Р. Д. ПЕТРОСЯН

ОБ ОДНОЙ ОБЩЕЙ СХЕМЕ ДЕКОДИРОВАНИЯ ЦИКЛИЧЕСКИХ КОДОВ

В работе дается описание общей декодирующей схемы для циклических (n, k)-кодов, наиболее целесообразной при любом из следующих условий:

а) число исправляемых ошибок $r \leqslant 3$, k — любое,

б) число информационных символов $k \leqslant 5$, r — любое.

Рассмотрим случай двоичных кодов. Пусть множество всех кодовых слов H двоичного циклического (n, k)-кода, исправляющего r ошибок, разбито на непересекающиеся подмножества $A_1, A_2, \cdots, A_k$; при этом подмножество A_i включает все те кодовые слова, среди информационных символов каждого из которых содержится i единиц.

Выпишем элементы $A_1 - \{l_1, l_2, \cdots, l_k\}$:

$$\begin{array}{l} l_1 - \\ l_2 - \\ \vdots \\ l_k - \end{array} \begin{bmatrix} \alpha_{1,1}, & \alpha_{1,2}, & \cdots, & \alpha_{1,k}, & \alpha_{1,k+1}, & \alpha_{1,k+2}, & \cdots, & \alpha_{1,k+h} \\ \alpha_{2,1}, & \alpha_{2,2}, & \cdots, & \alpha_{2,k}, & \alpha_{2,k+1}, & \alpha_{2,k+2}, & \cdots, & \alpha_{2,k+h} \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ \alpha_{k,1}, & \alpha_{k,2}, & \cdots, & \alpha_{k,k}, & \alpha_{k,k+1}, & \alpha_{k,k+2}, & \cdots, & \alpha_{k,k+h} \end{bmatrix}$$

Пусть $\alpha_{1,1} = \alpha_{2,2} = \cdots = \alpha_{k,k} = 1$, $\alpha_{i,i} \neq \alpha_{i,j}$ $(i \neq j,\ i, j \leqslant k)$. Рассмотрим $(k+j)$-ый $(j = 1, 2, \cdots, h)$ столбец матрицы A_1:

$$\alpha_{i,\,k+j} = \sum_{t=1}^{k} C_{k+j} \cdot \alpha_{i,\,t},$$

где $C_{k+j,\,t}$ — коэффициенты проверочного соотношения для проверочного символа $\alpha_{i,\,k+j}$.

Поскольку $\begin{bmatrix} \alpha_{1,1}, & \alpha_{1,2}, & \cdots, & \alpha_{1,k} \\ \alpha_{2,1}, & \alpha_{2,2}, & \cdots, & \alpha_{2,k} \\ \vdots & \vdots & & \vdots \\ \alpha_{k,1}, & \alpha_{k,2}, & \cdots, & \alpha_{k,k} \end{bmatrix}$ — единичная матрица,

справедливы следующие равенства:

$$
\begin{aligned}
a_{1,\,k+j} &= C_{k+j,\,1}\,, \\
a_{2,\,k+j} &= C_{k+j,\,2}\,, \\
&\vdots \\
a_{k,\,k+j} &= C_{k+j,\,k}.
\end{aligned}
\tag{1}
$$

Для циклических кодов справедливы также следующие равенства:

$$
\begin{aligned}
C_{k+j,\,1} &= C_{k+1,\,1} \cdot C_{k+j-1,\,k} \\
C_{k+j,\,2} &= C_{k+j-1,\,1} + C_{k+1,\,2} \cdot C_{k+j-1,\,k} \\
C_{k+j,\,3} &= C_{k+j-1,\,2} + C_{k+1,\,3} \cdot C_{k+j-1,\,k} \\
&\vdots \\
C_{k+j,\,k} &= C_{k+j-1,\,k-1} + C_{k+1,\,k} \cdot C_{k+j-1,\,k}.
\end{aligned}
\tag{2}
$$

Ниже будет показано, что техническая реализация устройства для получения коэффициентов $C_{k+j,\,1}, C_{k+j,\,2}, \cdots, C_{k+j,\,k}$ по сложности такая же, что и кодирующего устройства. Как известно [1], кодирование для циклического (n, k)-кода, порожденного многочленом $g(x)$ степени $n-k$, может быть произведено с помощью регистра сдвига, соединения в котором соответствуют многочлену $h(x) = (x^n - 1)/g(x)$ (рис. 1).

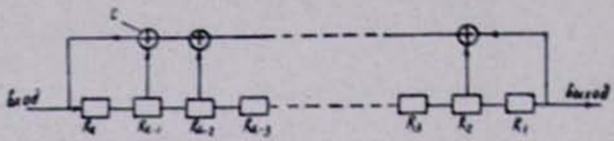

Рис. 1.

Рассмотрим теперь несколько видоизмененную схему (рис. 2), в которой каждый сумматор C, связанный, как и в предыдущей схеме, с регистром R_i в соответствии с многочленом $h(x)$, соединен еще с соседним с R_i справа регистром R_{i-1}, а сдвиг производится в противоположном направлении — по часовой стрелке.

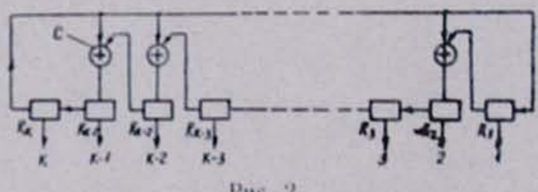

Рис. 2.

Рис. 1 и 2 соответствуют случаю, когда коэффициенты $C_{k+1,\,1}, C_{k+1,2}, \cdots, C_{k+1,\,k}$ многочлена $h(x)$ равны, соответственно, 1, 1, 0, $\cdots$, 0, 1, 1, 0.

Перед началом работы устройства (рис. 2) в регистрах $R_1, \cdots, R_k$ записываются коэффициенты, соответственно $C_{k+1,1}, C_{k+1,\,2}, \cdots, C_{k+1,\,k}$ проверочного соотношения для проверочного символа $a_{l,\,k+1}$. Работа устройства заключается в следующем: на l-ом такте либо происходит циклический сдвиг содержимого $R_1, \cdots, R_k$ (если $C_{k+l-1,k} = a_{k,k+l-1} = 0$ и на выходе каждого из сумматоров C будем иметь содержимое предыдущего регистра), либо к результату циклического сдвига содержимого регистров $R_1, \cdots, R_k$ прибавляется „1“ в тех разрядах, в которых перед началом работы устройства были записаны единицы (если $C_{k+l-1,k} = a_{k,k+l-1} = 1$).

Таким образом, на выходных шинах $1, 2, \cdots, k$ регистров $R_1, \cdots, R_k$ за $(h-1)$ тактов, ввиду (1) и (2), мы получим все проверочные символы кодовых слов, соответственно $l_1, l_2, \cdots, l_k$.

Теперь рассмотрим декодирующую схему (рис. 3).

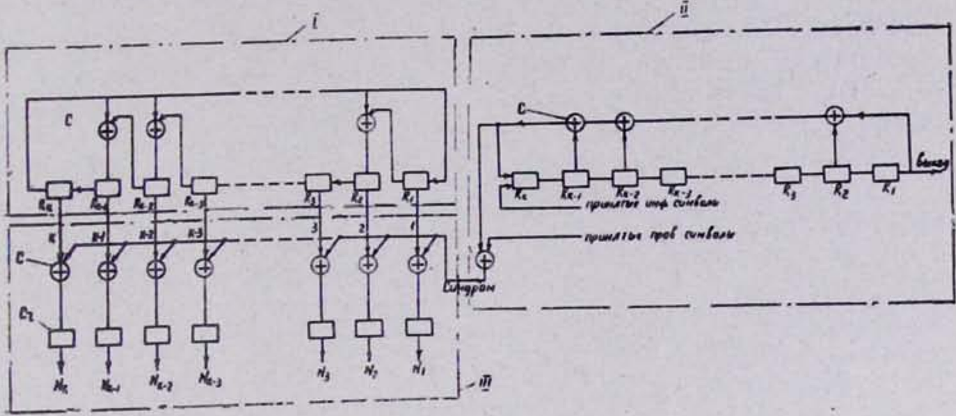

Рис. 3

Схема состоит из трех частей:

I — описанная выше схема (рис. 2);

II — кодирующее устройство, на вход которого подаются принятые информационные символы. Выходные символы вместе с принятыми проверочными символами поступают на вход сумматора, на выходе которого образуются компоненты проверочного вектора-синдрома;

III — компоненты проверочного вектора и проверочные символы кодовых слов $l_1, \cdots, l_k$ подаются на входы сумматоров „C“. При этом на l-ом такте происходит суммирование l-ой компоненты синдрома с l-ым столбцом матрицы A_1:

$$a_{1,k+l}\,,\ a_{2,k+l}\,,\ \cdots,\ a_{k,k+l}\,.$$

Результаты суммирования поступают на входы счетчиков — Сч. Через h тактов на счетчиках образуется k показаний: $N_1, \cdots, N_k$, по которым можно судить об ошибках, имевших место при передаче.

Пусть наш код исправляет 3 ошибки.

Возможные случаи:

1) одна ошибка в информационной части и 0, 1 или 2 ошибки в проверочной части принятого кодового слова. Очевидно, что среди $N_1, \cdots, N_k$ некоторое $N_i \leqslant 2$, $N_j > 2$, $j = 1, \cdots, k$, $j \neq i$. Тогда можно сказать, что i-ый информационный символ был принят ошибочно, остальные информационные символы — правильно;

2) 3 ошибки в информационной части, в проверочной части нет ошибок.

Обозначим множество всевозможных различных значений весов проверочной части кодовых слов (число единичных символов среди проверочных символов кодового слова) подмножеств A_2 и A_3 соответственно через $\hat{\varepsilon}_2$ и $\hat{\varepsilon}_3$. Тогда можно утверждать, что среди $N_1, \cdots, N_k$ какие-то три показания счетчиков будут

$$N_i, N_j, N_t \subset \hat{\varepsilon}_2, N_l \subset \hat{\varepsilon}_3, l \neq i, j, t.$$

Очевидно, что если $\hat{\varepsilon}_2$ и $\hat{\varepsilon}_3$ не пересекаются, номера i, j, t будут соответствовать ошибочно принятым информационным символам;

3) 2 ошибки в информационной части. В проверочной части 1 ошибка или нет ошибок.

Можно исправить двумя способами:

а) изменить первый информационный символ принятого слова на противоположный и проверить, имеет ли место случай 1. Затем это проделать со вторым информационным символом, и т. д. Ясно, что из k проверок две будут соответствовать случаю 1, и, следовательно, соответствующие два информационных символа и должны были быть ошибочно принятыми.

б) Если образовать все комбинации по два из проверочных символов кодовых слов $l_1, \cdots, l_k$, можно получить проверочные символы всех кодовых слов из A_2—суммированием каждой пары символов (рис. 4).

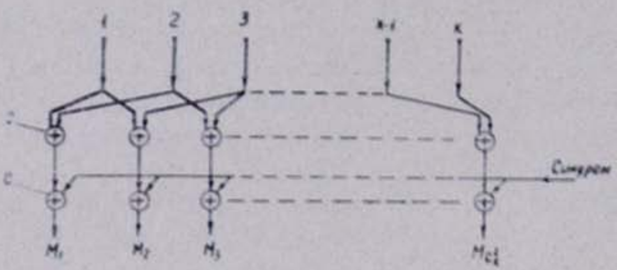

Рис. 4

Поэтому достаточно иметь еще $2 \cdot C_k^2$ сумматоров и C_k^2 счетчиков и тогда по показаниям $M_1, M_2, \cdots, M_{C_k^2}$ счетчиков можно будет определить номера i и j ошибочно принятых информационных символов:

$$M_i < 1, M_j < 1, M_t > 1, t \neq i, j.$$

Достоинством этого способа является то, что при этом не требуется повышения скорости обработки информации и требования к дополнительному оборудованию — счетчикам — минимальные. Однако при больших k, ввиду громоздкости, он может оказаться нецелесообразным.

4) Все информационные символы приняты правильно. Число единичных символов среди всех символов проверочного вектора (вес синдрома) должно быть не более 3. Потребуется еще один счетчик.

Аналогичные схемы можно построить и для (n, k)-кодов при $r > 3$, но $k \leqslant 5$.

Так, если $k = 5$, можно поступить следующим образом. Пусть принято кодовое слово $\alpha_1, \alpha_2, \cdots, \alpha_k, \alpha_{k+1}, \cdots, \alpha_n$. Образовать новое слово $\overline{\alpha}_1, \overline{\alpha}_2, \cdots, \overline{\alpha}_k, \alpha_{k+1}, \alpha_{k+2}, \cdots, \alpha_n$, отличающееся от первого в первых k разрядах:

$$\begin{aligned} \overline{\alpha}_1 &= \alpha_1 + 1, \\ \overline{\alpha}_2 &= \alpha_2 + 1, \\ &\vdots \\ \overline{\alpha}_k &= \alpha_k + 1, \end{aligned}$$

и проверить для этих двух слов вышеописанным способом выполнение условий 1, 3, 4. Ясно, что этим исчерпываются все возможные случаи.

Очевидно, что описанный способ декодирования можно обобщить для случая недвоичных (n, k)-кодов — это вытекает из возможности обобщения самой кодирующей схемы.

Автор благодарен Р. Р. Варшамову за внимание к данной работе.

Ռ. Դ. ՊԵՏՐՈՍՅԱՆ

ՑԻԿԼԻԿ ԿՈԴԵՐԻ ԱՊԱԿՈԴԱՎՈՐՄԱՆ ՄԻ ԸՆԴՀԱՆՈՒՐ ՍԽԵՄԱՅԻ ՄԱՍԻՆ

Ա մ փ ո փ ո ւ մ

Դիտարկվում է երկուական ցիկլիկ կոդերի ապակոդավորման բավական էֆեկտիվ սխեմա, որը հեշտությամբ ընդհանրացվում է նաև ոչ երկուական ցիկլիկ կոդերի համար, հետևյալ պայմաններից որևէ մեկի առկայության դեպքում.

1) Ուղղվող սխալների քանակը $r \leqslant 3$, ցանկացած k-ի համար,

2) Ինֆորմացիոն նիշերի քանակը $k \leqslant 5$. ցանկացած r-ի համար։
Հատուկ հաշվիչների միջոցով գտնվում է, թե ստուգողական վեկտորի և այն կոդային բառերի մեջ, որոնք ինֆորմացիոն նիշերի մեջ պարունակում են միայն մեկ հատ «1», քանի համընկնող նիշեր կան, ընդ որում օգտագործվում է այն հանգամանքը, որ այդ բառերի j-րդ ստուգողական նիշերը համընկնում են j-րդ ստուգողական հավասարման գործակիցներին, իսկ վերջիններս իրացնող հարմարանքի բարդությունը, ինչպես ցույց է տրվում, չի գերազանցում կոդավորման հարմարանքի բարդությանը։

ЛИТЕРАТУРА

1. *У. Питерсон*. Коды, исправляющие ошибки. М., 1964.