

АЛГЕБРАИЧЕСКАЯ ТЕОРИЯ БЛОЧНЫХ КОДОВ, ИСПРАВЛЯЮЩИХ НЕЗАВИСИМЫЕ ОШИБКИ

В. А. Зиновьев

Цель настоящего обзора-осветить те основные направления алгебраической теории блочных кодов, исправляющих независимые ошибки, которые касаются только построения и существования кодов и описания их некоторых свойств. Будут обсуждены достижения этого раздела алгебраической теории корректирующих кодов и, насколько это возможно, продемонстрированы его методы с тем, чтобы можно было представить современное состояние предмета. Наряду с традиционными направлениями алгебраической теории кодирования такими, как верхние и нижние оценки мощности наилучших кодов, циклические коды, коды БЧХ, нахождение весовых спектров в кодах, рассмотрены и наиболее интересные новые направления: каскадные коды, абелевы коды, аддитивные коды, коды Гоппы, теорема Глисона и другие вопросы. Ввиду ограниченности размеров данный обзор, конечно, не претендует на полноту даже в этой части алгебраической теории блочных кодов. Вопросы декодирования в обзоре не затрагиваются.

Автор искренне благодарен своим коллегам В. В. Зяблову, И. И. Грушко, В. К. Леонтьеву и В. И. Таиряну за полезные советы и особенно Л. А. Бассальго за тщательный просмотр рукописи и критические замечания по ней. Автор очень признателен также иностранным коллегам профессорам Касами из Японии, Вулфу и Слоэну из США. Гёгалсу и Дельсарту из Бельгии и Титвайнену из Финляндии за своевременную информацию и присылку своих работ.

§ 1. БЛОЧНЫЕ КОДЫ: ОПРЕДЕЛЕНИЯ И ОСНОВНЫЕ ПОНЯТИЯ

Пусть E^n — множество всех векторов длины n над некоторым конечным алфавитом $E = \{0, 1, \dots, q-1\}$. Весом Хэмминга $w(a)$ вектора $a \in E^n$ назовем число его ненулевых компонент,

а расстоянием Хэмминга $d(a, b)$ между a и b из E^n назовем число компонент, в которых векторы a и b различаются. Любое подмножество $A \subseteq E^n$ назовем блочным кодом над E и обозначим через $A(q, n, d, N)$. Здесь: q — основание кода; n — длина кода; N — мощность кода, т. е. число кодовых векторов в A ($N = |A|$); d — минимальное расстояние (Хэмминга) кода, т. е.

$$d = \min_{\substack{a \neq b \\ a, b \in A}} \{d(a, b)\}. \quad (1.1)$$

Скорость кода R определяется как $R = \frac{1}{n} \log_q N$. Так как все кодовые векторы различны, то $1 \leq N \leq q^n$ и $0 \leq R \leq 1$.

Пусть $S(a, r)$ — сфера с центром в a радиуса r , а $B(a, r)$ — шар с центром в a радиуса r , т. е.

$$S(a, r) = \{x \in E^n | d(a, x) = r\}, \quad (1.2)$$

$$B(a, r) = \bigcup_{i=0}^r S(a, i) = \{x \in E^n | d(a, x) \leq r\}. \quad (1.3)$$

Ясно, что

$$|S(a, r)| = (q-1)^r C_n^r, \quad (1.4)$$

$$|B(a, r)| = \sum_{i=0}^r (q-1)^i C_n^i. \quad (1.5)$$

Если $[x]$ — целая часть x , то код с расстоянием d исправляет любые $t = [(d-1)/2]$ случайных ошибки. Это означает, что шары $B(a, t)$ радиуса t с центрами в кодовых векторах не пересекаются, и каждой точке любого такого шара соответствует один кодовый вектор на расстоянии $\leq t$, а именно вектор, находящийся в центре этого шара.

Для данного кода A длины n и фиксированного вектора $a \in A$ пусть $\eta_i(a)$ обозначает число кодовых векторов b таких, что $d(a, b) = i$. Набор $n+1$ чисел $(\eta_0(a), \eta_1(a), \dots, \eta_n(a))$ называется спектром расстояний кода A относительно вектора a , и называется спектром весов, если $\omega(a) = 0$, т. е. если a — нулевой вектор.

Если элементы $E = \{0, 1, \dots, q-1\}$ обозначают элементы поля Галуа $GF(q)$, то E^n можно рассматривать как линейное пространство над $GF(q)$. Если код A является подпространством E^n , то A называется линейным кодом над полем $GF(q)$. В линейном коде мощность $N = q^k$, где k — число информационных символов и $R = k/n$. Число $n-k$ называется числом проверочных символов, а линейный код $A(q, n, d, q^k)$ называют также (n, k) -кодом. Базис (n, k) -кода A называется порождающей матрицей кода и обозначается через G_A . Пространство наибольшей размерности, ортогональное данному (n, k) -коду A ,

является некоторым $(n, n-k)$ -кодом A^\perp , называемым двойственным к коду A . Базис кода A^\perp , т. е. порождающая матрица G_{A^\perp} этого кода, называется проверочной матрицей исходного кода A и обозначается H_A , т. е. для любого $a = (a_1, \dots, a_n) \in A$ справедлива следующая система уравнений (или система проверок):

$$aH_A^T = 0, \quad (1.6)$$

где H^T — матрица, транспонированная к H .

Так как расстояние Хэмминга инвариантно относительно сдвига, т. е. для любых векторов a, b, x всегда $d(a, b) = d(a+x, b+x)$, то в любом коде попарные расстояния между векторами не изменятся, если ко всем словам прибавить один и тот же произвольный вектор. В линейном коде минимальное расстояние равно минимальному весу ненулевых кодовых слов и спектр расстояний $(\eta_0(a), \eta_1(a), \dots, \eta_n(a))$ относительно любого кодового слова a не зависит от выбора этого слова и совпадает со спектром весов $(\eta_0, \eta_1, \dots, \eta_n)$. Производящая функция $\eta(z)$ спектра $(\eta_0, \eta_1, \dots, \eta_n)$:

$$\eta(z) = \sum_{i=0}^n \eta_i z^i \quad (1.7)$$

называется весовой функцией кода.

§ 2. ВЕРХНИЕ И НИЖНИЕ ГРАНИЦЫ МОЩНОСТИ КОДА С ЗАДАНЫМ РАССТОЯНИЕМ

Пусть в множестве E^n имеется некоторый код $A(q, n, d, N) = \{a, b, c, \dots\}$ с минимальным расстоянием $d = 2t + 1$. Каждую кодовую точку a окружим шаром $B(a, r)$ некоторого радиуса r и обозначим через $v(e, r)$ число шаров, в которые входит произвольная точка e из E^n . Из определения следует, что

$$\sum_{e \in E^n} v(e, r) = N \cdot |B(a, r)| = N \cdot \sum_{i=0}^r (q-1)^i C_n^i. \quad (2.1)$$

Равенство (2.1) является основным для получения верхних и нижних оценок мощности $N = N(n, d)$ наилучшего кода (т. е. содержащего максимальное число кодовых слов при заданных n и d) как некоторой целочисленной функции длины кода n , и минимального расстояния d . Обозначим через $N(n, d, B_r)$ (соответственно, через $N(n, d, S_r)$) максимальное число кодовых точек, входящих в шар $B(a, r)$ (соответственно, лежащих на сфере $S(a, r)$) радиуса r . Тогда, очевидно, $v(e, r) \leq N(n, d, B_r)$ и, как заметил Л. А. Бассалыго [4], из (2.1) получаем, что

$$N(n, d) \leq N(n, d, B_r) \cdot q^n \Big/ \sum_{i=0}^r (q-1)^i C_n^i. \quad (2.2)$$

Тем самым мы получили возможность получать верхние оценки мощности кода $N(n, d)$ из верхних оценок для $N(n, d, S_r)$. Легко получить оценку на число $N(n, d, S_r)$ кодовых векторов, лежащих на сфере $S(a, r)$ радиуса r (Джонсон [186], Л. А. Бассальяго [4]):

$$N(n, d, S_r) \leq \left[\frac{q-1}{q} \cdot n \cdot d \left/ \left(r^2 - \frac{q-1}{q} (2r-d)n \right) \right. \right]. \quad (2.3)$$

Эта оценка справедлива, когда знаменатель под знаком целой части положителен. Если обозначить через r_1 минимальный корень уравнения $r^2 - (1-1/q)(2r-d)n = 0$, то $r_1 = (1-1/q)n \times \times (1 - \sqrt{1 - qd/(q-1)n})$ и оценка (2.3) справедлива при всех $r < r_1$. В частности, при значении

$$r_E = \frac{q-1}{q} n \left(1 - \sqrt{1 - \frac{2tq}{(q-1)n}} \right) \quad (2.4)$$

($r_E < r_1$, если учесть, что $d = 2t + 1$), называемом радиусом Элайеса, оценка (2.3) сводится к следующей оценке:

$$N(n, d, S_{r_E}) \leq d.$$

Отсюда сразу следует, что $N(n, d, B_{r_E}) \leq (r_E - t + 1)d$, и учет этого приводит к следующей верхней оценке:

$$N(n, d) \leq (r_E - t + 1) d q^n \left/ \sum_{i=0}^{r_E} (q-1)^i C_n^i \right., \quad (2.5)$$

где r_E — радиус Элайеса, определяемый выражением (2.4). В асимптотической форме (если положить $N(n, d) = q^k$ и $R = k/n$) при $n \rightarrow \infty$ эта верхняя граница (2.5) имеет вид:

$$R \leq 1 - H\left(\frac{r_E}{n}\right) \cdot \log_q 2 - \frac{r_E}{n} \log_q (q-1), \quad (2.6)$$

где функция

$$H(x) = -x \log_2 x - (1-x) \log_2 (1-x) \quad (2.7)$$

— двоичная энтропия. Граница (2.6), называемая границей Элайеса, была анонсирована Элайесом в работе Джонсона [186] без доказательства. Первое доказательство этой границы появилось в работе Л. А. Бассальяго [4].

Интересно, что из (2.1) можно получить и нижнюю границу на максимально возможную мощность $N(n, d)$ кода $A(q, n, d, N)$. В самом деле, в оптимальном коде $v(e, d-1) \geq 1$ (если бы $v(e, d-1) = 0$, то точку e можно было бы присоединить к коду без уменьшения его расстояния, что противоречило бы оптимальности кода). Тогда учет этого неравенства в (2.1) дает известную нижнюю границу Варшавова [20] — Гилберта [147]

$$N(n, d) \geq q^n \left/ \sum_{i=0}^{2t} (q-1)^i C_n^i \right., \quad (2.8)$$

или в асимптотической форме при $n \rightarrow \infty$

$$R \geq 1 - H\left(\frac{d}{n}\right) \log_q 2 - \frac{d}{n} \log_q (q-1). \quad (2.9)$$

Таким образом, скорость передачи R кода $A(q, n, d, N)$ не может превышать верхней оценки (2.6), но для любых d, n существует код $A(q, n, d, N)$, скорость передачи которого удовлетворяет неравенству (2.9). Как следует из выражения (2.4), радиус Элайеса r_E значительно меньше минимального расстояния $d=2t+1$, и соответственно верхняя граница (2.6) и нижняя граница (2.9) довольно сильно отличаются друг от друга. В настоящее время известно много семейств кодов (часть из них мы укажем ниже) про которые доказано, что среди них имеются коды, достигающие границы Варшамова—Гилберта (2.9). Более того, в ряде работ [45, 46, 55, 145, 277] доказано, что двоичный линейный случайно выбранный код почти наверное лежит на границе (2.9). Остановимся на этих результатах несколько подробнее.

Зададим на множестве всех двоичных $(k \times n)$ -матриц равномерную вероятностную меру, считая, что элементы этих матриц представляют собой взаимно независимые случайные величины, принимающие значения 0 или 1 с вероятностью $\frac{1}{2}$. Пусть ξ_n — случайная величина, равная минимальному расстоянию кода, порожденного такой случайно выбранной $(k \times n)$ -матрицей, и обозначим через $\beta_n(x) = P\{\xi_n > x\}$ ее функцию распределения. Пусть, далее, $R = k/n$, а $\rho < \frac{1}{2}$ — корень уравнения $1 - R = H(\rho)$. Границу Варшамова—Гилберта для случая $q=2$ можно сформулировать в следующей форме (М. В. Козлов [45]): если разность

$$n\rho + \frac{1}{2} \left(\log_2 \frac{1-\rho}{\rho}\right)^{-1} \log_2 n - s_n \quad (2.10)$$

ограничена снизу некоторой константой c_ρ (зависящей только от ρ), то $\beta_n(s_n) > 0$ (т. е. существует код с минимальным расстоянием s_n). Результат Галлагера [145] и В. Н. Кошелева [55] выглядит в этих терминах следующим образом: если разность (2.10) стремится к $+\infty$, то $\beta_n(s_n) \rightarrow 1$ при $n \rightarrow \infty$ (т. е. любой случайно выбранный код почти наверное имеет расстояние s_n). Пирс [277], однако, установил, что существует очень мало длинных кодов (т. е. кодов с большими n), для которых s_n/n превышает ρ на сколь угодно малую величину, т. е. что $\beta_n(\rho + \epsilon) \rightarrow 0$ при $n \rightarrow \infty$ для любого $\epsilon > 0$. Более точный результат получил М. В. Козлов [45]: если разность (2.10) стремится к $-\infty$, то $\beta_n(s_n) \rightarrow 0$ при $n \rightarrow \infty$. Следующий результат М. В. Козлова [45] несколько улучшает (правда, не асимптотически) границу Варшамова—Гилберта для $q=2$: если разность

$$n\rho + \left(\log_2 \frac{1-\rho}{\rho}\right)^{-1} \log_2 n - s_n$$

ограничена снизу некоторой константой, то $\beta_n(s_n) > 0$, т. е. существует (n, k) -код с минимальным весом

$$n\rho + \left(\log_2 \frac{1-\rho}{\rho}\right)^{-1} \log_2 n + O(1) \text{ или более.}$$

Помимо попыток улучшить нижнюю границу на R , не предпринимаются попытки улучшить верхнюю границу. Совсем недавно В. М. Сидельников [80] и В. И. Левенштейн [57] доказали для случая $q=2$ возможность асимптотического улучшения границы Элайеса (2.6). Это улучшение достигнуто за счет улучшения верхней оценки (2.3) числа $N(n, d, S_r)$. Принципиальная новизна подхода состоит в следующем. В. М. Сидельников [79], изучая взаимно корреляционные свойства векторов над конечным полем, ввел в рассмотрение для произвольного множества $X = \{X_i = (x_{i1}, \dots, x_{in}), i=1, \dots, m\}$ векторов n -мерного евклидова пространства R^n сумму

$$\sum_{i,j} (X_i, X_j)^h = \sum_{i=1}^m \sum_{j=1}^m \left(\sum_{s=1}^n x_{is} x_{js} \right)^h, \quad (2.11)$$

где h — натуральный параметр, а (X_i, X_j) — скалярное произведение. Стандартный переход от векторов $S(0, r)$ с метрикой Хэмминга к векторам R^n , лежащим на единичной сфере $S^{(1)}$, с обычной евклидовой метрикой, осуществляется взаимно однозначным отображением $U: 1 \leftrightarrow -\sqrt{(n-r)/nr}$, $0 \leftrightarrow \sqrt{r/n(n-r)}$. В. М. Сидельников установил [79], что сумма (2.11) для любого множества X неотрицательна и доказал [80], что для любого такого множества X из m векторов, принадлежащих единичной сфере $S^{(1)}$ пространства R^n и являющихся образами векторов из $S(0, r) \subset E^n$ при отображении U , и для любого $h=0, 1, 2, \dots$ справедлива оценка

$$\frac{1}{m} \sum_{i,j} (X_i, X_j)^h \geq \frac{m}{C_n^r} \sum_{s=0}^n C_r^s C_{n-r}^s \left(1 - \frac{sn}{r(n-r)}\right)^h. \quad (2.12)$$

Эта оценка (если ее переписать для метрики Хэмминга и выразить как верхнюю оценку на $N(n, d, S_r)$) позволяет получить верхнюю границу на R , которая при соответствующей минимизации по r приводит к оценке, лучшей оценки Элайеса (2.6) для всех скоростей передачи $0 < R < 1$ (Это было сделано в работе В. М. Сидельникова [80] и в улучшенном виде в работе В. И. Левенштейна [57]; см. также [325]).

В ряде работ рассматривались не асимптотические нижние и верхние оценки на мощности кода (или на расстояние). Из последних работ следует указать обзор Слоэна [304] по конструктивной алгебраической теории кодирования, а также

работы Хелгерта и Стинаффа [182] и Джонсона [188] (см. также ссылки в этих работах).

Верхние границы на $N(n, d, S_r)$, т. е. границы на мощность равновесных кодов, подробно исследовались Джонсоном [186, 189]. В. И. Левенштейн [56, 57] асимптотически улучшил границу Джонсона, а также некоторые ее обобщения, полученные Фрейманом [144] и Бергером [94]. Интересный подход, с помощью тождеств, выражающих нормированные центральные моменты кодового расстояния через линейные преобразования характеристической функции равновесного кода, предложен Э. М. Габидулиным и В. Р. Сидоренко [28]. Связь равновесных кодов с тактическими конфигурациями подробно исследована в работах Н. В. Семакова и В. А. Зиновьева [73, 74].

§ 3. СОВЕРШЕННЫЕ И РАВНОМЕРНО УПАКОВАННЫЕ КОДЫ

Если в неравенстве (2.2) положить $r=t=\lfloor (d-1)/2 \rfloor$, то $N(n, d, B_t)=1$ и (2.2) сводится к классической границе Хэмминга [169] (границе сферической упаковки)

$$N(n, d) \leq q^n \sum_{i=0}^t (q-1)^i C_n^i. \quad (3.1)$$

Получив некоторую границу, естественно попытаться найти случаи, когда эта граница достигается. Код $A(q, n, d, N)$ с $d=2t+1$, мощность которого N удовлетворяет равенству в (3.1), называется совершенным или плотно упакованным. Существование совершенного кода $A(q, n, 2t+1, N)$ означает, что пространство E^n полностью разбивается на N непересекающихся шаров $B(a, t)$ радиуса t с центрами в кодовых точках $a \in A(q, n, d, N)$. Помимо тривиальных случаев ((1) один кодовый вектор длины $n=t$; (2) два кодовых вектора длины $n=2t+1$ для случая $q=2$ (3) все пространство E^n с $t=0$), известны следующие совершенные коды:

(а) коды Хэмминга [169] длины $n=(q^m-1)/(q-1)$ и с $d=3$ ($t=1$), существующие для всех q , равных степени простого числа и для всех $m=2, 3, 4, \dots$ в линейном виде, а для $m>2$ ($m>3$ при $q=2$) существующие в нелинейном виде (Ю. Л. Васильев [26], Шонхейм [294], Линдстрем [228]);

(б) линейные коды Голея [157—159] $A(2, 23, 7, 2^{12})$ и $A(3, 11, 5, 3^6)$.

Коды Хэмминга и Голея были построены более 20 лет назад и тогда же возникло предположение о несуществовании других нетривиальных совершенных кодов. Это предположение было доказано недавно одновременно в двух работах.

Теорема 3.1. (В. А. Зиновьев и В. К. Леонтьев [40], Титвайнен [319]). Единственными нетривиальными совершенными q -ичными кодами для всех $q=p^s$, где p — простое число, а $s=1, 2, \dots$, являются указанные выше коды Хэмминга и Голея.

Различные частные случаи этой теоремы были доказаны ранее в работах [39, 229—232, 237, 296, 318, 321] (см. также ссылки в [234, 235]). Мы приведем основную идею доказательства теоремы 3.1. Главную роль играет следующее интересное необходимое условие существования совершенного кода, называемое теоремой Ллойда.

Теорема 3.2. (Ллойд [237]). Если существует совершенный код $A(q, n, d, N)$, исправляющий $t = (d-1)/2$ ошибок, то полином $P_t(n, \xi)$ (называемый полиномом Кравчука) степени t по переменной ξ , определяемый равенством

$$P_t(n, \xi) = \sum_{i=0}^t (-1)^i (q-1)^{t-i} C_{n-\xi}^{t-i} C_{\xi-1}^i, \quad (3.2)$$

где $C_a^i = a(a-1)\dots(a-i+1)/i!$ для любых a , имеет t различных целых корней среди чисел $1, 2, \dots, n$.

Ллойд [237] доказал эту теорему для $q=2$, Мак-Вильямс (ссылка в [232]) обобщила ее на случай $q=p^s$, p —простое число, $s=1, 2, \dots$, Глисон (ссылка в [232]) дал алгебраическое доказательство этой теоремы для этого случая, а Дельсарт [133], Ленстра [220] и Л. А. Бассальго [5, 6] независимо доказали эту теорему для любых q . Наиболее простое и естественное доказательство получил Л. А. Бассальго [6] и мы приведем схему его рассуждений. Каждому множеству $A \subseteq E^n$ может быть поставлена в соответствие его характеристическая функция. Рассмотрим теперь в пространстве всех комплекснозначных функций на E^n линейное преобразование M_t , которое характеристическую функцию каждой точки $a \in E^n$ переводит в характеристическую функцию шара $B(a, t)$ радиуса t с центром в a . Ясно, что это преобразование переводит характеристическую функцию любого совершенного кода, исправляющего t ошибок, в характеристическую функцию всего пространства E^n . Но если $A = A(q, n, d, N)$ —совершенный код, исправляющий t ошибок, то множество $a + A$ при любом $a \in E^n$ также является совершенным кодом $A(q, n, d, N)$ в силу инвариантности метрики относительно сдвигов. При этом характеристические функции множеств $a + A$, по крайней мере при всех $a \in B(0, t)$ (т. е. при всех a веса $w(a) \leq t$), линейно независимы, откуда следует, что в случае существования совершенного кода дефект линейного преобразования M_t достаточно велик (заведомо не меньше $|B(a, t)| - 1$). Это условие, когда найдена полная система собственных функций преобразования M_t и их собственных значений, эквивалентно тому, что достаточно много собственных функций имеет нулевое собственное значение. Ясно, что те же самые рассуждения могут быть проведены и с другими подходящим образом выбранными функциями множеств, в том числе и весовыми.

Основная идея получения теоремы 3.1 из теоремы Ллойда

состоит в следующем. Пусть существует совершенный код $A(q, n, d, N)$, где q — степень простого числа, а $d = 2t + 1$. Тогда условие равенства в (3.1) означает, что

$$\sum_{i=0}^t (q-1)^i C_n^i = q^{n-k}, \quad (3.3)$$

где $N = q^k$. По теореме 3.2 полином $P_t(n, \xi)$ имеет t различных целых корней $\xi_1, \dots, \xi_t \in \{1, 2, \dots, n\}$. Из (3.2) и (3.3) легко получить, что

$$\xi_1 \dots \xi_t = \frac{t!}{q^t} \sum_{i=0}^t (q-1)^i C_n^i = t! q^{n-k-t}, \quad (3.4)$$

$$\xi_1 + \dots + \xi_t = t \frac{q-1}{q} \left(n+1 - \frac{(t+1)(q-2)}{2(q-1)} \right). \quad (3.5)$$

Сравнивая с помощью (3.4) и (3.5) сумму и произведение корней ξ_1, \dots, ξ_t , нетрудно убедиться, что при достаточно больших n среднее арифметическое чисел ξ_1, \dots, ξ_t примерно равно их среднему геометрическому, т. е. эти числа должны быть примерно одинаковы. Однако условие целочисленности корней ξ_1, \dots, ξ_t , записанное в виде (3.4), показывает, что на самом деле эти корни должны существенно различаться. Исходя из этих соображений, можно получить верхнюю границу для длины n возможного совершенного кода. С другой стороны, довольно просто можно получить ряд нижних оценок на возможную длину n совершенного кода (см., например, [8, 39, 319, 320]). Сравнение этих оценок и приводит к теореме 3.1. Существенное упрощение технической стороны этой схемы доказательства получено в недавней работе Титвайнена [320] для случая $q > 2$.

Перенос техники доказательства теоремы 3.1 на случай произвольного $q = p_1^{a_1} \dots p_m^{a_m}$ позволяет только доказать (Л. А. Бассальго, В. А. Зиновьев, В. Л. Леонтьев [8]) наличие такой эффективно вычисляемой константы $t(q)$, что при всех $t \geq t(q)$ не существует нетривиальных совершенных кодов, исправляющих t ошибок. Доказательство же несуществования при всех $t \geq 2$ (случай $t=1$ требует особого рассмотрения; см. [163] и обсуждение соответствующей проблемы в [232, 235]) наталкивается на значительные технические трудности. Использование следующего результата, представляющего вариант известной теоремы А. О. Гельфонда: если h и l — натуральные числа и $lnl \geq 5$, то

$$|h \ln 3 - l \ln 2| > e^{-20 \cdot 0 \cdot n^2},$$

позволило преодолеть эти трудности в простейшем случае $q = 2^\alpha 3^\beta$, $\alpha, \beta = 1, 2, 3, \dots$ (Л. А. Бассальго, В. А. Зиновьев, В. К. Леонтьев и Н. И. Фельдман [9]).

Интерес к совершенным кодам и, в частности, к проблеме

их существования, не случаен. В значительной степени он объясняется интересной комбинаторной и алгебраической структурой этих кодов. По этому вопросу (и вообще по связи кодов с различными комбинаторными конфигурациями) смотри работы [1, 72, 77, 87—89, 92, 104, 111, 115, 134—137, 153, 269, 299]. Так векторы постоянного веса w в совершенном коде $A(q, n, d, N)$ образуют тактическую конфигурацию $T(n, w, (d+1)/(2, \alpha))$ (Ассмус и Матсон [88]). В частности, расширенные коды Голея $A(2, 24, 8, 2^{12})$ и $A(3, 12, 6, 3^6)$ (т. е. коды с добавленной позицией так, чтобы сумма всех элементов каждого кодового слова была равна нулю) приводят к двум замечательным системам Штейнера $T(24, 8, 5, 1)$ и $T(12, 6, 5, 1)$. Группами симметрии этих кодов являются известные пяти-транзитивные группы Матье M_{24} и M_{12} (Ассмус и Матсон [87]). На основе кодов Голея можно построить решетки Лича [215—218]. Доказан ряд интересных теорем единственности кодов Голея (Плесс [279]), Сновер (ссылка в [139]), Дельсарт и Гёталс [139]). Гёталс [152] (см. также [76]) рассмотрел подкоды двоичного кода Голея, а Берлекэмп [100] изучил группы симметрии этих подкодов. В связи с этим представляют интерес такие обобщения совершенных кодов, которые сохраняют все их интересные комбинаторные свойства.

Рассмотрим сейчас одно из таких возможных обобщений, введенное Л. А. Бассалыго, Г. В. Зайцевым и В. А. Зиновьевым [7]. Определим для кода $A = A(q, n, d, N)$ внешнее расстояние Λ как максимальное удаление точек множества E^n от данного кода A :

$$\Lambda = \max_{e \in E^n} \{ \min_{a \in A} d(e, a) \}. \quad (3.6)$$

Если $\Lambda = t$, то код $A(q, n, d, N)$ — совершенный, если же $\Lambda = t + 1$, код называется квазисовершенным.

Обозначим через $f_i(e)$ число кодовых векторов, лежащих на расстоянии i от вектора e . Назовем код A равномерно упакованным, если существуют (рациональные) числа $\alpha_0, \alpha_1, \dots, \alpha_\Lambda$ такие, что для любого вектора $e \in E^n$ выполняется равенство

$$\sum_{i=0}^{\Lambda} \alpha_i f_i(e) = 1. \quad (3.7)$$

Частный случай таких кодов, соответствующий значениям $\Lambda = t + 1$ и $\alpha_0 = \alpha_1 = \dots = \alpha_{t-1} = 1$, $\alpha_t = \alpha_{t+1} = 1/m$, где m — натуральное число, был рассмотрен ранее Г. В. Зайцевым, В. А. Зиновьевым и Н. В. Семаковым [77], а для значения $m = \lfloor n/(t+1) \rfloor$ рассмотрен Гёталсом и Сновером [156]. Для совершенных кодов $\alpha_0 = \alpha_1 = \dots = \alpha_t = 1$.

Число слов равномерно упакованного кода

$$N = q^n \left/ \sum_{i=0}^{\Lambda} \alpha_i (q-1)^i C_n^i \right. \quad (3.8)$$

Другое необходимое условие дается следующей теоремой, являющейся обобщением теоремы Ллойда 3.2:

Теорема 3.3 (Л. А. Бассалыго, Г. В. Зайцев, В. А. Зиновьев [7]). Пусть $A(q, n, d, N)$ — равномерно упакованный код с параметрами $\alpha_0, \alpha_1, \dots, \alpha_\Lambda$. Тогда многочлен по ξ степени Λ

$$\Psi_\Lambda(n, \xi) = \sum_{r=0}^{\Lambda} \alpha_r P_r(n, \xi), \quad (3.9)$$

где $P_r(n, \xi)$ определяется (3.2), имеет Λ различных целых корней, заключенных между 0 и n .

Как следствие этой теоремы, легко выписывается спектр весов [7]:

$$\eta(x) = \frac{(1 + (q-1)x)^n}{\sum_{r=0}^{\Lambda} \alpha_r (q-1)^r C_n^r} + \sum_{r=1}^{\Lambda} \beta_r (1 + (q-1)x)^{n-\xi_r} (1-x)^{\xi_r}, \quad (3.10)$$

где ξ_r — корни многочлена $\Psi_\Lambda(n, \xi)$, а β_r — константы, определяемые начальными условиями. Поэтому в равномерно упакованном коде с $\Lambda \leq d$ спектр расстояний от произвольного вектора $a \in A$ до других векторов кода полностью определяется основными параметрами кода, не зависит от выбора этого вектора и тождественен спектру весов кода с нулевым вектором. Так же, как и для совершенных кодов в равномерно упакованном коде $A(q, n, d, N)$ с $\Lambda < d$, множество всех векторов $a \in A$ веса w образует тактическую конфигурацию $T(n, w, d-\Lambda, \alpha)$. Коды, полученные расширением равномерно упакованных кодов, ведут к тактическим конфигурациям $T(n+1, w, d-\Lambda+1, \alpha)$.

Интереснейшим классом равномерно упакованных кодов являются коды Препарата [288] с параметрами

$$n = 4^m - 1, \quad k = 4^m - 4m, \quad d = 5, \quad m = 2, 3, \dots \quad (3.11)$$

Эти коды нелинейны и максимальны, так как удовлетворяют границе Джонсона [186]. Соответствующие коды БЧХ (см. п. 5) содержат в два раза меньше кодовых слов, хотя являются квазисовершенными. В [77] было показано, что коды Препарата равномерно упакованы с параметрами $\Lambda = 3$, $\alpha_0 = \alpha_1 = 1$, $\alpha_2 = \alpha_3 = 3/n$. Кердок [211] построил нелинейные коды с параметрами

$$n = 4^m - 1, \quad k = 4m, \quad d = ((n+1) - \sqrt{(n+1)})/2, \quad m = 2, 3, \dots \quad (3.12)$$

«двойственные» кодам Препарата в том смысле, что весовые спектры обоих кодов удовлетворяют тождеству Мак-Вильямс [249] (см. п. 4). Код Нордстрема—Робинсона [270] с параметрами $n=15$, $k=8$, $d=5$, построенный также независимо в [73] и являющийся младшим членом обоих семейств при $m=2$, был изучен в ряде работ [73, 76, 100, 152, 287, 289]. Коды Препарата и коды Кердока вызвали значительный интерес [38, 76, 77, 135, 156, 234, 248, 335]. В этой связи очень интересен результат Гёталса [154], который построил два подобных (и «двойственных» в том же смысле) семейства нелинейных кодов для длины 4^m-1 , $m=3, 4, \dots$. Коды одного из семейств имеют $d=7$ и в четыре раза больше кодовых слов, чем соответствующие коды БЧХ.

§ 4. ОГРАНИЧЕНИЯ НА ВЕСОВЫЕ СПЕКТРЫ В ПРОИЗВОЛЬНЫХ КОДАХ

Для нахождения весового спектра в произвольных линейных кодах главную роль играет ставшая уже классической следующая теорема Мак-Вильямс:

Теорема 4.1. (Мак-Вильямс [240]). Пусть $A = A(q, n, d, q^k)$ — линейный код над $GF(q)$ с весовым спектром $\eta(x)$ и пусть $A^\perp = A(q, n, d^\perp, q^{n-k})$ — двойственный к нему код с весовым спектром $\eta^\perp(x)$. Тогда

$$\eta(x) = q^{k-n} (1 + (q-1)x)^n \eta^\perp((1-x)/(1+(q-1)x)). \quad (4.1)$$

Теорема Мак-Вильямс дает систему $n+1$ уравнений, связывающих $n+1$ коэффициентов весовой функции $\eta(x)$ с $n+1$ коэффициентами $\eta^\perp(x)$:

$$\eta_j^\perp = \frac{1}{q^k} \sum_{i=0}^n \eta_i P_j(n, i), \quad 0 \leq j \leq n, \quad (4.2)$$

где $P_j(n, i)$ — полином Кравчука (3.2).

Дельсарт [133, 135] предложил рассмотреть и исследовать преобразование (4.2) для произвольного $(n+1)$ -набора $\eta = (\eta_0, \dots, \eta_n)$ рациональных чисел η_i . Обозначим через $\Delta(\eta)$ число ненулевых компонент набора η без учета η_0 , а через $d(\eta)$ наименьшее целое k , $k=1, \dots, n$, такое, что $\eta_k \neq 0$ (если такое число существует). Связь между $d(\eta)$ и $\Delta(\eta)$ дает следующая

Теорема 4.2. (Дельсарт [133]). Пусть дан произвольный $(n+1)$ -набор η с $\eta_0 \neq 0$. Тогда $\Delta(\eta^\perp) \geq (d(\eta) - 1)/2$.

Далее для произвольного кода $A = A(q, n, d, N)$ определим усредненный спектр расстояний как $(n+1)$ -набор $\eta(A) =$

$$=(\eta_0(A), \dots, \eta_n(A)) \text{ неотрицательных рациональных чисел } \eta_i(A)$$

$$\eta_i(A) = \frac{1}{N} |\{(a, b) \in A^2 \mid d(a, b) = i\}|. \quad (4.3)$$

Ясно, что $d(\eta(A)) = d$, а $\Lambda = \Lambda(\eta(A))$ равно числу различных значений, принимаемых функцией $d(a, b)$, $a \neq b$, $a, b \in A$. Дельсарт [133] доказал, что для любого кода A $\eta_k^\perp(A) \geq 0$ для всех $k=0, 1, \dots, n$. Этот результат Дельсарта естественным образом приводит к одной задаче линейного программирования, решение которой дает верхнюю границу на мощность кода A с заданной областью значений функции $d(a, b)$, $a, b \in A$.

Если $\eta = \eta(A)$ — усредненный спектр расстояний произвольного кода $A = A(q, n, d, N)$, то, кроме параметров $d = d(\eta)$ и $\Lambda = \Lambda(\eta)$, имеются еще два параметра $d^\perp = d(\eta^\perp)$ и $\Lambda^\perp = \Lambda(\eta^\perp)$, определяемых данным спектром η , которые также имеют комбинаторный смысл. Так, параметр Λ^\perp представляет собой внешнее расстояние кода A (см. (3.6)). Все эти четыре параметра d , Λ , d^\perp и Λ^\perp подробно исследованы Дельсартом [135].

Кроме того, Дельсарт обобщил теорему Мак-Вильямс на широкий класс аддитивных кодов. Отобразим произвольным образом алфавит E порядка q на некоторую аддитивную абелеву группу G порядка q . Тогда точки E^n можно рассматривать как элементы группы $G^n = (G, +)^n$ и расстояние Хэмминга $d(a, b)$ между векторами a и b равно весу их разности,

$$d(a, b) = w(a - b), \quad \forall a, b \in G^n. \quad (4.4)$$

Пусть $g_0 = 0, g_1, \dots, g_{q-1}$ — элементы G , а $\Phi_0, \Phi_1, \dots, \Phi_{q-1}$ — групповые характеры G , пронумерованные таким образом, что $\Phi_i(g_j) = \Phi_j(g_i)$. В частности, Φ_0 — главный характер: $\Phi_0(g_i) = 1$ для всех i . Тогда для $a, b \in G^n$ определим скалярное произведение ($a = (a_1, \dots, a_n), b = (b_1, \dots, b_n)$):

$$\langle a, b \rangle = \prod_{i=1}^n \Phi_{s_i}(a_i), \quad \text{где } g_{s_i} = b_i. \quad (4.5)$$

Код $A = A(q, n, d, N)$ над G назовем аддитивным кодом, если его слова образуют подгруппу G^n . Код A^\perp , двойственный к коду A , определим следующим образом:

$$A^\perp = \{b \in G^n \mid \langle a, b \rangle = 1, \quad \forall a \in A\}. \quad (4.6)$$

Когда q — простое число, аддитивный код есть просто линейный код над полем Галуа $GF(q)$ и двойственность есть классическое ортогональное дополнение. Если A — аддитивный код над G , то ясно, что усредненный спектр расстояний $\eta(A)$ сводится к обычному весовому спектру: $\eta_i(A)$ — число кодовых слов веса i .

Теорема 4.3. (Дельсарт [133]). Пусть A — аддитивный код над G , а A^\perp — двойственный к нему код. Тогда весовой спектр кода A^\perp представляет собой преобразование Мак-Вильямс (4.2) от весового спектра кода A ,

$$|A| \cdot \eta_k(A^\perp) = \eta_k^\perp(A), \quad 0 \leq k \leq n. \quad (4.7)$$

Интересным следствием теоремы Мак-Вильямс является результат В. К. Леонтьева [61, 62], полученный им для двоичных линейных кодов и легко обобщаемый на аддитивные коды. Если $\eta(x)$ — весовой спектр двоичного линейного кода A , то в силу симметрии отношения двойственности функция $\varphi(x) = \eta(x)\eta^\perp(x)(2/(1+x))^n$ должна удовлетворять уравнению

$$\varphi(x) = \varphi\left(\frac{1-x}{1+x}\right). \quad (4.8)$$

Решение этого функционального уравнения в поле рациональных чисел приводит к следующему результату.

Теорема 4.4. (В. К. Леонтьев [61, 62]). Весовая функция $\eta(x)$ произвольного двоичного линейного кода длины n удовлетворяет следующему соотношению:

$$\eta(x)\eta^\perp(x) = \sum_{i=0}^n c_i (1+x^2)^i (1+x)^{n-i}, \quad (4.9)$$

где c_i — рациональные числа.

Весовую функцию $\eta(x) = \sum_{i=0}^n \eta_i x^i$ иногда удобно представлять как функцию двух переменных

$$\eta(x, y) = \sum_{i=0}^n \eta_i x^{n-i} y^i.$$

Если (n, k) -код A над $GF(q)$ имеет весовую функцию $\eta(x, y)$, а двойственный к нему $(n, n-k)$ -код A^\perp имеет весовую функцию $\eta^\perp(x, y)$, то в этом случае формула Мак-Вильямс (4.1) переписывается следующим образом:

$$\eta(x, y) = q^{k-n} \eta^\perp(x + (q-1)y, x-y). \quad (4.10)$$

Назовем $(n, n/2)$ -код A самодвойственным, если $A^\perp = A$. В этом случае весовая функция $\eta(x, y)$ удовлетворяет условию

$$\eta(x, y) = \eta\left(\frac{x + (q-1)y}{\sqrt{q}}, \frac{x-y}{\sqrt{q}}\right). \quad (4.11)$$

Глисон [148] нашел в нескольких случаях все возможные решения функционального уравнения (4.11).

Теорема 4.5. (Глисон [148]). Пусть $\eta(x, y)$ — весовая функция самодвойственного кода длины n над $GF(q)$, все веса которого кратны c . Тогда

$$\eta(x, y) = \sum_{r,s} K_{r,s} f_1(x, y)^r f_2(x, y)^s,$$

где r, s — неотрицательные целые числа, $K_{r,s}$ — комплексные числа и

(1) $f_1(x, y) = x^2 + y^2$, $f_2(x, y) = x^2 y^2 (x^2 - y^2)$, $n = 2r + 8s$ и $\eta_{n-i} = \eta_i$ для всех i , если $q = c = 2$;

(2) $f_1(x, y) = x^8 + 14x^4 y^4 + y^8$, $f_2(x, y) = x^4 y^4 (x^4 - y^4)^4$ и $n = 8r + 24s$, если $2q = c = 4$;

(3) $f_1(x, y) = x^4 + 8xy^3$, $f_2(x, y) = y^3 (x^3 - y^3)^3$ и $n = 4r + 12s$, если $q = c = 3$.

Фейт, Томпсон (см. ссылки в [246]), а также Берлекэмп, Мак-Вильямс и Слоэн [105] дали несколько интересных доказательств теоремы Глисона, а Мак-Вильямс, Мэллоус и Слоэн [246] обнаружили связь этой теоремы с классической теорией инвариантов. Оказывается, ряд обобщений и сама теорема Глисона непосредственно следуют из теории инвариантов. Проблема нахождения весовой функции самодвойственного кода является специальным случаем более общей проблемы нахождения полиномов, инвариантных относительно группы линейных преобразований. Многие из теорем о весовых функциях были известны еще в прошлом столетии в другой формулировке (см. ссылки в [246]).

Мак-Вильямс, Слоэн и Томпсон для $q = 2$ [250], а Плесс и Пирс для других q [284] доказали, что среди самодвойственных кодов имеются коды, лежащие на границе Варшавова—Гилберта (2.9). Несколько работ [91, 142, 191, 280—283, 285] посвящены построению, классификации и перечислению самодвойственных кодов. Мэллоус и Слоэн [254] получили точное выражение для весовой функции самодвойственных кодов в том случае, когда расстояние d принимает максимально возможное значение, и привели все такие весовые функции для двоичных самодвойственных кодов с весами, кратными 4, для длин $n \leq 200$ и $n = 256$. Для случая, когда n кратно 24, а веса кодовых векторов кратны 4, Мэллоус и Слоэн [254] предположили существование интересного класса самодвойственных кодов с $d = n/6 + 4$. Первым двум значениям n соответствуют: расширенные (24, 12) — код Голея с $d = 8$ и квадратично вычетный (48, 24) — код с $d = 12$. Существование уже следующего самодвойственного (72, 36) — кода с $d = 16$ является открытым вопросом (Слоэн [305]). В дальнейшей работе Мэллоус и Слоэн [255] доказали аналог теоремы Глисона для двоичных $(n, (n-1/2))$ -кодов A таких, что $A \subset A^\perp$.

§ 5. ЦИКЛИЧЕСКИЕ КОДЫ И КОДЫ БЧХ

Линейный (n, k) -код называется циклическим, если он удовлетворяет следующему условию: циклический сдвиг любого кодового слова также является кодовым словом. Для цикличе-

ских кодов более удобно представление E^n как кольца $F[x]/(x^n-1)$ полиномов над $F=GF(q)$ по модулю x^n-1 , осуществляемое с помощью очевидного перехода

$$a = (a_0, \dots, a_{n-1}) \in E^n \leftrightarrow \sum_{i=0}^{n-1} a_i x^i = a(x) \in F[x]. \quad (5.1)$$

Тогда подпространство $A \subseteq E^n$ является циклическим (n, k) -кодом, если и только если оно является идеалом в $F[x]/(x^n-1)$ (см. книги [51, 96, 232, 273, 276]). Это означает, что слова $a(x)$ циклического кода A представимы в виде: $a(x) = f_a(x)g(x)$, где многочлен $g(x)$ степени $n-k$ называется порождающим многочленом кода и $g(x)$ делит x^n-1 . Многочлен $h(x) = (x^n-1)/g(x)$ степени k называется проверочным, так как для любого $a(x) \in A$ выполняется следующее условие ортогональности

$$a(x)h(x) \equiv 0 \pmod{x^n-1}. \quad (5.2)$$

Большинство рассмотренных и изученных к настоящему времени кодов являются циклическими. Среди них наилучшие коды — коды БЧХ, которые мы сейчас кратко рассмотрим. Пусть: $q = p^s$, где p — простое число, $s = 1, 2, \dots$; $m = \text{ord}_n(q)$ — порядок q по модулю n (т. е. наименьшее натуральное число m такое, что $q^m \equiv 1 \pmod{n}$); α — примитивный корень n -ой степени из 1 в $GF(q^m)$. Тогда БЧХ код (Боуза — Чоудхури [113, 114] — Хоквингема [184]) длины n над полем $GF(q)$, задаваемый проверочной матрицей

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \dots & \alpha^{(n-1)2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{d_0-1} & \alpha^{2(d_0-1)} & \dots & \alpha^{(n-1)(d_0-1)} \end{bmatrix}, \quad (5.3)$$

имеет параметры

$$k \geq n - m(d_0 - 1)(q - 1)/q, \quad d \geq d_0, \quad (5.4)$$

где $|x|$ — наименьшее целое, не меньшее x , а d_0 — конструктивное расстояние. Если обозначить через $m_l(x)$ — минимальный многочлен для α^l (т. е. неприводимый над $GF(q)$ нормированный многочлен, корнями которого являются $\alpha^l, \alpha^{lq}, \dots, \alpha^{lq^{m-1}}$), то порождающий многочлен данного кода БЧХ над $GF(q)$ находится по формуле

$$g(x) = \text{H. O. K. } [m_1(x) m_2(x) \dots m_{d_0-1}(x)]. \quad (5.5)$$

Так как любое кодовое слово $a(x)$ делится на $g(x)$, то из (5.4) вытекает, что $a(x)$ содержит в качестве корней элементы $\alpha, \alpha^2, \dots, \alpha^{d_0-1}$. Обобщением этой идеи является следующая

Теорема 5.1. (Граница БЧХ [273, 276]). Если для циклического кода длины n над $GF(q)$ элементы α^{m_0} , α^{m_0+1} , ..., $\alpha^{m_0+d_0-2}$, являются корнями любого кодового слова, где α — примитивный корень n -ой степени из 1 в соответствующем расширении поля $GF(q)$, то в этом коде расстояние $d \geq d_0$.

Большое число работ посвящено проблемам построения неприводимых полиномов над полями Гауа, необходимых для построения циклических кодов с заданным расстоянием [21—24, 29, 35, 96, 97, 107, 116, 117, 162, 219, 276, 316, 336].

Если $n = q^m - 1$, то код БЧХ называется примитивным. Питерсон [274] высказал предположение, что для примитивных кодов БЧХ $d = d_0$. В 1969 году Касами и Токура [208] показали, что для любого $m > 6$, $m \neq 8, 12$, имеются двоичные примитивные коды БЧХ длины $2^m - 1$, для которых $d > d_0$. В этой же работе они показали также, что для любого четного $m \geq 6$ имеются двоичные циклические коды длины $2^m - 1$, которые имеют больше информационных символов k , чем коды БЧХ с теми же n и d . Подход Касами и Токура основан на следующих двух интересных результатах:

Теорема 5.2. (Питерсон [274]). Расширенные примитивные коды БЧХ инвариантны относительно аффинной группы подстановок.

Теорема 5.3. (Соломон, Мак-Элиси [265, 312]). Пусть: A — двоичный циклический код с проверочным полиномом $h(x)$; r — наименьшее целое такое, что $\gamma_1 \gamma_2 \dots \gamma_r = 1$, где $h(\gamma_i) = 0$ и $\gamma_i \neq 1$ для всех $i = 1, \dots, r$. Тогда четные веса кодовых слов кода A делятся на 2^{r-1} .

С другой стороны, имеется целый ряд случаев, когда в примитивных кодах БЧХ $d = d_0$. В. К. Леонтьев [60] обнаружил, что если $d_0 - 1 < 2^{m/2}$, то двоичный БЧХ код длины $2^m - 1$ имеет $d = d_0$. Берлекэмп [98] показал, что если расширенный двоичный код БЧХ длины $n = 2^m$ имеет $d_0 = 2^{m-1} - 2^i$ для некоторого $i \geq m/2 - 1$, то $d = d_0$. В дальнейшем этот результат Берлекэмпа был обобщен Касами [197].

Выражение для k в кодах БЧХ (см. (5.4)) также является оценкой снизу. Нахождению числа информационных символов в кодах БЧХ посвящены работа Манна [257] и Берлекэмпа [95, 96]. Берлекэмп получил точное выражение для скорости расширенных примитивных БЧХ кодов с фиксированным отношением d/n . В другой работе Берлекэмп [101] вывел верхнюю и нижнюю границу на конструктивное и на действительное расстояния расширенных примитивных кодов БЧХ с фиксированной скоростью R . В частности, Берлекэмп получил следующую асимптотически точную оценку расстояния d_0 :

$$d_0 \approx n \left(\frac{2 \ln R^{-1}}{\log_2 n} \right)^{1 + (\ln R^{-1} / \ln n)} \left(1 + C \frac{2 \ln R^{-1}}{\log_2 n} \right),$$

где C ограничено. Поэтому в кодах БЧХ как d_0 , так и d при

$n \rightarrow \infty$ растут как $2n \ln R^{-1} / \log_2 n$. Отсюда следует, что для двоичных примитивных БЧХ кодов оценки (5.4) асимптотически точны. Тем не менее точное определение условий на n и d_0 , при которых $d = d_0$, остается нерешенной проблемой.

Укажем еще несколько интересных результатов, полученных для двоичных примитивных БЧХ кодов. Коды БЧХ с $t=1$ являются совершенными кодами Хэмминга (см. п. 3). Горенштейн, Питерсон и Цирлер [164] показали, что при $t=2$ эти коды БЧХ являются квазисовершенными, т. е. имеют внешнее расстояние $\Lambda=3$ (см. (3.6)), а Л. А. Бассальго, Г. В. Зайцев и В. А. Зиновьев [7] показали, что такие коды БЧХ длины $n=2^{2m+1}-1$ являются равномерно упакованными кодами (см. п. 3). Однако, как установил В. К. Леонтьев [60] при $2 < t < \sqrt{n} / \ln n$ и $m \geq 7$, коды БЧХ длины $n=2^m-1$ уже не являются квазисовершенными. В. М. Сидельников [78] получил асимптотические формулы весового спектра кодов БЧХ. Он показал, что для $t < \sqrt{n}/10$ число η_w слов веса w в коде БЧХ с $d_0=2t+1$ имеет вид (при некотором ограничении на w)

$$\eta_w = (n+1)^{-t} C_n^w (1+\varepsilon), \quad (5.6)$$

где $|\varepsilon| < cn^{-0.1}$. Используя известные теоретико-числовые результаты по оценке экспоненциальных сумм в конечных полях, Андерсон [86] показал, что в коде, двойственном к коду БЧХ длины $n=2^m-1$ и с $d_0=2t+1$, расстояние по меньшей мере равно $2^{m-1}-1-(t-1)2^{m/2}$ (по этому вопросу смотри также [63, 78]).

Из работ, посвященных построению циклических кодов с $d=d_0$, необходимо указать еще [201, 202, 275, 276]. Гёталс [150] и Касами [194] улучшили границу БЧХ для кодов составной длины. Хартманн и Тзенг [175] значительно упростили технику Касами и обобщили его результаты. Кроме того, Хартманн [170—173, 175—179] дал много дальнейших интересных обобщений границы БЧХ. Дело в том, что граница БЧХ для циклических кодов над $GF(q)$ не использует того, что коэффициенты кодовых слов принадлежат этому полю, а порождающий многочлен $g(x)$, кроме корней $\alpha^{m_0}, \alpha^{m_0+1}, \dots, \alpha^{m_0+d_0-2}$, имеет еще и другие корни. Хартманн смог учесть эти факты с помощью введенных Берлекэмпом [96] многочленов — локаторов кодовых векторов. В качестве примера приведем две теоремы Хартманна. Следующая теорема представляет собой нижнюю границу для минимального нечетного веса в коде.

Теорема 5.4. (Хартманн [179]). Пусть n_1 делит n . Если для некоторого $n_2 \leq n/n_1$ элементы $\alpha^{n_1 i}$ являются корнями порождающего многочлена $g(x)$ для всех $i=1, 2, \dots, n_2$, то минимальный нечетный вес в коде по меньшей мере равен n_2 .

Вторая теорема обобщает границу БЧХ на случай, когда $g(x)$ имеет несколько множеств последовательных корней.

Теорема 5.5. (Хартманн [179]). Если $g(\alpha^{m_0+i+\delta(r-1)})=0$ для $i=0, 1, \dots, d_0-2$ и $j=1, 2, \dots, r$, где $(\delta, n)=1$ так, что порождающий многочлен $g(x)$ имеет r множеств по d_0-1 корней в каждом, то $d \geq d_0+r$.

Из других работ по уточнению расстояния в циклических кодах необходимо указать также работы [25, 51, 54, 89, 90, 121, 122, 130, 149, 161, 213, 221, 238, 239, 241, 263, 278]. Интересно сопоставить следующий результат, независимо полученный в [51, 54] (и переоткрытый в [179, теорема 2]), с теоремой 5.4:

Теорема 5.6. (В. Д. Колесник и Е. Т. Мирончиков [51], В. И. Коржик [54]). Если циклический код над $GF(q)$ длины $n=n_1n_2$ имеет расстояние $d > n_1$, то хотя бы один элемент вида α^{in_1} , $i=0, 1, \dots, n_2-1$, является корнем порождающего многочлена $g(x)$ данного кода. В противном случае код содержит слово веса n_1 .

Варшамов Р. Р. и Тененгольц Г. М. [25] нашли расстояние в кодах (предложенных Г. М. Тененгольцем [84]), проверочный полином которых равен произведению различных примитивных полиномов с попарно взаимно простыми степенями (см. также [36]).

Определение расстояния в циклических кодах является частным случаем более общей и, конечно, значительно более трудной задачи нахождения весового спектра $\eta=(\eta_0, \eta_1, \dots, \eta_n)$. В п. 4 были рассмотрены некоторые общие результаты о спектрах линейных кодов. Ясно, что векторы любого циклического кода могут быть разбиты на циклы. Цикл состоит из всех различных циклических сдвигов одного вектора, называемого представителем этого цикла. Размер цикла, или его период, делит длину кода, все векторы в цикле имеют одинаковый вес и нахождение спектра сводится к перечислению представителей циклов по их весам и периодам.

Циклический код над $GF(q)$ длины n , $(q, n)=1$, является минимальным идеалом, если его проверочный многочлен $h(x)$ неприводим над $GF(q)$. Гёталс [149] и Нили (ссылка в [317]) дали метод нахождения циклических представителей для минимальных идеалов, а Мак-Вильямс [241] сделала это для прямой суммы двух минимальных идеалов. Пусть циклический (n, k) -код A над $GF(q)$ порожден полиномом $g(x)=(x^n-1)/h(x)$, где $(n, q)=1$ и $m=\text{ord}_n(q)$, т. е. $n=(q^m-1)/c$ для натурального c . Пусть, далее, $h(x)=h_1(x) \dots h_s(x)$, где $h_i(x)$ — неприводимый над $GF(q)$ полином степени m_i и периода e_i (т. е. e_i наименьшее число j , для которого $h_i(x)$ делит x^j-1), $i=1, \dots, s$. Пусть минимальный идеал A_i порожден $g_i(x)=(x^n-1)/h_i(x)$. Исходный код A является прямой суммой минимальных идеалов A_i и циклические представители A определяются представителями A_i , которые удобнее задавать с по-

$n \rightarrow \infty$ растут как $2n \ln R^{-1} / \log_2 n$. Отсюда следует, что для двоичных примитивных БЧХ кодов оценки (5.4) асимптотически точны. Тем не менее точное определение условий на n и d_0 , при которых $d = d_0$, остается нерешенной проблемой.

Укажем еще несколько интересных результатов, полученных для двоичных примитивных БЧХ кодов. Коды БЧХ с $t=1$ являются совершенными кодами Хэмминга (см. п. 3). Горенштейн, Питерсон и Цирлер [164] показали, что при $t=2$ эти коды БЧХ являются квазисовершенными, т. е. имеют внешнее расстояние $\Lambda=3$ (см. (3.6)), а Л. А. Бассальго, Г. В. Зайцев и В. А. Зиновьев [7] показали, что такие коды БЧХ длины $n=2^{2m+1}-1$ являются равномерно упакованными кодами (см. п. 3). Однако, как установил В. К. Леонтьев [60] при $2 < t < \sqrt{n} / \ln n$ и $m \geq 7$, коды БЧХ длины $n=2^m-1$ уже не являются квазисовершенными. В. М. Сидельников [78] получил асимптотические формулы весового спектра кодов БЧХ. Он показал, что для $t < \sqrt{n}/10$ число η_w слов веса w в коде БЧХ с $d_0=2t+1$ имеет вид (при некотором ограничении на w)

$$\eta_w = (n+1)^{-t} C_n^w (1+\epsilon), \quad (5.6)$$

где $|\epsilon| < cn^{-0.1}$. Используя известные теоретико-числовые результаты по оценке экспоненциальных сумм в конечных полях, Андерсон [86] показал, что в коде, двойственном к коду БЧХ длины $n=2^m-1$ и с $d_0=2t+1$, расстояние по меньшей мере равно $2^{m-1}-1-(t-1)2^{m/2}$ (по этому вопросу смотри также [63, 78]).

Из работ, посвященных построению циклических кодов с $d=d_0$, необходимо указать еще [201, 202, 275, 276]. Гёталс [150] и Касами [194] улучшили границу БЧХ для кодов составной длины. Хартманн и Тзенг [175] значительно упростили технику Касами и обобщили его результаты. Кроме того, Хартманн [170—173, 175—179] дал много дальнейших интересных обобщений границы БЧХ. Дело в том, что граница БЧХ для циклических кодов над $GF(q)$ не использует того, что коэффициенты кодовых слов принадлежат этому полю, а порождающий многочлен $g(x)$, кроме корней $\alpha^{m_0}, \alpha^{m_0+1}, \dots, \alpha^{m_0+d_0-2}$, имеет еще и другие корни. Хартманн смог учесть эти факты с помощью введенных Берлекэмпом [96] многочленов-локаторов кодовых векторов. В качестве примера приведем две теоремы Хартманна. Следующая теорема представляет собой нижнюю границу для минимального нечетного веса в коде.

Теорема 5.4. (Хартманн [179]). Пусть n_1 делит n . Если для некоторого $n_2 \leq n/n_1$ элементы $\alpha^{n_1 i}$ являются корнями порождающего многочлена $g(x)$ для всех $i=1, 2, \dots, n_2$, то минимальный нечетный вес в коде по меньшей мере равен n_2 .

Вторая теорема обобщает границу БЧХ на случай, когда $g(x)$ имеет несколько множеств последовательных корней.

Теорема 5.5. (Хартманн [179]). Если $g(\alpha^{m_0+i+\delta(j-1)})=0$ для $i=0, 1, \dots, d_0-2$ и $j=1, 2, \dots, r$, где $(\delta, n)=1$ так, что порождающий многочлен $g(x)$ имеет r множеств по d_0-1 корней в каждом, то $d \geq d_0+r$.

Из других работ по уточнению расстояния в циклических кодах необходимо указать также работы [25, 51, 54, 89, 90, 121, 122, 130, 149, 161, 213, 221, 238, 239, 241, 263, 278]. Интересно сопоставить следующий результат, независимо полученный в [51, 54] (и переоткрытый в [179, теорема 2]), с теоремой 5.4:

Теорема 5.6. (В. Д. Колесник и Е. Т. Мирончиков [51], В. И. Коржик [54]). Если циклический код над $GF(q)$ длины $n=n_1n_2$ имеет расстояние $d > n_1$, то хотя бы один элемент вида α^{in_1} , $i=0, 1, \dots, n_2-1$, является корнем порождающего многочлена $g(x)$ данного кода. В противном случае код содержит слово веса n_1 .

Варшамов Р. Р. и Тененгольц Г. М. [25] нашли расстояние в кодах (предложенных Г. М. Тененгольцем [84]), проверочный полином которых равен произведению различных примитивных полиномов с попарно взаимно простыми степенями (см. также [36]).

Определение расстояния в циклических кодах является частным случаем более общей и, конечно, значительно более трудной задачи нахождения весового спектра $\eta=(\eta_0, \eta_1, \dots, \eta_n)$. В п. 4 были рассмотрены некоторые общие результаты о спектрах линейных кодов. Ясно, что векторы любого циклического кода могут быть разбиты на циклы. Цикл состоит из всех различных циклических сдвигов одного вектора, называемого представителем этого цикла. Размер цикла, или его период, делит длину кода, все векторы в цикле имеют одинаковый вес и нахождение спектра сводится к перечислению представителей циклов по их весам и периодам.

Циклический код над $GF(q)$ длины n , $(q, n)=1$, является минимальным идеалом, если его проверочный многочлен $h(x)$ неприводим над $GF(q)$. Гёталс [149] и Нили (ссылка в [317]) дали метод нахождения циклических представителей для минимальных идеалов, а Мак-Вильямс [241] сделала это для прямой суммы двух минимальных идеалов. Пусть циклический (n, k) -код A над $GF(q)$ порожден полиномом $g(x)=(x^n-1)/h(x)$, где $(n, q)=1$ и $m=\text{ord}_n(q)$, т. е. $n=(q^m-1)/c$ для натурального c . Пусть, далее, $h(x)=h_1(x) \dots h_s(x)$, где $h_i(x)$ — неприводимый над $GF(q)$ полином степени m_i и периода e_i (т. е. e_i наименьшее число j , для которого $h_i(x)$ делит x^j-1), $i=1, \dots, s$. Пусть минимальный идеал A_i порожден $g_i(x)=(x^n-1)/h_i(x)$. Исходный код A является прямой суммой минимальных идеалов A_i и циклические представители A определяются представителями A_i , которые удобнее задавать с по-

мощью идемпотентов. Напомним, что идемпотентом A_i называется такой полином $\varepsilon_i(x)$ из A_i , что

$$\varepsilon_i(x) \equiv 1 \pmod{h_i(x)}, \quad (5.7)$$

$$\varepsilon_i^2(x) \equiv \varepsilon_i(x) \pmod{(x^n - 1)}. \quad (5.8)$$

Идемпотенты минимальных идеалов циклического кода ортогональны, т. е.

$$\varepsilon_i(x) \varepsilon_j(x) \equiv 0 \pmod{(x^n - 1)}. \quad (5.9)$$

а идемпотент $\varepsilon(x)$ циклического кода A равен сумме идемпотентов $\varepsilon_i(x)$ его минимальных идеалов. Нетрудно показать, что период всех циклов в минимальном идеале A_i равен e_i , т. е. периоду $h_i(x)$, и так как A_i содержит $q^{m_i} - 1$ ненулевых кодовых слов, то он имеет $c_i = (q^{m_i} - 1)/e_i$ циклических представителей, множество которых мы обозначим через $F_i(x)$. Нили (ссылка в [317]) и Гёталс [149] показали, что

$$F_i(x) = \{\alpha_j^i(x) \varepsilon_i(x), \quad j=0, 1, \dots, c_i-1\}, \quad (5.10)$$

где $\alpha_j^i(x)$ — любой примитивный элемент в поле Галуа $GF(q^{m_i})$, порожденном неприводимым полиномом $h_i(x)$. С. Ш. Оганесян и В. Г. Ягджян [67] и позже Таварес, Аллар и Шива [85, 317] получили рекуррентные выражения для всех циклических представителей произвольного двоичного циклического (n, k) -кода A нечетной длины через представители его минимальных идеалов. Формула для представителей идеала A , полученная С. Ш. Оганесяном и В. Г. Ягджяном [67], имеет следующий вид:

$$\sum_{i=1}^{s-1} f_i(x) x^{\sum_{j=1}^{s-1} k_j} + f_s(x), \quad (5.11)$$

где $k_j \in K_j$, $f_i(x) \in F_i(x)$, $K_j = \{0, 1, \dots, (\text{Н. О. К. } [b_1, \dots, b_j], b_{j+1} - 1)\}$; здесь $b_1 = 1$, если из множества $F_1(x)$ выбран 0, и $b_i = e_i$ в остальных случаях. Период этого представителя равен Н. О. К. $[b_1, \dots, b_s]$. Таварес и др. [85, 317] использовали другой подход. Некоторые интересные соображения по этому вопросу имеются также в работах [19, 295].

Вычислять спектр циклического кода, пользуясь выражениями (5.11), трудно даже для случаев, когда код является прямой суммой небольшого числа минимальных идеалов. Эти вычисления значительно упрощаются, если разбивать все кодовые слова на p -ичные представители, объединяющие циклические представители по одинаковым весам посредством возведения в степень, равную характеристике поля. Для минимальных идеалов подобное разбиение сделал Гёталс [149], а для прямой суммы двух минимальных идеалов это было сделано С. Ш. Оганесяном и В. Г. Ягджяном [68]. В последующей работе С. Ш. Оганесян, В. И. Таирян и В. Г. Ягджян [71] полностью решили задачу нахождения вида всех циклических и p -ичных

представителей для произвольного циклического кода длины n над $GF(q=p^m)$, $(n, q)=1$. Этот подход позволил найти весовые спектры для некоторых классов циклических кодов (С. Ш. Оганесян и В. Г. Ягджян [69, 70], С. Ш. Оганесян, В. И. Таирян и В. Г. Ягджян [271]).

В самом общем виде задачу нахождения спектров циклических кодов можно решать, разбивая код на непересекающиеся G -орбиты (G -орбитой называется множество кодовых векторов, переходящих друг в друга под воздействием группы G , сохраняющей вес векторов). Для группы G , порожденной преобразованиями: (1) $a(x) \rightarrow xa(x)$, (2) $a(x) \rightarrow a(x)^p$, (3) $a(x) \rightarrow \alpha^i a(x)$, где $a(x)$ — вектор циклического кода над $GF(q=p^m)$, α — примитивный элемент $GF(q)$, задача определения структуры G -орбит произвольных циклических кодов была решена В. И. Таиряном и Г. Г. Хачатряном [83].

Баумерт, Мак-Элис и Рамсей [93, 266], обобщая более раннюю работу Дельсарта и Гёталса [138], дали метод определения весового спектра всех минимальных идеалов и выписали спектры для всех таких двоичных кодов с $n < 10^6$.

Коды БЧХ над $GF(q)$ длины $n \leq q-1$, соответствующие значению $m=1$ в (5.3), называются иначе кодами Рида—Соломона (Р—С) [292] и имеют параметры

$$n, k, d = n - k + 1. \quad (5.12)$$

Так как для любого кода $d \leq n - k + 1$, то коды с параметрами (5.12) максимальны (их называют еще кодами, с максимальным достижимым расстоянием). Этот факт позволяет вычислить спектр весов кодов Р—С, что было сделано независимо Ассумсом, Матсоном и Турином (ссылка в [96]), Форни [143] и Касами, Лином и Питерсоном [202]: в коде $A(q, n, d, q^h)$ с $d = n + 1 - k$, в котором имеется вектор веса 0, число слов веса w , $w \geq d$, задается формулой

$$\eta_w = C_n^w (q-1) \sum_{i=0}^{w-d} (-1)^i C_{w-1}^i q^{w-d-i}. \quad (5.13)$$

Асмусс и Матсон [89] доказали, что любой циклический код с простой длиной n над $GF(p^m)$ для всех p (кроме конечного числа) является кодом с $d = n + 1 - k$ при всех m .

Коды Р—С эквивалентны изучаемым в комбинаторике ортогональным расположениям индекса 1 [111, 112, 120, 167, 256, 299, 300]. Буш [120] построил такие расположения длины $n = q + 1$ и в случае $q = 2^s$ и $k = 3$ или $k = n - 3$ длины $n = q + 2$. Поэтому коды Р—С всегда могут быть расширены до длины $q + 1$ или $q + 2$. Соответствующее расширение не dvoичных кодов БЧХ было осуществлено Вулфом [334]. Он показал, что если в коде БЧХ $d_0 \leq q + 1$, то добавление двух определенных столбцов веса 1 к матрице (5.3) H дает проверочную матрицу H' нового линейного кода с параметрами $n' = n + 2$, $k' = k + 2$, $d' \geq d_0$.

В другой работе Вулф [334] описал дальнейшее расширение кодов БЧХ длины $q^m - 1$ над $GF(q)$ с $d_0 \leq q + 1$. Пусть: α — примитивный элемент $GF(q^m)$; $m_1(x)$ — минимальный многочлен для α над $GF(q)$; M — сопровождающая матрица многочлена $m_1(x)$. Если в проверочной матрице H' заменить α^i на матрицу M^i , $i = 1, 2, \dots, q^m - 2$, элемент 1 заменить на единичную матрицу I_m порядка m , а элемент 0 заменить на $(m \times m)$ -матрицу из нулей, то получим проверочную матрицу кода над $GF(q)$ с параметрами

$$n = m(q^m + 1), k = n - m(d_0 - 1), d \geq d_0. \quad (5.14)$$

Интересное расширение циклических кодов предложили В. И. Андрианов и В. Н. Сасковец [2] (см. также [51, 96]). Несколько другое расширение кодов как линейных, так и нелинейных, основанное на разбиении кодов на подкоды с большим расстоянием, было рассмотрено независимо Слоэном, Редди и Ченом [307] и Г. В. Зайцевым, В. А. Зиновьевым и Н. В. Семановым [76, 335]. В частности, были расширены коды БЧХ [307], а используя разбиения кодов Хэмминга на коды Препарата, были получены новые нелинейные коды с $d = 5$ и с максимально возможным k [76, 307, 335]. Некоторые из этих кодов с $d = 5$ оказались квазивершенными, т. е. имеющими внешнее расстояние $\Lambda = 3$ [335].

Одним из важнейших вопросов, касающихся циклических кодов, является вопрос об асимптотическом поведении их параметров. Целый ряд интересных результатов здесь уже получен. Как мы уже видели для кодов БЧХ, $d \sim 2n \ln R^{-1} / \log_2 n$ (Берлекэмп [101]) и поэтому отношение $d/n \rightarrow 0$ при $n \rightarrow \infty$ (это впервые показано Лином и Велдоном [226]). Очень интересен результат С. Д. Бермана (см. теорему 7.1). Касами [195] доказал, что любой код с заданным отношением d/n , инвариантный относительно аффинной группы перестановок, должен иметь скорость $R \rightarrow 0$ при $n \rightarrow \infty$ (это относится и к БЧХ кодам, если учесть теорему 5.2 Питерсона). Результат Касами говорит о том, что хорошие линейные коды не могут быть слишком симметричными. В этой связи интересен результат Мак-Элиса [264]. Он доказал существование сколь угодно длинных кодов (не обязательно линейных), инвариантных относительно больших групп перестановок и удовлетворяющих границе (2.9) Варшавова—Гилберта. Иначе говоря, не только одна симметрия делает код плохим.

Существование сколь угодно длинных кодов, лежащих на границе Варшавова—Гилберта, доказано для укороченных циклических кодов (Касами [195], Чен [124]) и для скорости передачи $R = 1/3$ для квазициклических кодов (И. И. Грушко [34]). Касами [198], опираясь на результаты Чена, Питерсона и Велдона [126, 329], для скорости $R = 1/2$ доказал существование квазициклических кодов, удовлетворяющих несколько более слабой границе, чем граница Варшавова—Гилберта.

§ 6. КОДЫ ГОППЫ

Рассмотренные в п. 5 циклические коды над полями Галуа $GF(q)$ были связаны с представлением E^n как алгебры многочленов над $GF(q)$ по модулю $x^n - 1$. В. Д. Гоппа [31, 32] (см. также [102]) развил другой метод алгебраизации множества E^n . Ввиду важности этого подхода, рассмотрим его более подробно. Пусть: $L = \{\beta_1, \dots, \beta_n\}$, $\beta_i \neq \beta_j$, $\beta_i \in GF(q^m)$, и $GF(q^m)$ — минимальное поле, содержащее L ; Φ^n — векторное пространство рациональных функций вида

$$\xi(x) = \sum_{i=1}^n \frac{b_i}{x - \beta_i}, \quad b_i \in GF(q). \quad (6.1)$$

Отображение $b = (b_1, \dots, b_n) \rightarrow \xi_b(x)$ является изоморфизмом E^n на Φ^n , позволяющим определять коды как некоторые подмножества Φ^n . Пусть теперь $g(x)$ — многочлен над $GF(q^m)$, не имеющий корней в L . Определим (L, g) -код как множество элементов $\xi(x) \in \Phi^n$ таких, что $\xi(x) \equiv 0 \pmod{g(x)}$. Линейность такого кода над $GF(q)$ вполне очевидна, а параметры его имеют вид

$$n \leq q^m, \quad k \geq n - m \cdot \deg g(x), \quad d \geq \deg g(x) + 1. \quad (6.2)$$

Проверочная матрица (L, g) -кода может быть представлена несколькими способами (В. Д. Гоппа [32]). Один из них приведен здесь:

$$H(L, g) = \begin{bmatrix} g^{-1}(\beta_1) & \dots & g^{-1}(\beta_n) \\ g^{-1}(\beta_1)\beta_1 & \dots & g^{-1}(\beta_n)\beta_n \\ \vdots & & \vdots \\ g^{-1}(\beta_1)\beta_1^{v-1} & \dots & g^{-1}(\beta_n)\beta_n^{v-1} \end{bmatrix}, \quad v = \deg g(x). \quad (6.3)$$

(L, g) -коды называются кумулятивными (В. Д. Гоппа [32]), если $g(x) = (x - x_0)^v$, т. е. $g(x)$ имеет один корень $x_0 \in GF(q^m)$ кратности $v = \deg g(x)$. Длина кумулятивных кодов, очевидно, не превышает $q^m - 1$. Частным случаем таких кодов при $g(x) = x^v$ являются коды БЧХ. В этом случае проверочная матрица (6.3) $H(L, g)$ превращается в проверочную матрицу (5.2) H кода БЧХ. Ясно, что все кумулятивные коды с одним и тем же v имеют одинаковые весовые спектры. (L, g) -коды называются сепарабельными (В. Д. Гоппа [32]), если $g(x) = (x - x_1) \dots (x - x_v)$, т. е. $g(x)$ не имеет кратных корней. Двоичные сепарабельные коды так же, как и коды БЧХ, допускают улучшение оценки своих параметров. Так как любая дробь $\xi(x) \in \Phi^n$ может быть представлена в виде $\xi(x) = f'(x)/f(x)$, где $f(x) = (x - \beta_1)^{b_1} \dots (x - \beta_n)^{b_n}$, то из сравнения $\xi(x) \equiv 0 \pmod{g(x)}$ следует, что $\xi(x) \equiv 0 \pmod{g^2(x)}$ (ибо все корни $g(x)$ различны, а производная в поле характеристики 2 является квадратом). Следовательно, при $\deg g(x) = v$ двоич-

ные сепарабельные коды имеют параметры

$$n \leq 2^m, k \geq n - mv, d \geq 2v + 1. \quad (6.4)$$

Сепарабельные коды обладают следующей специфической формой проверочной матрицы (матрица Коши):

$$H_c(L, g) = [(x_i - \beta_j)^{-1}], \quad i = 1, \dots, v, \quad j = 1, \dots, n, \quad (6.5)$$

где x_1, \dots, x_v — корни $g(x)$ в поле $GF(q^m)$ или некотором его расширении.

Интересно, что среди (L, g) -кодов имеются и очень хорошие коды. Справедлива следующая

Теорема 6.1. (В. Д. Гоппа [32]). Пусть $L = GF(n = q^m)$, $H(x)$ — энтропия (см. (2.7)). Для любого $0 < \lambda < 1$ и $\epsilon > 0$ вероятность того, что случайно выбранный многочлен $g(x)$ над $GF(q^m)$ степени $[\lambda n / \log_2 n]$, не имеющий корней в L , порождает (L, g) -код с параметрами $k/n > 1 - H(d/n) - \epsilon$ стремится к единице с ростом n .

Частным случаем сепарабельных (L, g) -кодов являются коды Сриваставы, описанные в книге Берлекэмпа [96]. Порождающий многочлен этих кодов распадается в минимальном поле, содержащем L . Для кодов Сриваставы справедливы следующие оценки:

$$n \leq q^m - 2t, k \geq n - 2mt, d \geq 2t + 1. \quad (6.6)$$

Хелгерт [180] подробно рассмотрел коды Сриваставы, привел оценки для их параметров k и d и нашел целый ряд двоичных кодов Сриваставы с наилучшими известными параметрами. В другой работе [181] Хелгерт определил два класса линейных кодов, являющихся также (как и коды Гоппы) нециклическими обобщениями кодов БЧХ и кодов Сриваставы и проверочные матрицы которых основаны на модификациях матриц Вандермонда и Коши (т. е. вполне положительных матриц, все миноры которых порядка $\leq v$ положительны).

На основе (L, g) -кодов В. Д. Гоппа [33] построил линейные q -ичные коды с параметрами (сравни с (6.6) и с (5.14)):

$$n = q^m m, k = n - 2mt, d \geq 2t + 1, \quad (6.7)$$

$$n = q^m - 2t + m(2t - 1) + 1, k = n - m(2t - 1) - 1, d \geq 2t + 1. \quad (6.8)$$

Берлекэмп и Морено [106] показали, что расширенные коды Гоппы с расстоянием $d = 6$ являются циклическими кодами. В частности, расширенные $(2^m + 1, 2^m - 2m)$ -коды Гоппы с $d = 6$ изоморфны циклическим кодам с проверочным полиномом $(x + 1)f(x)$, где $f(x)$ — реверсивный (т. е. $f(x) = x^{\deg f(x)} f(x^{-1})$) неприводимый полином периода $2^m + 1$ (реверсивные коды рассматривались в работах [260, 323]).

§ 7. АБЕЛЕВЫ ГРУППОВЫЕ КОДЫ,
КОДЫ РИДА — МАЛЛЕРА И ПОЛИНОМИАЛЬНЫЕ КОДЫ

С. Д. Берман [11, 12] предложил следующее обобщение циклических кодов. Пусть $G = \{g_1, \dots, g_n\}$ — мультипликативная абелева группа порядка n , а $F = GF(q = p^s)$. Множество всех формальных сумм

$$a = a_1 g_1 + \dots + a_n g_n, \quad a_i \in F, \quad (7.1)$$

с очевидными сложением и умножением образует групповую алгебру GF . Любой идеал A алгебры FG назовем абелевым FG -кодом. Введенные таким образом коды являются естественным обобщением циклических кодов, которые можно рассматривать как идеалы групповой алгебры циклической группы. Многие свойства циклических кодов переносятся на абелевы FG -коды, как, например, существование порождающего кодового слова. С. Д. Берман [11, 12] выделил несколько классов таких кодов.

Абелев FG -код A назовем полупростым, если характеристика p поля F не делит порядок n группы G . В этом случае групповую алгебру FG можно представить в виде прямой суммы минимальных идеалов

$$FG = A_1 + \dots + A_m. \quad (7.2)$$

Следующие две теоремы С. Д. Бермана [12] показывают, что в одинаковых условиях абелевы полупростые коды лучше обычных циклических кодов:

Теорема 7.1. Пусть p_1, \dots, p_m — фиксированные простые числа, а $V = \{A\}$ — семейство циклических кодов над $GF(p^s)$, $p \neq p_i$, $i = 1, \dots, m$, каждый из которых имеет длину $n(A) = p_1^{\alpha_1} \dots p_m^{\alpha_m}$. Если для всех кодов $A \in V$ отношение $k(A)/n(A) \geq \beta > 0$, то существует такая константа C , что для каждого кода $A \in V$ расстояние $d(A)$ не превышает C .

Теорема 7.2. Пусть p_1, \dots, p_m — фиксированные простые числа ($p_i \neq 2$, $i = 1, \dots, m$). Существует класс $\{A\}$ двоичных абелевых кодов длины $n(A) = p_1^{\alpha_1} \dots p_m^{\alpha_m}$ такой, что

$$\lim_{(\alpha_1 + \dots + \alpha_m) \rightarrow \infty} k(A)/n(A) = 1$$

и при этом $d(A) \rightarrow \infty$.

Абелев FG -код A назовем p -кодом, если G является p -группой, т. е. группой порядка $n = p^r$. Пусть разложение p -группы G в прямое произведение циклических групп имеет вид: $G = (f_1) \times \dots \times (f_m)$, где (f_i) — циклическая группа порядка p^{α_i} ($i = 1, \dots, m$; $\alpha_1 \geq \dots \geq \alpha_m > 0$). Среди идеалов алгебры FG особую роль играет радикал R алгебры, т. е. максимальный идеал. Базис идеала R над полем F образуют элементы

$$(f_1 - 1)^{t_1} \dots (f_m - 1)^{t_m}, \quad (7.3)$$

где $i_j = 0, 1, \dots, p^{\alpha_j} - 1$ и $(i_1, \dots, i_m) \neq (0, \dots, 0)$. Базис идеала R^ν ($1 \leq \nu \leq p^{\alpha_1} + \dots + p^{\alpha_m} - m$) состоит из всех произведений вида (7.3), где $i_1 + \dots + i_m \geq \nu$.

Радикальными p -кодами назовем p -коды, соответствующие степеням радикала R^ν алгебры FG . С. Д. Берман [11] нашел минимальные расстояния всех радикальных p -кодов. Особенно интересен случай, когда группа G является группой типа (p, \dots, p) . Пусть ν , $1 \leq \nu \leq (p-1)m$, представляется в виде $\nu = (p-1)g + h$, где $0 \leq h < p-1$ и $0 \leq g \leq m$. Тогда идеал R^ν имеет $d = p^g(h+1)$, а число информационных символов k вычисляется по формуле

$$k = \sum_{l=\nu}^{m(p-1)} K(l, m, p), \quad (7.4)$$

где $K(l, m, p)$ — число разбиений l на m слагаемых, каждое из которых меньше p . В случае $p=2$ и $F=GF(2)$ коды R^ν совпадают с известными двоичными кодами Рида—Маллера $(P-M)$ [267, 291] $(m-\nu)$ -го порядка (см. также [51, 96, 273, 276]), имеющими параметры:

$$n = 2^m, \quad k = \sum_{l=\nu}^m C_m^l, \quad d = 2^\nu. \quad (7.5)$$

Коды $P-M$ первого порядка имеют параметры $k = m+1$ и $d = 2^{m-1} = n/2$ и эквивалентны линейным матрицам Адамара порядка $n = 2^m$. Берлекэмп и Слоэн [108, 109] нашли весовые спектры в кодах $P-M$ второго порядка, Касами и Токура [209] нашли выражения для части спектра, заключенного в пределах от d до $2d$, для кодов $P-M$ любого порядка r , а Касами, Токура и Азуми [196, 210] расширили этот результат до $2,5d$. Эти результаты позволили найти весовые спектры во всех кодах $P-M$ длины $n \leq 256$ [196, 314] (см. также ссылки в [210]). В. Д. Колесник и Е. Т. Мирончиков [50, 51] и независимо Касами, Лин и Питерсон [206] установили, что отбрасыванием одного символа и соответствующей перестановкой столбцов все коды $P-M$ приводятся к циклическому виду и нашли порождающие многочлены этих кодов. Аналогичный результат для радикальных кодов, в случае группы G типа (p, \dots, p) получен Г. К. Кладовым [44]. Берлекэмп [98] и Касами [197] нашли весовые спектры некоторых подкодов кодов $P-M$ второго порядка. Работы [99, 110, 111] посвящены нахождению весовых спектров в смежных классах при разложении группы E^n по двоичному коду $P-M$ первого порядка.

Кроме рассмотренного выше обобщения С. Д. Бермана [11] известен целый ряд других возможных обобщений кодов $P-M$ на недвоичный случай [13, 81, 82, 96, 140, 205—207, 262, 263, 327]. Мы рассмотрим только одно еще такое обобщение, введенное Касами, Лином и Питерсоном [205]. Обобщенным кодом

P — M длины $n=q^m$ и порядка r называется код, получаемый расширением циклического кода над $GF(q)$ длины q^m-1 , порождающий многочлен которого задается равенством

$$g(x) = \prod_{\substack{0 \leq j < q^m - 1 \\ 0 \leq \omega(j) < (q-1)m - r}} (x - \alpha^j), \quad (7.6)$$

где $\omega(j)$ — сумма цифр в q -ичном представлении числа j , а α — примитивный элемент поля $GF(q^m)$. Так же как и в обобщении С. Д. Бермана, число k информационных символов в обобщенном коде P — M r -го порядка определяется выражением типа (7.4)

$$k = \sum_{i=0}^r K(i, m, q). \quad (7.7)$$

Пусть теперь $r = (q-1)g + h$, где $0 \leq h < q-1$ и $0 \leq g \leq m$. Тогда обобщенный код P — M длины $n=q^m$ и порядка r является подкодом расширенного примитивного кода БЧХ длины n с конструктивным расстоянием $d_0 = (q-h)q^{m-1-g}$. В случае $q=p$ эти коды совпадают с радикальными p -кодами С. Д. Бермана, когда G — группа типа (p, \dots, p) , а $F = GF(p)$. Во всех других случаях они выигрывают по расстоянию (и проигрывают по простоте декодирования).

В последующей работе [207] Касами, Лин и Питерсон ввели широкий класс циклических кодов: полиномиальные коды, содержащий в качестве подклассов уже известные нам коды БЧХ, обобщенные коды P — M , коды P — C и другие коды. Для понимания идеи построения этих кодов очень кратко опишем представление циклических кодов с помощью полиномов Матсона — Соломона [263]. Пусть: $F = GF(2)$; $FG = F[x]/(x^n + 1)$ — кольцо полиномов над F по модулю $x^n + 1$; α — примитивный корень n -ой степени из 1 в $GF(2^m)$, где $m = \text{ord}_n(2)$. Если $b(x) = \sum_{i=0}^{n-1} b_i x^i$ — любой полином в FG , то полином Матсона — Соломона для $b(x)$ определяется следующим образом: $g_b(z) = \sum_{j=1}^n b(\alpha^j) z^{n-j}$. Это позволяет, кодовый вектор $(b_0, b_1, \dots, b_{n-1})$ представить через $g(z)$ как $(g(\alpha^0), g(\alpha), \dots, g(\alpha^{n-1}))$. Следующее полезное свойство $g(z)$ есть следствие предыдущего: вес $b(x)$ равен $n-r$, где r — степень наибольшего общего делителя $g(z)$ и $z^n + 1$ в кольце полиномов над $GF(2^m)$. В недавней работе Кердок, Мак-Вильямс и Одлышко [212] установили, что для любого полинома Матсона — Соломона $g(z)$ справедливо равенство $zg'(z)(z^n + 1) = g(z)g'(z) + 1$.

В полиномиальных кодах кодовый вектор $a(P)$ также представляется в виде

$$a(P) = (P(\alpha^0), P(\alpha), \dots, P(\alpha^{n-1})), \quad (7.8)$$

где α — примитивный элемент $GF(q^{ms})$, а $P(\alpha^j)$ — полином от m переменных

$$P(\alpha^j) = P(a_{1j}, \dots, a_{mj}) = \sum \beta_{v_1 \dots v_m} \alpha_{1j}^{v_1} \dots \alpha_{mj}^{v_m}, \quad (7.9)$$

где $\alpha^j = a_{1j}\alpha + a_{2j}\alpha^2 + \dots + a_{mj}\alpha^{m-1}$, $a_{ij} \in GF(q^s)$ и $\beta_{v_1 \dots v_m} \in GF(q^s)$; здесь $n = (q^{ms} - 1)/b$, а b — делитель $q^s - 1$. Множество всех векторов над $GF(q)$ вида (7.8), когда показатели v_i в (7.9) удовлетворяют условиям: (1) $0 \leq v_i < q^s$, (2) $v_1 + \dots + v_m = lb$, где $0 \leq l \leq \mu < m(q^s - 1)/b$; образуют циклический (n, m, s, μ, q) -полиномиальный код [207]. Случай $m=1$ и $\mu = n - d_0$ соответствует коду БЧХ длины $(q^s - 1)/b$ и с конструктивным расстоянием d_0 , а случай $s=1$ и $b=1$ соответствует обобщенному коду Р—М длины $q^m - 1$ порядка μ . Двойственными к полиномиальным кодам с $b=q^s - 1$ являются обобщенные проективно-геометрические коды (ПГ-коды), а если $b=1$ и $\mu = \delta(q^s - 1)$, то двойственными являются обобщенные евклидово-геометрические коды (ЕГ-коды). Оба указанных класса конечно геометрических кодов, введенных независимо В. Д. Колесником и Е. Т. Мирончиковым [48, 49], Рудольфом [293] и Велдоном [328, 330] и обобщенных Дельсартом [128], представляют значительный интерес, ввиду простоты их декодирования, и поэтому подверглись интенсивному исследованию [47, 50, 51, 66, 123, 125, 132, 155, 166, 168, 174, 223, 225, 247, 310]. Полиномиальные коды исследовались в работах [52, 127, 130, 200, 224]. В частности, В. Д. Колесник и Е. Т. Мирончиков [52] и одновременно Лин [224] получили выражения для числа информационных символов в полиномиальных кодах, которые в случае ПГ- и ЕГ-кодов значительно упрощаются. Дельсарт [131] показал, что, в свою очередь, полиномиальные коды являются специальным случаем более общего класса линейных кодов, которые инварианты относительно аффинной группы подстановок. Некоторые другие аспекты абелевых кодов рассмотрены в работах [129, 242, 243].

§ 8. КАСКАДНЫЕ КОДЫ И ПРОСТЫЕ СПОСОБЫ КОДИРОВАНИЯ

Идея каскадного кодирования чрезвычайно проста. Если в коде $A(q_2, n_2, d_2, N_2)$ (называемым внутренним кодом), где i -й символ, $i=0, 1, \dots, q_1-1$, заменить i -ым кодовым вектором кода $A(q_2, n_2, d_2, N_2)$ (называемым внутренним кодом), где $N_2 \geq q_1$, то получаемый при этом каскадный код, очевидно, имеет параметры

$$q = q_2, n = n_1 n_2, d \geq d_1 d_2, N = N_1. \quad (8.1)$$

Каскадные коды как некоторая схема кодирования и декодирования с применением двух различных типов кодов были рассмотрены Форни [143]. В. В. Зяблов [42] рассмотрел каскадные коды как линейные коды, порождающая матрица которых является кронекеровским произведением порождающих матриц подкодов. При таком подходе особенно наглядно видна связь итерированных кодов, введенных Элайесом [141] и представленных в виде кронекеровского произведения Слепяном [302], с каскадными кодами. Вулф [333] рассмотрел коды, проверочная матрица которых есть кронекеровское произведение проверочных матриц подкодов. Э. Л. Блох и В. В. Зяблов [14] объединили каскадные и итерированные коды в один класс. Целый ряд работ [10, 27, 65, 75, 119, 142, 150, 151, 160, 227, 233, 236, 272, 290, 304, 309, 313, 332] посвящен кодам, являющимся произведением, суммой или соединением нескольких кодов.

Интерес к каскадным кодам возрос после работ В. В. Зяблова [43] и Юстесена [190]. В. В. Зяблов предложил алгоритм построения каскадных двоичных линейных кодов, у которых отношение d/n при $n \rightarrow \infty$ и заданной скорости $R > 0$ ограничено снизу положительной константой (такие коды называют асимптотически «хорошими»):

$$\frac{d}{n} \geq \max_{R < r < 1} \{(1 - R/r) H^{-1}(1 - r)\}, \quad (8.2)$$

а число элементарных операций, необходимое для задания кода длины n , не превышает Cn^2 . В качестве внешних кодов В. В. Зяблов использовал коды Р—С, а в качестве внутренних кодов—коды, достигающие границы Варшавова—Гилберта (длины $n_2 < \log_2 n$). Все известные алгоритмы построения кодов с линейно растущим расстоянием и с фиксированной скоростью R до работы В. В. Зяблова [43] требовали экспоненциально по n числа операций. Юстесен [190] предложил другой более простой способ выбора внутреннего кода. Пусть: $0 < R < 1/2$; $a = (a_1, \dots, a_{n_1})$ — произвольный вектор (n_1, k_1) -кода Р—С с $d_1 = n_1 - k_1 + 1$ над $GF(q)$, $q = 2^m = n_1 + 1$; α — примитивный элемент в $GF(q)$. Каждому такому вектору a ставится в соответствие вектор $((a_1, \alpha a_1), (a_2, \alpha^2 a_2), \dots, (a_{n_1}, \alpha^{n_1} a_{n_1}))$ и полученный вектор над $GF(q)$ длины $2n_1$ представляется как двоичный вектор длины $n = 2n_1 m$. Множество таких векторов образует код с $R_n = k_1/2n_1 > R$ и с d , линейным по n :

$$\frac{d}{n} \geq (1 - 2R) H^{-1}(1/2) \approx 0,11(1 - 2R). \quad (8.3)$$

Коды в диапазоне скоростей $1/2 \leq R < 1$ получают отбрасыванием последних s позиций в двоичном представлении вектора $(a_i, \alpha^i a_i)$ для всех i . Полученное при этом расстояние d в коде ограничено следующим образом:

$$\frac{d}{n} \geq (1 - R/r) H^{-1}(1 - r), \quad (8.4)$$

где r — корень уравнения $1 + \log_2(1 - H^{-1}(1 - r)) = r^2/R$. Как это видно из (8.2) и (8.3), при скоростях $R < 0,3$ граница Юстесена (как и некоторые ее модификации [315, 330]) ведет себя хуже, чем граница (8.2) В. В. Зяблова. Несколько более точные оценки расстояния в кодах Юстесена имеются в работах Слоэна [303] и Мессе [261].

Интересен следующий факт, полученный при рассмотрении ансамбля случайных каскадных кодов:

Теорема 8.1 (Э. Л. Блох, В. В. Зяблов [15, 18]). Среди двоичных линейных каскадных кодов существуют коды, расстояния которых удовлетворяет границе Варшавова—Гилберта.

В последующих работах Э. Л. Блох и В. В. Зяблов [16, 17] ввели понятие обобщенных каскадных кодов m -го порядка. Эти коды линейны и строятся на основе m внутренних двоичных (n_1, k_1) -кодов с расстояниями d_{1i} , $i=1, \dots, m$, и m внешних q_i -ичных (n_2, k_2) -кодов с расстояниями d_{2i} , $q_i = 2^{k_{1i}}$, $i=1, \dots, m$ (в частности, кодов Р—С). Результирующий код имеет параметры

$$n = n_1 n_2, \quad k = k_1 k_2 + \sum_{i=2}^m (k_{1i} - k_{1(i-1)}) k_{2i}, \quad d \geq \min_i \{d_{1i}, d_{2i}\}. \quad (8.5)$$

Э. Л. Блох и В. В. Зяблов установили [16], что с ростом m параметры обобщенных каскадных кодов m -го порядка улучшаются, но граница Варшавова—Гилберта не достигается. В несколько более общем виде, включающем и нелинейные коды, обобщенные каскадные коды были рассмотрены В. А. Зиновьевым и Г. В. Зайцевым [37].

Берлекэмп и Юстесен [103] показали, что на основе любого двоичного циклического кода, проверочный полином которого неприводим, и соответствующего кода Р—С можно построить двоичный циклический каскадный код. Используя этот результат, авторы построили ряд таких кодов с наилучшими известными параметрами. В частности, используя в качестве внутренних кодов квадратично-вычетные коды простой длины p , такой, что $\text{ord}_p(2) = (p-1)/2$ (известны такие числа p до порядка 10^6), Берлекэмп и Юстесен построили линейные циклические коды до длин $n \sim 10^{10^6}$ со скоростью R и расстоянием

$$d \geq (1 - 2R)n / \sqrt{2 \log_2 n}, \quad (8.6)$$

что лучше, чем в кодах БЧХ (см. п. 5). Касами [199] обобщил результаты [103], показав, что любой циклический код длины $n_1 n_2$ над $GF(q)$, где $(q, n_1) = (q, n_2) = (n_1, n_2) = 1$, можно представить в каскадном виде с внутренним q -ичным циклическим кодом длины n_2 и с соответствующим внешним циклическим кодом длины n_1 .

Ответом на давно поставленный вопрос о возможности «простого» задания асимптотически «хороших» кодов явился отмеченный выше результат В. В. Зяблова [43]. Наряду с «прос-

тым» заданием «хороших» кодов, интересен также вопрос об их «простой» реализации. Еще результат Р. Р. Варшамова [20] о существовании «хорошего» линейного кода можно интерпретировать как «простой» способ реализации «хорошего» кода (так как любой линейный код может быть реализован на схеме из Cn^2 сумматоров по mod 2). С другой стороны, ясно, что при любом способе реализации «хорошего» кода на схемах из сумматоров по mod 2 число сумматоров не может быть меньше C_1n . Замечательный результат С. И. Гельфанда, Р. Л. Добрушина и М. С. Пинскера [146] состоит в том, что некоторые «хорошие» коды могут быть реализованы на схемах из сумматоров по mod 2, число которых не превышает C_2n (точнее, для любого $\varepsilon > 0$ существует код, реализуемый на схеме из $C_2(\varepsilon)n$ сумматоров, и удовлетворяющий границе Варшамова—Гилберта с точностью до ε). Интересно, что при ограничении на класс схем, а именно при переходе к схемам постоянной глубины, верхняя и нижняя оценки числа сумматоров при реализации «хороших» кодов асимптотически также совпадают и имеют порядок $Cn \log_2 n$ (С. И. Гельфанд, Р. Л. Добрушин [30]).

БИБЛИОГРАФИЯ

1. Алексеев В. Е., Марков Ал. А., Комбинаторно-алгебраические проблемы теории кодирования. В сб. «Избр. тр. Всес. межвуз. симпоз. по прикл. мат. и кибернет., Горький, 1967». М., «Наука», 1973, 283—285 (РЖМат, 1973, 6В467)
2. Андрианов В. И., Сасковец В. Н., Дециклические коды. Кибернетика, 1965, № 1, III—16 (РЖМат, 1966, 9В177)
3. Аракелов В. А., Тененгольц Г. М., Некоторые свойства рекуррентных периодических последовательностей. Тр. Вычисл. центра АН Арм.ССР и Ереван. ун-та, 1970, вып. 6, 18—28 (РЖМат, 1971, 4В506)
4. Бассальго Л. А., Новые верхние границы для кодов, исправляющих ошибки. «Пробл. передачи информ.», 1965, 1, № 4, 41—44
5. —, Обобщение теоремы Ллойда на случай произвольного алфавита. Пробл. упр. и теории информ., 1973, 2, № 2, 133—137 (рус.), 25—28 (англ.) (РЖМат, 1974, 7В636)
6. —, Необходимое условие существования совершенных кодов в метрике Лн. Мат. заметки, 1974, 15, № 2, 313—320 (РЖМат, 1974, 7В635)
7. —, Зайцев Г. В., Зиновьев В. А., О равномерно упакованных кодах. Пробл. передачи информ., 1974, 10, № 1, 9—14 (РЖМат, 1974, 7В637)
8. —, Зиновьев В. А., Леонтьев В. К., Совершенные коды над произвольным алфавитом. Третий международный симпозиум по теории информации, тезисы докладов. Москва—Таллин, 1973, часть II, 23—28
9. —, —, Фельдман Н. И., Несуществование совершенных кодов над некоторыми составными алфавитами. Проблемы передачи информации, 1975, 11, № 3, 3—13
10. Белов Б. И., Логачев В. Н., Сандимиров В. П., Построение класса линейных двоичных кодов, достигающих границы Варшамова—Грайсмера. Пробл. передачи информ., 1974, 10, № 3, 36—44 (РЖМат, 1975, 3В619)
11. Берман С. Д. К теории групповых кодов. Кибернетика, 1967, № 1, 31—39 (РЖМат, 1967, 8В254)

- большой длины. Пробл. передачи информ., 1965, 1, № 4, 45—48
56. Левенштейн В. И., О верхних оценках для кодов с фиксированным весом векторов. Пробл. передачи информ., 1971, 7, № 4, 3—12 (РЖМат, 1972, 6B342)
 57. —, О минимальной избыточности двоичных кодов, исправляющих ошибки. Пробл. передачи информ., 1974, 10, № 2, 26—42 (РЖМат, 1974, 11B584)
 58. Леонтьев В. К., Об одном свойстве плотно упакованных кодах. В сб. «Дискретный анализ». Новосибирск, «Наука», 1964, 2, 56—58 (РЖМат, 1964, 9B185)
 59. —, О нижней оценке мощности для почти всех кодов. В сб. «Дискретн. анализ». Новосибирск, «Наука», 1966, 8, 49—54 (РЖМат, 1967, 7B263)
 60. —, Об одной гипотезе о кодах Боуза—Чоудхури. Пробл. передачи информ., 1968, 4, № 1, 83—85 (РЖМат, 1968, 8B320)
 61. —, О спектрах групповых кодов. Второй международный симпозиум по теории информации, 2—8 сентября, 1971 г., Цахкадзор, Армянская ССР, тезисы докладов, Москва—Ереван, 1971, 153—155
 62. —, Спектры групповых кодов. Третий международный симпозиум по теории информации, тезисы докладов, Москва—Таллин, 1973, часть II, 102—106
 63. Мазур Л. Е., Об одном классе полиномиальных кодов. Пробл. передачи информ., 1972, 8, № 4, 99—101 (РЖМат, 1973, 3B475)
 64. —, О минимальном кодовом расстоянии одного класса подкодов кодов Рида—Соломона. Пробл. передачи информ., 1973, 9, № 2, 104—106 (РЖМат, 1973, 9B482)
 65. Марчуков А. С., О суммировании произведений кодов. Пробл. передачи информ., 1968, 4, № 2, 11—20 (РЖМат, 1969, 11B386)
 66. Мирончиков Е. Т., Преснякова Г. В., О циклических кодах. Пробл. передачи информ., 1969, 4, № 2, 19—22
 67. Оганесян С. Ш., Ягджян В. Г., Нахождение циклических представителей в бинарных циклических алфавитах. Тр. Вычисл. центра АН АрмССР и Ереван. ун-та, 1970, 6, 35—38 (РЖМат, 1971, 4B508)
 68. —, Объединение циклических представителей по одинаковым весам в бинарных алфавитах. Тр. Вычисл. центра АН АрмССР и Ереван. ун-та, 1970, 6, 39—48 (РЖМат, 1971, 4B509)
 69. —, Весовой спектр для некоторых классов корректирующих циклических кодов. Пробл. передачи информ., 1970, 6, № 3, 31—37 (РЖМат, 1971, 3B374)
 70. —, Класс оптимальных циклических кодов с основанием p . Пробл. передачи информ., 1972, 8, № 2, 109—111 (РЖМат, 1972, 10B466)
 71. —, Таирян В. И., Ягджян В. Г., Разбиение циклических кодов на равновесные классы. Пробл. упр. и теории информ., (венг.) 1974, 3, № 2, 117—125 (рус.), 13—21 (англ.) (РЖМат, 1975, 3B621)
 72. Семаков Н. В., Зиновьев В. А., Эквидистантные q -ичные коды с максимальным расстоянием и разрешимые уравновешенные неполные блок-схемы. Пробл. передачи информ., 1968, 4, № 2, 3—10 (РЖМат, 1969, 11B380)
 73. —, —, Совершенные и квазисовершенные равновесные коды. Пробл. передачи информ., 1969, 5, № 2, 14—18 (РЖМат, 1969, 10B265)
 74. —, —, Равновесные коды и тактические конфигурации. Пробл. передачи информ., 1969, 5, № 3, 28—36 (РЖМат, 1970, 2B451)
 75. —, —, Зайцев Г. В., Класс максимальных эквидистантных кодов. Пробл. передачи информ., 1969, 5, № 2, 84—87 (РЖМат, 1969, 11B383)
 76. —, —, —, О взаимосвязи кодов Хэмминга, Препарата и Голя и о расширениях кодов Хэмминга. Второй международный симпозиум по теории информации, 2—8 сентября, 1971, Цахкадзор, Армянская ССР, тезисы докладов. Москва—Ереван, 1971, 227—230
 77. —, —, —, Равномерно упакованные коды. Пробл. передачи информ., 1971, 7, № 1, 38—50 (РЖМат, 1971, 9B445)

78. Сидельников В. М., О спектре весов двоичных кодов Боуза—Чоудхури—Хоквингема. Пробл. передачи информ., 1971, 7, № 1, 14—22 (РЖМат, 1971, 9В447)
79. —, О взаимной корреляции последовательностей. В сб. «Пробл. кибернетики», М., «Наука», 1971, вып. 24, 15—42 (РЖМат, 1972, 6В344)
80. —, Верхние оценки числа точек двоичного кода с заданным кодовым расстоянием. Пробл. передачи информ., 1974, 10, № 2, 43—51 (РЖМат, 1974, 11В585)
81. Соколов О. Б., Енижеев И. И., Обобщение кодов Рида—Маллера. Уч. зап. Казанск. университета, 1974, 124, № 2, 112—129
82. —, —, Представление кодов Рида—Маллера в характеристическом виде. Уч. зап. Казанск. университета, 1969, 127, № 3, 62—73
83. Таирян В. И., Хачатрян Г. Г., К определению H -орбит циклических FG -кодов произвольной длины. Докл. АН Арм.ССР, 1974, 58, № 3, 139—144 (РЖМат, 1975, 3А336)
84. Тененгольц Г. М. Новый класс циклических корректирующих кодов: Сб. «Третья конференция по теории передачи и кодирования информации», М., «Наука», 1967, секция 1, 18—28
85. Allard P. E., Shiva S. G. S., Tavares S. E., A note on the decomposition of cyclic codes into cyclic classes. Inform. and Contr., 1973, 22, № 1, 100—106 (РЖМат, 1973, 6В463)
86. Anderson D. R., A new class of cyclic codes. SIAM J. Appl. Math., 1968, 16, 181—197
87. Assmus E. F., Jr., Mattson H. F., Jr., Perfect codes and the Mathieu groups. Arch. Math., 1966, 17, № 2, 121—135 (РЖМат, 1968, 1А213)
88. —, —, On tactical configurations and error-correcting codes. J. Combin. Theory, 1967, 2, № 3, 243—257 (РЖМат, 1968, 5В287)
89. —, —, New 5-designs. J. Combin. Theory, 1969, 6, № 2, 122—151 (РЖМат, 1970, 1В277)
90. —, —, On weights in quadratic-residue codes. Discrete Math., 1972, 3, № 1-3, 1—20 (РЖМат, 1973, 4А466)
91. —, —, Constructions of self-orthogonal codes. Discrete Math., 1972, 3, № 1-3, 21—32 (РЖМат, 1973, 3А347)
92. —, —, Coding and combinatorics. SIAM Rev., 1974, 16, № 3, 349—388 (РЖМат, 1975, 5В442)
93. Baumert L. D., McEliece R. J., Weights of irreducible cyclic codes. Inform. and Contr., 1972, 20, № 2, 158—175 (РЖМат, 1972, 8А490)
94. Berger E. R., Some additional upper bounds for fixed-weight codes of specified minimum distance. IEEE Trans. Inform. Theory, 1967, 13, № 2, 307—308 (РЖМат, 1968, 2В330)
95. Berlekamp E. R., The enumeration of information symbols in BCH codes. Bell Syst. Techn. J., 1967, 46, № 8, 1861—1880 (РЖМат, 1968, 7В340)
96. —, Algebraic coding Theory. New York—San, McGraw—Hill, Book Co., 1968, (Русский перевод: Берлекэмп Э. Алгебраическая теория кодирования. М., «Мир», 1971) (РЖМат, 1969, 12В390)
97. —, Factoring polynomials over large finite fields. Math. Comput., 1970, 24, № 111, 713—735 (РЖМат, 1971, 12А422)
98. —, The weight enumerators for certain subcodes of the second order binary Reed—Muller codes. Inform. and Contr., 1970, 17, № 5, 485—500 (РЖМат, 1973, 5В583)
99. —, Some mathematical properties of a scheme for reducing the bandwidth of motion pictures by Hadamard smearing. Bell. Syst. Techn. J. 1970, 49, № 6, 969—986 (РЖМат, 1971, 5В478)
100. —, Coding theory and the Mathieu groups. Inform. and Contr., 1971, 18, № 1, 40—64 (РЖМат, 1972, 3А185)
101. —, Long primitive binary BCH codes have distance $d \sim 2n \ln R^{-1} / \log n$. IEEE Trans. Inform. Theory, 1972, 18, № 3, 415—426
102. —, Goppa codes. IEEE Trans. Inform. Theory, 1973, 19, № 5, 590—592 (РЖМат, 1974, 5В531)

103. —, Justesen J., Some long cyclic linear binary codes are not so bad. *IEEE Trans. Inform. Theory*, 1974, 20, № 3, 351—356 (ПЖМат, 1975, 1B685)
104. —, Lint J. H. van, Seidel J. J., A strongly regular graph derived from the perfect ternary Golay code. *Surv. Combin. Theory*, Amsterdam e. a., 1973, 25—30 (ПЖМат, 1974, 4B298)
105. —, MacWilliams F. J., Sloane N. J. A., Gleason's theorem on self-dual codes. *IEEE Trans. Inform. Theory*, 1972, 18, № 3, 409—414 (ПЖМат, 1972, 10B456)
106. —, Moreno O., Extended double-error-correcting binary Goppa codes are cyclic. *IEEE Trans. Inform. Theory*, 1973, 19, № 6, 817—818 (ПЖМат, 1974, 6B588)
107. —, Rumsey H., Solomon G., On the solution of algebraic equations over finite fields. *Inform. and Contr.*, 1967, 10, № 6, 553—564 (ПЖМат, 1968, 6B363)
108. —, Sloane N. J. A., Restrictions on weight distribution of Reed—Muller codes. *Inform. and Contr.*, 1969, 14, № 5, 442—456 (ПЖМат, 1970, 1B355)
109. —, —, Weight enumerator for second order Reed—Muller codes. *IEEE Trans. Inform. Theory*, 1970, 16, № 6, 745—751
110. —, Welch L. R., Weight distributions of the (32,6) Reed—Muller code. *IEEE Trans. Inform. Theory*, 1972, 18, № 1, 203—207 (ПЖМат, 1972, 7B447)
111. Bose R. C., On some connections between the design of experiments and information theory. *Bull. Internat. Statist. Inst.*, 1961, 38, 257—271
112. —, Bush K. A., Orthogonal arrays of strength two and three. *Ann. Math. Stat.*, 1952, 23, 508—524
113. —, Ray-Chaudhuri D. K., On a class of error correcting binary group codes. *Inform. and Contr.*, 1960, 3, № 1, 68—79. (Русский перевод; Боуз Р. К., Рой—Чоудхури Д. К. Об одном классе двоичных групповых кодов с исправлением ошибок. *Кибернетический сборник*, вып. 2, ИЛ, М., 1961, 83—94)
114. —, —, Further results on error correcting binary group codes. *Inform. and Contr.*, 1960, 3, № 3, 279—290. (Русский перевод; Боуз Р. К., Рой—Чоудхури Д. К. Дальнейшие результаты относительно двоичных групповых кодов с исправлением ошибок. *Кибернетический сборник*, вып. 6, М., ИЛ., 1963, 7—12)
115. —, Shrikhande S. S., A note on a result in the theory of code construction. *Inform. and Control*, 1959, 2, N 2, 183—194
116. Brillhart J., Selfridge J. L., Some factorizations of $2^n \pm 1$ and related results. *Math. Computation*, 1967, 21, № 97, 87—96 (ПЖМат, 1968, 1A173)
117. —, —, Zierler N. On irreducible trinomials modulo 2. I, *Inform. and Control*, 1968, 13, 541—544 II, *ibid*, 1969, 14, 566—569
118. Broué M., Enguehard H., Polynômes des poids de certains codes et fonctions theta de certains reseaux. *Ann. sci. Ecole norm. supér.*, 1972, 5, № 1, 157—181 (ПЖМат, 1972, 10B455)
119. Burton H. O., Weldon E. J., Jr., Cyclic product codes. *IEEE Trans. Inform. Theory*, 1965, 11, № 3, 433—439 (ПЖМат, 1967, 12B329)
120. Bush K. A., Orthogonal arrays of index unity. *Ann. Math. Stat.*, 1952, 23, 426—434
121. Cerveria A. G., On a class of wide-sense binary BCH codes whose minimum distance exceed the BCH bound. *IEEE Trans. Inform. Theory*, 1968, 14, № 5, 784—785 (ПЖМат, 1969, 12B397)
122. Chen C. L., Computer results on the minimum distance of some binary cyclic codes. *IEEE Trans. Inform. Theory*, 1970, 16, № 3, 359—360 (ПЖМат, 1970, 12B429)
123. —, On majority-logic decoding of finite geometry codes. *IEEE Trans. Inform. Theory*, 1971, 17, № 3, 332—336 (ПЖМат, 1971, 12B746)
124. —, The existence of arbitrarily long pseudo-cyclic codes that meet the

- Gilbert bound. Proc. 5-th. Annu. Princeton Conf. Inform. Sci. and Syst., 1971, 242 (РЖМат, 1973, 8B436)
125. —, Note on majority-logic decoding of finite geometry codes. IEEE Trans. Inform. Theory, 1972, 18, № 4, 539—541 (РЖМат, 1972, 12B299)
 126. —, Peterson W. W., Weldon E. J., Jr., Some results on quasi-cyclic codes. Inform. and Contr., 1969, 15, № 5, 407—423 (РЖМат, 1970, 7B382)
 127. —, Lin S., Further results on polynomials codes. Inform. and Contr., 1969, 15, № 1, 38—60 (РЖМат, 1970, 5B393)
 128. Delsarte P., A geometric approach to a class of cyclic codes. J. Combin. Theory, 1969, 6, № 4, 340—358 (РЖМат, 1969, 11B374)
 129. —, Automorphisms of abelian codes. Philips Res. Repts, 1970, 25, № 5, 389—402 (РЖМат, 1971, 9A216)
 130. —, BCH bounds for a class of cyclic codes. SIAM J. Appl. Math., 1970, 19, № 2, 420—429 (РЖМат, 1971, 3B372)
 131. —, On cyclic codes that are invariant under the general linear group. IEEE Trans. Inform. Theory, 1970, 16, № 6, 760—769 (РЖМат, 1971, 7B582)
 132. —, Majority logic decodable codes derived from finite inversive planes. Inform. and Contr., 1971, 18, № 4, 319—325 (РЖМат, 1972, 2B481)
 133. —, Bounds for unrestricted codes, by linear programming. Philips Res. Repts, 1972, 27, 272—289
 134. —, Weights of linear codes and strongly regular normed spaces. Discrete Math., 1972, 3, № 1-3, 47—64 (РЖМат, 1973, 2B412)
 135. —, Four fundamental parameters of a code and their combinatorial significance. Inform. and Control., 1973, 23, № 5, 407—438
 136. —, An algebraic approach to the association schemes of coding theory. Philips Res. Repts Suppl., 1973, № 10, 97 pp. (РЖМат, 1974, 9B566)
 137. —, The association schemes of coding theory. Math. Centre Tracts, 1974, № 55, 139—157 (РЖМат, 1975, 3B617)
 138. —, Goethals J. M., Irreducible binary cyclic codes of even dimension. Univ. North Carolina at Chapel Hill, Inst. Statist., Mimeo Ser. № 600.27, 1970
 139. —, —, Unrestricted codes with the Golay parameters are unique. Discrete Math., 1975, 12, № 3, 211—224
 140. —, —, MacWilliams F. J., On generalized Reed—Muller codes and their relatives. «Inform. and Contr.», 1970, 16, № 5, 403—442 (РЖМат, 1971, 2B383)
 141. Elias P., Error-free coding. «IEEE Trans. Inform. Theory», 1954, 4, № 1, 29—37 (Русский перевод: Элайс П. Безошибочное кодирование. Сб. «Коды с обнаружением и исправлением ошибок». М., ИЛ, 1956, 59—71)
 142. Feit W., A self-dual even (96, 48, 16) code. IEEE Trans. Inform. Theory, 1974, 20, № 1, 136—138 (РЖМат, 1974, 9B577)
 143. Forney G. D., Jr., Concatenated codes. Cambridge, M. I. T. Press, 1966, 147 pp. (Русский перевод: Форни Д. Каскадные коды. М., «Мир», 1970) (РЖМат, 1968, 9B302 K)
 144. Freiman C. V., Upper bounds for fixed-weight codes of specified minimum distance. IEEE Trans. Inform. Theory, 1964, 10, № 3, 246—248
 145. Gallager R. G., Low-density paritycheck codes. Cambridge, M. I. T. Press, 1963. (Русский перевод: Галлагер Р. Дж. Коды с малой плотностью проверок на четность. М., «Мир», 1966)
 146. Gelfand S. I., Dobrushin R. L., Pinsker M. S., On the complexity of coding. 2nd Intern. Symp. Inform. Theory, Tsahkadsor, 1971, Budapest, 1973, 177—184 (РЖМат, 1974, 7B626)
 147. Gilbert E. N., A comparison of signalling alphabets. Bell System Tech. J., 1952, 31, 504—522
 148. Gleason A. M., Weight polynomials of self-dual codes and the MacWilliams identities. Actes Congr. int. mathématiciens, 1970, T. 3, Paris, 1971, 211—215 (РЖМат, 1972, 3B369)

149. Goethals J. M., Analysis of weight distribution in binary cyclic codes. IEEE Trans. Inform. Theory, 1966, 12, № 3, 401—402 (РЖМат., 1967, 4B250)
150. —, Factorization of cyclic codes. IEEE Trans. Inform. Theory, 1967, 13, № 2, 242—246 (РЖМат, 1968, 4B317)
151. —, Cyclic error-locating codes. Inform. and Control, 1967, 10, № 4, 378—385 (Русский перевод: Гёталс Дж. М. Циклические коды с локализацией ошибок. Сб. «Некоторые вопросы теории кодирования». М., «Мир», 1970, 91—100)
152. —, On the Golay perfect binary code. J. Combin. Theory, 1971, A11, № 2, 178—186 (РЖМат, 1972, 7B277)
153. —, Some combinatorial aspects of coding theory. Surv. Combin. Theoru, Amsterdam e. a., 1973, 189—208 (РЖМат, 1974, 5B372)
154. —, Two dual families of nonlinear binary codes. Electronics letters, 1974, 10, № 23, 471—472
155. —, Delsarte Ph., On a class of majority-logic decodable cyclic codes. IEEE Trans. Inform. Theory, 1968, 14, № 2, 182—188. (Русский перевод: Гёталс (Дж. М., Дельсарт П. Один класс циклических кодов с мажоритарным декодированием. Кибернетический сборник, новая серия, вып. 6, М., «Мир», 1969) (РЖМат, 1969, 5B373)
156. —, Snover S. L., Nearly perfect binary codes. Discrete Math., 1972, 3, № 1-3, 65—88 (РЖМат, 1973, 2B413)
157. Golay M. E., Notes on digital coding. Proc. IRE, 1949, 37, 657
158. —, Binary coding. Trans. I. R. E., 1954, PGIT-4, 23—28
159. —, Notes on the penny-weighting problem, lossless symbol coding with nonprimes. IEEE Trans. Inform. Theory, 1958, 4, № 3, 103—109 (РЖМат, 1960, 7959)
160. Goldberg M., Augmentation techniques for a class of product codes. IEEE Trans. Inform. Theory, 1973, 19, № 5, 566—672 (РЖМат, 1974, 5B533)
161. Goldman H. D., Kliman M., Smola H., The weight structure of some Bose—Chaudhuri codes. IEEE Trans. Inform. Theory, 1968, 14, № 1, 167—169
162. Goldstein R. M., Zierler N., On trinomial recurrences. IEEE Trans. Inform. Theory, 1968, 14, № 1, 150—151 (РЖМат, 1968, 12B348)
163. Golomb S. W., Posner E. C., Rook domains, latin squares, affine planes and error-distributing codes. IEEE Trans. Inform. Theory, 1964, 10, № 3, 196—208 (РЖМат, 1965, 5A122)
164. Gorenstein D. C., Peterson W. W., Zierler N., Two-error correcting Bose—Chaudhuri codes are quasi-perfect. Inform. and Control, 1960, 3, 291—294. (Русский перевод: Горенстейн Д. Питерсон В., Цирлер Н. Квазисовершенство кодов Боуза—Чоудхури с исправлением двух ошибок, «Кибернетический сборник», вып. 6, М., ИЛ, 1963, 20—24)
165. —, Zierler N. A class of error-correcting codes in p^m symbols. J. Soc. Indus. Appl. Math., 1961, 9, 207—214. (Русский перевод: Горенстейн Д., Цирлер Н. Класс кодов из p^m символов с исправлением ошибок, «Кибернетический сборник», вып. 7, М., ИЛ, 1963, 80—89)
166. Graham R. L., MacWilliams J., On the number of information symbols in difference-set cyclic codes. Bell Syst. Techn. J., 1966, 45, № 7, 1057—1070. (Русский перевод: Грехем Р. Л., Мак—Вильямс Дж., О числе информационных символов циклических кодов, задаваемых разностными множествами. Сб. «Некоторые вопросы теории кодирования». М., «Мир», 1970, 22—35)
167. Gulati V. R., Kounias E. G., On three level symmetrical factorial designs and ternary group codes. Sankhya. Indian J. Statist., 1973, A35, № 3, 377—392 (РЖМат, 1975, 5B660)
168. Hamada N., On the p -rank of the incidence matrix of a balanced or partially balanced incomplete block design and its applications to error correcting codes. Hiroshima Math. J., 1973, 3, № 1, 153—226. (РЖМат, 1974, 2B440)

169. **Hamming R. W.**, Error-detecting and error-correcting codes. Bell. Syst. Techn. J., 1950, 29, № 2, 147—160. (Русский перевод: Хэмминг Р. Коды с обнаружением и исправлением ошибок. Сб. «Коды с обнаружением и исправлением ошибок». М., ИЛ, 1956, 7—22)
170. **Hartmann C. R. P.**, On the weight structure of cyclic codes of composite length. Proc. Fourth Haw. Int. Conf. Syst. Sci., 1971, 117—119 (РЖМат, 1972, 2В472)
171. —, A note on the minimum-distance structure of cyclic codes. IEEE Trans. Inform. Theory, 1972, 18, № 3, 439—440 (РЖМат, 1972, 10В463)
172. —, Decoding beyond the BCH bound. IEEE Trans. Inform. Theory, 1972, 18, № 3, 441—444 (РЖМат, 1972, 10В450)
173. —, Theorems on the minimum distance structure of binary cyclic codes. 2nd Intern. Symp. Inform Theory, Tsahkadsor, 1971, Budapest, 1973, 185—190 (РЖМат, 1974, 7В639)
174. —, **Ducey J. B.**, **Rudolph L. D.**, On the structure of generalized finite-geometry codes. IEEE Trans. Inform. Theory, 1974, 20, № 2, 240—252 (РЖМат, 1974, 11В588)
175. —, **Tzeng K. K.**, A bound for cyclic codes of composite length. IEEE Trans. Inform. Theory, 1972, 18, № 2, 307 (РЖМат, 1972, 11В372)
176. —, —, Generalization of the BCH bound. Inform. and Contr., 1972, 20, 489—498 (РЖМат, 1973, 2В422)
177. —, —, On some classes of cyclic codes of composite length. IEEE Trans. Inform. Theory, 1973, 19, № 6, 820—825 (РЖМат, 1974, 6В590)
178. —, —, Decoding beyond the BCH bound using multiple sets of syndrome sequences. IEEE Trans. Inform. Theory, 1974, 20, № 2, 292—295 (РЖМат, 1974, 11В586)
179. —, —, **Chien R. T.**, Some results on the minimum distance structure of cyclic codes. IEEE Trans. Inform. Theory, 1972, 18, № 3, 402—409 (РЖМат, 1972, 10В462)
180. **Helgert H. J.**, **Srivastava** codes. IEEE Trans. Inform. Theory, 1972, 18, № 2, 292—297 (РЖМат, 1972, 8А488)
181. —, Noncyclic generalizations of BCH and **Srivastava** codes. Inform. and Contr., 1972, 21, № 3, 280—290 (РЖМат, 1973, 4В476)
182. —, **Stinaff R. D.**, Minimum-distance bounds for binary linear codes. IEEE Trans. Inform. Theory, 1973, 19, № 3, 344—356 (РЖМат, 1973, 11В571)
183. —, —, Shortened BCH codes. IEEE Trans. Inform. Theory, 1973, 19, № 6, 818—820 (РЖМат, 1974, 6В589)
184. **Hocquenghem A.**, Codes correcteurs d'erreurs. Chiffres, 1959, 2, 147—156
185. **Hoffner C. W.**, **Reddy S. M.**, Circulant bases for cyclic codes. IEEE Trans. Inform. Theory, 1970, 16, 511—512 (РЖМат, 1971, 2В450)
186. **Johnson S. M.**, A new upper bound for error-correcting codes. IRE Trans. Inform. Theory, 1962, 8, № 3, 203—207. (Русский перевод: Джонсон С. М. Новая верхняя граница для кодов, исправляющих ошибки. Сб. «Теория кодирования». М., «Мир», 1964, 208—224) (РЖМат, 1964, 9В186)
187. —, Improved asymptotic bounds for error-correcting codes. IEEE Trans. Inform. Theory, 1963, 9, № 3, 198—205 (РЖМат, 1965, 2В379)
188. —, On upper bounds for unrestricted binary error-correcting codes. IEEE Trans. Inform. Theory, 1971, 17, № 4, 466—478 (РЖМат, 1972, 1В711)
189. —, Upper bounds for constant weight error-correcting codes. Discrete Math., 1972, 3, № 1-3, 109—124 (РЖМат, 1973, 2В411)
190. **Justesen J.** A class of constructive, asymptotically good algebraic codes. IEEE Trans. Inform. Theory, 1972, 18, № 5, 652—656. (Русский перевод: Юстесен И., Класс конструктивных асимптотически хороших алгебраических кодов. «Кибернетический сборник, новая серия», вып. 10. М., «Мир», 1973, 39—50) (РЖМат, 1973, 2В421)
191. **Karlin M.**, New binary coding results by circulants. IEEE Trans. Inform. Theory, 1969, 15, № 1, 81—92 (РЖМат, 1970, 1В356)

192. —, MacWilliams F. J., On finding low weight vectors in quadratic residue codes for $p=8m-1$. SIAM J. Appl. Math., 1973, 25, № 1, 95—104 (РЖМат, 1974, 1B442)
193. Kasami T., Weight distribution of BCH codes, chap. 20 in R. C. Bose and T. A. Dowling (eds). Proceeding of the Conference on Combinatorial Mathematics and Its Applications (April 10—14, 1967), The University of North Carolina Press, Chapel Hill, N. C., 1968, 335—357
194. —, Some lower bounds on the minimum weight of cyclic codes of composite length. IEEE Trans. Inform Theory, 1968, 14, № 6, 814—818 (РЖМат, 1969, 11B377)
195. —, An upper bound on k/n for affine-invariant codes with fixed d/n . IEEE Trans. Inform Theory, 1969, 15, № 1, 174—176. (Русский перевод: Касами Т. Верхняя граница для k/n аффинно инвариантных кодов с фиксированным d/n . Кибернетический сборник, новая серия, вып. 8. М., «Мир», 1971, 5—11) (РЖМат, 1970, 2B445)
196. —, Some results on the weight structure of Reed—Muller codes. The Second International Symposium on Information Theory, September 2—8, 1971, Tsahkadsor, Armenian SSR, Abstracts of papers, Moscow—Eri-van, 1971, 351—353
197. —, The weight enumerators for several classes of subcodes of the second order binary Reed—Muller codes. Inform. and Contr., 1971, 18, № 4, 369—394 (РЖМат, 1972, 2B468)
198. —, A Gilbert—Varshamov bound for quasi-cyclic codes of rate $1/2$. IEEE Trans. Inform. Theory, 1974, 20, № 5, 679 (РЖМат, 1975, 4B565)
199. —, Construction and decomposition of cyclic codes of composite length. IEEE Trans. Inform. Theory, 1974, 20, № 5, 680—683 (РЖМат, 1975, 5B658)
200. —, Lin S., On majority-logic decoding for duals of primitive polynomial codes. IEEE Trans. Inform. Theory, 1971, 17, № 3, 322—331 (РЖМат, 1972, 1B724)
201. —, —, Some results on the minimum weight of primitive BCH codes. IEEE Trans. Inform. Theory, 1972, 18, № 6, 824—825 (РЖМат, 1973, 3B472)
202. —, —, Peterson W. W., Some results on weight distributions of BCH codes. IEEE Trans. Inform. Theory, 1966, 12, № 2, 274
203. —, —, —, Some results on cyclic codes which are invariant under the affine group and their applications. Inform. and Contr., 1967(1968), 11, № 5-6, 475—496 (РЖМат, 1969, 1B340)
204. —, —, —, Linear codes which are invariant under the affine group and some results on minimum weights in BCH codes. Electronics and Communications in Japan, 1967, 50, № 9, 100—106
205. —, —, —, New generalizations of the Reed—Muller codes. Part I. Primitive codes. IEEE Trans. Inform. Theory, 1968, 14, № 2, 189—199 (РЖМат, 1968, 11B358)
206. —, —, —, Generalized Reed—Muller codes. Electronics and Communications in Japan, 1968, 51—C, № 3, 96—104
207. —, —, —, Polynomial codes. IEEE Trans. Inform. Theory, 1968, 14, № 6, 807—814 (РЖМат, 1969, 8B257)
208. —, Tokura N., Some remarks on BCH bounds and minimum weights of binary primitive BCH codes. IEEE Trans. Inform. Theory, 1969, 15, № 3, 408—413 (РЖМат, 1970, 2B446)
209. —, —, On the weight structure of Reed—Muller codes. IEEE Trans. Inform. Theory, 1970, 16, № 6, 752—759 (РЖМат, 1971, 7B576)
210. —, —, Azumi S., Weight enumerator formulas of Reed—Muller codes for $2d \leq \omega < 2.5d$. The Third International Symposium on Information Theory, Tallinn, USSR (June 18—23, 1973), Part II, 217—219
211. Kerdock A. M., A class of low-rate nonlinear binary codes. Inform. and Contr., 1972, 20, № 2, 182—187. (Русский перевод: Кердок А. М. Класс нелинейных двоичных кодов с низкой скоростью передачи. Ки-

- бернетический сборник, новая серия, вып. 10. М., «Мир», 1973, 33—38) (ПЖМат, 1972, 8В491)
212. —, MacWilliams F. J., Odlyzko A. M., A new theorem about the Mattson—Solomon polynomial and some applications. IEEE Trans. Inform. Theory, 1974, 20, № 1, 85—89 (ПЖМат, 1974, 9В570)
 213. Кнее D., Goldman H. D., Quasi-self-reciprocal polynomials and potentially large minimum distance BCH codes. IEEE Trans. Inform. Theory, 1969, 15, № 1, 118—121 (ПЖМат, 1970, 3В382)
 214. Kurshan R. P., Sloane N. J. A., Coset analysis of Reed—Muller codes via translates of finite vector spaces. Inform. and Contr., 1972, 20, № 5, 410—414 (ПЖМат, 1973, 1В650)
 215. Leech J., Some sphere packings in higher space. Can. J. Math., 1964, 16, № 4, 657—682 (ПЖМат, 1965, 7А433)
 216. —, Notes on sphere packings. Can. J. Math., 1967, 19, № 2, 251—267 (ПЖМат, 1969, 2А652)
 217. —, Sloane N. J. A., New sphere packings in dimensions 9—15. Bull. Amer. Math. Soc., 1970, 76, № 5, 1006—1010 (ПЖМат, 1971, 4А648)
 218. —, Sphere packing and error-correcting codes. Can. J. Math., 1971, 23, № 4, 718—745 (ПЖМат, 1972, 4В307)
 219. Lempel A., Analysis and synthesis of polynomials and sequences over $GF(2)$. IEEE Trans. Inform. Theory, 1971, 17, № 3, 297—303 (ПЖМат, 1972, 1В721)
 220. Lenstra H. W., Jr. Two theorems on perfect codes. Discrete Math., 1972, 3, № 1-3, 125—132 (ПЖМат, 1973, 2В415)
 221. Levi J. E., A weight distribution bound for linear codes. IEEE Trans. Inform. Theory, 1968, 14, № 3, 487—490
 222. Lin S., Some codes which are invariant under a transitive permutation and their connection with balanced incomplete group block design. chap. 24 in R. C. Bose and T. A. Dowling (eds.) Proceedings of the Conference on Combinatorial Mathematics and Its Applications (April 10—14, 1967), The University of North Carolina Press, Chapel Hill, N. C., 1968
 223. —, Shortened finite geometry codes. IEEE Trans. Inform. Theory, 1972, 18, № 5, 692—696 (ПЖМат, 1973, 3В481)
 224. —, On the number of information symbols in polynomial codes. IEEE Trans. Inform. Theory, 1972, 18, № 6, 785—794 (ПЖМат, 1973, 4В474)
 225. —, Multifold Euclidean geometry codes. IEEE Trans. Inform. Theory, 1973, 19, № 4, 537—548 (ПЖМат, 1974, 1В440)
 226. —, Weldon E. I., Jr., Long BCH codes are bad. Inform. and Control, 1967, 11, № 4, 445—451 (ПЖМат, 1968, 11В360)
 227. —, Further results on cyclic product codes. IEEE Trans. Inform. Theory, 1970, 16, № 4, 452—459 (ПЖМат, 1971, 2В382)
 228. Lindström B., On group and nongroup perfect codes in q symbols. Math. Scand., 1969, 25, 149—158
 229. Lint J. H. van., On the nonexistence of perfect 2- and 3-Hamming-error-correcting codes over $GF(q)$. Inform. and Contr., 1970, 16, № 4, 396—401 (ПЖМат, 1970, 11В350)
 230. —, On the nonexistence of perfect 5-, 6- and 7-Hamming-error-correcting codes over $GF(q)$. Techn. hogesch. Eindhoven. Onderafdel. wisk. Rept., 1970, № 6, 1—5 (ПЖМат, 1972, 10В446)
 231. —, Nonexistence theorems for perfect error-correcting codes. Comput. Algebra and Number Theory, (SIAM—AMS Proc., vol. 4), Providence, R. I., 1971, 89—95 (ПЖМат, 1972, 10В445)
 232. —, Coding Theory. Lect. Notes Math., 1971, 201, VIII, 136 pp. (ПЖМат, 1971, 11В643)
 233. —, A new description of the Nadler code. IEEE Trans. Inform. Theory, 1972, 18, № 6, 825—827 (ПЖМат, 1973, 4В475)
 234. —, Recent results on perfect codes and related topics. Math. Centre Tracts, 1974, № 55, 158—178 (ПЖМат, 1975, 4В566)

235. —, A theorem on equidistant codes. *Discrete Math.*, 1973, 6, № 4, 353—358
236. Liu C. L., Ong B. G., Ruth G. R., A construction scheme for linear and nonlinear codes. *Discrete Math.*, 1973, 4, № 2, 171—184 (РЖМат, 1973, 8B433)
237. Lloyd S. P., Binary block coding. *Bell Syst. Techn. J.*, 1957, 36, № 2, 517—535. (Русский перевод: Ллойд С. П. Бинарное блочное кодирование. Кибернетический сборник, вып. 1. М., ИЛ, 1960, 206—226.)
238. Lum V., Comments on «The weight structure of some Bose—Chaudhuri codes». *IEEE Trans. Inform. Theory*, 1969, 15, № 5, 618—619 (РЖМат, 1970, 8B318)
239. —, Chien R. T., On the minimum distance of Bose—Chaudhuri—Hocquenghen codes. *SIAM*, 1968, 16, 1325—1337
240. MacWilliams F. J., A theorem on the distribution of weights in a systematic code. *Bell Syst. Techn. J.*, 1963, 42, № 1, 79—94
241. —, The structure and properties of binary cyclic alphabets. *Bell Syst. Techn. J.*, 1965, 44, № 2, 303—332. (Русский перевод: Мак-Вильямс Дж., Структура и свойства бинарных циклических алфавитов. Кибернетический сборник, новая серия, вып. 4. М., «Мир», 1967)
242. —, Codes and ideals in group algebras. Chap. 18 in R. C. Bose and T. A. Dowling (eds), *Proceedings of the Conferen. on Combin. Math. and its Applications* (april 10—14, 1967), The University of North Carolina Press, Chapel Hill, N. C.
243. —, Binary codes which are ideals in the group algebra of an Abelian group. *Bell Syst. Techn. J.*, 1970, 49, № 6, 987—1011 (РЖМат, 1971, 3B370)
244. —, On binary cyclic codes which are also cyclic codes over $CF(2^n)$. *SIAM J. Appl. Math.*, 1970, 19, № 1, 75—95 (РЖМат, 1971, 3B371)
245. —, Cyclotomic numbers, coding theory and orthogonal polynomials. *Discrete Math.*, 1972, 3, № 1-3, 133—151 (РЖМат, 1973, 2B416)
246. —, Orthogonal circulant matrices over finite fields. *J. Combin. Theory.*, 1971, A10, № 1, 1—17 (РЖМат, 1974, 11B475)
247. —, Mallows C. L., Sloane N. J. A. Generalizations of Gleason's theorem on weight enumerators of self-dual codes. «*IEEE Trans. Inform. Theory*», 1972, 18, № 6, 794—805
248. —, Mann H. B., On the p-rank of the design matrix of difference set. *Inform. and Control*, 1968, 12, № 5-6, 474—488 (РЖМат, 1969, 5B375)
249. —, Sloane N. J. A., Goethals J. M., The MacWilliams identities for nonlinear codes. *Bell Syst. Techn. J.*, 1972, 51, № 4, 803—819 (РЖМат, 1972, 11B369)
250. —, —, Thompson J. G., Good self-dual codes exist. *Discrete Math.*, 1972, 3, № 1-3, 153—162 (РЖМат, 1973, 2B417)
251. —, —, —, On the existence of a projective plane of order 10. *J. Combin. Theory*, 1973, 14(A), № 1, 66—78 (РЖМат, 1973, 8B320)
252. MacDonald J. E., Design methods for maximum minimum-distance error-correcting codes. *IBM J. Res. Develop.*, 1960, 4, № 1, 43—57 (РЖМат, 1963, 1B183)
253. Mallows C. L., Sloane N. J. A., The split weight enumerator of a code. Третий международный симпозиум по теории информации, тезисы докладов. Москва—Таллин, 1973, часть II, 220—224.
254. —, —, An upper bound for self-dual codes. *Inform. and Control*, 1973, 22, № 2, 188—200 (РЖМат, 1973, 9B477)
255. —, —, Weight enumerators of self-orthogonal codes. *Discrete Math.*, 1974, 9, № 4, 391—400 (РЖМат, 1975, 3B618)
256. Maneri C., Silverman R., A vector-space packing problem. *J. Algebra*, 1966, 4, № 3, 321—330 (РЖМат, 1967, 7A299)
257. Mann H. B., On the number of information symbols in Bose—Chaudhuri codes. *Inform. and Control*, 1962, 5, № 2, 153—162. (Русский перевод: Манн Г. Б. О числе информационных символов в кодах

- Боуза—Чоудхури. Кибернетический сборник, вып. 8. М., «Мир», 1964, 33—41) (РЖМат, 1963, 5В361)
258. —, Ed. Error correcting codes. New York: Wiley, 1968
259. Massey J. L., Threshold decoding. Cambridge, Mass.: M. I. T. Press, 1963, 129 pp. (Русский перевод: Мессис Дж. Пороговое декодирование. М., «Мир», 1966) (РЖМат, 1965, 11В181К)
260. —, Reversible codes. Inform. and Control, 1964, 7, 369—380 (РЖМат, 1965, 5В156)
261. —, On the fractional weight of distinct binary n -tuples. IEEE Trans. Inform. Theory, 1974, 20, № 1, 131 (РЖМат, 1974, 9В574)
262. —, Costello D. J., Jr., Justesen J., Polynomial weights and code constructions. IEEE Trans. Inform. Theory, 1973, 19, № 1, 101—110 (Русский перевод: Мессис Дж. Л., Кастелло Д. Дж., Юстесен И. Веса многочленов и кодовые конструкции. Кибернетический сборник, новая серия, вып. 11. М., «Мир», 1974, 24—47) (РЖМат, 1973, 6В466)
263. Mattson H. F., Solomon G., A new treatment of Bose—Chaudhuri codes. J. Soc. Indus. Appl. Math., 1961, 9, № 4, 654—669. (Русский перевод: Маттсон Г., Соломон Г. Новая трактовка кодов Боуза—Чоудхури. Сб. «Теория кодирования». М., «Мир», 1964, 7—29) (РЖМат, 1963, 9В281)
264. McEliece R. J., On the symmetry of good nonlinear codes. IEEE Trans. Inform. Theory, 1970, 16, № 5, 609—611 (РЖМат, 1971, 5В480)
265. —, On periodic sequences from $GF(q)$. J. Combin. Theory, 1971, A10, № 1, 80—91 (РЖМат, 1972, 1В512)
266. —, Rumsey H., Jr., Euler products, cyclotomy and coding. J. Number Theory, 1972, 4, № 3, 302—311 (РЖМат, 1972, 11А84)
267. Muller D. E., Application of Boolean algebra to switching circuit design and to error detection. IEEE Computers, 1954, 3, № 1, 6—12 (РЖМат, 1955, 5З43)
268. Nadler M., A 32-point $n=12$, $d=5$ code. IEEE Trans. Inform. Theory, 1962, 8, № 1, 58 (РЖМат, 1962, 9В254)
269. Neumann P. G., A note on cyclic permutation error-correcting codes. Inform. and Control, 1962, 5, № 1, 72—86 (Русский перевод: Нейман П. Заметка о циклически перестановочных кодах, исправляющих ошибки. Сб. «Теория кодирования». М., «Мир», 1964, 65—82) (РЖМат, 1963, 6В286)
270. Nordstrom A. W., Robinson J. P. An optimum nonlinear code. Inform. and Control, 1967(1968), 11, № 5-6, 613—616 (РЖМат, 1969, 2В324)
271. Oganessian S. Sh., Yagdzyan V. G., Tairyan V. I., On a class of optimal cyclic codes. 2-nd Intern. Symp. Inform. Theory, Tsahkadzor, 1971, Budapest, 1973, 219—224 (РЖМат, 1974, 9А385)
272. Patel A. M., Maximal group codes with specified minimum distance. IBM J. Res. Develop., 1970, 14, № 4, 434—443 (РЖМат, 1971, 6В459)
273. Peterson W. W., Error correcting codes. The M. I. T. Press, Cambridge, Mass., 1961. (Русский перевод: Питерсон. Коды, исправляющие ошибки. М., «Мир», 1964) (РЖМат, 1962, 4В256К)
274. —, On the weight structure and symmetry of BCH codes. J. IECE Japan, 1967, 50, 1183—1190
275. —, Some new results on finite fields and their applications to the theory of BCH Codes. Chap. 19 in R. C. Bose and T. A. Dowling (eds), Proceedings of the Conference on Combinatorial Mathematics and Its Applications (April 10—14, 1967), The University of North Carolina Press, Chapel Hill, N. C., 1968
276. —, Weldon E. J., Jr., Error correcting codes, 2nd ed. Cambridge, Mass.: M. I. T. Press, 1972
277. Pierce J. N., Limit distribution of the minimum distance of random linear codes. IEEE Trans. Inform. Theory, 1967, 13, № 4, 595—599 (Русский перевод: Пирс Дж. Н. Предельное распределение для мини-

- мального расстояния в случайном линейном коде. Кибернетический сборник, новая серия, вып. 7. М., «Мир», 1970, 5—17) (РЖМат, 1969, 4В331)
278. Ples V., Power moment identities on weight distributions in error-correcting codes. Inform. and Control, 1963, 6, № 2, 147—152 (РЖМат, 1964, 4В310)
 279. —, On the uniqueness of the Golay codes. J. Combin. Theory, 1968, 5, 215—228
 280. —, On a new family of symmetry codes and related new five-designs. Bull. Amer. Mat. Soc., 1969, 75, № 6, 1339—1342 (РЖМат, 1970, 10В217)
 281. —, A classification of self-orthogonal codes over GF(2). Discrete Math., 1972, 3, № 1-3, 209—246 (РЖМат, 1973, 2В418)
 282. —, Symmetry codes over GF(3) and new five-designs. J. Combin. Theory, 1972, 12(A), № 1, 119—142 (РЖМат, 1972, 6В253)
 283. —, Symmetry codes and their invariant subcodes. Proj. MAC Techn. Memo., 1974, № 44, 1—13 (РЖМат, 1975, 3В616)
 284. —, Pierce J. N., Self-dual codes over GF(q) satisfy a modified Varshamov—Gilbert bound. Inform. and Control, 1973, 23, № 1, 35—40 (РЖМат, 1974, 1В439)
 285. —, Sloane N. J. A., Binary self-dual codes of length 24. Bull. Amer. Math. Soc., 1974, 80, № 6, 1173—1178 (РЖМат, 1975, 6В675)
 286. Plotkin M., Binary codes with specified minimum distance. IRE Trans. Inform. Theory, 1960, 6, № 4, 445—450. (Русский перевод: Плоткин М., Двоичные коды с заданным минимальным расстоянием. Кибернетический сборник, вып. 7. М., ИЛ, 1963, 60—73) (РЖМат, 1962, 10В266)
 287. Preparata F. P., Weight and distance structure of Nordstrom—Robinson quadratic code. Inform. and Control, 1968, 12, № 5-6, 466—473 (РЖМат, 1969, 5В381)
 288. —, A class of optimum nonlinear double-error-correcting codes. Inform. and Control, 1968, 13, № 4, 378—400 (Русский перевод: Препарата Ф. П. Класс оптимальных нелинейных кодов с исправлением двойных ошибок. Кибернетический сборник, новая серия, вып. 7. М., «Мир», 1970, 18—42) (РЖМат, 1969, 11В385)
 289. —, A new look at the Golay (23, 12) code. IEEE Trans. Inform. Theory, 1970, 16, № 4, 510—511 (РЖМат, 1971, 5В481)
 290. Rao V. V., Reddy S. M., A (48, 31, 8) linear code. IEEE Trans. Inform. Theory, 1973, 19, № 5, 709—711 (РЖМат, 1974, 5В534)
 291. Reed I. S., A class of multiple-error-correcting codes and the decoding scheme. IRE Trans. Inform. Theory, 1954, 4, № 1, 38—49 (Русский перевод: Рид И. С., Класс кодов с исправлением нескольких ошибок и схема декодирования. Кибернетический сборник, вып. 1. М., ИЛ, 1960, 189—205) (РЖМат, 1956, 3390)
 292. —, Solomon G., Polynomial codes over certain finite fields. J. Soc. Industr. and Appl. Math., 1960, 8, № 2, 300—304 (Русский перевод: Рид И. С., Соломон Г. Полиномиальные коды над некоторыми конечными полями. Кибернетический сборник, вып. 7. М., ИЛ, 1963, 74—79) (РЖМат, 1961, 10А299)
 293. Rudolph L. D., A class of majority logic decodable codes. IEEE Trans. Inform. Theory, 1967, 13, № 2, 305—307 (РЖМат, 1968, 4В319)
 294. Schonheim J., On linear and nonlinear single-error correcting q-nary perfect codes. Inform. and Control, 1968, 12, № 1, 23—26 (РЖМат, 1969, 1В337)
 295. Seguin G., On the weight distribution of cyclic codes. IEEE Trans. Inform. Theory, 1970, 16, № 3, 358 (РЖМат, 1970, 12В428)
 296. Shapiro H. S., Slotnick D. L., On the mathematical theory of error-correcting codes. IBM J. Res. Develop., 1959, 3, 1, 25—34 (Русский перевод: Шапиро Г. С., Злотник Д. П. К математической тео-

- при кодов с исправлением ошибок. Кибернетический сборник, вып. 5. М., ИЛ 1962, 7—32) (ПЖМат, 1961, 9B193)
297. Shaughnessy E. P., Codes with simple automorphism groups. *Archiv Math.*, 1971, 22, № 5, 459—466 (ПЖМат, 1972, 6A194)
 298. Shiva S. G. S., Certain group codes. *Proc. IEEE*, 1967, 55, 2162—2163
 299. Silverman R., A metrization for power-sets with applications to combinatorial analysis. *Canad. J. Math.*, 1960, 12, № 1, 156—176 (ПЖМат, 1960, 9993)
 300. Singleton R. C., Maximum distance q -nary codes. *IEEE Trans. Inform. Theory*, 1964, 10, № 2, 116—118 (ПЖМат, 1965, 2B383)
 301. Slepian D., A class of binary signaling alphabets. *Bell Syst. Techn. J.*, 1956, 35, № 1, 203—234 (Русский перевод: Слепян Д., Класс двоичных сигнальных алфавитов. Сб. «Теория передачи сообщений». М., ИЛ, 1957, 82—113) (ПЖМат, 1960, 9245)
 302. —, Some further theory of group codes. *Bell Syst. Techn. J.*, 1960, 9, 1219—1252
 303. Sloane N. J. A., Sphere packings constructed from BCH and Justesen codes. *Mathematika (Gr. Brit.)*, 1972, 19, № 2, 183—190 (ПЖМат, 1973, 9B480)
 304. —, A survey of constructive coding theory, and a table of binary, codes of highest known rate. *Discrete Math.*, 1972, 3, № 1-3, 265—294 (Русский перевод: Слоэн Н. Дж. А. Обзор конструктивной теории кодирования и таблица двоичных кодов с наибольшими известными скоростями. Кибернетический сборник, новая серия, вып. 10. М., «Мир», 1973, 5—32) (ПЖМат, 1973, 2B419)
 305. —, Is there a $(72,36) d=16$ self-dual code? *IEEE Trans. Inform. Theory*, 1973, 19, № 2, 251 (ПЖМат, 1973, 9B478)
 306. —, Weight enumerators of codes. *Math. Centre Tracts*, 1974, № 55, 111—138 (ПЖМат, 1975, 4B563)
 307. —, Reddy S. M., Chen C.-L., New binary codes. *IEEE Trans Inform. Theory*, 1972, 18, № 4, 503—510 (ПЖМат, 1972, 12B295)
 308. —, Seidel J. J., A new family of nonlinear codes obtained from conference matrices. *Ann. N. Y. Acad. Sci.*, 1970, 175, № 1, 363—365 (ПЖМат, 1971, 4B390)
 309. —, Whitehead D. S., New family of single-error correcting codes. *IEEE Trans. Inform. Theory*, 1970, 16, № 6, 717—719 (ПЖМат, 1971, 7B577)
 310. Smith K. J. C., On the p -rank of the incidence matrix of points and hyperplanes in a finite projective geometry. *J. Combin. Theory*, 1969, 7, № 2, 122—129 (ПЖМат, 1970, 3B286)
 311. Solomon G., A weight formula for group codes. *IEEE Trans. Inform. Theory*, 1962, 8, № 5, 1—4 (ПЖМат, 1963, 7B338)
 312. —, McEliece R., Weights of cyclic codes. *J. Combin. Theory*, 1966, 1, № 4, 459—475 (ПЖМат, 1967, 11B251)
 313. —, Stiffler J. J., Algebraically punctured cyclic codes. *Inform. and Control*, 1965, 8, № 2, 170—179 (ПЖМат, 1965, 11B173)
 314. Sugino M., Ienaga Y., Tokura N., Kasami T., Weight distribution of $(128, 64)$ Reed—Muller code. *IEEE Trans. Inform. Theory*, 1971, 17, № 5, 627—628 (ПЖМат, 1972, 4B400)
 315. Sugiyama Y., Kasahara M., Hirasawa Sh., Namekawa T., A modification of the constructive asymptotically good codes of Justesen for low rates. *Inform. and Contr.*, 1974, 25, № 4, 341—350 (ПЖМат, 1975, 2B657)
 316. Swan R. G., Factorization of polynomials over finite fields. *Pacific. J. Math.*, 1962, 12, № 3, 1099—1106 (ПЖМат, 1963, 10A186)
 317. Tavares S. E., Allard P. E., Shiva S. G. C., On the decomposition of cyclic codes into cyclic classes. *Inform. and Control*, 1971, 18, 342—354 (ПЖМат, 1972, 1B718)
 318. Tietäväinen A., On the nonexistence of perfect 4-hamming-error-correcting codes. *Suomalais. tiedekat. toimituks.*, 1970, Ser. AI, № 485, 1—6 (ПЖМат, 1971, 9B448)

319. —, On the nonexistence of perfect codes over finite fields. *SIAM J. Appl. Math.*, 1973, 24, № 1, 88—96 (РЖМат, 1973, 9B479)
320. —, A short proof for the nonexistence of unknown perfect codes over $GF(q)$, $q > 2$. *Suomalais. tiedekat. toimituks.*, 1974, Ser. AI, № 580, 1—6 (РЖМат, 1975, 4A388)
321. —, Perko A., There are no unknown perfect binary codes. *Turun yliopiston julk.*, 1971, Ser. AI, № 148, 1—10 (РЖМат, 1971, 12B732)
322. Townsend R. L., Weldon E. J., Jr., Self-orthogonal quasi-cyclic codes. *IEEE Trans. Inform. Theory*, 1967, 13, № 2, 183—195 (Русский перевод: Таунсенд Р. Л., Велдон И. Дж. Собственно ортогональные квазициклические коды. Сб. «Некоторые вопросы теории кодирования» М., «Мир», 1970, 36—67) (РЖМат, 1968, 3B331)
323. Tzeng K. K., Reversible residue codes. *Proc. UMR—Mervin J. Kelly Communs. Conf.*, Rolla Mo., 1970. New York, N. Y., 1970, (5—3)/1—(5—3)/5 (РЖМат, 1971, 10B650)
324. Wagner T. J., A search technique for quasi-perfect codes. *Inform. and Control*, 1966, 9, № 1, 94—99 (РЖМат, 1966, 11B231)
325. Welch L. R., McEliece R. J., Rumsey H., Jr., A low-rate improvement on the Elias bound. *IEEE Trans. Inform. Theory*, 1974, 20, № 5, 676—678 (РЖМат, 1975, 4B564)
326. Weldon E. J., Jr., Difference-set cyclic codes. *Bell Syst. Techn. J.*, 1966, 25, № 7, 1045—1055 (Русский перевод: Велдон И. Дж. Циклические коды, задаваемые разностными множествами. Сб. «Некоторые вопросы теории кодирования». «Мир», М., 1970, 9—21)
327. —, New generalizations of the Reed—Muller codes. Part II. Nonprimitive codes. *IEEE Trans. Inform. Theory*, 1968, 14, № 2, 199—205 (РЖМат, 1968, 11B359)
328. —, Euclidean geometry cyclic codes. Chap. 23 in R. C. Bose and T. A. Dowling (eds), *Proc. Confer. Combin. Math. Appl.*, (April 10—14, 1967), The University of North Carolina Press, Chapel Hill, N. C.
329. —, Long quasi-cyclic codes are good. *IEEE Trans. Inform. Theory*, 1970, 16, № 1, 130
330. —, Justesen's construction — a low rate case. *IEEE Trans. Inform. Theory*, 1973, 19, № 5, 711—713 (РЖМат, 1974, 5B535)
331. Wolf J. K., On codes derivable from the tensor product of check matrices. *IEEE Trans. Inform. Theory*, 1965, 11, 281—284
332. —, On an extended class of error-locating codes. *Inform. and Control*, 1965, 8, № 2, 163—169
333. —, Adding two information symbols to certain nonbinary BCH and some applications. *Bell Syst. Techn. J.*, 1969, 48, № 7, 2405—2424
334. —, Nonbinary random error correcting codes. *IEEE Trans. Inform. Theory*, 1970, 16, № 2, 236—237
335. Zaitsev G. V., Zinoviev V. A., Semakov N. V., Interrelation of Preparata and Hamming codes and extension of Hamming codes to new double-error-correcting codes. 2nd Intern. Symp. Inform. Theory, Thsahkadors, 1971, Budapest, 1973, 257—263 (РЖМат, 1974, 9B569)
336. Zierler N., Linear recurring sequences. *J. Soc. Ind. Appl. Math.*, 1959, 7, № 1, 31—48 (Русский перевод: Цирлер Н., Линейные возвратные последовательности. Кибернетический сборник, вып. 6. М., ИЛ, 1963, 55—79) (РЖМат, 1960, 4875)