ՀԱՅԿԱԿԱՆ ՍՍՌ ԳԻՏՈՒԹՅՈՒՆՆԵՐԻ ԱԿԱԴԵՄԻԱՅԻ ՏԵՂԵԿԱԳԻՐ
ИЗВЕСТИЯ АКАДЕМИИ НАУК АРМЯНСКОЙ ССР

Ֆիզիկա-մաթեմատ. գիտություններ XVI, № 6, 1963 Физико-математические науки

ВЫЧИСЛИТЕЛЬНАЯ МАТЕМАТИКА

Г. А. Гаракоп

Коды Р. К. Боуза—Д. К. Рой-Чоудхури и вопросы их схемной реализации

В статье приводятся основные сведения из теории кодов Боуза-Чоудхури. На примере построения и реализации кода (63, 45), исправляющего до трех независимых ошибок, рассматриваются вопросы схемной реализации кодов Боуза—Чоудхури.

§ 1. Коды Боуза—Чоудхури

В работе [1] достаточно подробно излагаются вопросы теории кодов Боуза—Чоудхури. В целях полноты изложения в настоящей статье приводятся (без доказательств) необходимые нам результаты из указанной работы.

1. Определение кодов Боуза—Чоудхури

Для любых целых положительных m и t существует код длины $n=2^m-1$, исправляющий t ошибок, число избыточных разрядов которого не более $m\cdot t$.

Такой код можно построить, исходя из неприводимого полинома

$$P(x)=a_0+a_1x+a_2x^2+\cdots+a_mx^m \qquad (1.1)$$

с коэффициентами 0 и 1, степени m ($a_m=1$), принадлежащего показателю $l=2^m-1$ [4].

По числу m и полиному $P(x)$ определяется поле Галуа $GF(2^m)$. Оно содержит все полиномы:

$$f(\alpha)=b_0+b_1\alpha+b_2\alpha^2+\cdots+b_{m-1}\alpha^{m-1} \qquad (1.2)$$

с коэффициентами 0 и 1 и степени не более $m-1$. Полиномы (1.2) можно почленно складывать по mod 2 обычным способом.

Умножение этих полиномов производится также обычным способом, но только коэффициенты полученного полинома приводятся по mod 2, а сам полином приводится по mod $P(x)$, в результате чего получается снова полином с коэффициентами 0 и 1, степень которого не более $m-1$.

Из совокупности (1.2) полином $\Pi(\alpha)=\alpha$, удовлетворяющий соотношению

$$\alpha^m = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{m-1}\alpha^{m-1},$$

где $a_0, a_1, \cdots a_{m-1}$ — коэффициенты многочлена (1.1), называется примитивным элементом поля $GF(2^m)$.

Любой ненулевой элемент поля $GF(2^m)$ удовлетворяет уравнению

$$X^{2^m-1} = 1. \tag{1.3}$$

Элементы поля $f(\alpha) = b_0 + b_1\alpha + b_2\alpha^2 + \cdots + b_{m-1}\alpha^{m-1}$ можно представить в виде m-мерных векторов $[b_0, b_1, \cdots b_{m-1}]$.

Код Боуза—Чоудхури длины $n = 2^m - 1$, исправляющий t ошибок, определяется проверочной матрицей

$$M = \begin{vmatrix} 1 & 1 & \cdots & 1 \\ \alpha & \alpha^3 & & \alpha^{2t-1} \\ \alpha^2 & (\alpha^3)^2 & & (\alpha^{2t-1})^2 \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \alpha^{2^m-2} & (\alpha^3)^{2^m-2} & & (\alpha^{2t-1})^{2^m-2} \end{vmatrix},$$

где α — примитивный элемент поля $GF(2^m)$.

Вектор $r = [r_0, r_1, \cdots, r_{n-1}]$ или полином

$$r(x) = r_0 + r_1 x + r_2 x^2 + \cdots + r_{n-1} x^{n-1} \qquad (n = 2^m - 1)$$

принимается как кодовое слово, если произведение этого вектора на матрицу M дает нулевой вектор.

В результате умножения любого вектора $[r_0, r_1, \cdots, r_{n-1}]$ слева на матрицу M получится вектор, имеющий t координат, являющихся элементами поля $GF(2^m)$. Первая из этих координат: $r_0 + r_1\alpha + r_2\alpha^2 + \cdots + r_{n-1}\alpha^{n-1} = r(\alpha)$, а последующие координаты соответственно будут: $r(\alpha^3), r(\alpha^5), \cdots, r(\alpha^{2t-1})$.

Таким образом, вектор $r = [r_0, r_1 \cdots, r_{n-1}]$ будет кодовым, если для него все проверки $r(\alpha), r(\alpha^3), r(\alpha^5), \cdots, r(\alpha^{2t-1})$ суть нули.

Поэтому можно дать и такое эквивалентное определение кодов Боуза—Чоудхури:

Полином $S(x)$ степени $\leqslant n-1$ является кодовым словом для кода Боуза—Чоудхури длины $n = 2^m - 1$, исправляющего t ошибок, тогда и только тогда, когда $\alpha, \alpha^3, \alpha^5, \cdots, \alpha^{2t-1}$ являются корнями $S(x)$.

2. Процедура исправления ошибок

Для проверки правильности принятого вектора $r = [r_0, r_1, \cdots r_{n-1}]$ и исправления возможных ошибок, из числа допустимых не более t ошибок, рассмотрим вектор $rxM = [s_1, s_3, s_5, \cdots s_{2t-1}]$, где $s_j = r(\alpha^j)$,

$j=1, 3, 5, \cdots, 2t-1$. Если все s_j равны нулю, то вектор r кодовый и не содержит ошибки, в противном случае он содержит ошибки.

Пусть в принятом векторе r произошло t ошибок в разрядах, номера которых (считая с нулевой позиции) совпадают с порядковыми номерами элементов $X_1, X_2, \cdots, X_t$ поля $GF(2^m)$. Легко доказать [1], что имеют место соотношения:

$$s_j = \sum_{i=1}^{t} X_i^j, \tag{1.4}$$

где

$$j = 1, 3, 5, \cdots, 2t-1.$$

В частности, если произошла только одна ошибка, то проверка $s_1 = r(\alpha)$ дает элемент X_1 поля Галуа $GF(2^m)$, порядковый номер которого указывает на место ошибки. Это есть точный аналог исправления ошибок в кодах Хэмминга [3].

Систему t уравнений (1.4) невозможно решить прямым способом, ибо потребуется перебрать $C^t_{2^m-1}$ комбинации по t элементов поля, а это число велико.

Однако, если бы нам удалось найти уравнение степени t:

$$x^t + \sigma_1 x^{t-1} + \sigma_2 x^{t-2} + \cdots + \sigma_t = 0 \tag{1.5}$$

с коэффициентами $\sigma_1, \sigma_2, \cdots, \sigma_t$ из поля $GF(2^m)$, которое имеет своими корнями $X_1, X_2, \cdots, X_t$, то тогда нам пришлось бы перебрать всего лишь $n = 2^m - 1$ элементов поля.

Для нахождения $\sigma_1, \sigma_2, \cdots, \sigma_t$ можно воспользоваться известными тождествами Ньютона [5]

$$\begin{aligned}
&s_1 - \sigma_1 = 0,\\
&s_2 - s_1\sigma_1 + 2\sigma_2 = 0,\\
&s_3 - s_2\sigma_1 + s_1\sigma_2 - 3\sigma_3 = 0,\\
&s_4 - s_3\sigma_1 + s_2\sigma_2 - s_1\sigma_3 + 4\sigma_4 = 0,\\
&s_5 - s_4\sigma_1 + s_3\sigma_2 - s_2\sigma_3 + s_1\sigma_4 - 5\sigma_5 = 0
\end{aligned}$$

и т. д.

Для уравнения (1.5), выписывая из этих тождеств строки, соответствующие нечетным индексам, получим:

$$\begin{aligned}
&s_1 + \sigma_1 = 0,\\
&s_3 + s_2\sigma_1 + s_1\sigma_2 + \sigma_3 = 0,\\
&s_5 + s_4\sigma_1 + s_3\sigma_2 + s_2\sigma_3 + s_1\sigma_4 + \sigma_5 = 0,\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
&s_{2t-3} + s_{2t-4}\sigma_1 + s_{2t-5}\sigma_2 + \cdots + s_{t-3}\sigma_t = 0,\\
&s_{2t-1} + s_{2t-2}\sigma_1 + s_{2t-3}\sigma_2 + \cdots + s_{t-1}\sigma_t = 0.
\end{aligned} \tag{1.6}$$

Величины $s_1, s_3, s_5, \cdots, s_{2t-1}$ вычисляются непосредственно по

формулам $s_j = r(\alpha^j)$, а значения s с четными индексами можно найти, учитывая тот факт, что

$$(a+b)^2 = a^2 + b^2 \pmod 2$$

и поэтому

$$s_1^2 = \left[\sum_{i=1}^{t} x_i\right]^2 = \sum_{i=1}^{t} x_i^2 = s_2.$$

Аналогично, $s_4 = s_1^4$, $s_6 = s_3^2$ и т. д.

Подставляя значения величины s в уравнения (1.6), получим систему t линейных уравнений с коэффициентами из элементов поля $GF(2^m)$, из которой и определим неизвестные $\sigma_1, \sigma_2, \cdots, \sigma_t$.

Элементы поля $GF(2^m)$, которые удовлетворяют уравнению

$$x^t + \sigma_1 x^{t-1} + \sigma_2 x^{t-2} + \cdots + \sigma_t = 0$$

имеют порядковые номера, соответствующие ошибочным позициям.

Для частного случая $t = 3$ система уравнений Ньютона будет

$$\begin{aligned} &s_1 + \sigma_1 = 0, \\ &s_3 + s_2\sigma_1 + s_1\sigma_2 + \sigma_3 = 0, \\ &s_5 + s_4\sigma_1 + s_3\sigma_2 + s_2\sigma_3 = 0. \end{aligned} \tag{1.7}$$

Подставляя $s_2 = s_1^2$, $s_4 = s_1^4$ и решая систему, получим:

$$\begin{aligned} \sigma_1 &= s_1, \\ \sigma_2 &= \frac{s_5 + s_1^2 \cdot s_3}{s_1^3 + s_3}, \\ \sigma_3 &= s_1^3 + \frac{s_1 \cdot s_5 + s_3^2}{s_1^3 + s_3}, \end{aligned}$$

в предположении, что определитель системы $s_1^3 + s_3 \neq 0$. В этом случае в сообщении имеются либо две, либо три ошибки. Для нахождения ошибочных позиций, составим уравнение

$$x^3 + \sigma_1 x^2 + \sigma_2 x + \sigma_3 = 0$$

и подставим элементы поля $GF(2^m)$ в это уравнение.

Порядковые номера тех элементов поля, которые удовлетворяют последнему уравнению, укажут на места ошибочных позиций.

В случае $s_1^3 + s_3 = 0$ в сообщении будет одна ошибка, в позиции, соответствующей порядковому номеру элемента поля $s_1 = r(\alpha)$.

3. Циклическая структура кодов Боуза—Чоудхури

Для кода Боуза-Чоудхури длины $n = 2^m - 1$, исправляющего t ошибок, можно определить некоторый полином $f(x)$ степени $\leqslant mt$ таким образом, что все кодовые полиномы будут кратными $f(x)$ и, следовательно, коды Боуза—Чоудхури будут циклическими кодами [2]. Легко показать, что в этом случае $\alpha, \alpha^2, \alpha^3, \cdots, \alpha^{2t-1}$ должны являться корнями $f(x)$.

Каждый элемент поля α^j является корнем единственного неприводимого полинома $P_j(x)$ минимальной степени, являющегося дели-

телем $x^n - 1$. Поэтому $f(x)$ должен делиться на каждый из полиномов $P_1(x)$, $P_3(x), \cdots, P_{2t-1}(x)$, а следовательно, и на их наименьшее общее кратное [НОК].

Учитывая, что полиномы $P_j(x)$ — неприводимые, имеем:

$$f(x) = \prod P_j(x), \quad j = 1, 3, 5, \cdots, 2t-1$$

с опусканием дубликатов, т. е. если среди полиномов $P_j(x)$ встречаются совпадающие, то в $f(x)$ берется только один экземпляр.

Полином $P_1(x) = P(x)$, то есть тому полиному, который дан с самого начала образования поля $GF(2^m)$. Для определения любого другого полинома $P_j(x)$ через полином $P(x)$, имеется точная формула [1]:

$$P_j(x) = P(x^{\frac{1}{j}})\, P(\beta x^{\frac{1}{j}})\, P(\beta^2 x^{\frac{1}{j}}) \cdots P(\beta^{j-1} x^{\frac{1}{j}}), \tag{1.8}$$

где β — примитивный корень j-ой степени из единицы [5]. После перемножения в правой части (1.8) останутся только целые степени x с коэффициентами 0 и 1.

Таким образом, для данного кода Боуза-Чоудхури, исправляющего t ошибок, определяется порождающий полином $f(x)$. Его степень ($\leqslant m \cdot t$) и определит число проверочных разрядов кода (n, k), исправляющего t ошибок.

Так как каждый неприводимый полином $P_j(x)$ является делителем $x^n - 1 \,[= x^n + 1 \,(\mathrm{mod}\, 2)]$, то очевидно, $x^n + 1$ без остатка будет делиться на $f(x)$.

Пусть

$$\frac{x^n+1}{f(x)} = q(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_k x^k, \tag{1.9}$$

где коэффициенты b_i — 0 и 1 ($b_0 = b_k = 1$).

Важным результатом здесь является тот факт, что любая последовательность $[R_0, R_1, \cdots, R_{n-1}]$ символов из 0 и 1 будет кодовым словом для кода (n, k), исправляющего t ошибок, если она удовлетворяет рекурсивному соотношению [1]:

$$R_i = \sum_{j=1}^{k} b_j R_{i-j}, \tag{1.10}$$

где b_j являются коэффициентами полинома $q(x)$.

Задавая произвольно k символов $[R_0, R_1, \cdots, R_{k-1}]$ (информационную часть сообщения), по рекурсивному соотношению (1.10) определим $n - k$ символов $R_k, R_{k+1}, \cdots, R_{n-1}$, которые будут контрольными символами сообщения.

Циклическая структура кодов Боуза—Чоудхури дает возможность с помощью регистров сдвига с обратной связью сравнительно легко осуществить кодирование, а с помощью системы таких регистров и схем модульного сложения провести проверку и исправление ошибок в коде.

§ 2. Построение кода Боуза—Чоудхури (63, 45), исправляющего до трех независимых ошибок и его схемная реализация

1. Код (63, 45) и кодирующее устройство

Длина кода $n = 2^6 - 1 = 63$, $m = 6$, $t = 3$.

В качестве исходного полинома можно взять

$$P(x) = 1 + x + x^6,$$

который принадлежит показателю $e = 2^6 - 1$.

Образуем поле Галуа $GF(2^6)$ с законом

$$\alpha^6 = 1 + \alpha, \quad \text{(см. фиг. 1)}.$$

Все элементы поля $GF(2^6)$ удовлетворяют уравнению $x^{63} = 1$. Производящий полином кода

$$f(x) = P(x) P_3(x) P_5(x),$$

где

$$P(x) = 1 + x + x^6,$$

$$P_3(x) = P(x^{\frac{1}{3}}) P(\beta x^{\frac{1}{3}}) P(\beta^2 x^{\frac{1}{3}}) = (1 + x^{\frac{1}{3}} + x^2)(1 + \beta x^{\frac{1}{3}} + \beta^2 x^{\frac{2}{3}})(1 + \beta^2 x^{\frac{1}{3}} + \beta^4 x^{\frac{2}{3}}),$$

$$P_5(x) = P(x^{\frac{1}{5}}) P(\gamma x^{\frac{1}{5}}) P(\gamma^2 x^{\frac{1}{5}}) P(\gamma^3 x^{\frac{1}{5}}) P(\gamma^4 x^{\frac{1}{5}}) =$$

$$= (1 + x^{\frac{1}{5}} + x^{\frac{2}{5}})(1 + \gamma x^{\frac{1}{5}} + \gamma^2 x^{\frac{2}{5}})(1 + \gamma^2 x^{\frac{1}{5}} + \gamma^4 x^{\frac{2}{5}})(1 + \gamma^3 x^{\frac{1}{5}} + \gamma^6 x^{\frac{2}{5}})(1 + \gamma^4 x^{\frac{1}{5}} + \gamma^8 x^{\frac{2}{5}}),$$

а β и γ — примитивные корни из единицы соответственно 3-й и 5-й степеней.

Производя перемножение скобок и учитывая, что $\beta^3 = 1$ и $\gamma^5 = 1$, получим:

$$P_3(x) = 1 + x + x^2 + x^4 + x^6,$$

$$P_5(x) = 1 + x + x^2 + x^5 + x^6.$$

$P_3(x)$ и $P_5(x)$ — неприводимые полиномы 6-ой степени; элементы α^3 и α^5 поля $GF(2^6)$ — соответственно корни этих полиномов.

Подставляя выражение полиномов $P(x)$, $P_3(x)$ и $P_5(x)$ в $f(x)$, получим:

$$f(x) = (1 + x + x^6)(1 + x + x^2 + x^4 + x^6)(1 + x + x^2 + x^5 + x^6) =$$

$$= 1 + x + x^2 + x^3 + x^6 + x^7 + x^{15} + x^{16} + x^{17} + x^{18}.$$

Степень полинома $f(x)$ — 18, поэтому код Боуза—Чоудхури, исправляющий до трех независимых ошибок, будет иметь 18 контрольных разрядов и 45—информационных, т. е. будет кодом (63, 45).

Поле Галуа $GF(2^6)$, $\alpha^6 = 1+\alpha$

α^0	1
α^1	α
α^2	α^2
α^3	α^3
α^4	α^4
α^5	α^5
α^6	$1+\alpha$
α^7	$\alpha+\alpha^2$
α^8	$\alpha^2+\alpha^3$
α^9	$\alpha^3+\alpha^4$
α^{10}	$\alpha^4+\alpha^5$
α^{11}	$1+\alpha+\alpha^5$
α^{12}	$1+\alpha^2$
α^{13}	$\alpha+\alpha^3$
α^{14}	$\alpha^2+\alpha^4$
α^{15}	$\alpha^3+\alpha^5$
α^{16}	$1+\alpha+\alpha^4$
α^{17}	$\alpha+\alpha^2+\alpha^5$
α^{18}	$1+\alpha+\alpha^2+\alpha^3$
α^{19}	$\alpha+\alpha^2+\alpha^3+\alpha^4$
α^{20}	$\alpha+\alpha^3+\alpha^4+\alpha^5$
α^{21}	$1+\alpha+\alpha^3+\alpha^4+\alpha^5$
α^{22}	$1+\alpha^2+\alpha^4+\alpha^5$
α^{23}	$1+\alpha^3+\alpha^5$
α^{24}	$1+\alpha^4$
α^{25}	$\alpha+\alpha^5$
α^{26}	$1+\alpha+\alpha^2$
α^{27}	$\alpha+\alpha^2+\alpha^3$
α^{28}	$\alpha^2+\alpha^3+\alpha^4$
α^{29}	$\alpha^3+\alpha^4+\alpha^5$
α^{30}	$1+\alpha+\alpha^4+\alpha^5$
α^{31}	$1+\alpha^2+\alpha^5$
α^{32}	$1+\alpha^3$
α^{33}	$\alpha+\alpha^4$
α^{34}	$\alpha^2+\alpha^5$
α^{35}	$1+\alpha+\alpha^3$
α^{36}	$\alpha+\alpha^2+\alpha^4$
α^{37}	$\alpha^2+\alpha^3+\alpha^5$
α^{38}	$1+\alpha+\alpha^3+\alpha^4$
α^{39}	$\alpha+\alpha^2+\alpha^4+\alpha^5$
α^{40}	$1+\alpha+\alpha^2+\alpha^3+\alpha^5$
α^{41}	$1+\alpha^2+\alpha^3+\alpha^4$
α^{42}	$\alpha+\alpha^3+\alpha^4+\alpha^5$
α^{43}	$1+\alpha+\alpha^2+\alpha^4+\alpha^5$
α^{44}	$1+\alpha^2+\alpha^3+\alpha^5$
α^{45}	$1+\alpha^3+\alpha^4$
α^{46}	$\alpha+\alpha^4+\alpha^5$
α^{47}	$1+\alpha+\alpha^2+\alpha^5$
α^{48}	$1+\alpha^2+\alpha^3$
α^{49}	$\alpha+\alpha^3+\alpha^4$
α^{50}	$\alpha^2+\alpha^4+\alpha^5$
α^{51}	$1+\alpha+\alpha^3+\alpha^5$
α^{52}	$1+\alpha^2+\alpha^4$
α^{53}	$\alpha+\alpha^3+\alpha^5$
α^{54}	$1+\alpha+\alpha^2+\alpha^4$
α^{55}	$\alpha+\alpha^2+\alpha^3+\alpha^5$
α^{56}	$1+\alpha+\alpha^2+\alpha^3+\alpha^4$
α^{57}	$\alpha+\alpha^2+\alpha^3+\alpha^4+\alpha^5$
α^{58}	$1+\alpha+\alpha^2+\alpha^3+\alpha^4+\alpha^5$
α^{59}	$1+\alpha^2+\alpha^3+\alpha^4+\alpha^5$
α^{60}	$1+\alpha^3+\alpha^4+\alpha^5$
α^{61}	$1+\alpha^4+\alpha^5$
α^{62}	$1+\alpha^5$

Фиг. 1.

Полином

$$q(x) = \frac{x^{63}+1}{f(x)} \quad \text{[см. (1.9)]},$$

Производя деление, получим:

$$q(x) = 1 + x + x^4 + x^5 + x^6 + x^7 + x^{11} + x^{14} + x^{16} + x^{17} + x^{20} + x^{21} + x^{22} + x^{24} + x^{27} + x^{30} + x^{31} + x^{37} + x^{40} + x^{41} + x^{44} + x^{45}.$$

Последовательность $[R_0, R_1, \cdots, R_{62}]$ из 0 и 1 будет кодовым словом для кода (63, 45), если она удовлетворяет рекурсивному соотношению:

$$R_i = \sum_{j=1}^{45} b_j R_{i-j},$$

где b_j — коэффициенты полинома $q(x)$.

Схема устройства, осуществляющего кодирование информации в коде Боуза-Чоудхури (63, 45), исправляющем до трех независимых ошибок, изображена на фиг. 2.

Сообщение $[R_0, R_1, \cdots, R_{44}]$ с регистра R' в обратном порядке передается в регистр R. После 18 сдвигов схема определяет все 18 контрольных разрядов кода, которые через шину „И" и триггер „r_{17}" поступают в регистр r, и таким образом, на регистре rR получается кодированное сообщение

$$(r_0, r_1, \cdots, r_{17}, R_0, R_1, \cdots, R_{44}).$$

2. Проверка и исправление ошибок в коде (63, 45)

Для возможности проверки правильности сообщения

$$r(x) = r_0 + r_1 x + r_2 x^2 + \cdots + r_{62} x^{62}$$

и коррекции ошибок необходимо устройство, которое могло бы:

1. Вычислять $r(\alpha) = s_1$, $r(\alpha^3) = s_3$ и $r(\alpha^5) = s_5$.
2. Определять числа σ_1, σ_2 и σ_3 по формулам:

$$\sigma_1 = s_1,$$

$$\sigma_2 = \frac{s_1^2 \cdot s_3 + s_5}{s_1^3 + s_3},$$

$$\sigma_3 = s_1^3 + \frac{s_1 s_5 + s_3^2}{s_1^3 + s_3}.$$

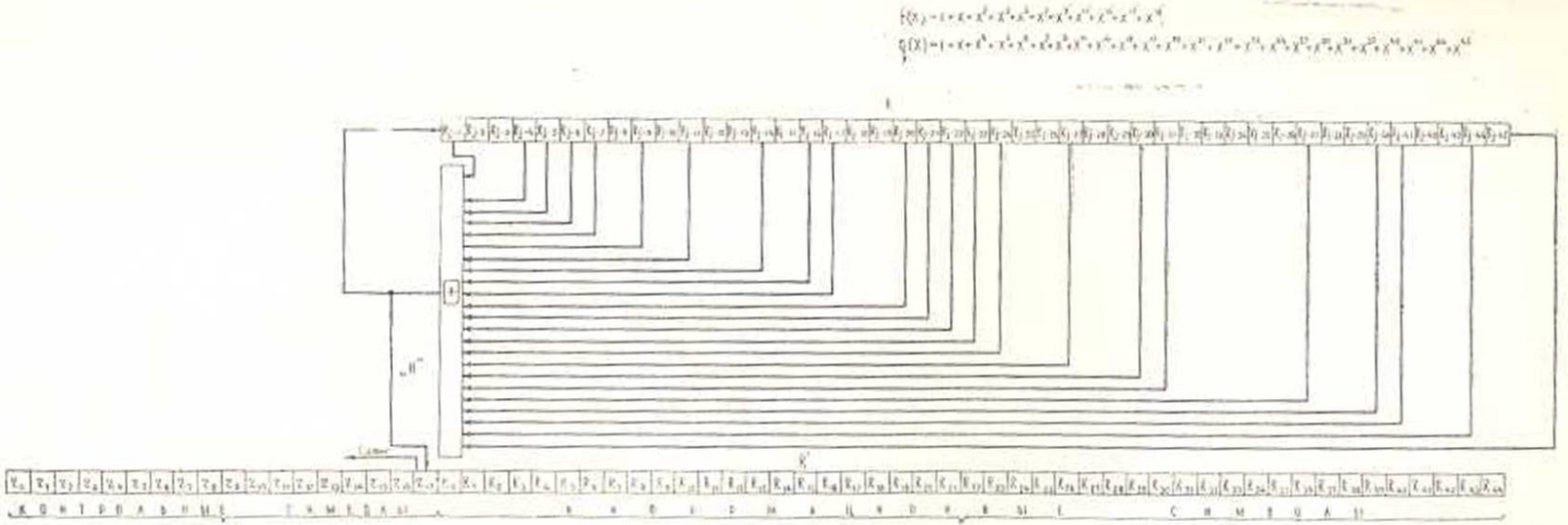
3. Проверять удовлетворяет ли элемент X поля $GF(2^6)$ уравнению

$$x^3 + \sigma_1 x^2 + \sigma_2 x + \sigma_3 = 0,$$

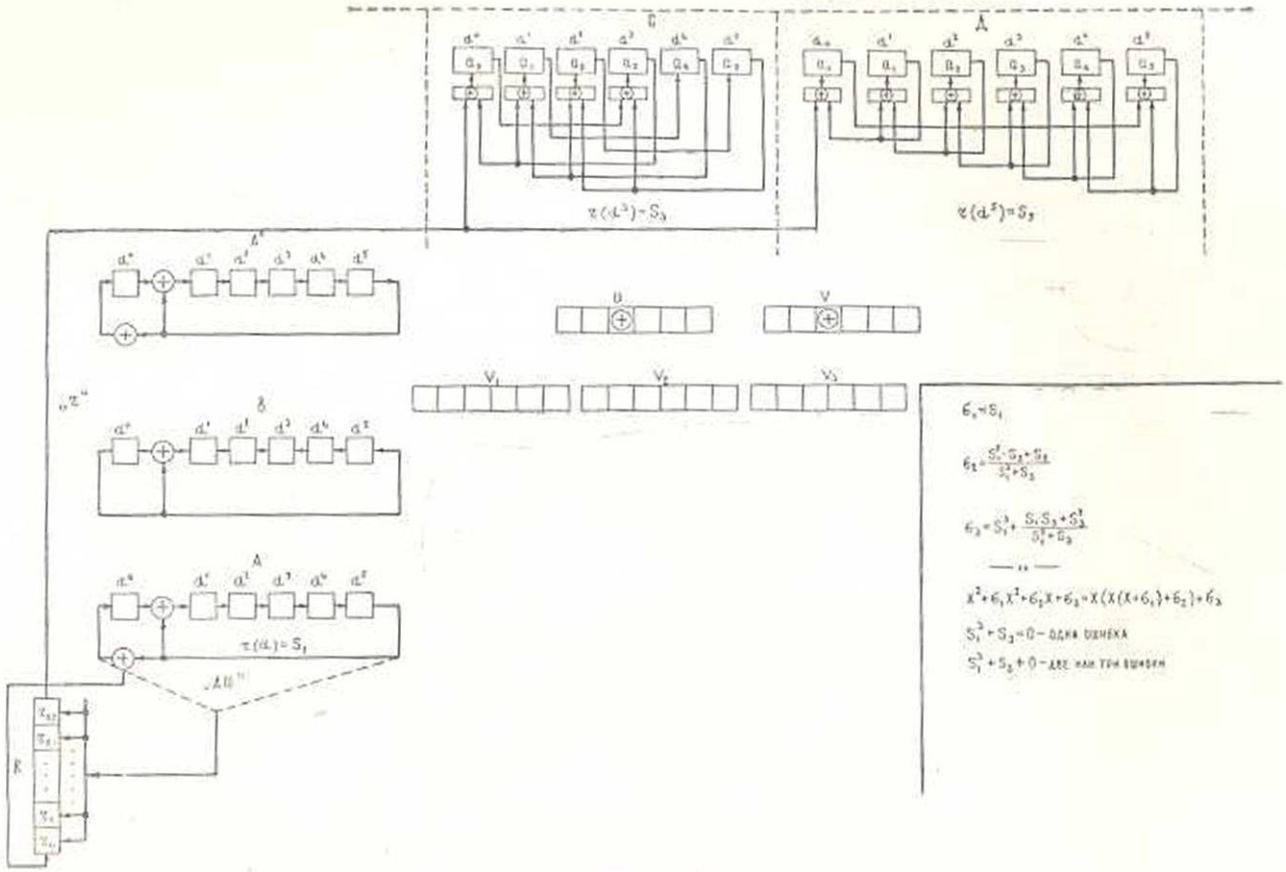
4. Исправлять ошибочные позиции в сообщении $r(x)$.

На фиг. 3 изображена схема основных узлов такого устройства.

Регистр R — имеет 63 разряда. Сообщение $r(x)$ подается в этот регистр для проверки.



Фиг. 2. Схема устройства кодирования в коде Боуза—Чоудхури (63, 45), исправляющем до трех независимых ошибок.



Фиг. 3. Схема проверки и исправления ошибок в коде Боуза—Чоудхури (63,45), исправляющем до трех независимых ошибок.

Узел A — в нем вычисляется $r(\alpha) = s_1$ и осуществляется исправление ошибочных позиций сообщения в регистре R через шестиразрядный дешифратор „ДШ".

Сообщение $r(x)$ старшими степенями вперед поразрядно передается в A, причем при каждом сдвиге посылается один разряд. Сдвиг в регистре этого узла на один разряд соответствует умножению находящейся на регистре информации на α. С помощью обратных связей этого регистра степени α выше 5 заменяются меньшими степенями α в соответствии с законом поля

$$\alpha^6 = 1 + \alpha.$$

После 63 сдвигов, когда все разряды сообщения $r(x)$ поступят в регистр A, в нем будет подсчитана сумма:

$$r(\alpha) = r_0 + r_1\alpha + r_2\alpha^2 + \cdots + r_{62}\alpha^{62}$$

в виде окончательного состояния регистра, соответствующего элементу $s_1 = r(\alpha)$ поля $GF(2^6)$.

Узлы „C и Д". В них вычисляются соответственно $r(\alpha^3)$ и $r(\alpha^5)$. Схемы устройств этих узлов вытекают из преобразований:

$$\alpha^3(a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + a_4\alpha^4 + a_5\alpha^5) = a_3 + (a_3 + a_4)\alpha +$$
$$+ (a_4 + a_5)\alpha^2 + (a_0 + a_5)\alpha^3 + a_1\alpha^4 + a_2\alpha^5,$$
$$\alpha^5(a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + a_4\alpha^4 + a_5\alpha^5) = a_1 + (a_1 + a_2)\alpha +$$
$$+ (a_2 + a_3)\alpha^2 + (a_3 + a_4)\alpha^3 + (a_4 + a_5)\alpha^4 + (a_0 + a_5)\alpha^5.$$

Правые части этих выражений получаются после замены степеней α выше пятой меньшими степенями α в соответствии с таблицей элементов поля Галуа $GF(2^6)$ (см. фиг. 1).

Сдвиг в регистрах этих узлов на 1 разряд равносилен умножению находящейся на регистре информации соответственно на α^3 и α^5.

Разряды сообщения $r(x)$ одновременно с поступлением в A через шину „r" поступают в C и $Д$ и после 63 сдвигов состояние регистров этих узлов определяют соответственно

$$r(\alpha^3) = s_3 \text{ и } r(\alpha^5) = s_5.$$

Регистр A' — такой же регистр, что и регистр A, только без дешифратора. На этом регистре, как и на регистре A, можно получить все элементы поля, начиная с 1 (состояние регистра 100000) путем 62 последовательных сдвигов.

Регистр B — в нем при каждом сдвиге на один разряд осуществляется деление находящейся на регистре информации на α. На этом регистре можно получить все элементы поля $GF(2^6)$ в обратном порядке, начиная с элемента $1 + \alpha^5$ (т. е. состояния регистра — 100001) путем 62 последовательных сдвигов влево.

Узлы „U и V" — схемы сложения по mod 2 шестиразрядных наборов из 0 и 1 элементов поля $GF(2^6)$.

Регистры V_1, V_2, V_3 — шестиразрядные регистры для памяти. В описанной схеме можно осуществить операции умножения и деления элементов поля $GF(2^6)$.

Умножение. Для умножения β на γ достаточно посылать β в регистр A' (или A), а γ — в регистр B.

Оба регистра A' и B одновременно сдвигаются до тех пор, пока на „B“ появится „1“ (100000), тогда в A' будет $\beta\gamma$.

Получение обратного элемента. Для элемента γ получение обратного элемента $\frac{1}{\gamma}$ можно осуществить так: посылая γ в A', а 1 — в A, оба регистра A и A' сдвигаются одновременно до тех пор, пока на регистре A' появится единица „1“ (100000), тогда на A будет $\frac{1}{\gamma}$.

Действительно, пусть $\gamma = \alpha^k$, появление „1“ на A означает сдвиг в этом регистре на $63-k$ разряда, так как $\alpha^k\alpha^{63-k} = 1$. Поэтому после такого же количества сдвигов в регистре A получится:

$$1 \cdot \alpha^{63-k} = \frac{\alpha^{63}}{\alpha^k} = \frac{1}{\alpha^k} = \frac{1}{\gamma}.$$

Деление. Операция деления $\frac{\beta}{\gamma}$ сводится к операции умножения $\beta \cdot \frac{1}{\gamma}$.

Снабдив оборудование описанной схемы несложным управлением, обеспечивающим выполнение списка операций (см. фиг. 5), можно эффективно провести проверку и исправление ошибок в коде (63, 45).

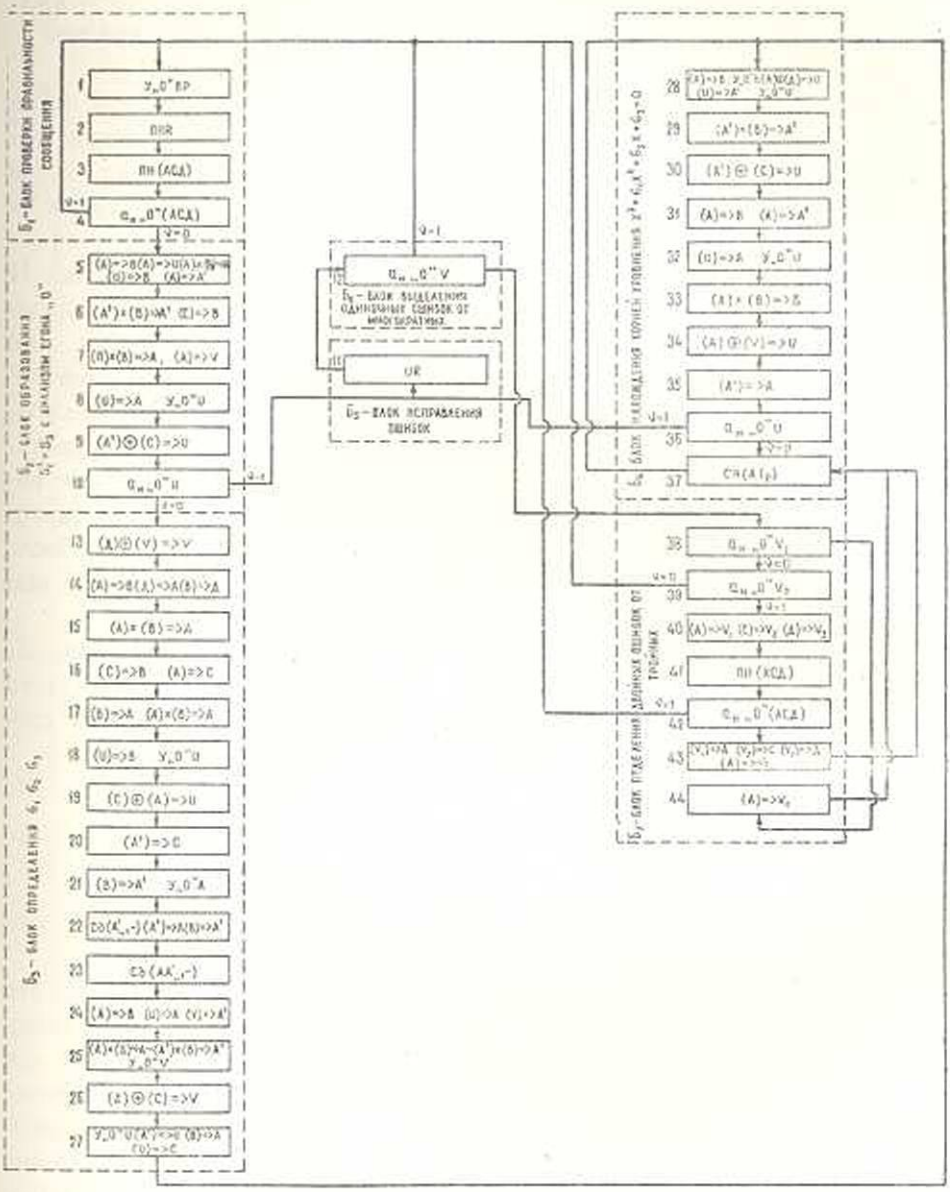
На фиг. 4 изображена блок-схема проверки и исправления ошибок в коде Боуза—Чоудхури (63, 45), исправляющем до трех независимых ошибок включительно.

Блок $Б_1$ (1—4) — блок проверяет правильность сообщения. Набор из регистра R одновременно поступает в регистры A, C и $Д$. Если содержание всех трех регистров нули, то набор правильный и сигнал возвращается к выполнению команды 1. В противном случае сигнал поступает в следующий блок.

Блок $Б_2$ (5—10) — в нем образуется выражение $s_1^3 + s_3$ и проводится его анализ на „0“. Если $s_1^3 + s_3 = 0$, то в наборе одна ошибка, сигнал поступает в блок 5(10), где исправляется ошибка и через блок 6 (11) возвращается к выполнению команды 1. Если же $s_1^3 + s_3 \neq 0$, то имеются две или три ошибки, тогда выходной сигнал из блока $Б_2$ поступает в следующий блок.

Блок $Б_3$ (13—27) — в нем определяются фактически σ_2 и σ_3, а σ_1 определяется в блоке $Б_1$.

Блок $Б_4$ (28—37) — в нем для элемента X_i поля $GF(2^6)$ (начиная с единичного) образуется выражение $X^3 + \sigma_1 X^2 + \sigma_2 X + \sigma_3$, которое



Фиг. 4. Блок-схема проверки и исправления ошибок в коде Боуза—Чоудхури (63, 45), исправляющем до трех независимых ошибок включительно.

далее проверяется на нуль. Если это выражение для данного элемента X_1 отлично от нуля, то переходим к следующему порядковому элементу X_2 поля и цикл 28—35 повторяется до тех пор, пока встретим элемент, для которого указанное выражение будет нулем; после этого выходящий из блока сигнал поступает в следующий блок.

Блок $Б_5$ (11) — исправляет через дешифратор ошибочную позицию, соответствующую порядковому номеру элемента, находящегося на регистре A.

Блок $Б_6$ (12) — различает одиночную ошибку от многократных. Случай одиночной ошибки соответствует $(\nu) = 0$, а многократной — $(\nu) \neq 0$.

Блок $Б_7$ (38—44) — назначение блока состоит в том, чтобы после исправления двух ошибок в коде проверить стало исправленное сообщение кодовым или нет. Без такой проверки в тех случаях, когда в сообщении произошли только две ошибки, мы тратили бы время на нахождение несуществующей третьей ошибки.

После второго исправления ошибки в коде сигнал из блока 11 поступает через путь 12, 38—42 в блок 42. В блоке 42 анализируется состояние регистров A, C и $Д$ для сообщения дважды уже исправленного. В случае, если содержание этих регистров одновременно нули, то третьей ошибки нет и сигнал идет к проверке следующего набора. В противном случае сигнал по ветви $\nu = 0$ (42) поступит в блок 43, в котором восстанавливается прежнее содержание регистров A, C и $Д$. Кроме того, посылается в ν_2 содержание A (которое заведомо не равно нулю, как ненулевой элемент поля). После нахождения и исправления третьей ошибки сигнал из блока 38 возвратится ($\nu = 0$) к проверке очередного набора.

Код (63, 45) был построен, исходя из неприводимого полинома $P(x) = 1 + x + x^6$, принадлежащего к показателю 63. Кроме этого полинома имеется еще 5 других неприводимых полиномов 6-й степени, также принадлежащих максимальному показателю 63.

Эти полиномы суть:

$$1 + x^5 + x^6, \quad 1 + x^2 + x^3 + x^5 + x^6, \quad 1 + x + x^3 + x^4 + x^6,$$
$$1 + x + x^4 + x^5 + x^6, \quad 1 + x + x^2 + x^5 + x^6.$$

Каждый из этих полиномов может быть исходным для образования кода (63, 45).

Производя соответствующие вычисления, можно убедиться, что кодирующие устройства кодов (63, 45), построенных на этих шести полиномах будут эквивалентными в смысле оборудования, так как все они будут иметь схему модульного сложения из 24 компонент. Однако, схемы проверки и исправления ошибок будут у них различными в смысле оборудования; наименьшее количество оборудования требует схема кода (63, 45), образованного при исходном полиноме $P(x) = 1 + x + x^6$.

В заключение рассмотрим вопрос о том, какие изменения произойдут в описанных схемах реализации кодов Боуза—Чоудхури при увеличении длины кода и числа корректируемых ошибок.

Вначале рассмотрим отдельно код Боуза-Чоудхури, длины $n = 2^7 - 1 = 127$, корректирующий до трех независимых ошибок. Для коррекции t ошибок код Боуза—Чоудхури длины 127 требует $7 \cdot t$ контрольных разрядов и поэтому для коррекции трех ошибок потребуется 21 контрольный разряд и 106 информационных разрядов, т. е. получим код (127, 106).

СПИСОК ОПЕРАЦИЙ

к блок-схеме проверки и исправления ошибок в коде Боуза—Чоудхури, исправляющем до трех независимых ошибок (см. фиг. 2, 4)

№№ п.п.	Символ операции	Содержание операции
1	$У.О^{*}ВР$	Установка на нуль всех регистров схемы
2	$У.О^{*}М$	Установка на нуль регистра M
3	$ПНР$	Подача следующего набора в регистр R
4	$ПН(АСД)$	Поразрядная подача набора одновременно в регистры A, C и $Д$
5	$a_{н}.О^{*}М$	Анализ на нуль содержания регистра M, выработка сигнала ν; $\nu=1$, если $(M)=0$, $\nu=0$, если $(M)\neq 0$
6	$a_{н}.О^{*}(АСД)$	Анализ на одновременное содержание нуля в регистрах A, C, $Д$, выработка сигнала ν; $\nu=1$, если (A), (C) и $(Д)$ одновременно нули и $\nu=0$, если хотя бы одно из этих содержаний $\neq 0$
7	$(M)=>N$	Передача содержания регистра M в регистр N с предварительной очисткой этого регистра (за исключением регистров U и V)
8	$(M)\times(B)=>M$	Умножение содержания регистра M на содержание регистра B с получением результата в регистре M
9	$(A)\times(B)=>A\sim(A')\times(B')=>A'$	Одновременно выполнение двух умножений: $(A)\times(B)=>A$ и $(A')\times(B)=>A'$
10	$сдМ_{1}$	Сдвиг в регистре M до появления состояния „1“ (т. е. 100000).
11	$сд(A_{(p)})$	Сдвиг в регистре A на один разряд.
12	$(M)\oplus(N)=>L$	Сложение по mod 2 содержания регистров M и N с передачей результата в регистр L
13	UR	Исправление ошибочной позиции в регистре R, соответствующей номеру элемента, находящегося на регистре A.

Фиг. 5.

В кодирующей схеме (см. фиг. 2) регистр r будет иметь длину 21, а R' — 106. Изменится также число компонент модульного сложения схемы.

В схеме проверки и исправления ошибок (см. фиг. 3) регистр R будет иметь длину 127 (этот регистр можно и не причислять к оборудованию схемы), а все остальные регистры схемы будут 7-ми разрядными, изменятся их обратные связи, но количество узлов, а также блок-схема коррекции ошибок не изменятся.

В общем же случае, при увеличении длины кода $n=2^{m}-1$ при постоянном числе коррекции t в схемах фиг. 2 и 3 существенных изменений не будет. Незначительно удлинятся регистры схемы фиг. 3 в соответствии с зависимостью $m\approx\log_{2}n$, несколько изменится расположение обратных связей, но не изменится количество узлов, а также блок-схема коррекции.

Увеличение числа корректируемых ошибок при постоянной длине кода в схеме кодирования, кроме соответствующего увеличения числа контрольных и уменьшения числа информационных разрядов, других изменений не вызовет.

В схеме же проверки и коррекции ошибок к имеющимся узлам прибавятся новые, осуществляющие вычисление

$$r(\alpha^1),\ r(\alpha^2),\cdots,\ r(\alpha^{2t-1}).$$

Кроме того, потребуется увеличение числа регистров для памяти, усложнится блок-схема коррекции ошибок, однако, принципиальных изменений в методике построения кодов Боуза—Чоудхури и их схемной реализации не будет.

Գ. Հ. Գաւակով

Ռ. Կ. ԲՈՈՒԶԻ—Դ. Կ. ՌՈՅ-ՋՈՈՒԴԽՈՒՐԻ ԿՈԴԵՐԸ ԵՎ ՆՐԱՆՑ ՍԽԵՄԱՅԻՆ ԻՐԱԿԱՆԱՑՄԱՆ ՀԱՐՑԵՐԸ

Ա Մ Փ Ո Փ Ո Ւ Մ

Հոդվածի առաջին մասում բերված են Բոուզի և Ջոուդխուրի կոդերի կառուցման ու այդ կոդերում սխալների հայտնաբերման և ուղղման տեսության հիմնական հարցերը։

Հոդվածի երկրորդ մասը նվիրված է այդ կոդերի կառուցման, նրանցում սխալների հայտնաբերման և ուղղման սխեմայինն իրականացմանը։

Ուսումնասիրված են վերոհիշյալ սխեմաների հատկությունները և տրված են նրանց նկարագրությունները։ Կառուցված է (63, 45) օպտիմալ կոդը, որի միջոցով հնարավոր է հայտնաբերել և ուղղել տվյալ կոդում հանդիպող մինչև 3 անկախ սխալներ։

ЛИТЕРАТУРА

1. *Peterson W. W.* Encoding and Error—correction procedures for the Bose—Chaudhuri codes. IRE Transactions on Information Theory. Vol. IT—6, № 4, 1960, pp. 459—470.
2. *Peterson W. W.* and *Brown D. T.* Cyclic Codes for Error Detection. Proceeding of the IRE Special Issue on Computers, Vol. 49, № 1, 1961, pp. 228—235.
3. *Хэмминг А. А.* Коды с обнаружением и исправлением ошибок. ИЛ, М., 1956.
4. *Гаврков Г. А.* Об использовании циклических кодов для контроля записи и считывания с магнитной ленты ЭЦВМ. Вопросы Радиоэлектроники, серия VII, № 5, 1963. Изд ГК при СМ СССР по Радиоэлектронике.
5. *Курош А. Г.* Курс высшей алгебры. Физматгиз, М., 1962.