ՀԱՅԿԱԿԱՆ ՍՍՌ ԳԻՏՈՒԹՅՈՒՆՆԵՐԻ ԱԿԱԴԵՄԻԱՅԻ ԶԵԿՈՒՅՑՆԵՐ
ДОКЛАДЫ АКАДЕМИИ НАУК АРМЯНСКОЙ ССР
XXXVII 1963 1

МАТЕМАТИКА

А. В. Петросян, Б. С. Мнацаканян и Ш. Е. Бозоян

Некоторые свойства кода Хемминга

(Представлено академиком АН Армянской ССР С. Н. Мергеляном 17/I 1963)

В работе ([1]) Р. В. Хеммингом полностью решена теоретическая сторона вопроса о нахождении и исправлении одиночных ошибок, однако, как показывает опыт, техническое осуществление таких исправляющих устройств является сложным для параллельных ([2]) и непрактичным для последовательных передач.

До сих пор не разработан достаточно надежный и простой метод обнаружения и исправления даже одиночных ошибок при передаче цифровой информации, представленной в двоичном виде.

В данной работе выявляются некоторые свойства кода с обнаружением и исправлением одиночных ошибок, которые существенно упрощают его использование.

В работе ([1]) рассматривался код с исправлением одиночных ошибок, который из общего числа позиций n для передачи информации использует m позиций. $k = n - m$ позиций используются в качестве проверочных, причем между n и m имеется следующее соотношение:

$$2^m \leqslant \frac{2^n}{n+1}. \qquad (1)$$

Начиная с первого пронумеруем позиции этого кода $\alpha_1, \alpha_2, \cdots \alpha_n$ (где α_i может быть нулем или единицей) и номера позиций представим с помощью k—разрядных двоичных чисел

$$i = \beta_{k,i}\, \beta_{k-1,i} \cdots \beta_{1,i}$$

далее все позиции разобем на k групп так, чтобы данная позиция i входила в r-тую группу, тогда и только тогда, когда $\beta_{r,i} = 1$. Проверочные позиции надо распределить так, чтобы в каждую группу входила хотя бы одна из них.

Для того чтобы эффективность кода $R = \frac{n}{m}$ была большой, необходимо при фиксированном m брать k минимальным, удовлетворяющим условию (1), а это означает, что необходимо брать в каждой группе по одной контрольной позиции.

Такими позициями, которые в соответствии с вышеизложенным разбиением содержались по одной в каждой группе, являются позиции с номерами 2^{r-1}. Для заданного m-позиционного двоичного набора проверочные разряды заполняются таким образом, чтобы в каждой группе число позиций, содержащих единицу, было четным, т. е. принимается:

$$\alpha_{2^{r-1}} = \sum_{\substack{\text{По всем воз-} \\ \text{можным } i \neq 2^{r-1}}} \alpha_{\beta_{k,i} \cdots \beta_{r+1,i} \beta_{r-1,i} \cdots \beta_{1,i}} \qquad (2)$$

$$(r = 1, 2, \cdots, k)^{*}.$$

Определение 1. n—разрядный двоичный код называется кодом Хемминга, если он удовлетворяет условию (2).

Если происходит изменение кода Хемминга только в одном i-том разряде, то нарушается условие (2) только для тех r, для которых $\beta_{r,i} = 1$.

Таким образом, чтобы исправить одиночную ошибку, надо найти все те $r_1, r_2, \cdots, r_s$, для которых нарушено условие (2), и в позиции $l = 2^{r_1-1} + 2^{r_2-1} + \cdots + 2^{r_s-1}$ исправить ошибку.

При конкретном применении этого способа исправления одиночных ошибок необходимо создать устройства, обладающие следующими возможностями:

1) определение значений проверочных разрядов по формуле (2);

2) определение того, является ли данный код кодом Хемминга, т. е. для всех ли групп имеет место соотношение (2) или нет;

3) в случае несоответствия нахождение чисел $r_1, r_2, \cdots, r_s$ и исправление ошибки в l-й позиции.

Нижеприведенные теоремы выясняют некоторые свойства кодов Хемминга, которые существенно упрощают создание устройства с вышеизложенными возможностями для последовательных передач информаций.

После этого, когда будем говорить о двоичном коде, будем предполагать, что в нем имеется n позиций, из которых m используется для передачи информации, причем n выбирается минимальным, удовлетворяющим условию (1).

Теорема 1. *Для того чтобы данный n-разрядный двоичный код был кодом Хемминга, необходимо и достаточно, чтобы поразрядная сумма по модулю два всех номеров тех позиций, где записана единица, равнялась нулю.*

Доказательство этой теоремы непосредственно следует из следующей системы равенств:

---

* $\sum \oplus$ означает сложение по модулю 2.

$$\sum_{i=1}^{n} \oplus x_i \beta_{r,i} = \sum_{\text{по всем возможным } i} \oplus x_{i_k,i} \cdots \beta_{r+1,i} \beta_{r-1,i} \cdots \beta_{1,i} \qquad (3)$$

$$(r = 1, 2, \cdots, k).$$

Из равенства (2) следует, что

$$\sum_{\text{по всем возможным } i} \oplus x_{i_k,i} \cdots \beta_{r+1,i} \beta_{r-1,i} \cdots \beta_{1,i} =$$

$$= \alpha_{2^{r-1}} \oplus \sum_{\substack{\text{по всем возможным} \\ i \neq 2^{r-1}}} x_{i_k,i} \cdots \beta_{r+1,i} \beta_{r-1,i} \cdots \beta_{1,i} = x_{2^{r-1}} \oplus x_{2^{r-1}} = 0.$$

$$(r = 1, 2, \cdots, k).$$

Но тогда из равенства (3) следует, что

$$\sum_{i=1}^{n} \oplus x_i \beta_{r,i} = 0, \qquad (4)$$

$$(r = 1, 2, \cdots, k).$$

И наоборот, если равенства (4) имеют место, то из равенств (3) следует, что их правые части тоже равны нулю, т. е. имеют место соотношения (2). Этим доказательство теоремы завершается.

Теорема 2. *k—разрядный двоичный код* $x_{2^{k-1}} \cdots x_{2^{r-1}} \cdots x_{2^0}$, *составленный из всех проверочных позиций кода Хемминга, является поразрядной суммой по модулю два всех номеров информационных позиций, где записаны единицы.*

Доказательство этой теоремы сводится к доказательству следующих равенств:

$$\alpha_{2^{r-1}} = \sum_{\substack{i=1 \\ i \neq 2^{r-1}}}^{n} \oplus x_i \beta_{r,i} \quad (r = 1, 2, \cdots, k; \quad \gamma - \text{любое целое}). \qquad (5)$$

Для доказательства этого равенства заметим, что

$$\sum_{\substack{i=1 \\ i \neq 2^{\gamma-1}}}^{n} \oplus \alpha_i \beta_{r,i} = \sum_{\substack{i=1 \\ i \neq 2^{r-1}}} \oplus \alpha_i \beta_{r,i} \quad (r = 1, 2, \cdots, k; \quad \gamma - \text{любое целое}) \qquad (6)$$

потому, что для остальных γ, r-тый разряд его двоичного представления равен нулю. Теперь, так как код является кодом Хемминга, по теореме 1 удовлетворяются условия (4), откуда, если учесть равенства (6), непосредственно получим (5), чем и завершится доказательство теоремы.

Теорема 3. *Номер позиции одиночного сбоя, происшедшего в коде Хемминга, равен поразрядной сумме по модулю два всех номеров тех позиций ошибочного кода, где записаны единицы.*

Доказательство: Предположим, что этот одиночный сбой произошел в позиции с номером $l = \beta_{k,l}\beta_{k-1,l}\cdots\beta_{1,l}$. Таким образом, доказательство теоремы сводится к доказательству равенств:

$$\beta_{r,l} = \sum_{i=1}^{n} \oplus \alpha_i \beta_{r,i} \quad (r = 1, 2, \cdots, k).$$

Но

$$\sum_{i=1}^{n} \oplus \alpha_i \beta_{r,i} = \alpha_l \beta_{r,l} \oplus \sum_{i+l}^{n} \oplus \alpha_i \beta_{r,i} =$$

$$= \alpha_l \beta_{r,l} \oplus \bar{\alpha}_l \beta_{r,l} \oplus \left(\bar{\alpha}_l \beta_{r,l} \oplus \sum_{\substack{i-1 \\ i-l}} \oplus \alpha_i \beta_{r,i}\right) = \beta_{r,l}.$$

Так как сумма в скобках является аналогичной сумме (4) для восстановленного кода Хемминга, поэтому она равна нулю, а

$$\bar{\alpha}_l \beta_{r,l} \oplus \alpha_l \beta_{r,l} = \beta_{r,l}.$$

Этим завершается доказательство теоремы.

Проведен полный анализ логических схем, практически осуществляющих применения этого кода, с исправлением одиночных ошибок для последовательных устройств (магнитная лента, ввод).

Проведенный анализ показал, что вышеизложенные теоремы существенно упрощают его применение и в несколько раз уменьшают количество дополнительного оборудования, требуемого для исправления одиночных ошибок.

Предприятие п/я 13, г. Ереван

Ա. Վ. ՊԵՏՐՈՍՅԱՆ. Բ. Ս. ՄՆԱՑԱԿԱՆՅԱՆ ԵՎ Շ. Ե. ԲՈՋՈՅԱՆ

Հեմինգի կոդի որոշ հատկություններ

Հեմինգը (1) աշխատանքում դիտարկել է երկուական սիստեմայով կոդավորված տվյալների աղմուկների առկայության դեպքում, անսխալ հաղորդելու խնդիրը։ Այնպիսի աղմուկների դեպքում, որոնք կարող են աղավաղել ոչ ավելի քան մեկ երկուական կարգ յուրաքանչյուր n երկարություն ունեցող հաջորդականության մեջ, Հեմինգը առաջարկել է կոդավորման մի մեթոդ, որը հնարավորություն է տալիս իրականացնել տվյալների անսխալ հաղորդումը։

Սակայն, այդ կոդերի իրականացումը կապված էր մեծ դժվարությունների հետ։ Այդ դժվարություններն պայմանավորված էին նրանով, որ անհրաժեշտ էր n երկարություն ունեցող կոդը վերածել իրար հետ հաավոդ, որոշ քանակությամբ խմբերի և գործողություններ կատարել յուրաքանչյուր խմբի հետ առանձին։

Այս աշխատանքում ի հայտ են բերված Հեմինգի կոդերի որոշ հատկություններ, որոնք ամփոփված են երեք թեորեմներում։ Այդ հատկությունները ցույց են տալիս, որ կարելի է գործողությունները կատարել առանց խմբերի բաժանման, որը էապես պարզեցնում է նրանց կիրառությունը։

ЛИТЕРАТУРА — ԳՐԱԿԱՆՈՒԹՅՈՒՆ

[1] *Р. В. Хемминг*, Сб.: Коды с обнаружением и исправлением ошибок, ИЛ, М., 1956. [2] *Б. С. Мнацаканян*. Автоматический контроль ЭВМ параллельного действия. Вопросы радиоэлектроники, Серия VII, электронная вычислительная техника. Вып. 2, 1962.