ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том VI *1970* *Вып. 3*

УДК 621.391.15

НОВЫЙ КЛАСС ЛИНЕЙНЫХ КОРРЕКТИРУЮЩИХ КОДОВ

В. Д. Гоппа

Описан класс двоичных линейных кодов, исправляющих ошибки. Каждый код из этого класса задается некоторым многочленом над $GF(2^m)$. Зная степень t этого многочлена, можно получить следующие оценки для параметров кода: $n \leqslant 2^m$, $k \geqslant n - mt$, $d \geqslant 2t + 1$.

Описанные коды, вообще говоря, нециклические. Единственный циклический код, входящий в рассматриваемый класс,— код Боуза — Чоудхури — Хоквингема (БЧХ). Все основные свойства кода БЧХ определяются, по-видимому, его принадлежностью этому классу кодов, а не классу циклических кодов. Так для всех кодов рассматриваемого класса существует схема декодирования, аналогичная алгоритму Питерсона для кодов БЧХ.

Построение кодов основано на отождествлении исходного пространства двоичных векторов с некоторым множеством рациональных функций.

§ 1. Введение

Линейный код, исправляющий t ошибок, определяется некоторой матрицей с ненулевыми минорами порядка $\leqslant 2t$. В классическом матричном анализе изучаются некоторые специальные типы матриц (над полями характеристики 0) с определенными требованиями к минорам некоторого порядка.

В частности, в книге [1] описаны так называемые вполне положительные матрицы, у которых все миноры порядка $\leqslant r$ положительны. Самой известной вполне положительной матрицей является матрица Вандермонда, и на ее основе построен код Боуза — Чоудхури — Хоквингема (БЧХ). Другая вполне положительная матрица — матрица $\|(x_i - y_j)^{-1}\|$. Эта матрица стала отправным пунктом для создания класса рассматриваемых здесь линейных кодов.

Каждый код из этого класса, так же как и циклический код, задается некоторым порождающим многочленом. Отличие заключается в том, что знание порождающего многочлена циклического кода в общем случае ничего не говорит о корректирующих способностях кода, а по одной только степени порождающего многочлена описываемых кодов можно получить следующие оценки для параметров кода: $n \leqslant 2^m$, $k \geqslant n - m \deg g(z)$, $d \geqslant 2 \deg g(z) + 1$ (здесь $\deg g(z)$ — степень многочлена $g(z)$). Единственный циклический код, входящий в рассматриваемый класс кодов,— это код БЧХ. По-видимому, все основные особенности кода БЧХ объясняются его принадлежностью к построенному классу, а не к классу циклических кодов. Например, для всех описанных в этой статье кодов существует схема декодирования, сводящаяся к решению системы линейных уравнений над конечным полем.

§ 2. Определение класса кодов

Пусть L — некоторое множество элементов поля $GF(2^m)$: $L = \{\alpha_1, \ldots$ $\ldots, \alpha_n\}$, $n \leqslant 2^m$, S — векторное пространство размерности n над $GF(2)$.

Поставим в соответствие каждому вектору $x = (a_1, \ldots, a_n)$, $a_i \in GF(2)$, $i = 1, \ldots, n$ рациональную функцию

$$R_x(z) = \sum_{i=1}^{n} \frac{a_i}{z - \alpha_i}.$$

Отображение $x \to R_x(z)$ — гомоморфизм S в аддитивную группу рациональных функций над $GF(2^m)$.

Выберем некоторый многочлен $g(z)$ с коэффициентами из $GF(2^m)$, не имеющий корней в L. Определим линейный код как множество векторов x, для которых $R_x(z) \equiv 0 \operatorname{mod} g(z)$. Задавая различным образом многочлен $g(z)$ (назовем его порождающим по аналогии с циклическими кодами), можно получать коды с различными свойствами. Вместе с каждым вектором x, имеющим единицы на местах $i_1, i_2, \ldots, i_k$, будем рассматривать многочлен $f(z) = (z - \alpha_{i_1})(z - \alpha_{i_2}) \ldots (z - \alpha_{i_k})$. Очевидно, $R_x(z) = f'(z)/f(z)$, где $f'(z)$ — формальная производная многочлена $f(z)$.

§ 3. Проверочная матрица. Мощность кода

Для кодового вектора $x = (a_1, \ldots, a_n)$ выполняется соотношение

$$R_x(z) = \sum_{i=1}^{n} \frac{a_i}{z - \alpha_i} \equiv 0 \operatorname{mod} g(z).$$

Это сравнение эквивалентно равенству

$$\sum_{i=1}^{n} a_i \{(z - \alpha_i)^{-1}\}_m = 0,$$

где $\{(z - \alpha_i)^{-1}\}_m$ — элемент, обратный к $(z - \alpha_i)$ в алгебре многочленов по $\operatorname{mod} g(z)$. Этот элемент находится следующим образом:

$$\{(z - \alpha_i)^{-1}\}_m = \frac{g(z) - g(\alpha_i)}{z - \alpha_i} g^{-1}(\alpha_i),$$

так как в правой части стоит многочлен степени, меньшей чем степень $g(z)$, и

$$\frac{1}{z - \alpha_i} \equiv \frac{g(z) - g(\alpha_i)}{z - \alpha_i} g^{-1}(\alpha_i) \operatorname{mod} g(z).$$

Поэтому проверочная матрица кода состоит из следующей строки:

$$T = \left(\frac{g(z) - g(\alpha_1)}{z - \alpha_1} g^{-1}(\alpha_1) \ldots \frac{g(z) - g(\alpha_n)}{z - \alpha_n} g^{-1}(\alpha_n) \right).$$

Пусть $g(z) = \sum_{i=0}^{r} b_i z^i$ $(\deg g(z) = r)$.

Тогда матрицу T можно представить так:

$$\begin{pmatrix} b_r g^{-1}(\alpha_1) & \ldots\ldots\ldots\ldots & b_r g^{-1}(\alpha_n) \\ (b_{r-1} + b_r \alpha_1) g^{-1}(\alpha_1) & \ldots\ldots\ldots & (b_{r-1} + b_r \alpha_1) g^{-1}(\alpha_n) \\ \ldots\ldots\ldots\ldots & \ldots\ldots\ldots\ldots & \ldots\ldots\ldots\ldots \\ (b_1 + b_2 \alpha_1 + \ldots + b_r \alpha_1^{r-1}) g^{-1}(\alpha_1) & \ldots & (b_1 + \ldots + b_r \alpha_n^{r-1}) g^{-1}(\alpha_n) \end{pmatrix}.$$

Отсюда видно, что T — линейное преобразование строк матрицы T^*:

$$T^* = \begin{pmatrix} g^{-1}(\alpha_1) & \ldots & g^{-1}(\alpha_n) \\ \alpha_1 g^{-1}(\alpha_1) & \ldots & \alpha_n g^{-1}(\alpha_n) \\ \ldots & \ldots & \ldots \\ \alpha_1^{r-1} g^{-1}(\alpha_1) & \ldots & \alpha_n^{r-1} g^{-1}(\alpha_n) \end{pmatrix}.$$

Итак, проверочная матрица кода получается умножением матрицы Вандермонда справа на диагональную матрицу

$$T = \begin{pmatrix} 1 & \ldots & 1 \\ \alpha_1 & & \alpha_n \\ \ldots & \ldots & \ldots \\ \alpha_1^{r-1} & \ldots & \alpha_n^{r-1} \end{pmatrix} \begin{pmatrix} g^{-1}(\alpha_1) & & \\ & g^{-1}(\alpha_2) & \\ \ldots & \ldots & \ldots \\ & & g^{-1}(\alpha_n) \end{pmatrix}.$$

В частности, если выбрать $n = 2^k - 1$, в качестве L — все элементы группы порядка n, $g(z) = z^{2r}$, то получается матрица кода БЧХ

$$\begin{pmatrix} 1 & \alpha^{-2r} & \ldots & \alpha^{-(n-1)2r} \\ \ldots & \ldots & \ldots & \ldots \\ 1 & \alpha^{-1} & \ldots & \alpha^{-(n-1)} \end{pmatrix}.$$

Зная проверочную матрицу, легко получить следующую оценку для числа проверочных символов кода.

Код длины $n \leqslant 2^m$ имеет не больше $m \deg g(z)$ проверочных символов.

§ 4. Корректирующая способность кодов

Так как для кодовых многочленов $f'(z) \equiv 0 \bmod g(z)$ и $f'(z) \equiv 0 \bmod \bar{g}(z)$, где $\bar{g}(z)$ — многочлен минимальной степени, являющийся полным квадратом и такой, что $g(z) \mid \bar{g}(z)$, то $\deg f(z) \geqslant \deg \bar{g}(z) + 1$, так что для веса кода получается оценка

$$d \geqslant \deg \bar{g}(z) + 1.$$

Если все корни $g(z)$ различны, то $\bar{g}(z) = g^2(z)$ и

$$d \geqslant 2 \deg g(z) + 1.$$

§ 5. Декодирование

Пусть $y = x + e$; $y, x, e \in S$; x — переданный кодовый вектор, e — вектор ошибки. При переходе к функциям $R_y(z)$, $R_x(z)$ и $R_e(z)$, соответствующим y, x и e, получаем

$$\frac{f_y'(z)}{f_y(z)} = \frac{f_x'(z)}{f_x(z)} + \frac{f_e'(z)}{f_e(z)},$$

а так как $\dfrac{f_x'(z)}{f_x(z)} \equiv 0 \mod \bar{g}(z)$, имеем

$$\frac{f_e'}{f_e} \equiv \frac{f_y'}{f_y} \mod \bar{g}(z).$$

Величина $\theta(z) = \dfrac{f_y'}{f_y} \mod \bar{g}(z)$ — синдром, т. е. результат умножения вектора y на проверочную матрицу кода. Если единицы в векторе y расположены на местах $i_1, \ldots, i_k$, то

$$\theta(z) = \frac{\bar{g}(z) - \bar{g}(\alpha_{i_1})}{z - \alpha_{i_1}} \bar{g}^{-1}(\alpha_{i_1}) + \ldots + \frac{\bar{g}(z) - \bar{g}(\alpha_{i_k})}{z - \alpha_{i_k}} \bar{g}^{-1}(\alpha_{i_k}).$$

Искомый многочлен ошибки f_e определяется по синдрому θ из сравнения

$$f_e' \equiv f_e\theta \bmod \bar{g}(z). \tag{1}$$

Пусть $\deg g(z) = 2t$, $f'/f \equiv \theta \bmod \bar{g}(z)$, $\deg f \leqslant t$ и корни f лежат в L. Если φ — некоторое другое решение сравнения (1), причем $\deg \varphi \leqslant t$, то

$$\varphi' \equiv \varphi\theta \bmod \bar{g}, \quad \varphi' \equiv \varphi \frac{f'}{f} \bmod \bar{g}, \quad (\varphi f)' \equiv 0 \bmod \bar{g}.$$

Так как $(\varphi f)'$ имеет степень $< 2t$, то $(\varphi f)' = 0$, и поскольку f' и f взаимно просты, то $f = \gamma\varphi$, $\gamma \in GF(2^m)$. Таким образом, f_e можно искать по данному θ как единственное (с точностью до постоянного множителя) решение сравнения (1) в виде многочлена степени $\leqslant t$.

Ограничимся рассмотрением случая, когда все корни $g(z)$ различны. Тогда $\bar{g}(z) = g^2(z)$, $\deg g(z) = t$, и f_e можно находить, решая сравнение

$$f_e' \equiv f_e\theta \bmod g. \tag{2}$$

Это сравнение также имеет единственное решение f_e, $\deg f_e \leqslant t$, так как из $(\varphi f)' \equiv 0 \bmod g$ следует $(\varphi f)' \equiv 0 \bmod g^2$. Ищем решение в виде $f_e = 1 + zu$, $\deg u < t$. Для определения u имеем линейное дифференциальное уравнение в алгебре многочленов по $\bmod g$

$$u'z + u(1 + z\theta) = \theta$$

или в операторной записи: $(M + T_\theta)u = \theta$, где M — линейный оператор в алгебре многочленов по $\bmod g(z)$, проектирующий многочлен на его нечетную часть $Mu = u'z$. В базисе $1, z, \ldots, z^{t-1}$ матрица этого оператора имеет вид

$$M = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

T_θ — линейный оператор умножения на элемент $(1 + z\theta)$ в той же алгебре. Матрица T_θ имеет вид

$$T_\theta = \begin{pmatrix} c_{00} & \ldots & c_{t-1,\,0} \\ \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots \\ c_{0,\,t-1} & \ldots & c_{t-1,\,t-1} \end{pmatrix}, \text{ где } (1 + z\theta)z^i \equiv (c_{i0} + \ldots + c_{i,\,t-1}z^{t-1}) \bmod g.$$

Из доказанной единственности решения сравнения (2) следует, что матрица $(M + T_\theta)$ невырождена в случае, когда $f_e(z)$ не имеет нулевого корня. В случае, когда ошибка произошла на месте, соответствующем $\alpha_n = 0$, существует решение однородного уравнения $(M + T_\theta)u = 0$, т. е. матрица $(M + T_\theta)$ оказывается вырожденной. В этом случае следует исправить одну ошибку (заменить символ на месте α_n), найти вновь синдром θ и решить новую систему с невырожденной матрицей.

Таким образом, получается следующий алгоритм декодирования: 1) найти синдром $\theta(z)$; 2) вычислить $(1+z\theta)z^i$, $i=0, 1, \ldots, t-1$ в алгебре многочленов по $\operatorname{mod} g(z)$; 3) построить матрицу $(M+T_\theta)$; 4) если она оказывается вырожденной, то положение одной ошибки известно; исправить ее и перейти к п. 1); 5) в случае невырожденности матрицы решить систему уравнений $(M+T_\theta)u=\theta$; 6) найти корни многочлена $f=1+zu$.

§ 6. Пример кода

Построим код $(16, 8, 5)$, исправляющий все двойные ошибки. В этом случае $m=4$, $t=2$. По таблицам неприводимых многочленов находим, что второй старший коэффициент минимального многочлена для α^3 (α — примитивный элемент $GF(2^4)$) равен 1. Следовательно, $Tr\alpha^3 \neq 0$, и многочлен $g(z)=z^2+z+\alpha^3$ неприводим над $GF(2^4)$ [2]. Выберем его в качестве порождающего многочлена кода. Проверочная матрица состоит из двумерных столбцов $\begin{pmatrix} a_{1k} \\ a_{0k} \end{pmatrix}$, где

$$a_{0k}+a_{1k}z = \frac{g(z)-g(\alpha_k)}{z-\alpha_k}\, g^{-1}(\alpha_k) = (z+1+\alpha_k)\frac{1}{\alpha_k{}^2+\alpha_k+\alpha^3}.$$

Подставляя вместо α_k все элементы $GF(2^4)$, получаем матрицу

γ	α	α^2	α^3	α^4	α^5	α^6	α^7	α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}	α^{15}	0
a_1	α^4	α^3	α^9	α^4	α	α^8	α^6	α^3	α^6	α	α^2	α^2	α^8	α^9	α^{12}	α^{12}
a_0	α^8	α^{11}	α^8	α^5	α^{11}	α^6	1	α^5	α^{13}	α^6	α^{14}	α^{13}	α^{14}	α^{12}	0	α^{12}.

В таком виде матрицу будем использовать для декодирования. Для кодирования эту матрицу нужно разложить над полем $GF(2)$ и привести к каноническому виду

α	α^2	α^3	α^4	α^5	α^6	α^7	α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}	α^{15}	0
1	0	0	1	0	1	0	0	0	0	0	0	1	0	1	1
1	0	0	0	0	1	0	0	0	1	1	1	1	1	1	0
0	0	0	1	0	1	1	0	0	0	0	1	1	0	0	0
0	0	0	1	0	1	0	1	0	0	1	0	1	1	1	0
1	0	1	0	0	1	0	0	0	0	0	0	0	1	1	0
0	0	0	0	1	1	0	0	0	0	1	1	0	1	0	0
1	0	0	0	0	1	0	0	1	0	1	0	1	0	0	0
1	1	0	1	0	1	0	0	0	0	0	1	0	1	0	0

С помощью последней матрицы находим кодовый вектор 0 0 1 0 0 0 0 1 0 1 0 0 0 0 1 1 с единицами на позициях 3, 8, 10, 15, 16. Ему соответствует многочлен

$$f(z) = (z-\alpha^3)(z-\alpha^8)(z-\alpha^{10})(z-1)z = z^5+\alpha^7 z^4+z^3+\alpha^{10}z^2+\alpha^6 z.$$

Производная этого многочлена $f'(z)=z^4+z^2+\alpha^6=g^2(z)$. Следовательно, это действительно кодовый многочлен.

Допустим, что произошла одна ошибка на 5-й позиции, т. е. на позиции, соответствующей α^5. Умножая вектор

1) 0 0 1 0 1 0 0 1 0 1 0 0 0 0 1 1 на проверочную матрицу (над полем $GF(2^4)$), получаем синдром $\theta(z)=\alpha^{11}+\alpha z$.

2) Находим $1+z\theta=1+\alpha^{11}z+\alpha z^2=1+\alpha^{11}z+\alpha(z+\alpha^3)=\alpha+\alpha^6 z$; $(1+z\theta)z=\alpha^9+\alpha^{11}z$.

3) Матрицы T_θ, M имеют вид

$$T_\theta=\begin{pmatrix}\alpha & \alpha^9\\ \alpha^6 & \alpha^{11}\end{pmatrix},\quad M=\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix},\qquad T_\theta+M=\begin{pmatrix}\alpha & \alpha^9\\ \alpha^6 & \alpha^{12}\end{pmatrix},\quad \theta=\begin{pmatrix}\alpha^{11}\\ \alpha\end{pmatrix}.$$

4) Решая систему уравнений $(T_\theta+M)u=\theta$,

$$\alpha x_1+\alpha^9 x_2=\alpha^{11},\quad \alpha^6 x_1+\alpha^{12}x_2=\alpha,$$

получаем $x_2=0$, $x_1=\alpha^{10}$, так что искомый многочлен $f_e(z)=1+\alpha^{10}z$.

5) Корень этого многочлена α^5 определяет положение ошибки.

Пусть теперь произошли 2 ошибки на позициях 15 и 16 (т. е. α^{15} и 0). В этом случае $\theta(z)=\alpha^{12}$, $1+z\theta=1+\alpha^{12}z$, $(1+z\theta)z=1+\alpha^{11}z$, и матрица $T_\theta+M=\begin{pmatrix}1 & 1\\ \alpha^{12} & \alpha^{12}\end{pmatrix}$ оказывается вырожденной. Это говорит о том, что f_e имеет нулевой корень, т. е. одна ошибка произошла на 16-й позиции. После исправления этой ошибки получаем синдром $\theta=\alpha^{12}z$ и новую систему

$$\begin{pmatrix}0 & 1\\ \alpha^{12} & \alpha^{11}\end{pmatrix}\begin{pmatrix}x_1\\ x_2\end{pmatrix}=\begin{pmatrix}0\\ \alpha^{12}\end{pmatrix}.$$

Решая ее, находим $x_2=0$, $x_1=1$, так что $f_e=1+z$.

§ 7. Связь с циклическими кодами

Рассмотрим случай, когда в качестве множества L выбираются все корни n-й степени из 1 над $GF(2)$: $L=\{1,\alpha,\ldots,\alpha^{n-1}\}$, α — первообразный корень уравнения $X^n-1=0$; допустим, что α порождает расширение $GF(2^m)$ поля $GF(2)$. В множестве S всех n-разрядных двоичных слов наряду со структурой аддитивной группы рассмотрим две структуры кольца:

а) с векторным умножением, при котором произведением двух элементов $x=(a_0,\ldots,a_{n-1})$ и $y=(b_0,\ldots,b_{n-1})$ является $z=(a_0b_0,\ldots,a_{n-1}b_{n-1})$ (здесь $a_i, b_i\in GF(2)$), обозначим это кольцо VS;

б) с многочленным умножением по $\mathrm{mod}(X^n-1)$, назовем это кольцо MS.

Х. Матсон и Г. Соломон в своей новой трактовке кодов БЧХ [3] использовали отображение

$$f(X)=a_0+\cdots+a_{n-1}X^{n-1}\to f(\alpha)X^{n-1}+\cdots+f(\alpha^n)=F(X),$$

которое каждому многочлену $f(X)$ над $GF(2)$ ставит в соответствие некоторый многочлен над $GF(2^m)$. Это соответствие взаимно-однозначно, причем обратное отображение совпадает с прямым. Его можно получить, построив, например, интерполяционный многочлен Лагранжа

$$f(X)=\sum_{k=0}^{n-1}\frac{X^n-1}{X-\alpha^k}\,\frac{f(\alpha^k)}{\alpha^{k(n-1)}}=\sum_{i=0}^{n-1}F(\alpha^{i+1})\,X^{n-1-i}.$$

В множестве K всех многочленов степени $<n$ над $GF(2^m)$ можно ввести такие же структуры кольца, что и в S — с векторным умножением (VK) и многочленным по mod (X^n-1) (MK). Легко проверяется, что отображение $f(X)\to F(X)$ — гомоморфизм $MS\to VK$ и $VS\to MK$. Так как все

элементы VS идемпотентны, то образ множества S при этом отображении состоит из идемпотентов кольца MK. Наоборот, любой идемпотент MK принимает значения 0 или 1 на всех корнях n-й степени из 1. Обозначим через E множество идемпотентов кольца MK. Оно является подкольцом MK (назовем его ME) и в то же время подкольцом VK (назовем его VE). Следовательно, отображение $f(X) \to F(X)$ есть изоморфизм

$$MS \rightleftarrows VE, \quad VS \rightleftarrows ME.$$

Пользуясь этим изоморфизмом, можно определять коды как некоторые подмножества E. Линейные коды — это аддитивные подгруппы E, циклические коды — идеалы кольца VE. Каждый идеал VE — множество многочленов, у которых коэффициенты при некоторых степенях $X^{i_1}, \ldots, X^{i_k}$ равны 0. Например, код БЧХ — это идеал в VE, состоящий из многочленов, у которых или l старших коэффициентов, или l младших равны 0.

Пусть $y = (a_0, \ldots, a_{n-1}) \in S$. Справедлива следующая диаграмма, устанавливающая связь между отображением $S \to E$ и $y \to R_y(X)$:

$$\begin{tikzcd}[column sep=small]
 & f(X) = a_0 + \ldots + a_{n-1}X^{n-1} \arrow[r] & F(X) = f(\alpha)X^{n-1} + \ldots + f(\alpha^n) \arrow[d] \\
y = (a_0 \ldots a_{n-1}) \arrow[ur] \arrow[dr] & & \\
 & R_y(X) = \dfrac{a_0}{X-\alpha^0} + \ldots + \dfrac{a_{n-1}}{X-\alpha^{n-1}} \arrow[r] & \{R_y(X)(X^{n+1}+X)\}_m,
\end{tikzcd}$$

где $\{R_y(X)(X^{n+1}+X)\}_m$ означает остаток от деления $R_y(X)(X^{n+1}+X)$ на $X^n - 1$, а вертикальная стрелка — тождественное отображение.

Приведенная диаграмма позволяет установить следующую симметрию между циклическими кодами и кодами, описанными в этой работе.

Циклический код — это множество многочленов, кратных некоторому фиксированному многочлену над $GF(2)$ в пространстве MS. Код, определяемый сравнением $R_x(z) \equiv 0 \bmod g(z)$, в случае, когда L является множеством корней многочлена $X^n - 1$, совпадает с множеством многочленов, кратных фиксированному многочлену над $GF(2^m)$ в пространстве ME.

Теорема. *Если код, определяемый условием* $R_x(z) \equiv 0 \bmod g(z)$ — *циклический, то он является кодом* БЧХ, *т. е.* $g(z) = z^l$.

Доказательство. Допустим, что $g(z)$ имеет ненулевой корень β и порождает циклический код. В пространстве VE этому коду соответствует некоторый идеал C. По определению идеалов кольца VE, если $F(X) \in C$ то и $F(\alpha^i X) \in C$ для всех $i = 0, \ldots, n-1$, поэтому $F(\alpha^i X) \equiv 0 \bmod g(X)$, $i = 0, 1, \ldots, n-1$, откуда $F(X) \equiv 0 \bmod g(\alpha^{-i}X)$ и $F(X)$ вместе с корнем $\beta \neq 0$ должен иметь n ненулевых корней, т. е. делиться на $X^n - 1$, что невозможно.

§ 8. Заключение

В настоящей статье описаны только двоичные коды. Обобщение на недвоичный случай и некоторые другие результаты, полученные пока статья находилась в печати, предполагается опубликовать в дальнейшем.

Данная работа обсуждалась на семинаре по теории кодирования при МГУ. Пользуюсь случаем выразить признательность всем лицам, принявшим участие в обсуждении, в результате которого был устранен ряд неточностей.

ЛИТЕРАТУРА

1. Гантмахер Ф. Р., Крейн М. Г. Осцилляционные матрицы и ядра и малые колебания механических систем. М., Гостехиздат, 1950.
2. Ленг С. Алгебра. М., «Мир», 1968.
3. Матсон Х., Соломон Г. Новая трактовка кодов Боуза — Чоудхури. Сб. «Теория кодирования». М., «Мир», 1964.

Поступила в редакцию
28 апреля 1969 г.