Math-Net.Ru

Общероссийский математический портал

С. Гонсалес, Е. Коусело, В. Марков, А. Нечаев, Параметры рекурсивных МДР-кодов, *Дискрет. матем.*, 2000, том 12, выпуск 4, 3–24

DOI: <https://doi.org/10.4213/dm353>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 35.173.219.12

26 апреля 2023 г., 06:34:07

Параметры рекурсивных МДР-кодов

© 2000 г. С. Гонсалес, Е. Коусело, В. Марков, А. Нечаев

Полный рекурсивный m -код длины $n > m$ в алфавите из $q \geq 2$ элементов — это множество всех отрезков длины n рекуррентных последовательностей, удовлетворяющих некоторому фиксированному закону рекурсии $f(x_1, \dots, x_m)$. Изучаются условия, при которых существует такой код с расстоянием $n - m + 1$ (рекурсивный МДР-код). Пусть $\nu^r(m, q)$ — максимум чисел n с указанным свойством. В предыдущей статье авторов было отмечено, что условие $\nu^r(m, q) \geq n$ равносильно существованию m -квазигруппы f , которая вместе со своими $n - m - 1$ последовательными рекурсивными производными образует ортогональную систему m -квазигрупп (латинских квадратов для $m = 2$), и доказано, что $\nu^r(m, q) \geq 4$ для всех значений $q \in \mathbf{N}$ за исключением, возможно, шести из них. Здесь эта оценка усиливается для ряда значений $q < 100$ и приводятся некоторые нижние оценки $\nu^r(m, q)$ для $m > 2$, основанные на изучении линейных рекурсивных кодов. В частности, доказано, что $\nu^r(m, q) \geq q + 1$ для примарных q и $m \in \{1, \dots, q\}$ и $\nu^r(2^t - 1, 2^t) = 2^t + 2$ для $t = 2, 3, 4$. Кроме того, доказано, что существует линейный рекурсивный $[6, 3, 4]$ -МДР-код над группой $Z_2 \oplus Z_2$, но не существует такого линейного рекурсивного кода над полем F_4 .

1. Основные определения и результаты

Пусть $\Omega = \{a_1, \dots, a_q\}$ — конечный алфавит и $f: \Omega^m \rightarrow \Omega$ — произвольная функция. Полным m -рекурсивным кодом длины $n \geq m$ над Ω называется код $\mathcal{K}(n, f)$, состоящий из всех слов вида

$$u(0, n-1) = (u(0), \dots, u(n-1)) \in \Omega^n,$$

где $u(i+m) = f(u(i), \dots, u(i+m-1))$, $i = 0, 1, \dots, n-m-1$, и $u(0, m-1)$ — произвольная строка из Ω^m . Таким образом, $\mathcal{K}(n, f)$ — систематический $[n, m]$ -код, и его расстояние Хэмминга d удовлетворяет неравенству $d \leq n - m + 1$ (граница Синглтона [1]). Мы исследуем, в основном, параметр $\nu^r(m, q)$, максимальное число n такое, что для некоторой функции $f: \Omega^m \rightarrow \Omega$ расстояние кода $\mathcal{K}(n, f)$ равно $d = n - m + 1$, то есть $\mathcal{K}(n, f)$ является МДР-кодом. В [2] отмечено, что код $\mathcal{K}(n, f)$ имеет вид

$$\mathcal{K}(n, f) = \{v(1, n) = (v(1, m), f^{(0)}(v(1, m)), \dots, f^{(n-m-1)}(v(1, m))), v(1, m) \in \Omega^m\} \quad (1.1)$$

где

$$\begin{aligned} f^{(0)}(\vec{x}) &= f^{(0)}(x_1, \dots, x_m) = f(\vec{x}), \\ f^{(1)}(\vec{x}) &= f(x_2, \dots, x_m, f^{(0)}(\vec{x})), \\ f^{(t)}(\vec{x}) &= f(x_{t+1}, \dots, x_m, f^{(0)}(\vec{x}), \dots, f^{(t-1)}(\vec{x})), \quad t < m, \\ f^{(t)}(\vec{x}) &= f(f^{(t-m)}(\vec{x}), \dots, f^{(t-1)}(\vec{x})), \quad t \geq m. \end{aligned} \quad (1.2)$$

Функция $f^{(t)}(\vec{x})$ из (1.2) называется рекурсивной производной порядка t функции $f(\vec{x})$.

Предложение 1. Код $\mathcal{H}(n, f)$ является МДР-кодом тогда и только тогда, когда выполняются следующие два условия:

- (1) любая функция $f^{(t)}(\vec{x})$, $t = 0, 1, \dots, n - m - 1$, является m -квазигруппой, то есть любое уравнение

$$f^{(t)}(c_1, \dots, c_{s-1}, x_s, c_{s+1}, \dots, c_m) = c_s$$

имеет единственное решение $x_s \in \Omega$;

- (2) система функций $f^{(0)}, \dots, f^{(n-m-1)}$ является ортогональной системой m -квазигрупп, то есть значения любых m функций из множества

$$x_1, \dots, x_m, f^{(0)}(\vec{x}), \dots, f^{(n-m-1)}(\vec{x})$$

однозначно определяют значения остальных $n - m$ функций из этого множества.

В первом случае функция $f(\vec{x})$ называется рекурсивно $(n - m - 1)$ -дифференцируемой m -квазигруппой, а во втором — $(n - m - 1)$ -стабильной m -квазигруппой. Конечно, из второго условия следует первое, однако при $m > 2$ обратное неверно (см. [2]).

Если $m = 2$, то первое условие означает, что таблица Кэли каждой бинарной операции $f^{(t)}(x_1, x_2)$ является латинским квадратом, а второе условие означает, что $f^{(0)}, \dots, f^{(n-3)}$ является системой попарно ортогональных латинских квадратов. В этом случае справедливо следующее утверждение.

Теорема 1 ([2]). Квазигруппа $f(x_1, x_2)$ рекурсивно t -дифференцируема тогда и только тогда, когда она t -стабильна, то есть из первого условия следует второе при $m = 2$.

Таким образом, чтобы доказать неравенство $\nu^r(2, q) \geq 4$ (это первая нетривиальная оценка при $m = 2$), достаточно построить 1-дифференцируемую квазигруппу порядка q . В [2] было показано, что последнее неравенство справедливо для всех натуральных чисел q кроме, конечно, $q \in \{2, 6\}$ и, возможно, $q \in \{14, 18, 26, 42\}$.

Ниже мы усиливаем нижнюю оценку параметра $\nu^r(2, q)$ для ряда значений $q \in \{21, \dots, 99\}$ (таблица 1 и теорема 2) и получаем первые нетривиальные результаты для $m > 2$, основанные на изучении линейных рекурсивных кодов.

Для более точного описания постановки задач и полученных результатов введем следующие обозначения и понятия.

Назовем код $\mathcal{K} \subset \Omega^n$ линейным (в широком смысле), если существует некоторая операция $+$ на Ω такая, что $(\Omega, +)$ — абелева группа и $\mathcal{K}$ — подгруппа в $(\Omega^n, +)$, $\mathcal{K} < (\Omega^n, +)$. Заметим, что если P — конечное поле, то в соответствии с классическим определением код $\mathcal{K}$ называется линейным, если он является P -подпространством в P^n . Мы будем называть такие коды линейными в классическом (или узком) смысле. Эти понятия совпадают тогда и только тогда, когда $q = |\Omega|$ — простое число.

Пусть $\lambda(m, q)$ — максимум длин линейных m -мерных МДР-кодов над алфавитом из q элементов (для любого $q \in \mathbf{N}$) и $\mu(m, q)$ — аналогичный параметр для линейных кодов в классическом смысле (определен только для примарных q). По аналогии с $\nu^r(m, q)$ мы вводим параметры $\lambda^r(m, q)$ для любого q и $\mu^r(m, q)$ только для примарных q . Далее, назовем функцию $f: \Omega^n \rightarrow \Omega$ и соответствующий код $\mathcal{K}(n, f)$ идемпотентными, если выполнено тождество $f(x, \dots, x) = x$. Последнее равносильно условию, что код $\mathcal{K}(n, f)$ содержит все константы, то есть $(a, \dots, a) \in \mathcal{K}(n, f)$ для любого $a \in \Omega$. В дополнение к предшествующим 6 параметрам определим $\nu^r(m, q)$ как максимум длин идемпотентных рекурсивных m -мерных МДР-кодов и аналогичные параметры $\lambda^r(m, q)$ и $\mu^r(m, q)$ для случая линейных и линейных в классическом смысле кодов, соответственно.

Итак, получаем матрицу параметров

$$M(m, q) = \begin{pmatrix} [\mu^{ir}(m, q) & \mu^r(m, q) & \mu(m, q)] \\ \lambda^{ir}(m, q) & \lambda^r(m, q) & \lambda(m, q) \\ \nu^{ir}(m, q) & \nu^r(m, q) & \nu(m, q) \end{pmatrix}$$

элементы которой не убывают по строкам слева направо и по столбцам сверху вниз. Естественно, первая строка матрицы (заключенная в квадратные скобки) присутствует только тогда, когда q — примарное число. Интересно оценить и сравнить элементы матрицы $M(m, q)$ для различных значений m и q . В дальнейшем равенство $x^{yz}(m, q) = t$ означает, что соответствующей m -квазигруппы не существует. Для оценки указанных выше параметров можно использовать следующие два факта.

Предложение 2 ([2]). *Если q — примарное число (то есть степень простого числа), то*

$$\mu^r(2, q) = \nu(2, q) = q + 1.$$

Предложение 3. *Для любых $x \in \{\lambda, \nu\}$, $y \in \{\emptyset, r, ir\}$ и $m, q_1, q_2 \in \{2, \dots, \infty\}$ выполняется неравенство*

$$x^y(m, q_1 q_2) \geq \min\{x^y(m, q_1), x^y(m, q_2)\}$$

Ниже мы будем говорить, что оценка соответствующего параметра матрицы $M(m, q)$ является стандартной, если она следует из этих двух фактов.

Мы будем также использовать следующие результаты.

Предложение 4 ([2]). *Если $p \geq 3$ — простое число, то $\mu^{ir}(2, p) \geq p$.*

Предложение 5 ([2]). *Если $q \geq 3$ — примарное число, то $\mu^{ir}(2, q) \geq q - 1$.*

При $m = 2$ и малых значениях q (иногда с использованием компьютера) получе-

Таблица 1. Нижние границы параметров $\nu^r(2, q)$ и $\nu(2, q)$

	0	1	2	3	4	5	6	7	8	9
0(100)	$\frac{5}{10}$	∞/∞	$\frac{3}{3}^*$	$\frac{4}{4}^*$	$\frac{5}{5}^*$	$\frac{6}{6}^*$	$\frac{3}{3}$	$\frac{8}{8}^*$	$\frac{9}{9}^*$	$\frac{10}{10}^*$
10	$\frac{4}{4}$	$\frac{12}{12}^*$	$\frac{4}{7}$	$\frac{14}{14}^*$	$\frac{?}{5}$	$\frac{4}{6}$	$\frac{17}{17}^*$	$\frac{18}{18}^*$	$\frac{?}{5}$	$\frac{20}{20}^*$
20	$\frac{5}{6}$	$\frac{5}{6}$	$\frac{4}{5}$	$\frac{24}{24}^*$	$\frac{5}{6}$	$\frac{26}{26}^*$	$\frac{?}{5}$	$\frac{28}{28}^*$	$\frac{5}{5}$	$\frac{20}{20}^*$
30	$\frac{4}{5}$	$\frac{32}{32}^*$	$\frac{33}{33}^*$	$\frac{4}{6}$	$\frac{4}{5}$	$\frac{6}{6}$	$\frac{4}{5}$	$\frac{38}{38}^*$	$\frac{4}{5}$	$\frac{5}{6}$
40	$\frac{4}{6}$	$\frac{42}{42}^*$	$\frac{?}{5}$	$\frac{44}{44}^*$	$\frac{5}{5}$	$\frac{4}{5}$	$\frac{4}{6}$	$\frac{48}{48}^*$	$\frac{4}{6}$	$\frac{50}{50}^*$
50	$\frac{7}{8}$	$\frac{4}{6}$	$\frac{5}{5}$	$\frac{54}{54}^*$	$\frac{6}{6}$	$\frac{6}{7}$	$\frac{8}{9}$	$\frac{7}{9}$	$\frac{7}{7}$	$\frac{60}{60}^*$
60	$\frac{5}{6}$	$\frac{62}{62}^*$	$\frac{6}{6}$	$\frac{8}{8}$	$\frac{65}{65}^*$	$\frac{7}{9}$	$\frac{6}{7}$	$\frac{68}{68}^*$	$\frac{6}{7}$	$\frac{6}{8}$
70	$\frac{7}{8}$	$\frac{72}{72}^*$	$\frac{9}{9}$	$\frac{74}{74}^*$	$\frac{6}{7}$	$\frac{6}{7}$	$\frac{6}{7}$	$\frac{8}{8}$	$\frac{7}{8}$	$\frac{80}{80}^*$
80	$\frac{8}{9}$	$\frac{82}{82}^*$	$\frac{6}{10}$	$\frac{84}{84}^*$	$\frac{7}{8}$	$\frac{7}{8}$	$\frac{7}{8}$	$\frac{6}{8}$	$\frac{9}{9}$	$\frac{90}{90}^*$
90	$\frac{6}{6}$	$\frac{8}{8}$	$\frac{7}{7}$	$\frac{6}{6}$	$\frac{7}{7}$	$\frac{7}{7}$	$\frac{7}{7}$	$\frac{98}{98}^*$	$\frac{7}{7}$	$\frac{10}{10}$

ны равенства

$$M(2, 2) = \begin{pmatrix} 2 & 3 & 3 \\ 2 & 3 & 3 \\ 2 & 3 & 3 \end{pmatrix}; \quad M(2, 3) = \begin{pmatrix} 3 & 4 & 4 \\ 3 & 4 & 4 \\ 3 & 4 & 4 \end{pmatrix}; \quad M(2, 4) = \begin{pmatrix} 3 & 5 & 5 \\ 3 & 5 & 5 \\ 3 & 5 & 5 \end{pmatrix};$$

$$M(2, 5) = \begin{pmatrix} 5 & 6 & 6 \\ 5 & 6 & 6 \\ 5 & 6 & 6 \end{pmatrix}; \quad M(2, 7) = \begin{pmatrix} 7 & 8 & 8 \\ 7 & 8 & 8 \\ 7 & 8 & 8 \end{pmatrix}$$

и, разумеется (Эйлер),

$$M(2, 6) = \begin{pmatrix} 2 & 3 & 3 \\ 3 & 3 & 3 \end{pmatrix}.$$

Основные новые результаты для $m = 2$, $q \leq 100$ представлены в таблице 1 нижних границ параметров $\nu^r(2, q)$. Клетка на пересечении строки, отмеченной слева числом i , и столбца, отмеченного числом j , соответствует числу $q = i + j$, за исключением верхней левой клетки, соответствующей $q = 100$. Таблица содержит также известные нижние границы для $\nu(2, q)$ (знаменатели дробей), взятые из рис. 1 книги [3]. Нижние оценки для $\nu^r(2, q)$ (числители дробей) либо стандартны (не подчеркнуты), либо получены в [2] (подчеркнутые значения, равные 4), либо доказаны в следующем разделе (остальные подчеркнутые значения). Клетки, помеченные звездочкой в правом верхнем углу, соответствуют примарным числам.

Наши результаты для случая $m \geq 3$ связаны с исследованием параметров $\lambda^r(m, q)$, $\mu^r(m, q)$. Прежде всего напомним некоторые известные оценки, которые собраны из разных источников и частично усилены в [1, 4].

Теорема 2. (1) Если $q \leq m$, то $\nu(m, q) = m + 1$.

(2) Если $m < q$, то $\nu(m, q) \leq q + m - 1$.

- (3) Если $3 \leq m \leq q$ и q нечетно, или $4 \leq m \leq q$ и q не делится на 18, или $3 \leq m \leq q$, $q \equiv 1, 2 \pmod{4}$ и существует простое $p \equiv 3 \pmod{4}$, входящее в каноническое разложение q в нечетной степени (в частности, если $q \equiv 6 \pmod{8}$), то $\nu(m, q) \leq q + m - 2$.
- (4) Если $3 \leq m \leq q$, q четно и $(m-1)!$ не делит $(q-2)q(q+1) \dots (q+m-4)$, или $4 \leq m \leq q$ и q не делится на 9, то $\nu(m, q) \leq q + m - 3$.
- (5) Если $m < q$ и q примарно (то есть q — степень простого числа), то $\nu(m, q) \geq q + 1$.
- (6) $\nu(3, q) = q + 1$ для любого примарного нечетного q .
- (7) $\nu(3, 2^t) = \nu(2^t - 1, 2^t) = 2^t + 2$ для $t \geq 2$.

Для линейных в классическом смысле кодов имеются более точные результаты. Для произвольных $m \in \mathbb{N}$ и примарного q введем функцию

$$\mu^*(m, q) = \begin{cases} m + 1, & \text{если } m \geq q, \\ q + 2, & \text{если } q \text{ четно и } m \in \{3, q - 1\}, \\ q + 1 & \text{в остальных случаях.} \end{cases}$$

Имеет место неравенство $\mu(m, q) \geq \mu^*(m, q)$. В [5, 4] высказана гипотеза, что

$$\mu(m, q) = \mu^*(m, q). \quad (1.3)$$

Эта гипотеза доказана, в частности, в случаях, когда

$$m \in \{1, \dots, 5\} \cup \{q - 3, \dots, \infty\} \quad (\text{см. [6, 7, 8, 9, 10]}),$$

$$q \leq 11 \quad (\text{см. [11, 12, 13]}),$$

$$q \text{ нечетно, } q > (4m - 9)^2 \quad (\text{см. [8]}).$$

Далее важны также следующие известные результаты.

Теорема 3 ([14, 4]). Для заданных примарного q и $m \in \{1, \dots, q + 1\}$ существует линейный над $GF(q)$ циклический $[q + 1, m, q - m + 2]$ -код тогда и только тогда, когда q четно или m нечетно.

Так как любой циклический код над полем рекурсивен, эта теорема дает оценку $\mu^r(m, q) \geq q + 1$ для указанных m, q . Для нечетных q и четных m не существует линейных над $GF(q)$ циклических $[q + 1, m, q - m + 2]$ -кодов (см. [14]), и в этих случаях последнее неравенство не следует из теоремы 3. Здесь приходится отметить ошибку в теореме 11.9 из [1], где теорема 3 приведена без ограничений на m для нечетного q (но и без доказательств для этого случая). Эти результаты могут быть усилены следующим образом.

Прежде всего приведем более подробное описание линейного рекурсивного кода. Пусть $(M, +)$ — конечная абелева группа и $A = \text{End}_{\mathbb{Z}} M$ — ее кольцо эндоморфизмов с единицей e . Группа $(M, +)$ есть естественный A -модуль, на котором операция умножения элементов $\alpha \in M$ слева на элементы $f \in A$ определяется равенством

$f\alpha = f(\alpha)$. Для произвольного унитарного (со старшим коэффициентом e) многочлена

$$F(x) = x^m - f_{m-1}x^{m-1} - \dots - f_1x - f_0 \in A[x] \quad (1.4)$$

обозначим через $L_M(F)$ множество всех линейных рекуррентных последовательностей (ЛРП) над M с характеристическим многочленом $F(x)$, то есть множество всех последовательностей (функций) $u: \mathbf{N}_0 \rightarrow M$, удовлетворяющих соотношениям

$$u(i+m) = f_{m-1}u(i+m-1) + \dots + f_1u(i+1) + f_0u(i).$$

Каждая такая рекуррента однозначно определяется своим начальным отрезком

$$u(0, m-1) = (u(0), \dots, u(m-1))$$

и, как нетрудно увидеть, группа $L_M(F)$ изоморфна группе $(M^m, +)$. Для произвольного $n \in \mathbf{N}$, $n \geq m$, рассмотрим множество

$$\mathcal{K} = L_M^{0, n-1}(F) = \{u(0, n-1) \in M^n : u \in L_M(F)\} \quad (1.5)$$

всех начальных отрезков $u(0, n-1) = (u(0), \dots, u(n-1))$ длины n линейных рекуррент $u \in L_M(F)$. Это — подгруппа группы M^n , изоморфная M^m . В частности, $\mathcal{K}$ — систематический $[n, m, d]$ -код с системой определяющих позиций $0, 1, \dots, m-1$ и расстоянием Хэмминга

$$d(\mathcal{K}) = d \leq n - m + 1.$$

Код (1.5) представляет собой линейный в широком смысле рекурсивный код над группой M в общем виде. Если $M = GF(q)$ — поле из q элементов и коэффициенты f_s многочлена $F(x)$ суть не произвольные эндоморфизмы группы $(M, +)$, а гомоморфизмы поля, то есть, попросту — элементы поля M , то (1.5) есть общий вид линейного в классическом смысле рекурсивного кода над полем. Последний код является циклическим тогда и только тогда, когда $F(x)$ — реверсивный многочлен и его период делит n , то есть $F(x) \mid x^n - e$.

Теорема 4. Для любого примарного q и любого $m \in \{1, \dots, q\}$ справедливо неравенство $\mu^r(m, q) \geq q + 1$. Пусть γ — элемент порядка $q + 1$ из расширения $Q = GF(q^2)$ поля $P = GF(q)$, $\beta \in Q$ — элемент такой, что

$$\beta^{q-1} = \gamma^{m-1}, \quad (1.6)$$

и пусть

$$\beta_i = \beta\gamma^i, \quad i \in \{0, 1, \dots, m-1\}. \quad (1.7)$$

Тогда многочлен

$$F(x) = (x - \beta_0) \dots (x - \beta_{m-1}) \quad (1.8)$$

принадлежит $P[x]$ и $\mathcal{K} = L_P^{0, q+1}(F)$ есть $[q+1, m, q-m+2]_q$ -код. В частности, если q четно, или m нечетно, то элемент β можно выбрать так, что его порядок равен $q+1$, и тогда $\mathcal{K}$ — циклический код.

Таким образом, из теоремы 4 следует теорема 3 в части, касающейся существующих циклических кодов.

Более того, пусть $N_q^r(n, m)$ — число различных линейных над полем $P = GF(q)$ рекурсивных $[n, m, n - m + 1]$ -кодов и $\varphi(x)$ — функция Эйлера. Мы имеем основания предполагать, что теорема 4 описывает все линейные рекурсивные и, в частности, циклические коды над полем, и справедлива следующая гипотеза. Для любого примарного $q \geq 3$ и любого $m \in \{2, \dots, q - 2\}$ имеют место равенства

$$\mu^r(m, q) = q + 1, \quad (1.9)$$

$$N_q^r(m, q + 1) = (q - 1)(\varphi(q + 1)/2). \quad (1.10)$$

В подтверждение этой гипотезы мы можем привести, в дополнение к указанным выше, следующие результаты.

Теорема 5. В обозначениях теоремы 4 для любого $m \in \{2, \dots, q - 2\}$ существует $(q - 1)(\varphi(q + 1)/2)$ различных многочленов вида (1.8) таких, что $\mathcal{H}$ — МДР-код. Справедливо неравенство

$$N_q^r(m, q + 1) \geq (q - 1)(\varphi(q + 1)/2).$$

Заметим, что если гипотеза (1.10) верна, то из последней теоремы следует, что теоремой 4 описаны все линейные рекурсивные МДР-коды и результат [14] об отсутствии циклических кодов получается как следствие теоремы 4. Вычисления на компьютере в некоторых частных случаях дали следующие точные результаты.

Предложение 6. Для всех примарных $q \in \{4, \dots, 128\}$ при $m = 3$ и для всех примарных $q \in \{3, \dots, 13\}$ при любых $m \in \{2, \dots, q - 1\}$, за исключением случаев $q = 8, m = 7$, справедливо равенство

$$\mu^r(m, q) = q + 1.$$

Более того, если $m \in \{2, \dots, q - 2\}$, то в каждом из этих случаев

$$N_q^r(m, q + 1) = (q - 1)(\varphi(q + 1)/2).$$

Отметим также равенство $\mu^r(12, 13) = 14$, которое представляет собой дальнейшее подтверждение гипотезы (1.3). Наконец, справедлива следующая теорема.

Теорема 6 ([16, 17, 18]). Для любого $q = 2^t \geq 8$

$$\mu^r(3, q) = \lambda^r(3, q) = q + 1$$

и

$$\mu^r(3, 4) = 5 < \lambda^r(3, 4) = \nu^r(3, 4) = \mu(3, 4) = \nu(3, 4) = 6.$$

Интересно отметить, что при переходе от $m = q - 2$ к $m = q - 1$ значение параметра $N_q^r(q + 1, m)$ резко возрастает. Это — отражение следующего более общего факта.

Предложение 7. Если q примарно и $m \leq q - 1$, то

$$N_q^r(m + 2, m) = (q - 1) \dots (q - m). \quad (1.11)$$

Для многочлена

$$F(x) = x^m - f_{m-1}x^{m-1} - \dots - f_1x^1 - f_0$$

над полем $P = GF(q)$ код $L_P^{0,m+1}(F)$ есть МДР-код тогда и только тогда, когда

$$\begin{aligned} f_i &\in S_0 = P^*, & i &\in \{0, 1, \dots, m-1\}, \\ f_{m-2} &\in S_1 = P^* \setminus \{-f_{m-1}^2\}, \\ f_{m-3} &\in S_2 = P^* \setminus \{-f_{m-1}f_{m-2}, f_{m-1}^{-1}f_{m-2}^2\}, \\ &\dots \\ f_{m-i-1} &\in S_i = P^* \setminus \{-f_{m-1}f_{m-i}, f_{m-i+1}^{-1}f_{m-i}^2, \dots, f_{m-1}^{-1}f_{m-i}f_{m-2}\}, \\ &\dots \\ f_0 &\in S_m = P^* \setminus \{-f_{m-1}f_2, f_3^{-1}f_2^2, f_4^{-1}f_2f_3, \dots, f_{m-1}^{-1}f_2f_{m-2}\}. \end{aligned}$$

В частности,

$$N_q^r(q+1, q-1) = (q-1)!.$$

Остается не исследованным до конца значение параметра $\mu^r(2^t-1, 2^t)$; вычисления на компьютере показали, что

$$\mu^r(2^t-1, 2^t) = 2^t + 2, \quad t = 3, 4. \quad (1.12)$$

Переход от линейных рекурсивных МДР-кодов над полем к линейным рекурсивным в широком смысле МДР-кодам дает лучшее приближение к гипотезе (1.3). Разумеется, для простого q справедливо равенство

$$\lambda^r(m, q) = \mu^r(m, q).$$

Вычисления на компьютере дали следующие результаты.

Предложение 8. Если $q \in \{4, 8, 9\}$ и $m \in \{2, \dots, q-1\}$, то $\lambda^r(m, q) = q+2$ для $q \in \{4, 8\}$, $m = q-1$ и $\lambda^r(m, q) = q+1$ для остальных значений q и m .

В заключение приведем без доказательства следующий результат относительно линейных в широком смысле рекурсивных $[2^t+2, 2^t-1, 4]$ -кодов над $\mathbf{Z}_{2^t}$, названных в [18] Астурийскими.

Теорема 7. Для любого $q = 2^t \geq 4$, расширенный $[q+2, q-1, 4]$ -код Руда-Соломона над $GF(q)$ с проверочной матрицей

$$H = \begin{pmatrix} 1 & 1 & \dots & 1 & 1 & 0 & 0 \\ 1 & \alpha_1 & \dots & \alpha_{q-2} & 0 & 1 & 0 \\ 1 & \alpha_1^{2^{t-1}} & \dots & \alpha_{q-2}^{2^{t-1}} & 0 & 0 & 1 \end{pmatrix}$$

линейно в широком смысле эквивалентен линейному рекурсивному циклическому коду над $\mathbf{Z}_2^t$. Таким образом, справедливо неравенство

$$\lambda^r(q-1, q) \geq q+2.$$

Первый Астурийский код есть $[6, 3, 4]$ -код над полем $GF(4) = \{0, 1, \alpha, \alpha+1\}$ с законом рекурсии

$$u(i+3) = u^2(i+2) + \alpha u(i+1) + \alpha u^2(i).$$

Рис. 1.

2. Псевдогеометрии с нуклеусами

Понятие псевдогеометрии (см. [19]) было использовано в [2] для доказательства неравенства $\nu^r(2, q) \geq 4$. Здесь мы напомним его и рассмотрим несколько более сложную конструкцию.

Назовем пару $(P, \mathcal{L})$ псевдогеометрией (PG), если P — некоторое непустое множество (элементы которого будем называть точками) и $\mathcal{L}$ — некоторое множество непустых подмножеств P (называемых прямыми) такое, что каждые две различные точки принадлежат ровно одной прямой.

Пример 1. В качестве примера рассмотрим основную для наших целей конструкцию, сопровождающую псевдогеометрию для множества попарно ортогональных латинских квадратов.

Пусть q — натуральное число, и пусть существует множество из k попарно ортогональных латинских квадратов порядка q

$$\{f_i: (\{0, 1, \dots, q-1\})^2 \rightarrow \{0, 1, \dots, q-1\}, i \in \{1, \dots, k\}.$$

Рассмотрим множество P всех пар (x, y) точек декартовой плоскости таких, что $x \in \{0, 1, \dots, q-1\}$, $y \in \{-1, \dots, k\}$. Определим прямые двух типов: горизонтальные прямые

$$\{(x, y): x \in \{0, 1, \dots, q-1\}\}, \quad y \in \{-1, \dots, k\},$$

и наклонные прямые

$$\{(i, -1), (j, 0)\} \cup \{(f_y(i, j), y): y \in \{1, \dots, k\}\}, \quad i, j \in \{0, 1, \dots, q-1\}.$$

Образованная таким способом псевдогеометрия содержит $q(k+2)$ точек, $k+2$ горизонтальных и q^2 наклонных прямых, причем каждая горизонтальная (наклонная) прямая содержит q (соответственно, $k+2$) точек.

Мы будем обозначать указанную псевдогеометрию $\text{APG}(q, k+2)$. Ее можно представить как матрицу точек P размера $(k+2) \times q$ с некоторым множеством прямых $\mathcal{L}$, соединяющих эти точки, причем все горизонтальные прямые входят в $\mathcal{L}$. Например, поскольку существует система из трех (и даже из четырех) попарно ортогональных 5×5 латинских квадратов, то существует $\text{APG}(5, 5)$, которую можно схематически изобразить так, как показано на рис. 1. Каждая прямая этой PG имеет длину 5.

Рис. 2.

Рис. 3.

В одном случае мы также используем легкую модификацию этой конструкции. Рассмотрим произвольную псевдогеометрию $(P, \mathcal{L}) = \text{APG}(q, s)$ и добавим одну бесконечно удаленную точку, точку A , к множеству P и к каждой горизонтальной прямой (подобно тому, как аффинная плоскость вкладывается в проективную). Более формальное описание состоит в следующем. Пусть $\mathcal{H}$ (соответственно, $\mathcal{S}$) — множество всех горизонтальных (соответственно, наклонных) прямых в $\mathcal{L}$, $A \notin P$ и $P' = P \cup \{A\}$. Образует множества

$$\mathcal{H}' = \{L \cup \{A\} \mid L \in \mathcal{H}\}, \quad \mathcal{L}' = \mathcal{S} \cup \mathcal{H}'.$$

Легко видеть, что $(P', \mathcal{L}')$ — псевдогеометрия и длины ее прямых равны $q + 1$ или s . Эта псевдогеометрия будет обозначаться $\text{PAPG}(q, s)$ (P от слова проективная). Пример $\text{PAPG}(5, 5)$ изображен на рис. 2.

Пусть $(P, \mathcal{L})$ — любая псевдогеометрия и P' — произвольное непустое подмножество множества P . Положим

$$\mathcal{L}' = \{L \cap P' : L \in \mathcal{L}, L \cap P' \neq \emptyset\}.$$

Легко видеть, что $(P', \mathcal{L}')$ — псевдогеометрия. Мы назовем ее приведенной псевдогеометрией для $(P, \mathcal{L})$.

Пример 2. Если удалить 4 точки фиксированной наклонной прямой псевдогеометрии $\text{APG}(5, 5)$ (рис. 1), то получится приведенная псевдогеометрия $(P', \mathcal{L}')$ с $|P'| = |P| - 4 = 21$. Она может быть схематически изображена так, как показано на рис. 3.

Эта псевдогеометрия содержит горизонтальные прямые длин 4 и 5 и наклонные прямые длин 1, 4, 5.

Рис. 4.

В общем случае, имея псевдогеометрию $APG(n, k)$, $k \geq 3$, можно зафиксировать $l \leq k$ горизонтальных прямых и удалить с этих прямых $n - d_1, \dots, n - d_l$ точек, соответственно, где $d_1, \dots, d_l \in \{1, n - 1\}$. Так будет получена приведенная $PG(P', \mathcal{L}')$

$$|P'| = n(k - l) + d_1 + \dots + d_l$$

точками, которая содержит горизонтальные прямые длины $n, d_1, \dots, d_l$ и наклонные прямые, длины которых принадлежат множеству $\{n, k, k - 1, \dots, k - l\}$.

Такую PG можно представить схемой, приведенной на рис. 4.

Она будет обозначаться $APG(n, k \mid d_1, \dots, d_l)$. Например, PG , изображенная на рис. 3, есть $APG(5, 5 \mid d_1 = \dots = d_4 = 4)$.

Пусть $(P, \mathcal{L})$ — псевдогеометрия. Произвольное подмножество $\mathcal{N} \subset \mathcal{L}$, состоящее из попарно параллельных (не пересекающихся) прямых называется нуклеусом псевдогеометрии $(P, \mathcal{L})$.

Наши результаты основаны на следующем обобщении одного утверждения из [2].

Теорема 8. Пусть $(P, \mathcal{L})$ — PG с нуклеусом $\mathcal{N}$ такая, что для некоторого $t \in \mathbb{N}$ выполняются следующие условия:

- для любой прямой $L \in \mathcal{L} \setminus \mathcal{N}$ существует идемпотентная t -дифференцируемая квазигруппа $g_L(x, y)$ на множестве L ,
- для любой прямой $N \in \mathcal{N}$ существует t -дифференцируемая (идемпотентная) квазигруппа $h_N(x, y)$ на множестве N .

Тогда существует t -дифференцируемая (идемпотентная) квазигруппа на множестве P .

Положим

$$P' = \bigcup_{N \in \mathcal{N}} N$$

и определим функцию $f: P^2 \rightarrow P$, полагая

$$f(x, y) = \begin{cases} h_N(x, y), & \text{если } x, y \in N \text{ для некоторой прямой } N \in \mathcal{N}, \\ x, & \text{если } x = y \in P \setminus P', \\ g_L(x, y), & \text{если } x \neq y, x, y \in L \text{ для некоторой прямой } L \in \mathcal{L} \setminus \mathcal{N}. \end{cases} \quad (2.1)$$

Надо показать, что $f(x, y)$ — t -дифференцируемая квазигруппа. Ввиду идемпотентности квазигрупп $g_L(x, y)$, следующая лемма очевидна.

Лемма 1. Если $L \in \mathcal{L} \setminus \mathcal{N}$, $x, y \in L$ и $x \neq y$, то $g_L(x, y) \in L \setminus \{x, y\}$.

Теперь можно показать, что $f(x, y)$ — квазигруппа. Рассмотрим уравнение

$$f(x, u) = v \quad (2.2)$$

для некоторых $u, v \in P$. Если $u, v \in N$ для некоторого $N \in \mathcal{N}$, то существует точка $x_1 \in N$ такая, что $h_N(x_1, u) = v$. Тогда x_1 — решение (2.2). Если $u = v \in P \setminus P'$, то решением (2.2) является $x_2 = u$. В случае $u \neq v$, $u, v \in L$, $L \in \mathcal{L} \setminus \mathcal{N}$ существует точка $x_3 \in L$ такая, что $g_L(x_3, u) = v$. В силу (2.1) $x_3 \neq u$ и $x_3, u \in L$. Согласно (2.1)

$$f(x_3, u) = g_L(x_3, u) = v$$

и x_3 — решение (2.2). Уравнение $f(u, y) = v$ решается точно так же, поэтому $f(x, y)$ — квазигруппа.

Рассмотрим теперь функцию $f_i(x, y)$ вида

$$f_i(x, y) = \begin{cases} h_N^{(i)}(x, y), & \text{если } x, y \in N \text{ для некоторой прямой } N \in \mathcal{N}, \\ x, & \text{если } x = y \in P \setminus P', \\ g_L^{(i)}(x, y), & \text{если } x \neq y, x, y \in L \text{ для некоторой прямой } L \in \mathcal{L} \setminus \mathcal{N}. \end{cases} \quad (2.3)$$

Поскольку каждая из функций h_N, g_L является t -дифференцируемой, можно утверждать, что $f_i(x, y)$ — квазигруппа для всех $i \in \{0, 1, \dots, t\}$.

Теперь остается показать, что

$$f^{(i)}(x, y) = f_i(x, y). \quad (2.4)$$

Это равенство докажем по индукции.

При $i = 0$ очевидно, что (2.3) совпадает с (2.2) и потому верно (2.4).

При $i = 1$ справедливо равенство

$$f^{(1)}(x, y) = f(y, f(x, y))$$

В первом случае определения функции $f(x, y) = h_N(x, y) \in N$, $y \in N$, и

$$f^{(1)}(x, y) = f(y, h_N(x, y)) = h_N(y, h_N(x, y)) = h_N^{(1)}(x, y) = f_1(x, y)$$

В втором случае

$$f^{(1)}(x, y) = f(x, f(x, y)) = f(x, x) = x = f_1(x, y).$$

Наконец, в третьем случае $f(x, y) = g_L(x, y)$, и, ввиду леммы 1,

$$f^{(1)}(x, y) = f(y, g_L(x, y)) = g_L(y, g_L(x, y)) = g_L^{(1)}(x, y) = f_1(x, y).$$

Таким образом, равенство (2.4) справедливо при $i = 0, 1$.

Индуктивный переход доказывается аналогичными рассуждениями.

Обозначим через $\mathcal{D}(t)$ (через $\mathcal{J}(t)$) множество всех чисел $q \in \mathbf{N}$ таких, что существует t -дифференцируемая (t -дифференцируемая идемпотентная) квазигруппа порядка q . В дальнейшем псевдогеометрии вида $\text{APG}(n, k \mid d_1, \dots, d_l)$ с фиксированным нуклеусом $\mathcal{N}$ будут обозначаться $\text{APG}(n, k \mid d_1, \dots, d_l \mid \mathcal{N})$. Имеет место следующее утверждение.

Следствие 1. Пусть для некоторого $n \in \mathbf{N}$ существует система из $k-2$ попарно ортогональных латинских квадратов порядка n и для некоторого $l < k$ задана приведенная сопровождающая псевдогеометрия

$$(P, \mathcal{L}) = \text{APG}(n, k \mid d_1, \dots, d_l \mid \mathcal{N})$$

с нуклеусом $\mathcal{N}$. Допустим, что для некоторого $t \in \mathbf{N}$ выполнены следующие условия:

- для любого числа $x \in \{n, k, k-1, \dots, k-l, d_1, \dots, d_l\}$, либо $x \in \mathcal{J}(t)$, либо все прямые из $\mathcal{L}$ длины x принадлежат нуклеусу $\mathcal{N}$;
- для любой прямой $N \in \mathcal{N}$

$$|N| \in \mathcal{D}(t). \quad (2.5)$$

Тогда существует t -дифференцируемая квазигруппа порядка $q = n(k-l) + d_1 + \dots + d_l$ и $\nu^r(2, q) \geq t+3$. Если условие (2.5) можно заменить условием $|N| \in \mathcal{J}(t)$, то существует идемпотентная t -дифференцируемая квазигруппа порядка q .

В большинстве случаев следствие 1 достаточно для наших целей, но иногда нам потребуется некоторое его уточнение.

3. Доказательства оценок

Суммируем нестандартные оценки из таблицы 1 в виде следующего утверждения.

Теорема 9. Верны следующие оценки:

$$\nu^r(2, q) \geq 8 \text{ для } q = 80.$$

$$\nu^r(2, q) \geq 7 \text{ для } q \in \{50, 57, 58, 65, 70, 78, 84, 85, 86, 92, 94, 95, 96, 96, 98\}.$$

$$\nu^r(2, q) \geq 6 \text{ для } q \in \{54, 62, 66, 68, 69, 74, 75, 76, 82, 87, 90, 93\}.$$

$$\nu^r(2, q) \geq 5 \text{ для } q \in \{21, 24, 39, 60\}.$$

$$\nu^{ir}(2, q) \geq 7 \text{ для } q \in \{50, 57, 58, 65, 70, 78, 80, 84, 85, 86, 92, 94, 95, 96, 98\}.$$

$$\nu^{ir}(2, q) \geq 5 \text{ для } q \in \{21, 54, 62, 66, 68, 69, 74, 75, 76, 82, 87, 90, 93\}.$$

Доказательство. Доказательство состоит в рассмотрении каждого нестандартного числа q отдельно. В каждом случае мы приводим только конструкцию псевдогеометрии, удовлетворяющей условиям следствия 1, длины прямых и наилучшие нестандартные (из найденных нами) оценки для $\nu^{ir}(2, q)$ и $\nu^r(2, q)$. В том случае, когда полученные оценки совпадают, приводится только первая, когда они различны, но первая стандартна (в частности, меньше либо равна четырем) — только вторая.

$q = 21$: PAPG(4,4). Длина каждой прямой $5 \in \mathcal{J}(2)$, $\nu^{ir}(2, 21) \geq 5$.

$q = 24$: APG(5,5 | $d_1 = 4$ | $\mathcal{N}$) (удаление одной точки). $\mathcal{N}$ — множество всех прямых длины $4 \in \mathcal{D}(2)$. Длины остальных прямых — $5 \in \mathcal{J}(2)$, $\nu^r(2, 21) \geq 5$.

$q = 39$: APG(8,5 | $d_1 = 7$ | $\mathcal{N}$) (удаление одной точки). $\mathcal{N}$ — множество всех прямых длины $4 \in \mathcal{D}(2)$. Длины остальных прямых — $8, 7, 5 \in \mathcal{J}(2)$, $\nu^r(2, 21) \geq 5$.

$q = 50$: APG(7,8 | $d_1 = 1$) (удаление 6 точек фиксированной горизонтальной прямой). Длины прямых — $8, 7, 1 \in \mathcal{J}(4)$, $\nu^{ir}(2, 50) \geq 7$.

$q = 54$: APG(7,8 | $d_1 = 5$ | $\mathcal{N}$) (удаление 2 точек фиксированной горизонтальной прямой). $\mathcal{N}$ — единственная прямая длины 5, $5 \in \mathcal{D}(3)$. Длины остальных прямых — $7, 8 \in \mathcal{J}(4)$, $\nu^r(2, 54) \geq 6$, $\nu^{ir}(2, 54) \geq 5$, так как $7, 8, 5 \in \mathcal{J}(2)$.

$q = 57$: APG(8,8 | $d_1 = 1$) (удаление 7 точек фиксированной горизонтальной прямой). Длины прямых — $1, 7, 8 \in \mathcal{J}(4)$, $\nu^{ir}(2, 57) \geq 7$.

$q = 58$: APG(8,9 | $d_1 = d_2 = 1$) (удаление по 7 точек двух горизонтальных прямых). Длины прямых — $1, 7, 8, 9 \in \mathcal{J}(4)$, $\nu^{ir}(2, 58) \geq 7$.

$q = 60$: APG(8,8 | $d_1 = 4$ | $\mathcal{N}$) (удаление 4 точек фиксированной горизонтальной прямой). $\mathcal{N}$ — единственная прямая длины 4, $4 \in \mathcal{D}(2)$. Длины остальных прямых — $7, 8 \in \mathcal{J}(4)$, $\nu^r(2, 60) \geq 5$.

$q = 62$: APG(8,9 | $d_1 = \dots = d_7 = 7, d_8 = 5$ | $\mathcal{N}$) (удаление 8 последних точек некоторой наклонной прямой и еще 2 точек одной горизонтальной прямой). $\mathcal{N}$ — единственная прямая длины 5, $5 \in \mathcal{D}(3)$. Длины остальных прямых — $1, 7, 8, 9 \in \mathcal{J}(4)$, $\nu^r(2, 62) \geq 6$, $\nu^{ir}(2, 62) \geq 5$, так как $1, 5, 7, 8, 9 \in \mathcal{J}(2)$.

$q = 65$: APG(8,9 | $d_1 = 1$) (удаление 7 точек фиксированной горизонтальной прямой). Длины прямых — $1, 8, 9 \in \mathcal{J}(4)$, $\nu^{ir}(2, 65) \geq 7$.

$q = 66$: APG(8,9 | $d_1 = d_2 = 5$ | $\mathcal{N}$) (удаление по 3 последних точки двух горизонтальных прямых). $\mathcal{N}$ — две прямых длины 5, $5 \in \mathcal{D}(3)$. Длины остальных прямых — $2, 7, 8 \in \mathcal{J}(4)$, $\nu^r(2, 66) \geq 6$, $\nu^{ir}(2, 66) \geq 5$, так как $5, 7, 8, 9 \in \mathcal{J}(2)$.

$q = 68$: APG(8,9 | $d_1 = 7, d_2 = 5$ | $\mathcal{N}$) (удаление 2 последних точек фиксированной наклонной прямой длины 9 и еще 2 точек одной горизонтальной прямой). $\mathcal{N}$ — единственная прямая длины 5, $5 \in \mathcal{D}(3)$. Длины остальных прямых — $1, 7, 8, 9 \in \mathcal{J}(4)$, $\nu^r(2, 68) \geq 6$, $\nu^{ir}(2, 68) \geq 5$, так как $5, 7, 8, 9 \in \mathcal{J}(2)$.

$q = 69$: APG(8,9 | $d_1 = 3$ | $\mathcal{N}$) (удаление 3 точек горизонтальной прямой длины 8). $\mathcal{N}$ — единственная прямая длины 5, $5 \in \mathcal{D}(3)$. Длины остальных прямых — $7, 8, 9 \in \mathcal{J}(4)$, $\nu^r(2, 69) \geq 6$, так как $5, 7, 8, 9 \in \mathcal{J}(2)$.

- $q = 70$: $\text{APG}(9, 8 \mid d_1 = 7)$ (удаление 2 точек горизонтальной прямой). Длины прямых — $7, 8, 9 \in \mathcal{J}(4)$, $\nu^{ir}(2, 70) \geq 7$.
- $q = 74$: $\text{APG}(9, 9 \mid d_1 = d_2 = d_3 = 8, d_4 = 5 \mid \mathcal{N})$ (удаление 4 последних точек одной наклонной прямой и еще 3 точек последней горизонтальной прямой). $\mathcal{N}$ — две прямых длины 5, $5 \in \mathcal{D}(3)$. Длины остальных прямых — $7, 8, 9 \in \mathcal{J}(4)$, $\nu^r(2, 74) \geq 6$, $\nu^{ir}(2, 74) \geq 5$, так как $5, 7, 8, 9 \in \mathcal{J}(2)$.
- $q = 75$: $\text{APG}(9, 9 \mid d_1 = 7, d_2 = 5 \mid \mathcal{N})$ (удаление 2 точек одной и 4 точек другой горизонтальной прямой). $\mathcal{N}$ — единственная прямая длины 5, $5 \in \mathcal{D}(3)$. Длины остальных прямых — $7, 8, 9 \in \mathcal{J}(4)$, $\nu^r(2, 75) \geq 6$, $\nu^{ir}(2, 75) \geq 5$, так как $5, 7, 8, 9 \in \mathcal{J}(2)$.
- $q = 76$: $\text{APG}(9, 9 \mid d_1 = 8, d_2 = 5 \mid \mathcal{N})$ (удаление 4 точек одной и 1 точки другой горизонтальной прямой). $\mathcal{N}$ — единственная прямая длины 5, $5 \in \mathcal{D}(3)$. Длины остальных прямых — $7, 8, 9 \in \mathcal{J}(4)$, $\nu^r(2, 76) \geq 6$, $\nu^{ir}(2, 76) \geq 5$, так как $5, 7, 8, 9 \in \mathcal{J}(2)$.
- $q = 78$: $\text{APG}(9, 9 \mid d_1 = 8, d_2 = 7)$ (удаление 2 точек одной и 1 точки другой горизонтальной прямой). Длины прямых — $7, 8, 9 \in \mathcal{J}(4)$, $\nu^{ir}(2, 78) \geq 7$.
- $q = 80$: $\text{APG}(9, 9 \mid d_1 = 8 \mid \mathcal{N})$ (удаление 1 точки). $\mathcal{N}$ — прямые длины 8, $8 \in \mathcal{D}(6)$. Длины остальных прямых — $9 \in \mathcal{J}(5)$, $\nu^r(2, 80) \geq 8$, $\nu^{ir}(2, 80) \geq 7$, так как $8, 9 \in \mathcal{J}(4)$.
- $q = 82$: $\text{APG}(11, 8 \mid d_1 = 5 \mid \mathcal{N})$ (удаление 6 точек одной горизонтальной прямой). $\mathcal{N}$ — единственная прямая длины 5, $5 \in \mathcal{D}(3)$. Длины остальных прямых — $11, 8, 7 \in \mathcal{J}(4)$, $\nu^r(2, 82) \geq 6$, $\nu^{ir}(2, 82) \geq 5$, так как $11, 8, 7, 5 \in \mathcal{J}(2)$.
- $q = 84$: $\text{APG}(11, 8 \mid d_1 = 7)$ (удаление 4 точек одной горизонтальной прямой). Длины прямых — $11, 8, 7 \in \mathcal{J}(4)$, $\nu^{ir}(2, 84) \geq 7$.
- $q = 85$: $\text{APG}(11, 8 \mid d_1 = 8)$. (удаление 3 точек одной горизонтальной прямой). Длины прямых — $11, 8, 7 \in \mathcal{J}(4)$, $\nu^{ir}(2, 85) \geq 7$.
- $q = 86$: $\text{APG}(11, 8 \mid d_1 = 9)$. (удаление 2 точек одной горизонтальной прямой). Длины прямых — $11, 9, 8, 7 \in \mathcal{J}(4)$, $\nu^{ir}(2, 86) \geq 7$.
- $q = 87$: $\text{APG}(11, 9 \mid d_1 = 5, d_2 = 5 \mid \mathcal{N})$ (удаление по 6 точек двух последних горизонтальных прямых). $\mathcal{N}$ — две прямых длины 5, $5 \in \mathcal{D}(3)$. Длины остальных прямых — $11, 9, 8, 7 \in \mathcal{J}(4)$, $\nu^r(2, 87) \geq 6$, $\nu^{ir}(2, 87) \geq 5$, так как $11, 9, 8, 7, 5 \in \mathcal{J}(2)$.
- $q = 90$: $\text{APG}(11, 9 \mid d_1 = 8, d_2 = 5 \mid \mathcal{N})$ (удаление 6 точек одной и 3 точек другой горизонтальной прямой). $\mathcal{N}$ — единственная прямая длины 5, $5 \in \mathcal{D}(3)$. Длины остальных прямых — $11, 9, 8, 7 \in \mathcal{J}(4)$, $\nu^r(2, 90) \geq 6$, $\nu^{ir}(2, 90) \geq 5$, так как $11, 9, 8, 7 \in \mathcal{J}(2)$.
- $q = 92$: $\text{APG}(13, 8 \mid d_1 = 1)$ (удаление 12 точек одной горизонтальной прямой). Длины прямых — $13, 8, 7, 1 \in \mathcal{J}(4)$, $\nu^{ir}(2, 92) \geq 7$.
- $q = 93$: $\text{APG}(11, 9 \mid d_1 = 5 \mid \mathcal{N})$ (удаление 6 точек одной горизонтальной прямой). $\mathcal{N}$ — единственная прямая длины 5, $5 \in \mathcal{D}(3)$. Длины остальных прямых — $11, 9, 8 \in \mathcal{J}(4)$, $\nu^r(2, 93) \geq 6$, $\nu^{ir}(2, 93) \geq 5$, так как $11, 9, 8, 5 \in \mathcal{J}(2)$.

$q = 94$: $\text{APG}(11, 9 \mid d_1 = 9, d_2 = 8)$ (удаление 3 точек одной и 2 точек другой горизонтальной прямой). Длины прямых — $11, 9, 8, 7 \in \mathcal{J}(4)$, $\nu^{ir}(2, 94) \geq 7$.

$q = 95$: $\text{APG}(11, 9 \mid d_1 = 7)$ (удаление 4 точек одной горизонтальной прямой). Длины прямых — $11, 9, 8, 7 \in \mathcal{J}(4)$, $\nu^{ir}(2, 95) \geq 7$.

$q = 96$: $\text{APG}(11, 9 \mid d_1 = 8)$ (удаление 3 точек одной горизонтальной прямой). Длины прямых — $11, 9, 8 \in \mathcal{J}(4)$, $\nu^{ir}(2, 96) \geq 7$.

$q = 98$: $\text{APG}(13, 8 \mid d_1 = 7)$ (удаление 6 точек одной горизонтальной прямой). Длины прямых — $13, 8, 7 \in \mathcal{J}(4)$, $\nu^r(2, 98) \geq 7$.

4. Критическая матрица линейного рекурсивного кода

Очевидно, что код (1.5) есть код с проверочной $(n - m) \times n$ матрицей

$$H^{(1)} = \begin{pmatrix} f_0 & f_1 & \dots & f_{m-1} & -e & 0 & 0 & \dots & 0 & 0 \\ 0 & f_0 & \dots & f_{m-2} & f_{m-1} & -e & 0 & \dots & 0 & 0 \\ & & \dots & & & & & \dots & & \\ 0 & 0 & \dots & \dots & \dots & \dots & \dots & \dots & f_{m-1} & -e \end{pmatrix}. \quad (4.1)$$

Матрица

$$S(F) = \begin{pmatrix} 0 & e & \dots & 0 \\ 0 & 0 & \dots & 0 \\ & & \dots & \\ 0 & 0 & \dots & e \\ f_0 & f_1 & \dots & f_{m-1} \end{pmatrix}.$$

называется сопровождающей для многочлена $F(x)$. С ее помощью любой отрезок длины m линейной рекурренты $u \in L_M(F)$ выражается через начальный отрезок этой рекурренты по формуле

$$u(i, i + m - 1)^T = S(F)^i u(0, m - 1)^T. \quad (4.2)$$

Пусть S_i — последняя строка матрицы $S(F)^i$ и для любого $n > m$

$$\mathfrak{S}_{(n-m) \times m} = \mathfrak{S}(F) = \begin{pmatrix} S_1 \\ S_2 \\ \dots \\ S_{n-m} \end{pmatrix}$$

Матрица $\mathfrak{S}$ названа в [2] критической матрицей кода (1.5), поскольку справедливо следующее утверждение.

Предложение 9 ([2]). *Код (1.5) есть МДР-код тогда и только тогда, когда в его критической матрице все квадратные подматрицы (всех порядков) обратимы.*

Это утверждение основано на том, что проверочная матрица (4.1) кода (1.5) путем умножения слева на подходящие элементарные матрицы может быть преобразована в проверочную матрицу этого кода в стандартной форме, причем последняя имеет вид

$$H^{(2)} = (\mathfrak{S}_{(n-m) \times m}(F) - E_{(n-m) \times (n-m)}), \quad (4.3)$$

где $E_{(n-m) \times (n-m)}$ — единичная $(n-m) \times (n-m)$ матрица. Остается заметить, что справедлива следующая лемма.

Лемма 2. *Код (1.5) есть МДР-код тогда и только тогда, когда в его проверочной $(n-m) \times n$ матрице любые $n-m$ столбцов образуют обратимую матрицу.*

Доказательство. Ввиду точности модуля $\mathbb{A}M$ последнее свойство проверочной матрицы равносильно тому, что любые m позиций кода являются определяющими, а это — критерий того, что код есть МДР-код.

Заметим, что в общем случае выписать условия на коэффициенты многочлена $F(x)$, обеспечивающие выполнение условий предложения 9 весьма сложно из-за сложного строения коэффициентов матрицы $\mathfrak{S}$. Например, в случае $n = m + 3$

$$\mathfrak{S}(F)_{3 \times m} = \begin{pmatrix} f_0 & f_1 & \dots & f_s & \dots & f_{m-1} \\ f_{m-1}f_0 & f_{m-1}f_1+f_0 & \dots & f_{m-1}f_s+f_{s-1} & \dots & f_{m-1}^2+f_{m-2} \\ \delta f_0 & \delta f_1+f_{m-1}f_0 & \dots & \delta f_s+f_{m-1}f_{s-1}+f_{s-2} & \dots & \delta f_{m-1}+f_{m-1}f_{m-2}+f_{m-3} \end{pmatrix}, \quad (4.4)$$

где $\delta = f_{m-1}^2 + f_{m-2}$.

Однако этот подход дает возможность доказать предложение 7 о числе линейных в классическом смысле рекурсивных $[m+2, m, 3]$ -кодов над полем P из $q > m$ элементов. Согласно предложению 9 код $L_P^{0, m+1}(F)$ есть МДР-код тогда и только тогда, когда в его критической матрице $\mathfrak{S}(F)_{2 \times m}$, получающейся из (4.4) вычеркиванием последней строки, все миноры отличны от нуля. Это равносильно следующим условиям:

- элементы первой строки матрицы $f_i \neq 0$ для $i \in \{0, 1, \dots, m-1\}$,
- элементы второй строки $f_i \neq -f_{i+1}f_{m-1}$ для $i \in \{0, 1, \dots, m-2\}$,
- миноры второго порядка $f_i \neq f_{j+1}^{-1}f_{i+1}f_j$ для $0 \leq i < j \leq m-2$.

Нетрудно видеть, что эта система условий равносильна системе условий предложения 7 и его доказательство завершает следующая лемма.

Лемма 3. *Пусть $m < q$. Тогда для любого $i \in \{1, \dots, m-1\}$, если выполнена система первых i условий предложения 7, то $|S_i| = q - 1 - i$.*

Доказательство. Используем индукцию по i . Для $i = 1$ утверждение очевидно. Допустим, что оно верно для всех $i \in \{1, \dots, t-1\}$ при некотором $t > 1$, и рассмотрим случай $i = t$. Достаточно показать, что любые два элемента совокупности

$$\bar{S}_i = P^* \setminus S_i = \{-f_{m-1}f_{m-i}, f_{m-i+1}^{-1}f_{m-i}^2, f_{m-i+2}^{-1}f_{m-i}f_{m-i+1} \dots, f_{m-1}^{-1}f_{m-i}f_{m-2}\},$$

различны. Действительно, если

$$-f_{m-1}f_{m-i} = f_{m-i+s}^{-1}f_{m-i}f_{m-i+s-1}$$

для некоторого $s \in \{1, \dots, i-1\}$, то $f_{m-i+s-1} = -f_{m-1}f_{m-i+s}$, то есть для $j = (i-s) < t$ выполняется равенство

$$f_{m-1-j} = -f_{m-1}f_{m-1-j+1} \in \bar{S}_j,$$

противоречащее j -у условию предложения 7.

Если имеет место равенство

$$f_{m-i+s-1}^{-1}f_{m-i}f_{m-i+s-2} = f_{m-i+r-1}^{-1}f_{m-i}f_{m-i+r-2}$$

где $2 \leq s < r \leq m-1$, то

$$f_{m-i+s-2} = f_{m-i+r-1}^{-1}f_{m-i+s-1}f_{m-i+r-2}$$

и для $j = i-s+1 < t$

$$f_{m-j-1} = f_{m-j+r-s}^{-1}f_{m-j}f_{m-j+r-s-1} \in \bar{S}_j,$$

что также противоречит j -у условию.

Отметим в заключение, что один из возможных способов доказать равенство (1.12) для $t > 4$ — доказать, что в поле $GF(q)$ при $q = 2^t$ можно выбрать элементы $f_0, \dots, f_{q-2}$ так, что в матрице (4.4) при $m = q-1$ все миноры отличны от нуля. Другой подход к конструированию линейных рекурсивных МДР-кодов, основанный на рассмотрении их порождающих матриц, иллюстрируется в следующем разделе.

5. Линейные рекурсивные $[q+1, m, q+2-m]$ -коды

В этом разделе изучаются линейные в классическом смысле рекурсивные коды

$$\mathcal{K} = L_P^{0,q}(F) = \{u(0, q) \in P^n : u \in L_P(F)\} \quad (5.1)$$

над полем $P = GF(q)$, то есть коды вида (1.5), для которых $M = P$, $n = q+1$ и характеристический многочлен (1.4) удовлетворяет условию $F(x) \in P[x]$. Здесь мы докажем теоремы 4 и 5.

Доказательство теоремы 4. Покажем, прежде всего, что многочлен (1.8) принадлежит $P[x]$. Так как по условию $\gamma^q = \gamma^{-1}$, из (1.6), (1.7) следуют равенства

$$\beta_i^q = \beta_{m-1-i}, \quad i \in \{0, 1, \dots, m-1\}. \quad (5.2)$$

Таким образом, множество корней $F(x)$ инвариантно относительно автоморфизмов Q над P , и так как $F(x)$ не имеет кратных корней, $F(x) \in P[x]$. Рассматриваемый линейный рекурсивный код $\mathcal{K} = L_P^{0,q}(F)$ имеет длину $q+1$ и размерность m . Для доказательства теоремы достаточно показать, что расстояние этого кода не меньше (а следовательно, равно) $q+2-m$. Так как $L_P^{0,q}(F) \subset L_Q^{0,q}(F)$, достаточно доказать, что

$$d(L_Q^{0,q}(F)) = q+2-m. \quad (5.3)$$

Из разложения (1.8) следует, что пространство $L_Q(F)$ имеет над полем Q базис, состоящий из последовательностей u_s , $s \in \{0, 1, \dots, m-1\}$, где $u_s(i) = \beta_s^i$, $i \in \mathbf{N}_0$ (см. [20, 15]). Это означает, что код $L_Q^{0,q}(F)$ имеет порождающую матрицу вида

$$G = \begin{pmatrix} 1 & \beta_0 & \beta_0^2 & \dots & \beta_0^q \\ 1 & \beta_s & \beta_s^2 & \dots & \beta_s^q \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \beta_{m-1} & \beta_{m-1}^2 & \dots & \beta_{m-1}^q \end{pmatrix}.$$

Для доказательства равенства (5.3) достаточно доказать, что в матрице G любая система из m столбцов линейно независима (см. 11.2 в [1]). Воспользуемся тем, что последнее свойство сохраняется при умножении любого столбца матрицы на любой обратимый элемент из Q . Нетрудно видеть, что после умножения i -го столбца матрицы G на β^{-i} , $i \in \{1, \dots, q\}$, последняя преобразуется в матрицу

$$G_1 = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \gamma_1 & \gamma_1^2 & \dots & \gamma_1^q \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \gamma_{m-1} & \gamma_{m-1}^2 & \dots & \gamma_{m-1}^q \end{pmatrix},$$

где $\gamma_s = \beta_s$, $s \in \{0, 1, \dots, q\}$. Матрицу G_1 можно записать также в виде

$$G_1 = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ \gamma_0 & \gamma_1 & \gamma_2 & \dots & \gamma_q \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \gamma_0^{m-1} & \gamma_1^{m-1} & \gamma_2^{m-1} & \dots & \gamma_q^{m-1} \end{pmatrix}.$$

Так как элементы $\gamma_0 = 1, \gamma_1, \dots, \gamma_q$ попарно различны, любые m столбцов матрицы G_1 линейно независимы, поскольку определитель составленной из них матрицы есть определитель Вандермонда. Это доказывает равенство (5.3).

Для того, чтобы рассматриваемый код $\mathcal{X}$ был циклическим, необходимо и достаточно, чтобы порядки всех корней (1.7) делили $q+1$, что равносильно условию $\text{ord } \beta \mid q+1$. Последнее эквивалентно разрешимости уравнения

$$\beta = \gamma^x, \quad x \in \{1, \dots, q\}, \quad (5.4)$$

при условии (1.6), то есть разрешимости сравнения

$$x(q-1) \equiv m-1 \pmod{q+1}. \quad (5.5)$$

Если q четно, то $(q-1, q+1) = 1$ и сравнение (5.5) разрешимо для любого $m \in \{1, \dots, q\}$. Если же q нечетно, то $(q-1, q+1) = 2$ и (5.5) разрешимо лишь для нечетных m . Теорема 4 доказана.

Докажем теперь теорему 5 о числе линейных рекурсивных $[q+1, m, q+2-m]$ -кодов. Сначала докажем вспомогательное утверждение. Зафиксируем $n \in \mathbf{N}$, $n > 2$, и будем рассматривать числа $0, 1, \dots, n-1$ как элементы кольца $\mathbf{Z}_n$ с операциями $\oplus, \otimes$.

Лемма 4. Если $d \in \{1, \dots, n-1\}$, $(d, n) = 1$ и для некоторых $m \in \{2, \dots, n-2\}$, $s \in \{0, 1, \dots, n-1\}$ верно соотношение

$$d \otimes \{0, 1, \dots, m-1\} = s \oplus \{0, 1, \dots, m-1\} \quad (5.6)$$

то $d \in \{1, \dots, n-1\}$ и, соответственно, $s \in \{0, n-m+1\}$.

Доказательство. Покажем прежде всего, что можно считать, что $m \leq n/2$. Действительно, очевидно, что

$$d \otimes \{0, 1, \dots, n-1\} = \{0, 1, \dots, n-1\} = s \oplus \{0, 1, \dots, n-1\},$$

поэтому из (5.6) следует, что

$$d \otimes \{m, \dots, n-1\} = s \oplus \{m, \dots, n-1\} = (s \oplus m) \oplus \{0, 1, \dots, n-m-1\},$$

$$d \otimes \{m, \dots, n-1\} = (d \otimes m) \oplus d \otimes \{0, 1, \dots, n-m-1\},$$

$$d \otimes \{0, 1, \dots, n-m-1\} = r \oplus \{0, 1, \dots, n-m-1\},$$

где $r = s \oplus m \ominus d \otimes m$. Остается заметить, что $\min\{m, n-m\} \leq n/2$.

Из (5.6) следует, что

$$d \otimes \{1, \dots, m\} = d \oplus d \otimes \{0, 1, \dots, m-1\} = s \oplus d \oplus \{0, 1, \dots, m-1\},$$

и так как

$$|\{0, 1, \dots, m-1\} \cap \{1, \dots, m\}| = m-1,$$

получаем, что

$$|d \otimes \{0, 1, \dots, m-1\} \cap d \otimes \{1, \dots, m\}| = m-1,$$

то есть

$$|\{0, 1, \dots, m-1\} \cap d \oplus \{0, 1, \dots, m-1\}| = m-1. \quad (5.7)$$

Так как $m \leq n/2$, соотношение

$$\{0, 1, \dots, m-1\} \cap d \oplus \{0, 1, \dots, m-1\} \neq \emptyset$$

выполняется либо если $d < m$, и тогда

$$|\{0, 1, \dots, m-1\} \cap d \oplus \{0, 1, \dots, m-1\}| = m-d,$$

и (5.7) эквивалентно равенству $d = 1$, либо если $n-m+1 \leq d$, и тогда

$$|\{0, 1, \dots, m-1\} \cap d \oplus \{0, 1, \dots, m-1\}| = d+m-n,$$

и (5.7) эквивалентно равенству $d = n-1$.

Лемма доказана.

Докажем теорему 5. Зафиксируем произвольную систему элементов (1.7), удовлетворяющую теореме 4, и заметим, что для произвольных $a \in P^*$, $\delta \in \mathbf{Z}_n^*$, где $n = q+1$, множество элементов

$$\bar{\beta}_i = a\beta^\delta \gamma^{\delta i}, \quad i \in \{0, 1, \dots, m-1\}, \quad (5.8)$$

также удовлетворяет теореме 4. Покажем, что можно построить $(q-1)(\varphi(q+1)/2)$ таких различных множеств, то есть различных многочленов $F(x)$, для которых верна теорема 4. Для этого достаточно показать, что множества элементов (5.8), соответствующие различным парам элементов a, δ , таким, что $\delta < n/2$, различны. Действительно, пусть $b \in P^*$, $\xi \in \mathbf{Z}_n^*$, $\xi < n/2$, и множество элементов

$$\hat{\beta}_i = b \beta^\xi \gamma^{\xi i}, \quad i \in \{0, 1, \dots, m-1\} \quad (5.9)$$

удовлетворяет равенству

$$\{\hat{\beta}_0 \dots \hat{\beta}_{m-1}\} = \{\bar{\beta}_0 \dots \bar{\beta}_{m-1}\}. \quad (5.10)$$

Тогда существует перестановка $r_0, \dots, r_{m-1}$ чисел $\{0, 1, \dots, m-1\}$ такая, что

$$\hat{\beta}_i = \bar{\beta}_{r_i}, \quad i \in \{0, 1, \dots, m-1\}. \quad (5.11)$$

Возводя обе части каждого из этих равенств в степень $\delta^{-1} \in \mathbf{Z}_n^*$, после несложных преобразований получаем, что

$$c\beta^d \gamma^{di-r_i} = \beta, \quad d = \xi \otimes \delta^{-1}, \quad c = (a^{-1}b)^{\delta^{-1}}. \quad (5.12)$$

Отсюда следует система равенств

$$\gamma^{di} = \gamma^{r_i-r_0}, \quad i \in \{0, 1, \dots, m-1\}, \quad (5.13)$$

эквивалентная равенству (5.6) при $s = \ominus r_0$. В таком случае по лемме 4 $d \in \{1, n-1\}$. Но равенство $d = n-1$ невозможно, так как влечет соотношения

$$\xi = (n-1) \otimes \delta = \ominus \delta = n - \delta > n/2.$$

Следовательно, $d = 1$, и по лемме 4 $s = 0$. В этом случае $\xi = \delta$, и ввиду (5.13) $r_i = i$, $i \in \{0, 1, \dots, m-1\}$. Поэтому из (5.10) следует, что $a = b$. Теорема 5 доказана.

Список литературы

1. МакВильямс Ф. Дж., Слоэн Н. Дж. А., *Теория кодов, исправляющих ошибки*. Связь, Москва, 1979.
2. Коусело Е., Гонсалес С., Марков В., Нечаев А., Рекурсивные МДР-коды и рекурсивно дифференцируемые квазигруппы, *Дискретная математика* (1998), 10 №. 2, 3–29.
3. Dénes J., Keedwell A. D., *Latin squares and their applications*. Akadémiai Kiadó, Budapest; Academic Press, new York; English Universities Press, London, 1974.
4. Heise W., Quattrocchi P., *Informations- und Codierungstheorie*. Springer, Berlin, 1995.
5. Bush K. A., Orthogonal arrays of index unity. *Ann. Math. Stat.* (1952) 23, 426–434.
6. Segre B., Curve razionali normali e k -archi negli spazi finiti. *Ann. Mat. Pura Appl.* (1955) 39, 357–379.
7. Segre B., *Lectures on modern geometry*. Cremonese, Roma, 1961.
8. Thas J., Normal rational curves and k -arcs in Galois spaces. *Rend. di Mat. Roma* (1968) 1, 331–334.

9. Thas J., Connection between the Grassmanian $G_{k-1;n}$ and the set of k -arcs in Galois space $S_{n,q}$. *Rend. di Mat. Roma* (1969) **2**, 121–133.
10. Casse L., A solution to Benjamino Segre's problem $I_{r,q}$ for q even. *Atti Accad. naz. Lincei. Rend. Cl. Sci. Fis. Mat. nat.* (1969) **46**, 13–20.
11. Maneri C., Silverman R., A vector space packing problem. *J. Algebra* (1996) **4**, 321–330.
12. Maneri C., Silverman R., A combinatorial problem with applications to geometry. *J. Comb. Theory* (1971) **11**, 118–121.
13. Jurick R. R., An algorithm for determining the largest maximally independent set of vectors from an r -dimensional vector space over a Galois field of n elements. Tech. Rep. ASD-TR-68-40 Air Force Systems Command. Wright-Patterson Air Force Base. Ohio, September 1968.
14. Georgiades J., Cyclic $(q+1, k)$ -codes of odd order q and even dimension k are not optimal. *Atti Sem. Mat. Fis. Univ. Modena* (1982) **30**, 284–285.
15. Kurakin V. L., Kuzmin A. S., Mikhalev A. V., Nechaev A. A., Linear recurrences over rings and modules. *J. Math. Sci.* (1995) **76**, №6, 2793–2915.
16. Абашин А. С., Линейные рекурсивные МДР-коды размерностей 2 и 3. *Дискретная математика* (2000) **12**, №2, 140–153.
17. Couselo E., Gonzalez S., Markov V., Nechaev A., Recursive MDS-codes and recursively differentiable k -quasigroups, *Proc. Sixth Intern. Workshop on Algebraic and Combinatorial Coding Theory*. Pskov, Russia, 1998, 78–84.
18. Couselo E., Gonzalez S., Markov V., Nechaev A., Recursive MDS-codes. *Proc. WCC'99 Workshop on Coding and Cryptography*. Paris, France, 1999, 271–278.
19. Brayton R. K., Coppersmith D., Hoffman A. J., Self orthogonal Latin squares for all orders $n \neq 2, 3, 6$. *Bull. Amer. Math. Soc.* (1974) **80**, 116–119.
20. Zierler N., Linear recurring sequences. *J. Soc. Ind. Appl. Math.* (1969) **7**, №1, 31–48.

Статья поступила 26.06.2000.