В. В. Чепыжов, Новые нижние границы для минимального расстояния линейных квазициклических и почти линейных циклических кодов, *Пробл. передачи информ.*, 1992, том 28, выпуск 1, 39–51

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 28 1992 Вып. 1

УДК 621.391.15

© 1992 г. **В.В. Чепыжов**

НОВЫЕ НИЖНИЕ ГРАНИЦЫ ДЛЯ МИНИМАЛЬНОГО РАССТОЯНИЯ ЛИНЕЙНЫХ КВАЗИЦИКЛИЧЕСКИХ И ПОЧТИ ЛИНЕЙНЫХ ЦИКЛИЧЕСКИХ КОДОВ

Получены новые нижние границы для минимального расстояния линейных (np, kp) квазициклических кодов над произвольными полями $GF(q)$ при скорости передачи $R = k/n$ и для почти линейных циклических кодов длины p над непростыми полями $GF(q^n)$ при скорости передачи $R = k/n$, p – любое простое число. При этом не предполагается, что q является первообразным корнем по модулю p. Этот результат позволяет установить асимптотическую достижимость соответствующих границ Варшамова–Гилберта квазициклическими и почти линейными циклическими кодами с указанными характеристиками для почти всех простых чисел p.

§ 1. Введение

Квазициклическим (np, kp)-кодом (КЦ-кодом) с шагом n, где $n \geqslant 2$, $k < n$ (p – некоторое целое число), над полем $GF(q)$ называется линейный блоковый код длины np, который инвариантен относительно циклической перестановки индекса i с шагом n: $i \to i + n (\mathrm{mod}\, np)$, т.е.

$$(c_0, c_1, c_2, \ldots, c_{np-1}) \to (c_n, c_{n+1}, \ldots, c_{np-1}, c_0, c_1, \ldots, c_{n-1}).$$

Можно объединить в подблоки элементы кодовых слов, отстоящие друг от друга на расстояния, кратные n. При этом образуется n подблоков длины p: $(x_1, x_2, \ldots, x_n)$, где $x_i = (x_{i0}, x_{i1}, \ldots, x_{ip-1})$, $i = \overline{1, n}$. При такой перестановке элементов КЦ-код инвариантен относительно одновременного циклического сдвига на один шаг всех подблоков, т.е.:

$$(x_{i0}, x_{i1}, x_{i2}, \ldots, x_{ip-1}) \to (x_{i1}, x_{i2}, \ldots, x_{ip-1}, x_{i0}), \quad i = \overline{1, n}.$$

Представляет интерес проблема нахождения нижних границ для минимального расстояния КЦ-кодов. В работе [1] было доказано, что если 2 – первообразный корень по модулю p, то над полем $GF(2)$ существуют систематические КЦ-коды длины np с шагом n, скоростью $R = 1/n$ или $R = (n-1)/n$ и минимальным расстоянием d таким, что:

$$H_2\left(\frac{d}{np}\right) \geqslant (1-R)\left(\frac{p-1}{p}\right).$$

Здесь и далее $H_q(z) = -z \log_q(z) - (1-z) \log_q(1-z) + z \log_q(q-1)$. Достижение асимптотической границы Варшамова–Гилберта обеспечивалось бы существованием бесконечной последовательности $\{p_i\}_{i \in N}$ простых чисел, для которых 2 – первообразный корень по модулю p. (Насколько нам известно, эта существенная проблема теории чисел еще не решена.)

Результат работы [1] получил развитие в работе [2], где было установлено, что если 2 – первообразный корень по модулю p и $2^{p-1} \not\equiv 1 \mathrm{mod}\,(p^2)$, то для любого $\alpha \in N$ существуют систематические КЦ-коды длины $p^\alpha n$ со скоростью $R = 1/n$ или $R = (n-1)/n$

и кодовым расстоянием d_α, удовлетворяющим неравенству:

$$H_2\left(\frac{d_\alpha}{p^\alpha n}\right) \geqslant (1-R)\left(\frac{p-1}{p}\right). \qquad (1)$$

Из приведенной теоремы уже следует существование бесконечных последовательностей чисел $\{p^\alpha n\}_{\alpha \in N}$, образующих геометрическую прогрессию, для которых существуют КЦ-коды длины $p^\alpha n$ с кодовым расстоянием, очень близко подходящим к границе Варшамова–Гилберта, если найдено достаточно большое простое число p, удовлетворяющее нужным ограничениям.

Далее, в работе [3] изложенные результаты были обобщены на случай произвольных полей $GF(q)$ и любых скоростей $R = k/n$ при условии, что q – первообразный корень по модулю p.

Наконец, Круку в работе [4] удалось поднять границу (1) до границы Варшамова–Гилберта:

$$H_q\left(\frac{d_\alpha}{p^\alpha n}\right) \geqslant 1 - R,$$

для $(p^\alpha n,\ p^\alpha k)$ КЦ-кодов со скоростью $R = k/n$ над полями $GF(q)$ с условием, что q – первообразный корень по модулю p и $q^{p-1} \not\equiv 1 \bmod (p^2)$. Следует, однако, отметить, что под этот результат подпадают не все поля. Например, для $GF(4)$ число 4 не является первообразным корнем по модулю p при любом простом p.

В работе [3] была установлена связь между КЦ-кодами и циклическими почти линейными кодами. В этой статье было отмечено, что из доказанной в ней теоремы следует существование бесконечной последовательности "хороших" циклических почти линейных кодов длины p^α со скоростью $R = k/n$ над непростыми полями $GF(q^n)$, т.е. для которых кодовое расстояние d_α удовлетворяет неравенству $(d_\alpha/p^\alpha) \geqslant \delta > 0$, где $\delta = H_q^{-1}(1-R)$. Однако получающаяся при этом граница ниже соответствующей границы Варшамова–Гилберта $H_{q^n}^{-1}(1-R)$.

В настоящей работе мы исследуем нижние границы для кодового расстояния линейных квазициклических $(np,\ kp)$ кодов над произвольными полями $GF(q)$ и для почти линейных циклических кодов длины p над непростыми полями $GF(q^n)$ при скорости передачи $R = k/n$, $n \geqslant 2$, где p – простое число. При этом не требуется, чтобы число q было первообразным корнем по модулю p. Получены новые нижние границы, которые для почти всех p являются соответствующими асимптотическими границами Варшамова–Гилберта.

§ 2. Границы для квазициклических кодов над $GF(q)$

Рассмотрим линейные квазициклические $(np,\ kp)$-коды над полем $GF(q)$ со скоростью передачи $R = k/n$ (p – некоторое целое число). Для описания КЦ-кодов удобно использовать алгебру A_p вычетов многочленов над $GF(q)$ по модулю $D^p - 1$. Элементами алгебры A_p являются многочлены степени не выше $p-1$. Любой (np, kp) КЦ-код задается матрицей $G(D) = \{g_{ij}(D)\}_{i=1,\ldots,n}^{j=1,\ldots,k}$ элементов алгебры A_p, где

$$g_{ij}(D) = g_{ij0} + g_{ij1}D + \ldots + g_{ijp-1}D^{p-1}, \quad i = \overline{1,n},\ j = \overline{1,k}.$$

Кодовые слова можно также представить в виде последовательностей $\bar{x}(D) = (x_1(D), x_2(D), \ldots, x_n(D))$ элементов A_p, а информационные слова в виде последовательностей $\bar{u}(D) = (u_1(D), u_2(D), \ldots, u_k(D))$ ($x_i(D)$ и $u_j(D)$ – многочлены степени не выше $p-1$). Коду $G(D)$ соответствует множество кодовых слов:

$$x_i(D) = \sum_{j=1}^{k} u_j(D)\, g_{ij}(D) \bmod (D^p - 1), \quad i = \overline{1,n},$$

где $\bar{u}(D) = (u_1(D), u_2(D), \ldots, u_k(D))$ – всевозможные информационные слова.

Сформулируем основной результат статьи.

Теорема 1. *Пусть p – простое число $(p>q)$, m – порядок q по модулю p, $t = (p-1)/m$. Тогда существует (np, kp) КЦ-код G со скоростью $R = k/n$, для которого кодовое расстояние $\hat{d}$ удовлетворяет неравенству*

$$H_q\left(\frac{\hat{d}}{np}\right) \geqslant 1 - R - R\frac{\log_q(k(2q)^k t)}{m}. \qquad (2)$$

Существует эквивалентный способ задания КЦ-кодов, основанный на использовании циркулянтов. Наряду с многочленами $g_{ij}(D)$, $u_i(D)$, $x_j(D)$, $i=\overline{1,n}$, $j=\overline{1,k}$ рассмотрим векторы коэффициентов:

$$\mathbf{g}_{ij} = (g_{ij0}, g_{ij1}, \ldots, g_{ijp-1})^T,$$
$$\mathbf{x}_i = (x_{i0}, x_{i1}, \ldots, x_{ip-1})^T,$$
$$\mathbf{u}_j = (u_{j0}, u_{j1}, \ldots, u_{jp-1})^T, \quad i=\overline{1,n}, \quad j=\overline{1,k}$$

(T – обозначает транспонирование строки или матрицы). Циркулянтом вектора $\mathbf{u} = (u_0, u_1, \ldots, u_{p-1})^T$ называется $(p\times p)$-матрица следующего вида:

$$\mathbf{U} = \begin{Vmatrix} u_0 & u_{p-1} & \ldots & u_1 \\ u_1 & u_0 & \ldots & u_2 \\ u_2 & u_1 & \ldots & u_3 \\ u_{p-2} & u_{p-3} & \ldots & u_{p-1} \\ u_{p-1} & u_{p-2} & \ldots & u_0 \end{Vmatrix}.$$

Каждому информационному слову $\bar{u}(D) = (u_1(D), u_2(D), \ldots, u_k(D))$ соответствует последовательность циркулянтов $\bar{\mathbf{U}} = (\mathbf{U}_1, \ldots, \mathbf{U}_k)$, которую мы будем также называть информационным словом. Наконец, кодовые слова $\bar{\mathbf{x}} = (\mathbf{x}_1, \ldots, \mathbf{x}_n)$ кода $\mathbf{G} = \{\mathbf{g}_{ij}\}_{\substack{i=1,\ldots,n \\ j=1,\ldots,k}}$ задаются соотношениями

$$\mathbf{x}_i = \sum_{j=1}^{k} \mathbf{U}_j \mathbf{g}_{ij}, \quad i=\overline{1,n}.$$

Последние равенства будем коротко записывать в следующем виде

$$\bar{\mathbf{x}} = \bar{\mathbf{U}}\mathbf{G}.$$

Зафиксируем произвольный многочлен $u(D)$ и соответствующий ему циркулянт $\mathbf{U}$. Рассмотрим линейный оператор в алгебре A_p, который многочлену $g(D)$ ставит в соответствие многочлен $x(D) = u(D)\,g(D) \bmod (D^p - 1)$ или на языке циркулянтов: $\mathbf{x} = \mathbf{U}\mathbf{g}$. Обозначим $r(\mathbf{U}) = \operatorname{rank}(\mathbf{U})$ ранг введенного оператора.

Следующие два простых утверждения, вытекающие из теории циклических кодов, нам удобно оформить в виде отдельных лемм.

Лемма 1. $r(\mathbf{U}) = p - d$, *где* $d = \deg$ Н.О.Д. $(D^p - 1, u(D))$.

Лемма 2. *Если $r = r(\mathbf{U})$, то первые r столбцов и первые r строк циркулянта $\mathbf{U}$ линейно независимы.*

Начиная с этого места будем предполагать, что p – простое число, причем $p>q$. Изучим распределение циркулянтов размера $p\times p$ по рангам r. Для этого разложим многочлен $D^p - 1$ над полем $GF(q)$ на неприводимые сомножители:

$$D^p - 1 = (D-1)\,z_1(D)\ldots z_t(D). \qquad (3)$$

Обозначим для удобства изложения $z_0(D) = D - 1$. Поскольку p – простое число и $p>q$, то, как следует из теории разложения многочлена $D^p - 1$ на множители, все его неприводимые делители $z_i(D)$ $i=\overline{1,t}$ различны и имеют одинаковую степень m, где m – наименьшее натуральное число, для которого $q^m \equiv 1 \bmod (p)$ (см., например, [5]). Такое m называется порядком числа q по модулю p. Ясно также, что $p = mt + 1$.

Обозначим $N_p(r)$ число циркулянтов $\mathbf{U}$ размерности $p \times p$, имеющих ранг r.

Лемма 3. *Если* p *– простое число и* $p > q$, *то*

1) *ранг матрицы* $\mathbf{U}$ *может принимать значения*: 0; 1; m; $m+1$; ...; mt; $mt+1$;

2) $N_p(jm) = \binom{t}{j}(q^m-1)^j$, $N_p(jm+1) = \binom{t}{j}(q^m-1)^j(q-1)$, $j = 0, 1, \ldots, t$.

Доказательство. Пусть $z(D) = \text{Н.О.Д.}(D^p-1;\ u(D))$, $D^p - 1 = z(D)\,\tilde{z}(D)$. Из леммы 1 вытекает, что $r(\mathbf{U}) = \deg \tilde{z}(D)$. В силу (3) $\tilde{z}(D)$ – произведение некоторых сомножителей $z_i(D)$, которые имеют степень m при $i \geqslant 1$ и степень 1 при $i = 0$. Следовательно, $r(\mathbf{U}) = mj + 1$ или $r(\mathbf{U}) = mj$, где j – число сомножителей $\tilde{z}(D)$, отличных от $D-1$. Пункт 1) доказан.

Докажем пункт 2). Пусть $r = mj$ или $r = mj+1$, где $j = \overline{0,t}$. Найдем $N_p(r)$. Зафиксируем некоторую пару многочленов $z(D)$ и $\tilde{z}(D)$, для которых $z(D)\,\tilde{z}(D) = D^p - 1$ и $\deg \tilde{z}(D) = r$. Обозначим через I множество индексов i из $\{0, 1, \ldots, t\}$, для которых $z_i(D)$ является делителем $\tilde{z}(D)$, т.е. $\tilde{z}(D) = \prod\limits_{i \in I} z_i(D)$, $z(D) = \prod\limits_{i \notin I} z_i(D)$. Множество I содержит ровно j индексов, отличных от нуля. Найдем число многочленов $u(D)$ степени не выше $p-1$, для которых $\text{Н.О.Д.}(D^p-1, u(D)) = z(D)$. Это условие эквивалентно следующему:

$$u(D) = 0 \bmod (z_i(D)) \quad \text{при} \quad i \notin I, \tag{4}$$

$$u(D) \neq 0 \bmod (z_i(D)) \quad \text{при} \quad i \in I. \tag{5}$$

Из китайской теоремы об остатках следует, что многочлен $u(D)$ однозначно восстанавливается по остаткам от деления на $z_i(D)$, $i = 0, 1, \ldots, t$. (Напомним, что все $z_i(D)$ различны и неприводимы.) В силу (4) остатки от деления на $z_i(D)$ при $i \notin I$ зафиксированы. Если же $i \in I$, то число возможных ненулевых остатков от деления на $z_i(D)$ равно $q^m - 1$ для $i \geqslant 1$ и равно $q-1$ для $i = 0$; поскольку остаток – это ненулевой многочлен степени не выше $m-1$ для $i \geqslant 1$, и ненулевой элемент поля $GF(q)$ для $i = 0$ (нулевой остаток исключается в силу (5)).

Следовательно, при фиксированных $z(D)$ и $\tilde{z}(D)$ число многочленов $u(D)$, для которых $\text{Н.О.Д.}(D^p-1, u(D)) = z(D)$, равно $(q^m-1)^j$ при $r = jm$ и равно $(q^m-1)^j(q-1)$ при $r = jm+1$.

Осталось заметить, что при фиксированном $r = mj$ или $r = mj+1$ число различных многочленов $\tilde{z}(D)$ степени r определяется числом всевозможных множеств I объема j из множества индексов $\{1, 2, \ldots, t\}$, т.е. равно $\binom{t}{j}$. Следовательно, $N_p(r) = \binom{t}{j}(q^m-1)^j$ при $r = jm$ и $N_p(r) = \binom{t}{j}(q^m-1)^j(q-1)$ при $r = jm+1$. ▲

Доказательство теоремы 1. Обозначим через $\mathbf{G}_p$ множество всех (np, kp) КЦ-кодов. Имеем $|\mathbf{G}_p| = q^{knp}$ ($|\,|$ – мощность множества). Пусть d – некоторое число. Обозначим через $\mathbf{G}_p(d)$ множество кодов $\mathbf{G} \in \mathbf{G}_p$, для которых существует ненулевое информационное слово $\bar{\mathbf{U}} = (\mathbf{U}_1, \mathbf{U}_2, \ldots, \mathbf{U}_k)$ такое, что $W(\bar{\mathbf{U}}\mathbf{G}) \leqslant d$, где $W(\bar{\mathbf{x}}) = \sum\limits_{i=1}^{n} W(\mathbf{x}_i)$, $W(\mathbf{x})$ – хэммингов вес вектора $\mathbf{x}$.

Оценим сверху мощность множества $\mathbf{G}_p(d)$. Для произвольного циркулянта $\mathbf{U}$ ранга r будем обозначать через $\mathbf{U}^s$ матрицу размера $s \times p$, состоящую из первых s строк матрицы $\mathbf{U}$. Из леммы 2 вытекает, что матрица $\mathbf{U}^r$ имеет полный ранг r.

Для произвольного информационного слова в его циркулянтном представлении $\bar{\mathbf{U}} = (\mathbf{U}_1, \mathbf{U}_2, \ldots, \mathbf{U}_k)$ мы будем обозначать $\bar{\mathbf{U}}^r = (\mathbf{U}_1^r, \mathbf{U}_2^r, \ldots, \mathbf{U}_k^r)$, где $r = \max\{r_1, r_2, \ldots, r_k\}$, $r_j = \operatorname{rank}(\mathbf{U}_j)$, $j = \overline{1,k}$. Ясно, что $r_j = r$ для некоторого j и матрица $\mathbf{U}_j$ имеет полный ранг r.

Пусть $\mathbf{G} \in \mathbf{G}_p(d)$, тогда для некоторого ненулевого информационного слова $\bar{\mathbf{U}}$ выполнено неравенство $W(\bar{\mathbf{U}}\mathbf{G}) \leqslant d$. Пусть $r = \max\{r_1, r_2, \ldots, r_k\}$, где $r_j = \operatorname{rank}(\mathbf{U}_j)$, $j = \overline{1,k}$.

Покажем, что, быть может, для другого информационного слова $\bar{\mathbf{V}} = (\mathbf{V}_1, \mathbf{V}_2, \ldots, \mathbf{V}_k)$ характеризующегося теми же параметрами $r_1, r_2, \ldots, r_k (\operatorname{rank}(\mathbf{V}_j) = r_j)$, имеет место неравенство:

$$W(\bar{\mathbf{V}}^r \mathbf{G}) \leqslant \frac{dr}{p}. \tag{6}$$

Для этого рассмотрим p информационных слов $\bar{\mathbf{U}}(0), \bar{\mathbf{U}}(1), \bar{\mathbf{U}}(2), \ldots, \bar{\mathbf{U}}(p-1)$ таких, что $\bar{\mathbf{U}}(0) = \bar{\mathbf{U}}$, а каждое $\bar{\mathbf{U}}(l)$ соответствует информационному слову $D^l \bar{u}(D) \bmod (D^p - 1) = (D^l u_1(D), \ldots, D^l u_k(D)) \bmod (D^p - 1)$, $l = \overline{0, p-1}$ в полиномиальном представлении, где $\bar{u}(D) = (u_1(D), \ldots, u_k(D))$ – полиномиальное представление исходного информационного слова $\bar{\mathbf{U}}$.

Заметим, что вектор $\mathbf{x}(l)_i = \sum_{j=1}^{k} \mathbf{U}(l)_j g_{ij}$ получается из вектора $\mathbf{x}_i = \sum_{j=1}^{k} \mathbf{U}_j \mathbf{g}_{ij}$ циклическим сдвигом на l позиций. Следовательно, имеет место равенство

$$\sum_{l=0}^{p-1} W(\bar{\mathbf{U}}(l)^r \mathbf{G}) = rW(\mathbf{UG}). \tag{7}$$

В самом деле, в силу указанной цикличности в левой части (7) каждый ненулевой элемент каждого вектора $\mathbf{x}_i = (\bar{\mathbf{U}}\mathbf{G})_i$ считается ровно r раз. Из равенства (7) вытекает, что для некоторого l

$$W(\bar{\mathbf{U}}(l)^r \mathbf{G}) \leqslant \frac{r}{p} W(\bar{\mathbf{U}}\mathbf{G}) \leqslant \frac{r}{p} d. \tag{8}$$

Осталось заметить, что $\operatorname{rank}(\mathbf{U}(l)_j) = \operatorname{rank}(\mathbf{U}_j) \quad j = \overline{1,k}$, поэтому можно положить $\bar{\mathbf{V}} = \bar{\mathbf{U}}(l)$.

Обозначим

$$X^r\left(\frac{rd}{p}\right) = \left\{ \bar{\mathbf{x}}^r = (\mathbf{x}_1^r, \mathbf{x}_2^r, \ldots, \mathbf{x}_n^r) : W(\bar{\mathbf{x}}^r) \leqslant \frac{rd}{p} \right\},$$

где $\mathbf{x}_i^r = (x_{i0}, x_{i1}, \ldots, x_{ir-1})^T$, $i = \overline{1,n}$ – векторы размерности r. Если теперь снова $\mathbf{G} \in \mathbf{G}_p(d)$, то в силу (6) для некоторого информационного слова $\bar{\mathbf{U}} = (\mathbf{U}_1, \mathbf{U}_2, \ldots, \mathbf{U}_k)$, характеризуемого своим параметром $r = \max\{\operatorname{rank}(\mathbf{U}_j),\ j = \overline{1,k}\}$, $r \neq 0$, имеет место включение

$$\bar{\mathbf{U}}^r \mathbf{G} = \bar{\mathbf{x}}^r \in X^r\left(\frac{rd}{p}\right) \tag{9}$$

или подробнее

$$\sum_{j=1}^{k} \mathbf{U}_j^r g_{ij} = \mathbf{x}_i^r, \qquad i = \overline{1,n}, \tag{10}$$

где

$$\bar{\mathbf{x}}^r = (\mathbf{x}_1^r, \ldots, \mathbf{x}_n^r) \in X^r\left(\frac{rd}{p}\right).$$

Зафиксируем теперь некоторое ненулевое информационное слово $\bar{\mathbf{U}} = (\mathbf{U}_1, \mathbf{U}_2, \ldots, \mathbf{U}_k)$ со своим параметром $r = \max\{\operatorname{rank}(\mathbf{U}_j),\ j = \overline{1,k}\}$, $r \neq 0$. Зафиксируем также любой вектор $\bar{\mathbf{x}}^r \in X^r\left(\frac{rd}{p}\right)$. Рассмотрим соотношения (10) как систему $r \times n$ уравнений относительно nkp неизвестных $G(D) = \{g_{ijl}\}_{i=1,\ldots,n;\ l=0,\ldots,p-1}^{j=1,\ldots,k}$. Эта система имеет

полный ранг, поскольку одна из матриц $\mathbf{U}_j^r$ имеет ранг $r_j = r$. Поэтому число различных решений системы (10) равно $q^{(kp-r)n}$.

Заметим, что в силу леммы 3 при фиксированном наборе чисел $(r_1, \ldots, r_k)$, в котором каждое число r_j принадлежит множеству $\{1, m, m+1, \ldots, mj, mj+1, \ldots, mt, mt+1\}$, существует ровно $N_p(r_1) N_p(r_2) \ldots N_p(r_k)$ различных информационных слов $\bar{\mathbf{U}} = (\mathbf{U}_1, \mathbf{U}_2, \ldots, \mathbf{U}_k)$, для которых $\operatorname{rank}(\mathbf{U}_j) = r_j$, $j = \overline{1,k}$. Причем при таком перечислении будут получены все возможные информационные слова.

В итоге, разрешая систему (10) для каждого допустимого значения $\bar{\mathbf{U}}$ и $\bar{\mathbf{x}}^r$, приходим к неравенству

$$|\mathbf{G}_p(d)| \leqslant \sum_{\substack{(r_1,\ldots,r_k)\neq 0 \\ r=\max\{r_j\}}} N_p(r_1) \ldots N_p(r_k) \times$$

$$\times \left(\left| X^r\left(\frac{rd}{p}\right)\right|\right) q^{n(kp-r)}.$$

Подставим известную оценку для $\left|X^r\left(\frac{rd}{p}\right)\right|$:

$$\left|X^r\left(\frac{rd}{p}\right)\right| = \sum_{i \leqslant (r/p)d} \binom{rn}{i} (q-1)^i < q^{H_q(d/np)rn} = q^{H_q(\rho)rn}. \tag{11}$$

Мы обозначили для удобства $\rho = d/(np)$. Приходим к неравенству

$$|\mathbf{G}_p(d)| \leqslant q^{knp} \sum_{(r_1,\ldots,r_k)\neq 0} N_p(r_1) \ldots N_p(r_k) \zeta^{\max\{r_1,\ldots,r_k\}}. \tag{12}$$

Здесь мы обозначили $\zeta = q^{H_q(\rho)n-n}$. Заметим, что $\zeta < 1$. Сумму в правой части неравенства (12) разобьем на два слагаемых:

$$\sum_{(r_1,\ldots,r_k)\neq 0} N_p(r_1) \ldots N_p(r_k) \zeta^{\max\{r_1,\ldots,r_k\}} = \sum_{\substack{(r_1,\ldots,r_k)\neq 0 \\ 0 \leqslant r_j \leqslant 1}} N_p(r_1) \ldots N_p(r_k) \zeta +$$

$$+ \sum_{\substack{(r_1,\ldots,r_k)\neq 0 \\ r=\max\{r_j\}>1}} N_p(r_1) \ldots N_p(r_k) \zeta^r = \Sigma_1 + \Sigma_2.$$

Вычислим Σ_1:

$$\Sigma_1 = \zeta \sum_{\substack{(r_1,\ldots,r_k)\neq 0 \\ 0 \leqslant r_j \leqslant 1}} N_p(r_1) \ldots N_p(r_k) = \zeta\left((N_p(0) + N_p(1))^k - N_p(0)^k\right).$$

При оценивании сверху слагаемого Σ_2 воспользуемся очевидным неравенством $r = \max\{r_1, \ldots, r_k\} \geqslant (r_1 + \ldots + r_k)/k$. Вместе с неравенством $\zeta < 1$ это дает нам

$$\Sigma_2 = \sum_{\substack{(r_1,\ldots,r_k)\neq 0 \\ r=\max\{r_j\}>1}} N_p(r_1) \ldots N_p(r_k) \zeta^r \leqslant$$

$$\leqslant \sum_{\substack{(r_1,\ldots,r_k)\neq 0 \\ r=\max\{r_j\}>1}} N_p(r_1) \ldots N_p(r_k) \zeta^{r_1/k} \ldots \zeta^{r_2/k} =$$

$$= \sum_{(r_1,\ldots,r_k)\ -\ \text{любые}} N_p(r_1) \ldots N_p(r_k) \zeta^{r_1/k} \ldots \zeta^{r_2/k} -$$

$$- \sum_{\substack{(r_1,\ldots,r_k) \\ r=\max\{r_j\}\leqslant 1}} N_p(r_1) \ldots N_p(r_k) \zeta^{r_1/k} \ldots \zeta^{r_2/k} =$$

$$= \left(\sum_{r \geqslant 0} N_p(r) \zeta^{r/k}\right)^k - \left(N_p(0) + N_p(1) \zeta^{1/k}\right)^k.$$

Подставим теперь значения r и $N_p(r)$ из леммы 3:

$$\Sigma_1 = \zeta(q^k - 1), \quad \Sigma_2 \leqslant (1 + (q-1)\zeta^{1/k})^k \{(1 + [q^m - 1]\,\zeta^{m/k})^{tk} - 1\}.$$

Следовательно, неравенство (12) влечет за собой оценку

$$|\mathbf{G}_p(d)| < q^{knp}\{\zeta(q^k - 1) + (1 + (q-1)\zeta^{1/k})^k\ ((1 + [q^m - 1]\,\zeta^{m/k})^{tk} - 1)\}. \quad (13)$$

Идея доказательства теоремы заключена в том, чтобы показать, что если число d не удовлетворяет оценке (2), то всегда $|\mathbf{G}(d)| < |\mathbf{G}_p| = q^{nkp}$, т.е. найдется код, для которого кодовое расстояние d' больше d. Итак, пусть d – некоторое число, для которого

$$H_q\left(\frac{d}{np}\right) < 1 - R - R\frac{\log_q(k(2q)^k t)}{m}. \quad (14)$$

Из (14) следует, что

$$H_q(\rho) < 1 - R, \quad (15)$$

где $\rho = d/(np)$. Покажем, что

$$\zeta(q^k - 1) + (1 + (q-1)\zeta^{1/k})^k((1 + [q^m - 1]\,\zeta^{m/k})^{tk} - 1) < 1. \quad (16)$$

Из неравенства (15) следует, что $H_q(\rho)\ n - n < -k$, поэтому $\zeta < q^{-k}$, т.е.

$$\zeta(q^k - 1) < 1 - q^{-k} \text{ и } (1 + (q-1)\zeta^{1/k}) < (2 - q^{-1})^k = \frac{(2q-1)^k}{q^k}.$$

Поэтому оценка (16) будет следовать из неравенства

$$(1 + (q^m - 1)\zeta^{m/k})^{kt} < 1 + \frac{1}{(2q-1)^k}. \quad (17)$$

Неравенство (17), в свою очередь, следует из оценки

$$kt\ln(1 + (q\zeta^{1/k})^m) < \ln\left(1 + \frac{1}{(2q-1)^k}\right). \quad (18)$$

В силу элементарных неравенств

$$\alpha - (1/2)\alpha^2 < \ln(1 + \alpha) < \alpha \quad \text{при} \quad |\alpha| < 1$$

имеем

$$\ln(1 + (q\zeta^{1/k})^m) < (q\zeta^{1/k})^m,$$

$$\ln(1 + (2q-1)^{-k}) > \frac{1}{(2q-1)^k} - \frac{1}{2(2q-1)^{2k}} > \frac{1}{(2q)^k}.$$

(Последнее неравенство доказано в Приложении (лемма 6)). Неравенство (18) будет следовать из неравенства $kt\,(q\zeta^{1/k})^m < 1/(2q)^k$, т.е. из

$$q\zeta^{1/k} = q^{(1+(1/k)(H_q(\rho)n - n))} < q^{-(1/m)\log(k(2q)^k t)}$$

или

$$H_q(\rho) < 1 - R - R\frac{\log_q(k(2q)^k t)}{m}.$$

Последнее неравенство совпадает с (14). Следовательно, неравенство (16) выполнено, а значит, в силу (13) $|\mathbf{G}_p(d)| < q^{nkp} = |\mathbf{G}_p|$. Теорема доказана. ▲

Следствие 1. *В условиях теоремы* 1, *если* $p \geqslant q^{k(2q)^k}$, *то существует* (np, kp) *КЦ-код с кодовым расстоянием* $\hat{d}$ *таким, что*:

$$H_q\left(\frac{\hat{d}}{np}\right) \geqslant 1 - R - R\frac{\log_q(p)}{m}. \tag{19}$$

Напомним, что $p - 1 = tm$. Теперь, поскольку $q^m \equiv 1 \bmod(p)$, имеем $q^m > p$, т.е. $m > \log_q(p) \geqslant k(2q)^k$. Следовательно, $p > p - 1 = tm \geqslant k(2q)^k t$. Таким образом, (19) следует из (2).

Следствие 2. *Для любого простого числа* $p \geqslant q^{k(2q)^k}$ *существует* (np, kp) *КЦ-код с кодовым расстоянием* $\hat{d}$ *таким, что*

$$H_q\left(\frac{\hat{d}}{np}\right) \geqslant 1 - 2R.$$

Для того чтобы убедиться в этом, еще раз заметим, что всегда $m \geqslant \log_q(p)$ и из (19) следует $H_q\left(\frac{\hat{d}}{np}\right) \geqslant 1 - R - R\frac{\log_q(p)}{m} \geqslant 1 - 2R$. Утверждение содержательно при $R < 1/2$.

Приступим теперь к доказательству асимптотической границы Варшамова–Гилберта. Из оценки (19) следует, что для этого достаточно доказать существование бесконечной последовательности простых чисел p_i, для которых $\frac{\log_q(p_i)}{m_i} \to 0$.

Для дальнейших построений нам потребуются некоторые классические результаты о распределении простых чисел. Пусть $\pi(N)$ – число простых чисел, не превосходящих N. Теорема Чебышева утверждает, что

$$a\frac{N}{\ln(N)} < \pi(N) < b\frac{N}{\ln(N)},$$

где

$$a \geqslant \frac{1}{2}\ln(2), \quad b \leqslant 2\ln(2). \tag{20}$$

Точная асимптотика для $\pi(N)$ следует, из теоремы Адамара и Ла Вале Пуссена, которая состоит в том, что $\lim\limits_{N\to 0}\left(\frac{\pi(N)}{N/\ln(N)}\right) = 1$. Тем самым константы a и b могут быть сделаны сколь угодно близкими к единице для достаточно больших N.

Пусть p – простое число $(p > q)$, m_p – порядок элемента q по модулю p. Пусть $\epsilon \in (0, 1)$ – некоторое число. Введем функцию $\varphi_q(y) = \sqrt{y/(2\log_2 q)}$. Будем называть простое число p "ϵ-плохим", если $m_p \leqslant \varphi_q(\epsilon p)$ и "ϵ-хорошим", если $m_p > \varphi_q(\epsilon p)$. Обозначим через $\beta_\epsilon(N)$ и $\gamma_\epsilon(N)$ соответственно количество ϵ-плохих и ϵ-хороших простых чисел, не превосходящих N. Ясно, что $\pi(N) = \beta_\epsilon(N) + \gamma_\epsilon(N)$. Выведем оценки для $\beta_\epsilon(N)$ и $\gamma_\epsilon(N)$.

Лемма 4.

$$\beta_\epsilon(N) \leqslant \frac{\epsilon N}{\ln(\epsilon N)}; \quad \gamma_\epsilon(N) \geqslant \pi(N) - \frac{\epsilon N}{\ln(\epsilon N)}.$$

Доказательство. Рассмотрим число $A_\epsilon(N) = \prod\limits_{i \leqslant \varphi_q(\epsilon N)}(q^i - 1)$. Заметим, что если p – ϵ-плохое число и $p \leqslant N$, то p делит $A_\epsilon(N)$. В самом деле, p делит $q^{m_p} - 1$, и $m_p \leqslant \varphi_q(\epsilon p) \leqslant \varphi_q(\epsilon N)$, так как p – ϵ-плохое. Тем самым p делит $A_\epsilon(N)$. Следовательно, число $\beta_\epsilon(N)$ не больше числа простых делителей $A_\epsilon(N)$. Оценим сверху

число $A_\epsilon(N)$:

$$A_\epsilon(N) = \prod_{i \leqslant \varphi_q(\epsilon N)} (q^i - 1) \leqslant \prod_{i \leqslant \varphi_q(\epsilon N)} q^i =$$

$$= q^{\left(\sum_{i \leqslant \varphi_q(\epsilon N)} i\right)} \leqslant q^{\varphi_q(\epsilon N)^2} = 2^{(\epsilon N/2)}.$$

Наконец, отметим, что если целое число $M \leqslant 2^R$, то число простых делителей M не больше $\dfrac{2R}{\ln(2R)}$ (см. Приложение, лемма 7). Следовательно,

$$\beta_\epsilon(N) \leqslant \frac{\epsilon N}{\ln(\epsilon N)} \quad \text{и} \quad \gamma_\epsilon(N) = \pi(N) - \beta_\epsilon(N) \geqslant \pi(N) - \frac{\epsilon N}{\ln(\epsilon N)}.$$

Лемма доказана. ▲

Следствие 3. *Пусть* $\epsilon \in (0, 1)$ *– некоторое число. Существует не менее чем* $\pi(N) - \epsilon N/\ln(\epsilon N)$ *простых чисел* p, *не превосходящих* N, *для которых существует* (np, kp) *КЦ-код со скоростью* $R = k/n$ *и кодовым расстоянием* $\hat{d}$ *таким, что при* $p \geqslant q^{k(2q)^k}$

$$H_q\left(\frac{\hat{d}}{np}\right) \geqslant 1 - R - \frac{1}{\sqrt{\epsilon}} R C_q \frac{\log_q(p)}{\sqrt{p}}, \quad C_q = \sqrt{2\log_2 q}.$$

В качестве таких чисел p можно взять все ϵ-хорошие числа. Для этих чисел $m_p > \sqrt{\dfrac{\epsilon p}{2\log_2 q}}$ и остаточный член в (19) допускает оценку:

$$\frac{\log_q(p)}{m_p} \leqslant \frac{1}{\sqrt{\epsilon}} C_q \frac{\log_q(p)}{\sqrt{p}}.$$

Следствие 4. (Асимптотическая граница Варшамова–Гилберта). *Существует бесконечно много простых чисел* p, *для которых найдется* (np, kp) *КЦ-код со скоростью* $R = k/n$, *кодовое расстояние* $\hat{d}$ *которого удовлетворяет неравенству*:

$$H_q\left(\frac{\hat{d}}{np}\right) \geqslant 1 - R - RO\left(\frac{\log_q(p)}{\sqrt{p}}\right). \tag{21}$$

Чтобы в этом убедиться, достаточно в следствии 4 выбрать ϵ из условия $\epsilon < a$ и воспользоваться оценкой (20) из теоремы Чебышева, чтобы показать, что $\gamma_\epsilon(N) \to \infty$ $(N \to \infty)$.

В заключение сделаем еще два замечания.

Из следствия 3 можно получить, что в некотором смысле почти все простые числа p допускают КЦ-коды, удовлетворяющие оценке (21). В самом деле, чем меньше число ϵ, тем меньше доля ϵ-плохих простых чисел среди всех простых чисел, не превосходящих N. Платой за это является рост коэффициента $(1/\sqrt{\epsilon})\, R C_q$ при остаточном члене $\log_q(p)/\sqrt{p}$ в неравенстве (21).

В связи с этим интересен вопрос о существовании последовательности $\{p_i\}$ "δ-очень плохих" простых чисел, т.е. таких, что $\log(p_i)/m_{p_i} \geqslant \delta > 0$. (Для таких последовательностей нельзя доказать асимптотическую границу Варшамова–Гилберта, опираясь на теорему 1). Применяя лемму 4, легко показать, что количество δ-очень плохих простых чисел, не превосходящих N, оценивается сверху величиной $\delta^{-2}(\log^2(N))$. Если же число p не является δ-очень плохим, то следствие 1 гарантирует нам границу $H(\rho) > 1 - (1 + \delta) R$. Из теорем о распределении простых чисел следует, что "подавляющее большинство" простых чисел не являются δ-очень плохими. Примером 1-очень

плохой последовательности для $GF(2)$ могла бы служить последовательность чисел Мерсенна, т.е. простых чисел вида $p = 2^r - 1$, для которых $m_p = r = \log_2(p-1)$. Однако, насколько известно автору, остается открытым вопрос о бесконечности чисел Мерсенна.

§ 3. Границы для почти линейных циклических кодов над $GF(q^n)$

Как было отмечено в работе [3], по квазициклическому (np, kp)-коду над $GF(q)$, имеющему длину np и скорость $R = k/n$, легко построить циклический код длины p над алфавитом из $GF(q^n)$ с той же скоростью R. На i-м месте этого кода следует поместить символ из $GF(q^n)$, который получается прямым произведением элементов из всех n подблоков квазициклического кода, стоящих на i-м месте. Полученный таким образом код не обязательно будет линейным над полем $GF(q^n)$, поскольку его слова можно будет складывать над $GF(q^n)$, а умножать лишь на элементы из $GF(q)$, но не на все элементы из $GF(q^n)$. Подобный код в работе [3] и был назван почти линейным. (Часто такие коды называют групповыми.)

Если кодовое расстояние $\hat{d}$ исходного (np, kp) КЦ-кода над $GF(q)$ удовлетворяло неравенству $H_q(\hat{d}/np) \geqslant 1 - R - o(1)$, то можно утверждать, что кодовое расстояние $\tilde{d}$ (уже в смысле метрики Хэмминга на $GF(q^n)$) построенного почти линейного кода длины p над $GF(q^n)$ удовлетворяет условию $H_q(\tilde{d}/p) \geqslant 1 - R - o(1)$. Однако получившаяся при этом граница $H_q^{-1}(1-R)$ меньше границы Варшамова–Гилберта $H_{q^n}^{-1}(1-R)$, отвечающей полю $GF(q^n)$.

В следующей теореме выводится граница для построенных выше почти линейных кодов скорости $R = k/n$ над полем $GF(q^n)$, из которой следует достижимость истинной границы Варшамова–Гилберта.

Теорема 2. *Пусть p – простое число $(p > q)$, m – порядок элемента q по модулю p; $t = (p-1)/m$. Тогда существует почти линейный код G длины p над $GF(q^n)$ со скоростью $R = k/n$, для которого кодовое расстояние $\tilde{d}$ удовлетворяет неравенству*

$$H_{q^n}\left(\frac{\tilde{d}}{p}\right) \geqslant 1 - R - R\,\frac{\log_q(k(2q)^k t)}{m}.$$

Доказательство. Как и прежде, обозначим $\mathbf{G}_p$ множество всех (np, kp) КЦ-кодов. Пусть d – некоторое число, $\mathbf{G}_p(d)$ обозначает множество кодов $\mathbf{G} \in \mathbf{G}_p$, у которых $W(\mathbf{UG}) \leqslant d$ для некоторого ненулевого циркулянта U. Здесь $W(\mathbf{x})$ обозначает вес Хэмминга вектора $\mathbf{x} = (\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n)$, рассматриваемого уже как элемент пространства $(GF(q^n))^p$. Обозначим

$$\tilde{X}^r\left(\frac{rd}{p}\right) = \left\{ \bar{\mathbf{x}}^r = (\mathbf{x}_1^r, \mathbf{x}_2^r, \ldots, \mathbf{x}_n^r):\ W(\bar{\mathbf{x}}^r) \leqslant \frac{rd}{p} \right\},$$

где $\mathbf{x}_i^r = (x_{i0}, x_{i1}, \ldots, x_{i\,r-1})^T$, $i = \overline{1,n}$ – векторы размерности r. Хэммингов вес W также берется в $GF(q^n)$.

Ясно, что

$$|\tilde{X}^r\left(\frac{rd}{p}\right)| = \sum_{i \leqslant (rd/p)} \binom{r}{i} (q^n - 1)^i < q^{(nH_{q^n}(d/p)r)} = q^{(H_{q^n}(\rho)rn)}.$$

Здесь обозначено $\rho = d/p$.

Теперь можно воспроизвести ход рассуждений доказательства теоремы 1, в котором вместо множества $X^r(rd/p)$ следует использовать $\tilde{X}^r(rd/p)$, а вместо функции $H_q(\cdot)$ подставить $H_{q^n}(\cdot)$, что повлечет за собой подстановку $\zeta = q^{(H_{q^n}(\rho)\,n-n)}$. Все остальные выкладки останутся без изменений. ▲

Все следствия из теоремы 1 могут быть сформулированы и для теоремы 2 с заменой функции $H_q(\cdot)$ на $H_{q^n}(\cdot)$.

§ 4. О границах для систематических КЦ-кодов

В этом параграфе мы распространим результаты § 2 на более узкий класс систематических КЦ-кодов. КЦ-код $G(D) = \{g_{ij}(D)\}_{i=1,\dots,n}^{j=1,\dots,k}$ называется систематически, если $g_{ij}(D) = \delta_{ij}$, $i = \overline{1,k}$, $j = \overline{1,\kappa}$, δ_{ij} – символы Кронекера.

Теорема 3. *В обозначениях теоремы 1 для любого простого числа p найдется систематический (np, kp) КЦ-код со скоростью $R = k/n$, для которого минимальное расстояние $\hat{d}$ удовлетворяет неравенству*

$$H_q\left(\frac{\hat{d}}{np}\right) \geqslant 1 - R - R\,\frac{\log_q(At)}{m}, \quad \text{где } A = k(4q^n)^k. \tag{22}$$

Здесь сразу же заметим, что все следствия из теоремы 1 остаются в силе и для систематических КЦ-кодов заменой условия $p \geqslant q^{k(2q)^k}$ на условие $p \geqslant q^A$.

Доказательство. Предположим, что порождающая матрица $G(D) = \{g_{ij}(D)\}_{i=1,\dots,n}^{j=1,\dots,k}$ имеет обратимую в A_p $k \times k$ подматрицу $G'(D) = \{g_{ij}(D)\}_{i=1,\dots,k}^{j=1,\dots,k}$. Тогда пространство кодовых слов кода $G(D)$ совпадает с пространством кодовых слов систематического кода $\tilde{G}(D) = G(D)\,G'(D)^{-1}$. В самом деле, если $\bar{x}(D)^T = G(D)\,\bar{u}(D)^T$, то $\bar{x}(D)^T = G(D)\,G'(D)^{-1}G'(D)\,\bar{u}(D)^T = \tilde{G}(D)\,\tilde{u}(D)^T$, где $\tilde{u}(D)^T = G'(D)\,\bar{u}(D)^T$. Последнее равенство в силу обратимости матрицы $G'(D)$ задает взаимнооднозначное отображение пространства информационных слов на себя. Следовательно, достаточно доказать теорему 3 для расширенного класса кодов $G(D)$, имеющих обратимую $k \times k$ подматрицу.

Введем в рассмотрение множество $\mathbf{G}'_{p,k}$ $k \times k$ обратимых в A_p матриц $G'(D) = \{g_{ij}(D)\}_{i=1,\dots,k}^{j=1,\dots,k}$, для которых $G'(1) = I$ – единичная матрица.

Лемма 5.

$$|\mathbf{G}'_{p,k}| \geqslant \left(\frac{1}{2}\right)^k q^{k^2(p-1)}.$$

Доказательство. Прежде всего заметим, что если $\det G'(D)$ обратим в A_p, то матрица $G'(D)$ имеет обратную матрицу, которая задается формулой Крамера. Обозначим $M_p(k) = |\mathbf{G}'_{p,k}|$. Ясно, что $M_p(1)$ – число обратимых элементов алгебры A_p, для которых $a(1) = 1$. Докажем неравенство

$$M_p(k) \geqslant M_p(k-1)\,q^{2(k-1)(p-1)}M_p(1). \tag{23}$$

Для этого покажем, как по матрице $G'_{p,k-1}$ из $\mathbf{G}'_{p,k-1}$ построить необходимое количество матриц из $\mathbf{G}'_{p,k}$. Для этого к матрице $G'_{p,k-1}$ добавим k-строку и k-столбец, состоящие из:

а) $2(k-1)$ произвольных элементов $(g_{1,k}(D), \dots, g_{k-1,k}(D))$ и $(g_{k,1}(D), \dots, g_{k,k-1}(D))$, обладающих свойством $g_{i,k}(1) = g_{k,i}(1) = 0$, $i = \overline{1,k-1}$. Таких наборов ровно $q^{2(k-1)(p-1)}$;

б) элемента $g_{k,k}(D)$, который однозначно определяется уже выбранными элементами и ненулевым детерминантом $\delta(D)$ матрицы размера $k \times k$ по формуле разложения детерминанта по последней строке:

$$\delta(D) = g_{k,k}(D)\,A_{k,k}(D) + g_{k,k-1}(D)\,A_{k,k-1}(D) + \dots + g_{k,1}(D)\,A_{k,1}(D)$$

(здесь $A_{k,i}(D)$ обозначает алгебраическое дополнение элемента $g_{k,i}(D)$). Таким образом, каждому обратимому элементу $\delta(D)$ из A_p соответствует единственный элемент $g_{k,k}(D)$ в силу обратимости элемента $A_{k,k}(D) = \det G'_{p,k}(D)$. Следовательно, можно выбрать $M_p(1)$ элементов $g_{k,k}(D)$.

В итоге каждую матрицу из $\mathbf{G}'_{p,k-1}$ можно $q^{2(k-1)(p-1)}M_p(1)$ способами дополнить до матрицы из $\mathbf{G}'_{p,k}$ и оценка (23) доказана.

Покажем теперь, что $M_p(1) \geqslant (1/2)\, q^{p-1}$. В самом деле, из леммы 3 вытекает, что $M_p(1) = N_p(p)\,(q-1)^{-1} = (q^m - 1)^t = q^{p-1}(1 - q^{-m})^t$. Теперь заметим, что

$$(1 - q^{-m})^t \geqslant 1 - tq^{-m} \geqslant 1 - (q^m/m)\, q^{-m} = 1 - 1/m \geqslant 1/2.$$

(Мы воспользовались неравенством Бернулли, а также тем, что из $q^m \equiv 1 \bmod (p)$ следует, что $p - 1 \leqslant q^m$, т.е. $t = (p-1)/m \leqslant q^m/m$. Ясно также, что $m \geqslant 2$, так как $q < p$.) Следовательно,

$$M_p(1) = q^{p-1}(1 - q^{-m})^t \geqslant (1/2)\, q^{p-1}.$$

Применим полученное неравенство к оценке (23):

$$M_p(k) \geqslant M_p(k-1)\, q^{2(k-1)(p-1)} M_p(1) \geqslant$$

$$\geqslant \left(\frac{1}{2}\right)^k q^{(p-1)(1+3+\ldots+2k-1)} = \left(\frac{1}{2}\right)^k q^{k^2(p-1)}.$$

Лемма 5 доказана. ▲

Продолжим доказательство теоремы 3. Как известно, над полем $GF(q)$ существует систематический (n, k)-код с минимальным расстоянием d_1, удовлетворяющим оценке Варшамова–Гилберта $H(d_1/n) \geqslant 1 - R$. Обозначим $n \times k$ матрицу этого кода через G^1. Рассмотрим теперь множество (np, kp) КЦ-кодов $\tilde{\mathbf{G}}_p$, которое задается свойствами: для любой матрицы $G(D) \in \tilde{\mathbf{G}}_p$ ее $k \times k$ подматрица $G'(D)$ принадлежит $\mathbf{G}'_{p,k}$ и $G(1) = G^1$. Из леммы 5 вытекает оценка для $|\tilde{\mathbf{G}}_p|$:

$$|\tilde{\mathbf{G}}_p| \geqslant \left(\frac{1}{2}\right)^k q^{k^2(p-1)} q^{k(n-k)(p-1)} = \left(\frac{1}{2}\right)^k q^{kn(p-1)}. \tag{24}$$

Обозначим $\tilde{\mathbf{G}}_p(d)$ множество, аналогичное $\mathbf{G}_p(d)$.

Если воспользоваться ходом рассуждений теоремы 1, то для числа $|\tilde{\mathbf{G}}_p(d)|$ получится оценка (12), в которой, однако, можно опустить Σ_1, т.е. те слагаемые, для которых $r = \max\{r_1, \ldots, r_k\} = 1$. В самом деле, если для некоторого информационного слова $\bar{u}(D) = (u_1(D), \ldots, u_k(D))$ величина r равна 1, то в силу леммы 1 и леммы 3 $u_i(D) = T(D)\,\alpha_i$, где $T(D) = (D^p - 1)/(D - 1) = 1 + D + \ldots + D^p$, $\alpha_i \in GF(q)$, $i = \overline{1,k}$. Тем самым кодовое слово $x(D) = (x_1(D), \ldots, x_n(D))$ имеет вид

$$x_i(D) = \sum_{j=1}^{k} u_j(D)\, g_{ij}(D) = \sum_{j=1}^{k} \alpha_j T(D)\, g_{ij}(D) = T(D)\Big(\sum_{j=1}^{k} \alpha_j g_{ij}(D)\Big).$$

Заметим, что $T(D)\, g(D) = T(D)\, g(1) \bmod (D^p - 1)$ для любого многочлена $g(D)$. Следовательно, $\bar{x}(D) = T(D)\, G^1 \bar{\alpha}^T$, где $\bar{\alpha} = (\alpha_1, \ldots, \alpha_k)$. Поэтому $W(\bar{x}(D)) = pW(G^1 \bar{\alpha}^T) \geqslant pd_1$ лежит выше границы Варшамова–Гилберта, т.е. информационные слова $\bar{u}(D)$, для которых $r = 1$, не портят минимальное расстояние кодов из $\tilde{\mathbf{G}}_p$. Это, в свою очередь, означает, что в оценке для $|\tilde{\mathbf{G}}_p(d)|$ можно исключить слагаемое Σ_1. В итоге приходим к неравенству

$$|\tilde{\mathbf{G}}_p(d)| < q^{knp}\left\{(1 + (q-1)\zeta^{1/k})^k ((1 + [q^m - 1]\,\zeta^{m/k})^{tk} - 1)\right\}. \tag{25}$$

Дальнейшие рассуждения повторяют ход доказательства теоремы 1. Аналогичным образом проверяется, что если число d не удовлетворяет неравенству (22), то имеет место оценка

$$(1 + (q-1)\zeta^{1/k})^k ((1 + [q^m - 1]\,\zeta^{m/k})^{tk} - 1) < \left(\frac{1}{2}\right)^k \left(\frac{1}{q}\right)^{kn},$$

т.е. в силу (25) и (24)

$$|\tilde{\mathbf{G}}_p(d)| < \left(\frac{1}{2}\right)^k \left(\frac{1}{q}\right)^{kn} q^{knp} \leqslant |\tilde{\mathbf{G}}_p|.$$

Теорема доказана. ▲

В заключение автор выражает глубокую признательность А.Н. Скоробогатову и И.Е. Шпарлинскому за полезные консультации в области теории чисел и обсуждение доказательства леммы 4.

ПРИЛОЖЕНИЕ

Лемма 6. *Если* $k \geqslant 1, q \geqslant 2$, *то* $\dfrac{1}{(2q-1)^k} - \dfrac{1}{2(2q-1)^{2k}} > \dfrac{1}{(2q)^k}$.

Доказательство. Обозначим для удобства $\epsilon = 1/(2q-1)$. Ясно, что $0 < \epsilon \leqslant 1/3$. Доказываемое неравенство примет вид

$\epsilon^k - (1/2)\,\epsilon^{2k} > \epsilon^k/(1+\epsilon)^k$, т.е. $1 - (1/2)\,\epsilon^k > 1/(1+\epsilon)^k$.

Из неравенства Бернулли следует, что $1/(1+\epsilon)^k < 1/(1+\epsilon k)$, поэтому достаточно проверить неравенство $1 - (1/2)\,\epsilon^k > 1/(1+\epsilon k)$, т.е. $k > (1/2)\,\epsilon^{k-1}(1+\epsilon)$. Последнее неравенство очевидно, так как

$(1/2)\,\epsilon^{k-1}(1+\epsilon) < (1/2)(1+\epsilon) \leqslant (1/2)(1+1/3) < 1 \leqslant k$. ▲

Лемма 7. *Целое число* $M \leqslant 2^R$ *имеет не более* $\dfrac{2R}{\ln(2R)}$ *простых делителей.*

Доказательство. Обозначим k число различных простых делителей M. Нетрудно установить, что $k! < M$, т.е. $k! < 2^R$. Из простого неравенства $(k/e)^k < k!$ следует, что $(k/e)^k < 2^R$, т.е. $k\ln(k) - k < R\ln(2)$.

Покажем, что $k < 2R/\ln(2R)$. В самом деле, функция $\varphi(k) = k\ln(k) - k$ монотонно возрастает, поэтому достаточно проверить неравенство $\varphi(2R/\ln(2R)) \geqslant R\ln(2)$, или после тождественных преобразований

$(1 - (1/2)\ln(2))\ln(2R) \geqslant 1 + \ln(\ln(R))$.

Легко убедиться в том, что последнее неравенство имеет место при $R > 16$. Следовательно, лемма доказана для $R > 16$. Для $R \leqslant 16$ утверждение можно проверить непосредственно, при этом его достаточно проверить лишь для чисел $M \leqslant 2^{16}$, которые имеют вид произведения первых подряд идущих простых чисел: $2 \cdot 3$, $2 \cdot 3 \cdot 5$, и т.д. до $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$. ▲

СПИСОК ЛИТЕРАТУРЫ

1. *Chen C.L., Peterson W.W., Weldom E.J.* Some Results on Quasi-Cyclic Codes//Inform. and Control. 1969. V. 15. № 5. P. 407–423.
2. *Kasami T.* A Gilbert–Varshamov Bound for Quasi-Cyclic Codes of Rate 1/2//IEEE Trans. Inform. Theory. 1974. V. 20. № 5. p. 679.
3. *Кабатянский Г.А.* О существовании хороших циклических почти линейных кодов над непростыми полями//Пробл. передачи информ. 1977. Т. 13. № 3. С. 18–21.
4. *Крук Е.А.* Передача сообщений обобщенными квазициклическими кодами по дискретным каналам связи. Дис. . . . канд. физ.-мат наук. Л., 1978.
5. *Lidl R., Niederreiter H.* Finite Fields. Encyclopedia of Mathematics and Applications. V. 20. Reading: Addison–Wesley. 1983.

Поступила в редакцию
26.03.91