111. Тогда слова в два раза большей длины будут образованы по правилу $(\bar{c}|\bar{c}\ \text{xor}\ \bar{a})$, т.е. 00000000; 11001100; 10101010; и т. д. Если ставится задача нахождения векторов только веса k, то на последнем шаге алгоритма создаются только вектора этого веса.

Идея алгоритма генерации всех векторов заданной длины $n=2^m-1$, веса k, принадлежащих коду Хэмминга или заданному смежному классу кода, состоит в следующем.

Рассмотрим множества этих векторов, которые обозначим через $V_0(k)$ и $V(k)$ соответственно. Заметим, что в общем случае не принципиально, какое из множеств $V_0(k)$ или $V(k)$ нами будет получено. Действительно, пусть даны множества $V_0(k-1)$ и $V_0(k+1)$. Тогда, прибавив к каждому вектору множества $V_0(k-1)$, не содержащему единицы в некоторой фиксированной позиции i и к каждому вектору $V_0(k+1)$, содержащему единицу в этой же фиксированной позиции, вектор с одной единицей в позиции i, получим все вектора множества $V(k)$. Также, очевидно, что множества $V(k)$, соответствующие различным смежным классам неразличимы с точностью до фиксированной подстановки. Т.е. достаточно уметь генерировать $V_0(k)$ - кодовые слова кода Хэмминга веса k. Предлагаемый алгоритм осуществляет генерацию всех векторов веса от 0 до заданного числа k расширенного кода Хэмминга, т. е. кода длины 2^m с добавлением общей проверки на четность. Получить векторы только веса k несложно, зная все вектора весов от 0 до k в два раза меньшей длины. Для этого на последнем шаге алгоритма, когда $i=m$, p_0 берут таким, чтобы выполнялось соотношение $j+2p_0=k$. Требуемые векторы заданного веса k кода Хэмминга получаются из векторов веса k (если k - четно) или k+1 (если k - нечетно) соответствующего расширенного кода путем удаления координаты, соответствующей нулевому столбцу проверочной матрицы расширенного кода Хэмминга.

Следует заметить, что идея данного алгоритма может быть использована при решении аналогичной задачи для примитивных кодов Боуза-Чоудхури-Хоквингема, исправляющих две ошибки, а также кодов Мелласа [1].

Литература

1. Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки: Пер. с англ. - М.: Связь, 1979. – 744 с.

2. Demidenko S., Piuri V., Ivanyukovich A. Error Localization in Test Outputs: a Generalized Analysis of Signature Compression // IEEE Second Asian Test Symposium (ATS-93). - Beijing, China, 1993. – P. 317-322.

3. Demidenko S., Ivanyukovich A., Makhnist L., Piuri V. Validity of the Compression Techniques on the Hamming Code and Its Modifications in Digital Circuit Testing // Sixth International Symposium on IC Technology, Systems & Applications (ISIC - 95), Singapore, September, 1995. – P. 301-305.