ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 57 **2021** **Вып. 4**

УДК 621.391.1 : 519.725

© 2021 г. **Н.А. Полянский**

О СПИСОЧНОМ ДЕКОДИРОВАНИИ НЕКОТОРЫХ $\mathbb{F}_q$-ЛИНЕЙНЫХ КОДОВ[1]

Представлен алгоритм списочного декодирования $\mathbb{F}_q$-линейных кодов, обобщающих s-коды Рида – Соломона.

Ключевые слова: списочное декодирование, s-коды Рида – Соломона, минимальное расстояние.

DOI: 10.31857/S0555292321040045

§ 1. Обозначения, определения и вспомогательные результаты

Множество натуральных чисел обозначим символом $\mathbb{N}$, причем будем считать, что $0 \in \mathbb{N}$. Множество последовательных целых чисел $\{i, i+1, \ldots, j\}$ для некоторых $i, j \in \mathbb{N}$, $i \leqslant j$, будем обозначать через $[i, j]$. Для множества $[1, j]$ будем использовать сокращение $[j]$. Для обозначения векторов будем использовать полужирные символы, например, $\boldsymbol{x}$, а i-ю координату вектора $\boldsymbol{x}$ будем записывать в виде x_i. Для векторов $\boldsymbol{i} = (i_1, \ldots, i_m)$ и $\boldsymbol{j} = (j_1, \ldots, j_m)$ из $\mathbb{N}^m$ определим естественное отношение частичного порядка: $\boldsymbol{i} \leqslant \boldsymbol{j}$, если выполнено $i_k \leqslant j_k$ для всех $k \in [m]$. Через $\binom{\boldsymbol{i}+\boldsymbol{j}}{\boldsymbol{i}}$ для некоторых $\boldsymbol{i}, \boldsymbol{j} \in \mathbb{N}^m$ будем обозначать произведение $\prod\limits_{k=1}^{m} \binom{i_k + j_k}{i_k}$. Запись $\max\{i_1, \ldots, i_m\}$ обозначает максимум из чисел $i_1, \ldots, i_m$. *Кодом* $\mathcal{C}$ длины n над алфавитом $\mathcal{A}$ будем называть произвольное подмножество множества $\mathcal{A}^n$, т.е. $\mathcal{C} \subseteq \mathcal{A}^n$. Через $|A|$ будем обозначать мощность множества A, например, объем кода равен $|\mathcal{C}|$. *Расстояние Хэмминга* между двумя векторами $\boldsymbol{x}, \boldsymbol{y} \in \mathcal{A}^n$ определим как $d_H(\boldsymbol{x}, \boldsymbol{y}) := |\{i : x_i \neq y_i\}|$. *Минимальное расстояние* в коде $\mathcal{C}$ равно минимуму величины $d_H(\boldsymbol{x}, \boldsymbol{y})$ по всем $\boldsymbol{x}, \boldsymbol{y} \in \mathcal{C}$, $\boldsymbol{x} \neq \boldsymbol{y}$.

В настоящей статье будем рассматривать лишь конечные поля $\mathbb{F}_q$ с характеристикой p, т.е. $q = p^c$ для некоторого $c \in \mathbb{N} \setminus \{0\}$ и простого числа p. Мультипликативную группу поля $\mathbb{F}_q$ будем обозначать через $\mathbb{F}_q^*$. Символом $\mathbf{0}$ будем обозначать вектор из всех нулей, длина которого будет ясна из контекста. Будем использовать прописные символы для обозначения переменных, например, T или $\boldsymbol{X} = (X_1, \ldots, X_m)$. В ходе рассуждений число переменных m будет чаще всего фиксировано. Обозначим через $\mathbb{F}_q[\boldsymbol{X}]$ кольцо многочленов от m переменных $X_1, \ldots, X_m$ над полем $\mathbb{F}_q$. Для вектора $\boldsymbol{v} = (v_1, \ldots, v_m) \in \mathbb{N}^m$ моном $\boldsymbol{X}^{\boldsymbol{v}} \in \mathbb{F}_q[\boldsymbol{X}]$ определяется как $\prod\limits_{j=1}^{m} X_j^{v_j}$. Для многочлена $f(\boldsymbol{X}) \in \mathbb{F}_q[\boldsymbol{X}]$ и вектора $\boldsymbol{i} \in \mathbb{N}^m$ будем обозначать через $[\boldsymbol{X}^{\boldsymbol{i}}]f(\boldsymbol{X})$ коэффициент перед $\boldsymbol{X}^{\boldsymbol{i}}$ в записи $f(\boldsymbol{X})$. Для вектора $\boldsymbol{x}_0 \in \mathbb{F}_q^m$ значение многочлена $f(\boldsymbol{X})$ в точке $\boldsymbol{x}_0$ будем записывать в виде $f(\boldsymbol{x}_0)$, где $f(\boldsymbol{x}_0) \in \mathbb{F}_q$. Пусть $\boldsymbol{X} = (X_1, \ldots, X_m)$

[1] Работа выполнена в Сколковском институте науки и технологий при поддержке гранта Российского научного фонда (номер проекта 19-71-00137).

и $\boldsymbol{Y} = (Y_1, \ldots, Y_k)$. Тогда для многочлена $f(\boldsymbol{X}, \boldsymbol{Y})$ из $\mathbb{F}_q[\boldsymbol{X}, \boldsymbol{Y}]$ через $\{\boldsymbol{Y}^{\boldsymbol{i}}\}f(\boldsymbol{X}, \boldsymbol{Y})$ будем обозначать многочлен из $\mathbb{F}_q[\boldsymbol{X}]$, определяемый равенством

$$\{\boldsymbol{Y}^{\boldsymbol{i}}\}f(\boldsymbol{X}, \boldsymbol{Y}) := \sum_{\boldsymbol{j} \in \mathbb{N}^m} \big([\boldsymbol{X}^{\boldsymbol{j}}\boldsymbol{Y}^{\boldsymbol{i}}]f(\boldsymbol{X}, \boldsymbol{Y})\big)\boldsymbol{X}^{\boldsymbol{j}}.$$

1.1. Производная Хассе и эквивалентные многочлены.

Определение 1. Пусть $\boldsymbol{X} = (X_1, \ldots, X_m)$ и $\boldsymbol{Y} = (Y_1, \ldots, Y_m)$. Для вектора $\boldsymbol{i} \in \mathbb{N}^m$ определим *$\boldsymbol{i}$-ю производную Хассе* многочлена $f(\boldsymbol{X}) \in \mathbb{F}_q[\boldsymbol{X}]$ как $\boldsymbol{i}$-й коэффициент "сдвинутого" многочлена $\widetilde{f}(\boldsymbol{X}, \boldsymbol{Y}) := f(\boldsymbol{X} + \boldsymbol{Y})$, т.е.

$$f^{(\boldsymbol{i})}(\boldsymbol{X}) := \{\boldsymbol{Y}^{\boldsymbol{i}}\}\widetilde{f}(\boldsymbol{X}, \boldsymbol{Y}).$$

Иногда для удобства будем использовать эквивалентное обозначение $D^{(\boldsymbol{i})}f(\boldsymbol{X}) := f^{(\boldsymbol{i})}(\boldsymbol{X})$. Таким образом, выполнено соотношение

$$f(\boldsymbol{X} + \boldsymbol{Y}) = \sum_{\boldsymbol{i} \in \mathbb{N}^m} f^{(\boldsymbol{i})}(\boldsymbol{X})\boldsymbol{Y}^{\boldsymbol{i}}.$$

Отметим несколько свойств производной Хассе, доказательство которых можно найти в [1].

Предложение 1. *Пусть* $f(\boldsymbol{X}), g(\boldsymbol{X}) \in \mathbb{F}_q[\boldsymbol{X}]$, $\lambda \in \mathbb{F}_q$, *и пусть* $\boldsymbol{i}, \boldsymbol{j} \in \mathbb{N}^m$. *Тогда справедливы следующие соотношения*:

1. $f^{(\boldsymbol{i})}(\boldsymbol{X}) + g^{(\boldsymbol{i})}(\boldsymbol{X}) = (f + g)^{(\boldsymbol{i})}(\boldsymbol{X})$;
2. $(\lambda f)^{(\boldsymbol{i})}(\boldsymbol{X}) = \lambda f^{(\boldsymbol{i})}(\boldsymbol{X})$;
3. $(fg)^{(\boldsymbol{i})}(\boldsymbol{X}) = \sum\limits_{\boldsymbol{0} \leqslant \boldsymbol{e} \leqslant \boldsymbol{i}} f^{(\boldsymbol{e})}(\boldsymbol{X})g^{(\boldsymbol{i}-\boldsymbol{e})}(\boldsymbol{X})$;
4. $(f^{(\boldsymbol{i})})^{(\boldsymbol{j})}(\boldsymbol{X}) = \binom{\boldsymbol{i}+\boldsymbol{j}}{\boldsymbol{i}} f^{(\boldsymbol{i}+\boldsymbol{j})}(\boldsymbol{X})$.

Определим функцию

$$\deg\colon \mathbb{N}^m \to \mathbb{N}, \quad \deg(\boldsymbol{v}) = \sum_{j=1}^{m} v_j,$$

и функцию

$$\deg_q\colon \mathbb{N}^m \to \mathbb{N}, \quad \deg_q(\boldsymbol{v}) = \sum_{j=1}^{m} \lfloor v_j/q \rfloor.$$

Степень $\deg(f(\boldsymbol{X}))$ многочлена $f(\boldsymbol{X}) \in \mathbb{F}_q[\boldsymbol{X}]$ определим как максимальное значение $\deg(\boldsymbol{i})$ для вектора $\boldsymbol{i} \in \mathbb{N}^m$, такого что $[\boldsymbol{X}^{\boldsymbol{i}}]f(\boldsymbol{X}) \neq 0$. Следующее утверждение напрямую вытекает из [2, следствие 6.50].

Предложение 2. *Для произвольного числа* $s \in [q-1]$ *определим многочлен от одной переменной* $f(T) := (T^q - T)^s \in \mathbb{F}_q[T]$. *Тогда*

$$f^{(i)}(T) = \begin{cases} (-1)^i \binom{s}{i} (T^q - T)^{s-i} & \text{для } 0 \leqslant i \leqslant s, \\ 0 & \text{для } i > s. \end{cases}$$

Через $f^{(<s)}(\boldsymbol{x}_0) \in \mathbb{F}_q^{\binom{s+m-1}{m}}$ будем обозначать вектор, $\boldsymbol{i}$-я компонента которого равна $f^{(\boldsymbol{i})}(\boldsymbol{x}_0)$ для всех $\boldsymbol{i} \in \mathbb{N}^m$, $\deg(\boldsymbol{i}) < s$.

Определение 2. Два многочлена $f(\boldsymbol{X}), g(\boldsymbol{X}) \in \mathbb{F}_q[\boldsymbol{X}]$ назовем *s-эквивалентными*, если $f^{(<s)}(\boldsymbol{x}_0) = g^{(<s)}(\boldsymbol{x}_0)$ для всех $\boldsymbol{x}_0 \in \mathbb{F}_q^m$. В таком случае будем также писать $f(\boldsymbol{X}) \equiv_s g(\boldsymbol{X})$.

Доказательства следующего и некоторых последующих утверждений, для которых не указаны ссылки на работы, содержащие доказательства, приведены в § 3.

Предложение 3. *Пусть q – степень простого числа p, и пусть $s \in [q-1]$. Тогда для всякого многочлена от одной переменной $f(T) \in \mathbb{F}_q[T]$ существует единственный многочлен $g(T) \in \mathbb{F}_q[T]$ степени не выше $sq-1$, такой что $f(T) \equiv_s g(T)$. Если s также является степенью p, то*

$$f(T) \equiv g(T) \pmod{T^{qs} + (-T)^s}.$$

В дальнейшем чаще всего будем предполагать, что s является степенью p. Это позволит существенным образом упростить анализ ввиду предложения 3. Определим функцию $\mathrm{Mod}_q^s \colon \mathbb{N} \to [0, qs-1]$ по следующему правилу:

- если $a < s$, то $\mathrm{Mod}_q^s(a) = a$;
- если $a \geqslant s$ и $a \equiv b \pmod{qs-s}$, $b \in [s, qs-1]$, то $\mathrm{Mod}_q^s(a) = b$.

Эта функция имеет смысл благодаря следующему наблюдению. Если s является степенью p, то

$$T^a \equiv_s (-1)^t T^{\mathrm{Mod}_q^s(a)}, \tag{1}$$

где $t = \dfrac{a - \mathrm{Mod}_q^s(a)}{qs-s}$.

1.2. Хорошие мономы и обобщение s-кодов Рида – Соломона. Определим отношение частичного порядка $\leqslant_p$ на множествах $\mathbb{N}$ и $\mathbb{N}^m$ для некоторого простого числа p.

Определение 3. Возьмем целые числа $n, k \in \mathbb{N}$, простое число p и положим $t := \lfloor \log_p(\max\{n,k\}) \rfloor$. Рассмотрим p-ичные представления чисел $n = \sum\limits_{i=0}^{t} n^{(i)} p^i$ и $k = \sum\limits_{i=0}^{t} k^{(i)} p^i$. Определим следующий порядок: $k \leqslant_p n$, если $k^{(i)} \leqslant n^{(i)}$ для всех $i \in [0,t]$. Для вектора $\boldsymbol{v} = (v_1, \ldots, v_m) \in \mathbb{N}^m$ будем писать $\boldsymbol{v} \leqslant_p n$, если $v_j \leqslant_p n$ для всех $j \in [m]$. Для двух векторов одной длины $\boldsymbol{v}, \boldsymbol{w} \in \mathbb{N}^m$ определим порядок $\boldsymbol{v} \leqslant_p \boldsymbol{w}$, если выполнено $v_j \leqslant_p w_j$ для всех $j \in [m]$.

Следующий результат, доказанный в [3], поясняет удобство использования вышеуказанного частичного порядка.

Предложение 4. *Пусть даны целые числа $n > 0$, $k \geqslant 0$, $k \leqslant n$, и простое число p. Определим $t := \lfloor \log_p(n) \rfloor$ и рассмотрим p-ичные представления чисел $n = \sum\limits_{i=0}^{t} n^{(i)} p^i$ и $k = \sum\limits_{i=0}^{t} k^{(i)} p^i$. Тогда для биномиального коэффициента справедливо соотношение*

$$\binom{n}{k} \equiv \prod_{i=0}^{t} \binom{n^{(i)}}{k^{(i)}} \pmod{p}.$$

В частности, равенство $\binom{n}{k} \equiv 0 \pmod{p}$ выполнено в том и только том случае, когда существует хотя бы один индекс $i \in [0,t]$, для которого $k^{(i)} > n^{(i)}$. Другими словами, соотношение $\binom{n}{k} \not\equiv 0 \pmod{p}$ верно тогда и только тогда, когда $k \leqslant_p n$.

Следствие 1. *Пусть даны целые числа* $n, k_j \in \mathbb{N}$, $j \in [m]$, $\sum\limits_{j=1}^{m} k_j = n$, *и простое число* p. *Тогда соответствующий мультиномиальный коэффициент не равен нулю,* $\binom{n}{k_1, \ldots, k_m} \not\equiv 0 \pmod{p}$, *тогда и только тогда, когда отношение порядка* $k_j \leqslant_p n$ *справедливо для всех* $j \in [m]$.

Определение 4. Пусть q и s являются степенью простого p, $s < q$, и пусть даны числа $m \geqslant 1$ и $d \in [sq]$. Будем говорить, что моном $\boldsymbol{X}^{\boldsymbol{v}} \in \mathbb{F}_q[\boldsymbol{X}]$, где $\boldsymbol{v} \in \mathbb{N}^m$, является $(m,d)_q^s$-*хорошим*, если выполнены следующие два условия:

1. $\deg_q(\boldsymbol{v}) \leqslant s-1$;
2. для всякого $\boldsymbol{i} \in \mathbb{N}^m$, такого что $\boldsymbol{i} \leqslant_p \boldsymbol{v}$, выполнено неравенство $\mathrm{Mod}_q^s(\deg(\boldsymbol{i})) < d$.

Заметим, что все мономы $\boldsymbol{X}^{\boldsymbol{v}}$, для которых выполнено первое условие определения 4 и при этом $\deg(\boldsymbol{v}) < d$, являются $(m,d)_q^s$-хорошими. Однако общее число $(m,d)_q^s$-хороших мономов может быть значительно большим. Вышеуказанное определение иллюстрирует следующий

Пример 1. Пусть $m = s = 2$, $d = 7$, $q = 2^2 = 4$; рассмотрим моном $f(X_1, X_2) = X_1^2 X_2^6$, т.е. $f(\boldsymbol{X}) = \boldsymbol{X}^{\boldsymbol{v}}$ для $\boldsymbol{v} = (v_1, v_2) = (2, 6)$ и $\deg(\boldsymbol{v}) = 8 > d$. Проверим, что этот моном является $(m,d)_q^s$-хорошим. Во-первых, выполнено

$$\deg_q(\boldsymbol{v}) = \left\lfloor \frac{v_1}{q} \right\rfloor + \left\lfloor \frac{v_2}{q} \right\rfloor = \left\lfloor \frac{2}{4} \right\rfloor + \left\lfloor \frac{6}{4} \right\rfloor = 1 \leqslant s-1.$$

Для проверки второго условия отметим, что существует несколько различных векторов $\boldsymbol{i} = (i_1, i_2)$, удовлетворяющих соотношению $\boldsymbol{i} \leqslant_2 \boldsymbol{v}$. Подходят все векторы (i_1, i_2), такие что $i_1 \in \{0, 2\}$ и $i_2 \in \{0, 2, 4, 6\}$. Поскольку функция $\mathrm{Mod}_q^s(\cdot)$ не увеличивает аргумент, достаточно проверить условие $\mathrm{Mod}_q^s(\deg(\boldsymbol{i})) < d = 7$ лишь для $\boldsymbol{i} = (2, 6)$. Действительно, для $\boldsymbol{i} = (2, 6)$ выполнено

$$\mathrm{Mod}_q^s(\deg(\boldsymbol{i})) = \mathrm{Mod}_q^s(8) = 2 < d,$$

поскольку $8 \equiv 2 \pmod{qs - s}$ и $2 \in [s, qs-1]$.

Обозначим множество $(m,d)_q^s$-хороших мономов через $G_q^s(m,d) \subseteq \mathbb{F}_q[\boldsymbol{X}]$, а его мощность – через $N_q^s(m,d)$. Заметим, что кольцо $\mathbb{F}_q[\boldsymbol{X}]$ можно рассматривать как $\mathbb{F}_q$-линейное векторное пространство. Пусть $V_q^s(m,d) \subseteq \mathbb{F}_q[\boldsymbol{X}]$ обозначает линейную оболочку множества $G_q^s(m,d)$ над $\mathbb{F}_q$. В следующем утверждении указано важнейшее свойство хороших мономов и пространства $V_q^s(m,d)$.

Предложение 5. *Пусть задан произвольный вектор из линейных многочленов от одной переменной* $\gamma(T) = \boldsymbol{a}T + \boldsymbol{b}$, $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{F}_q^m$, $\boldsymbol{a} \neq \boldsymbol{0}$, *а также произвольный многочлен* $f(\boldsymbol{X}) \in V_q^s(d,m)$. *Тогда многочлен* $g(T)$, *определяемый как композиция* $f \circ \gamma(T)$, s-*эквивалентен некоторому многочлену* $h(T) \in \mathbb{F}_q[T]$ *степени* $\deg(h(T)) < d$.

Замечание 1. Отметим, что в предложении 5 образ отображения вычисления значений функции $\gamma(T)\colon \mathbb{F}_q \to \mathbb{F}_q^m$ соответствует некоторой прямой в пространстве $\mathbb{F}_q^m$. Таким образом, предложение 5 утверждает, что если рассмотреть линейную комбинацию хороших многочленов и ограничить их на произвольную прямую в пространстве, то полученный многочлен от одной переменной может быть эквивалентным образом задан (с точки зрения вычисления значений многочлена и всех его производных до $(s-1)$-го порядка включительно) многочленом от одной переменной невысокой степени.

Обозначим отображение вычисления значений многочлена и всех его производных до $(s-1)$-го порядка включительно во всех точках пространства $\mathbb{F}_q^m$ через

$$\mathrm{Ev}_{q,m}^s \colon \mathbb{F}_q[\boldsymbol{X}] \to \left(\mathbb{F}_q^{\binom{s+m-1}{m}}\right)^{q^m}.$$

Для произвольного многочлена $f(\boldsymbol{X}) \in \mathbb{F}_q[\boldsymbol{X}]$ его образ равен

$$\mathrm{Ev}_{q,m}^s(f(\boldsymbol{X})) = \left(f^{(<s)}(\boldsymbol{x}_0)\right)\big|_{\boldsymbol{x}_0 \in \mathbb{F}_q^m}.$$

Наконец, определим коды, которые будут исследоваться в данной статье.

О п р е д е л е н и е 5 (обобщение s-кодов Рида – Соломона). Пусть q и s – степени простого числа p, $s < q$, и пусть даны положительные числа $m \geqslant 1$ и $d \leqslant sq$. Тогда определим код $\mathcal{C}_q^s(m,d)$ длины q^m над алфавитом $\mathbb{F}_q^{\binom{m+s-1}{m}}$ как

$$\mathcal{C}_q^s(m,d) := \left\{\mathrm{Ev}_{q,m}^s(f(\boldsymbol{X})) : \ f(\boldsymbol{X}) \in V_q^s(d,m)\right\}.$$

Определение 5 в указанном виде ранее в литературе не вводилось. Далее мы приведем историческую справку, которая раскрывает мотивацию для изучения обобщений s-кодов Рида – Соломона.

Код Рида – Соломона, один из наиболее исследованных в теории кодирования на данный момент, был изобретен в 1960 г. Ридом и Соломоном. Этот код в частном случае может быть задан как образ отображения вычисления значений многочленов от одной переменной степени не выше $d-1$ во всех точках поля $\mathbb{F}_q$. Отметим очевидное и при этом важное свойство, что при $d < q$ произвольная стертая координата кодового слова кода Рида – Соломона может быть восстановлена при чтении всех остальных координат.

Недвоичные коды Рида – Маллера, предложенные в ряде параллельных работ в 1968–1970 гг., являются естественным обобщением кодов Рида – Соломона. Подобный код может быть задан как образ отображения вычисления значений многочленов от $m \geqslant 2$ переменных степени не выше $d-1$ во всех точках пространства $\mathbb{F}_q^m$. При $d < q$ недвоичные коды Рида – Маллера обладают свойством локального восстановления: произвольная стертая координата кодового слова, соответствующая вычислению в точке $\boldsymbol{x}_0 \in \mathbb{F}_q^m$, может быть восстановлена после прочтения координат кодового слова, соответствующих произвольной прямой в $\mathbb{F}_q^m$, проходящей через $\boldsymbol{x}_0$. Это свойство выполнено, поскольку ограничение кодового слова недвоичного кода Рида – Маллера на произвольную прямую является кодовым словом кода Рида – Соломона. Однако кодовая скорость недвоичных кодов Рида – Маллера при $d < q$ и $m \geqslant 2$ не превышает $1/2$.

Чтобы построить код более высокой скорости, сохранив при этом свойство локального восстановления, Го, Коппарти и Судан [4] предложили в 2013 г. так называемые многомерные коды Рида – Соломона (lifted Reed–Solomon codes), соответствующие определению 5 при $s = 1$. Другой естественный способ обобщить коды Рида – Соломона был также предложен Розенблюмом и Цфасманом [5] в 1997 году в контексте введенной ими же новой метрики (так называемой s-метрики, или метрики Розенблюма – Цфасмана). Таким образом, в [5] был построен код, соответствующий определению 5 при $m = 1$, и назван s-кодом Рида – Соломона. Отметим, что s-код Рида – Соломона, так же как и обычный код Рида – Соломона, не обладает желанным сочетанием высокой скорости и локального восстановления. Таким образом, в 2014 г. Коппарти, Шараф и Еханин [6] разработали недвоичные s-коды Рида – Маллера (multiplicity codes), которые можно задать как образ отображения вычисления значений многочленов от $m \geqslant 2$ переменных степени не выше $d-1$ и

всех их производных до $(s-1)$-го порядка во всех точках пространства $\mathbb{F}_q^m$, т.е.

$$\mathcal{M}_q^s(d,m) := \left\{ \mathrm{Ev}_{q,m}^s(f(\boldsymbol{X})) :\ f(\boldsymbol{X}) \in \mathbb{F}_q[\boldsymbol{X}],\ \deg(f(\boldsymbol{X})) < d \right\}.$$

При $d \leqslant sq$ имеет место вложение $\mathcal{M}_q^s(d,m) \subseteq \mathcal{C}_q^s(d,m)$, поскольку множество $V_q^s(m,d)$ содержит всевозможные многочлены степени, меньшей d, а также некоторые многочлены значительно большей степени (см. подробнее [7]). В той же работе [6] было также показано, что недвоичные s-коды Рида – Маллера наряду с многомерными кодами Рида – Соломона могут достигать высокой скорости (сколь угодно близкой к 1), сохраняя при этом хорошие свойства локального восстановления.

Наконец, отметим, что наиболее родственные по смыслу коды, но все же отличные (см. [7]) от определения 5, – многомерные s-коды Рида – Соломона (чаще всего называемые в англоязычной литературе lifted multiplicity codes) – были изначально определены Ву [8] в 2015 г. с целью построить наиболее широкий класс кодов с высокой скоростью и отличными способностями локального восстановления. Подобный m-мерный s-код Рида – Соломона может быть задан как образ отображения вычисления значений всевозможных $(m,d)_q^s$-хороших многочленов и их производных. Здесь под $(m,d)_q^s$-хорошим многочленом мы понимаем такой многочлен, который при ограничении на произвольную прямую в пространстве $\mathbb{F}_q^m$ является s-эквивалентным некоторому многочлену от одной переменной степени не выше $d-1$. В работах [7–9] приведен анализ скорости многомерных s-кодов Рида – Соломона и предложены некоторые алгоритмы локального восстановления.

Очевидно, что обобщение s-кода Рида – Соломона $\mathcal{C}_q^s(m,d)$ является подкодом соответствующего m-мерного s-кода Рида – Соломона. В данной статье нам необходимо непосредственно использовать структурное свойство кода $\mathcal{C}_q^s(m,d)$, а именно то, что всякое кодовое слово этого кода соответствует линейной комбинации $(m,d)_q^s$-хороших мономов. В следующем предложении отметим несколько важных свойств кода $\mathcal{C}_q^s(m,d)$, которые более формально разъясняют вышеописанную мотивацию. Это утверждение было доказано в [7,9] для полей характеристики 2. В общем случае доказательство работает без изменений.

Предложение 6. *Пусть $m \geqslant 2$ и $\mathcal{C} = \mathcal{C}_q^s(m,d)$. Тогда имеют место следующие свойства.*

1. *Мощность кода удовлетворяет соотношению*

$$\log_q |\mathcal{C}| = N_q^s(m,d).$$

Другими словами, образ $(m,d)_q^s$-хороших мономов при отображении $\mathrm{Ev}_{q,m}^s$ задает $\mathbb{F}_q$-базис кода $\mathcal{C}$, и кодовое слово, состоящее из символов $\mathbf{0}$, соответствует лишь тождественно нулевому многочлену;

2. *Минимальное расстояние в коде $\mathcal{C}$ не меньше*

$$1 + \left\lceil \frac{qs-d-s+1}{s} \right\rceil (q-s)q^{m-2};$$

3. *Пусть даны точка в пространстве $\boldsymbol{x}_0 \in \mathbb{F}_q^m$ и $m-1$ множество $A_j \subseteq \mathbb{F}_q$, $|A_j| = s$, $j \in [m-1]$. Определим множество*

$$S := \{\boldsymbol{x}_0 + \lambda \boldsymbol{a} :\ \lambda \in \mathbb{F}_q^*,\ \boldsymbol{a} = (a_1, \ldots, a_{m-1}, 1),\ a_j \in A_j,\ j \in [m-1]\}.$$

Пусть $d \leqslant qs - s$. Тогда для произвольного $\boldsymbol{x}_0 \in \mathbb{F}_q^m$ компонента $f^{(<s)}(\boldsymbol{x}_0) \in \in \mathbb{F}_q^{\binom{s+m-1}{m}}$ кодового слова $\mathrm{Ev}_{q,m}^s(f(\boldsymbol{X}))$ может быть восстановлена с помощью вектора значений $\left(f^{(<s)}(\boldsymbol{y}_0)\right)\big|_{\boldsymbol{y}_0 \in S}$. Таким образом, можно найти $\left(\frac{q}{s}\right)^{m-1}$ вза-

имно непересекающихся восстанавливающих множеств для каждой компоненты $f^{(<s)}(\boldsymbol{x}_0)$ кодового слова кода $\mathcal{C}$.

Замечание 2. Как сказано ранее, интерес к кодам $\mathcal{C}_q^s(m,d)$ в последние годы во многом объясняется свойством 3 в предложении 6, а также тем фактом, что при $d \geqslant qs-q$, фиксированном m, и $q=p^c \to \infty$ скорость этих кодов можно оценить величиной

$$1 - O\left(s^{-1}\left(\frac{q}{qs-d}\right)^{\lambda_p}\right),$$

где константа $\lambda_p < 0$. Также отметим, что при $qs-q \leqslant d < qs$, фиксированном m и $q=p^c \to \infty$ скорость кодов $\mathcal{M}_q^s(d,m)$ (недвоичных s-кодов Рида – Маллера) равна $1-\Theta(s^{-1})$, что меньше вышеуказанной оценки скорости кодов $\mathcal{C}_q^s(m,d)$ (более подробно см. в [7]).

1.3. Списочное декодирование s-кодов Рида – Соломона. Обобщение списочного алгоритма декодирования Гурусвами – Судана на случай s-кодов Рида – Соломона было впервые предложено в работе [10]. Отметим, что в случае $m=1$ можно опустить ограничение на то, что s является степенью простого p в определениях 4, 5. Мы приведем чуть более слабую версию утверждения из [10], более удобную для использования.

Предложение 7. *Пусть даны целые положительные числа s и q, где q – степень простого числа p, а $s<q$. Выберем некоторое целое число $\varphi \geqslant 3$ и целое число $d \in [s, qs]$. Тогда существует алгоритм $\mathfrak{A}_q^s(d,\varphi)$, входом которого является произвольный вектор $\boldsymbol{r} \in (\mathbb{F}_q^s)^q$, а выходом – множество всевозможных кодовых слов s-кода Рида – Соломона $\mathcal{L} \subseteq \mathcal{C}_q^s(1,d)$, для которых расстояние Хэмминга $d_H(\boldsymbol{c},\boldsymbol{r})$ удовлетворяет неравенству*

$$d_H(\boldsymbol{c},\boldsymbol{r}) \leqslant q - (1+3/\varphi)\sqrt{q(d-1)/s} - 1, \quad \boldsymbol{c} \in \mathcal{L}.$$

Более того, время работы этого алгоритма равно $\mathrm{poly}(q,\varphi)$, *а размер списка* $|\mathcal{L}| = O(\varphi\sqrt{sq/d})$.

В дальнейшем были найдены [11,12] более эффективные списочные декодеры для s-кода Рида – Соломона, заданного над простым полем $\mathbb{F}_p$. Однако мы воспользуемся вышеуказанным утверждением, поскольку нам потребуется использовать биективное отображение между пространством $\mathbb{F}_q^m$ и полем $\mathbb{F}_{q^m}$, а поле $\mathbb{F}_{q^m}$ при $m \geqslant 2$ гарантированно не является простым. Также отметим, что при $s=1$ списочное декодирование соответствующих кодов $\mathcal{C}_q^1(m,d)$ (m-мерных кодов Рида – Соломона) было впервые предложено в работе [13]. Мы воспользуемся идеями из этой работы, а также структурой алгоритма списочного декодера кодов $\mathcal{M}_q^s(d,m)$ (недвоичных s-кодов Рида – Маллера) из работы [11].

1.4. Базис в поле $\mathbb{F}_{q^m}$ и параметризация пространства $\mathbb{F}_q^m$. Пусть элементы $\alpha_1,\ldots,\alpha_m \in \mathbb{F}_{q^m}$ образуют $\mathbb{F}_q$-*базис* поля $\mathbb{F}_{q^m}$, т.е. всякий элемент $\beta \in \mathbb{F}_{q^m}$ представим в виде $\beta = \sum\limits_{j=1}^{m} \lambda_j \alpha_j$ для некоторых $\lambda_j \in \mathbb{F}_q$, $j \in [m]$. Через $\boldsymbol{\alpha}$ обозначим вектор $(\alpha_1,\ldots,\alpha_m)$. В дальнейшем будем кратко говорить, что $\boldsymbol{\alpha} \in \mathbb{F}_{q^m}^m$ является *базисом*.

Определение 6. Будем говорить, что набор из базисов $\boldsymbol{\alpha}_1,\ldots,\boldsymbol{\alpha}_t \in \mathbb{F}_{q^m}^m$ находится в s-*общем положении*, если для произвольного ненулевого многочлена $r(\boldsymbol{X}) \in \mathbb{F}_{q^m}[\boldsymbol{X}]$ степени $\deg(r(\boldsymbol{X})) < s$ существует такое число $i \in [t]$, что $r(\boldsymbol{\alpha}_i) \neq 0$.

Следующее утверждение было доказано в [11, 14].

Предложение 8. *Пусть даны число q, являющееся степенью простого числа p, целое число $m \geqslant 2$, а также целое положительное число s, $s < q$. Если $t \geqslant s^m$, то существует набор из базисов $\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_t \in \mathbb{F}_{q^m}^m$, находящийся в s-общем положении. Более того, такой набор может быть найден за время* $\mathrm{poly}(q, m)$.

Пусть $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_m) \in \mathbb{F}_{q^m}^m$ является базисом. Определим биективное отображение $\gamma_{\boldsymbol{\alpha}} \colon \mathbb{F}_{q^m} \to \mathbb{F}_q^m$ следующим образом:

$$\gamma_{\boldsymbol{\alpha}}(x) := \big(\mathrm{Tr}(\alpha_1 x), \ldots, \mathrm{Tr}(\alpha_m x)\big),$$

где функция $\mathrm{Tr} \colon \mathbb{F}_{q^m} \to \mathbb{F}_q$ является стандартным *следом* элементов расширенного поля $\mathbb{F}_{q^m}$ в $\mathbb{F}_q$, т.е. $\mathrm{Tr}(y) = \sum\limits_{i=0}^{m-1} y^{q^i}$. Кроме того, будем использовать запись $\mathrm{Tr}(T)$ для обозначения многочлена $\sum\limits_{i=0}^{m-1} T^{q^i}$. Следующее естественное утверждение было также доказано в [11, 14].

Предложение 9. *Пусть даны число q, являющееся степенью простого числа p, и целое число $m \geqslant 2$. Пусть также заданы многочлен $f(\boldsymbol{X}) \in \mathbb{F}_q[\boldsymbol{X}]$ и базис $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_m) \in \mathbb{F}_{q^m}^m$. Определим*

$$g(T) := f \circ \gamma_{\boldsymbol{\alpha}}(T) \in \mathbb{F}_{q^m}[T].$$

Тогда для произвольной точки $x_0 \in \mathbb{F}_{q^m}$ и любого $i \in [0, q-1]$ выполнено следующее соотношение:

$$g^{(i)}(x_0) = \sum_{\substack{\boldsymbol{e} \in \mathbb{N}^m \\ \deg(\boldsymbol{e}) = i}} f^{(\boldsymbol{e})}(\gamma_{\boldsymbol{\alpha}}(x_0)) \prod_{j=1}^{m} \alpha_j^{e_j}.$$

§ 2. Основные результаты

Главным результатом данной статьи является следующее утверждение.

Теорема 1. *Пусть даны числа q и s, являющиеся степенями простого числа p, а также положительные числа $m \geqslant 2$ и d, для которых верно $d \leqslant sq - m - 2(s-1)$ и $m + s \leqslant q$. Определим целое число*

$$\widetilde{d} := q^{m-1}\left(s - 1 + \frac{q-1}{q}(m + d - 1)\right)$$

и зададим некоторый целочисленный параметр $\varphi \geqslant 3$. Тогда существует алгоритм $\mathfrak{A}_q^s(d, m, \varphi)$, входом которого является произвольный вектор $\boldsymbol{r} \in \left(\mathbb{F}_q^{\binom{s+m-1}{m}}\right)^{q^m}$, а выходом – множество $\mathcal{L} \subseteq \mathcal{C}_q^s(m, d)$ всевозможных кодовых слов кода $\mathcal{C}_q^s(m, d)$, для которых расстояние Хэмминга $d_H(\boldsymbol{c}, \boldsymbol{r})$ удовлетворяет неравенству

$$d_H(\boldsymbol{c}, \boldsymbol{r}) \leqslant q^m - (1 + 3/\varphi)\sqrt{q^m \widetilde{d}/s} - 1, \quad \boldsymbol{c} \in \mathcal{L}.$$

Более того, время работы этого алгоритма равно $\mathrm{poly}\left(q^m, \left(\varphi\sqrt{sq^m/\widetilde{d}}\right)^{s^m}\right)$, *а размер списка можно оценить величиной* $O\left(\left(\varphi\sqrt{sq^m/\widetilde{d}}\right)^{s^m}\right)$.

Замечание 3. Время работы данного алгоритма и размер списка равны $\mathrm{poly}(q^m)$ в случае $q = p^c \to \infty$, $s = O(1)$, $m = O(1)$. Отметим, что используя некоторые идеи из [14], можно привести списочный алгоритм декодирования со сложностью

и размером списка $\mathrm{poly}(q^m)$ без подобного ограничения на s и m. Однако радиус декодирования для подобного алгоритма будет уступать вышеуказанному.

Мы приведем алгоритм списочного декодирования в п. 2.1 и проанализируем его в п. 2.2. В процессе доказательства мы выведем утверждение, которое поможет (незначительно) улучшить оценку на минимальное расстояние кодов $\mathcal{C}_q^s(m,d)$, указанную ранее в предложении 6. Следующее утверждение будет доказано в п. 2.3.

Т е о р е м а 2. *Пусть даны числа q и s, являющиеся степенями простого числа p, а также положительные числа $m \geqslant 2$ и d, такие что*

$$d \leqslant sq - m - 2(s-1) \quad u \quad m + s \leqslant q.$$

Тогда минимальное расстояние кода $\mathcal{C}_q^s(m,d)$ находится в интервале $[\underline{d}, \overline{d}\,]$, где величины $\underline{d}$ и $\overline{d}$ заданы следующим образом:

$$\underline{d} := q^m - \left\lfloor \frac{s - 1 + \dfrac{q-1}{q}(m+d-1)}{s} q^{m-1} \right\rfloor, \quad \overline{d} := q^m - \left\lfloor \frac{d-1}{s} \right\rfloor q^{m-1}.$$

2.1. Алгоритм списочного декодирования. Опишем алгоритм списочного декодирования, которым воспользуемся для доказательства теоремы 1. Пусть входом алгоритма является $\boldsymbol{r} \in \left(\mathbb{F}_q^{\binom{s+m-1}{m}}\right)^{q^m}$. Пусть $\boldsymbol{y}_0 \in \mathbb{F}_q^m$ и $\boldsymbol{e} \in \mathbb{N}^m$, $\deg(\boldsymbol{e}) < s$. Для удобства обозначений будем писать $r^{(\boldsymbol{e})}(\boldsymbol{y}_0)$ при обращении к элементу (из $\mathbb{F}_q$) вектора $\boldsymbol{r}$, который естественно индексировать парой $(\boldsymbol{y}_0, \boldsymbol{e})$.

1. Пусть $t = s^m$. Найдем набор базисов $\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_t \in \mathbb{F}_{q^m}^m$, находящийся в s-общем положении.
2. Для всякого $\ell \in [t]$ определим функцию (вектор) $\boldsymbol{h}_\ell \colon \mathbb{F}_{q^m} \to \mathbb{F}_{q^m}^s$ по правилу

$$(h_\ell(x_0))_i = \sum_{\substack{\boldsymbol{e} \in \mathbb{N}^m \\ \deg(\boldsymbol{e}) = i}} r^{(\boldsymbol{e})}(\gamma_{\boldsymbol{\alpha}_\ell}(x_0)) \prod_{j=1}^{m} {\alpha_{\ell,j}}^{e_j}, \quad \forall x_0 \in \mathbb{F}_{q^m},\ i \in [0, s-1].$$

3. Для всякого $\ell \in [t]$ воспользуемся алгоритмом $\mathfrak{A}_q^s(\widetilde{d}+1, \varphi)$ из предложения 7 и восстановим множество $\mathcal{L}_\ell$ всевозможных кодовых слов $\boldsymbol{c} \in \mathcal{C}_{q^m}^s(1, \widetilde{d}+1)$, для которых выполнено

$$d_H(\boldsymbol{c}, \boldsymbol{h}_\ell) \leqslant q^m - (1 + 3/\varphi)\sqrt{q^m \widetilde{d}/s} - 1.$$

4. Для всякого набора $(\boldsymbol{c}_1, \ldots, \boldsymbol{c}_t) \in \mathcal{L}_1 \times \cdots \times \mathcal{L}_t$ найдем сначала соответствующий им набор $(\widetilde{g}_1(T), \ldots, \widetilde{g}_t(T)) \in (\mathbb{F}_{q^m}[T])^t$ многочленов степени не выше $\widetilde{d}$, а затем множество всевозможных "согласованных" многочленов $\widetilde{f}(\boldsymbol{X}) \in V_q^s(m,d)$, таких что

$$\widetilde{f} \circ \gamma_{\alpha_\ell}(T) \equiv_s \widetilde{g}_\ell(T), \quad \forall \ell \in [t]. \tag{2}$$

5. Выходом алгоритма будет список всевозможных многочленов $\widetilde{f}(\boldsymbol{X}) \in \mathbb{F}_q[\boldsymbol{X}]$, найденных на четвертом шаге, для которых выполнено

$$d_H(\mathrm{Ev}_{q,m}^s(\widetilde{f}(\boldsymbol{X})), \boldsymbol{r}) \leqslant q^m - (1 + 3/\varphi)\sqrt{q^m \widetilde{d}/s} - 1.$$

2.2. Анализ алгоритма. Сначала кратко рассмотрим каждый из шагов алгоритма, а затем проанализируем важные аспекты некоторых шагов более подробно.

Первый шаг. В силу предложения 8 такой набор существует и может быть найдет за время $\mathrm{poly}(q, m)$.

Второй шаг. В силу предложения 9 способ задания функции (вектора) $\boldsymbol{h}_\ell$ соответствует заданию функции $h_\ell(T) = r \circ \gamma_{\boldsymbol{\alpha}_\ell}(T)$, если интерпретировать вектор $\boldsymbol{r}$ как функцию $r(\boldsymbol{X})$.

Третий шаг. Пусть $f(\boldsymbol{X}) \in V_q^s(m, d)$. Тогда в силу леммы 3, которую мы докажем чуть позже, многочлен $g_\ell(T) := f \circ \gamma_{\boldsymbol{\alpha}_\ell}(T)$ является s-эквивалентным многочлену степени не выше $\widetilde{d}$. Таким образом, если расстояние Хэмминга между $\boldsymbol{r}$ и $\mathrm{Ev}_{q,m}^s(f(\boldsymbol{X}))$ невелико, то одно из кодовых слов в множестве $\mathcal{L}_\ell$ будет соответствовать многочлену $g_\ell(T)$ (см. более подробно лемму 1).

Четвертый шаг. Каждый многочлен $\widetilde{f}(\boldsymbol{X}) \in V_q^s(m, d)$ можно задать с помощью $N_q^s(m, d)$ коэффициентов из $\mathbb{F}_q$, каждый из которых соответствует некоторому $(m, d)_q^s$-хорошему моному (см. обозначения после определения 4). Многочлен, стоящий в правой части уравнения (2), уже определен, а в левой части стоит неопределенный многочлен с $N_q^s(m, d)$ неизвестными, для которого можно взять остаток при делении на $T^{sq^m} + (-T)^s$ (см. предложение 3). Отметим, что в силу леммы 3 степень многочлена, полученного как остаток, не превосходит $\widetilde{d}$. Таким образом, нужно решить систему линейных уравнений с $N_q^s(m, d)$ неизвестными и $t(\widetilde{d}+1)$ ограничениями. В силу леммы 2, которую мы докажем чуть позже, существует не более одного многочлена $\widetilde{f}(\boldsymbol{X}) \in V_q^s(m, d)$, удовлетворяющего системе уравнений (2) для данного набора $(\widetilde{g}_1(T), \ldots, \widetilde{g}_t(T))$. Таким образом, для поиска всевозможных $\widetilde{f}(\boldsymbol{X}) \in V_q^s(m, d)$ нужно потратить время $\mathrm{poly}\big(q^m, t\widetilde{d}, N_q^s(m, d)\big) \prod\limits_{\ell=1}^{t} |\mathcal{L}_\ell|$.

Пятый шаг. Перед выходом из алгоритма нужно будет отсеять те многочлены $f(\boldsymbol{X}) \in V_q^s(m, d)$, для которых выполнено

$$d_H(\mathrm{Ev}_{q,m}^s(f(\boldsymbol{X})), \boldsymbol{r}) > q^m - (1 + 3/\varphi)\sqrt{q^m \widetilde{d}/s} - 1.$$

Мы докажем корректность всего алгоритма в лемме 1.

Используя предложение 7, оценим суммарную сложность и время работы алгоритма. Сложность первого шага равна $\mathrm{poly}(q, m)$, второго – $\mathrm{poly}(q^m)$, третьего – $\mathrm{poly}(q^m, \varphi)$, четвертого и пятого шагов – $\mathrm{poly}\left(q^m, \left(\varphi\sqrt{sq^m/\widetilde{d}}\right)^{s^m}\right)$. Итоговый размер списка оценивается величиной $O\left(\left(\varphi\sqrt{sq^m/\widetilde{d}}\right)^{s^m}\right)$.

Наконец, докажем несколько оставшихся утверждений.

Лемма 1. *Предположим, что для некоторого многочлена $f(\boldsymbol{X}) \in V_q^s(m, d)$ расстояние Хэмминга удовлетворяет неравенству*

$$d_H(\mathrm{Ev}_{q,m}^s(f(\boldsymbol{X})), \boldsymbol{r}) \leqslant q^m - (1 + 3/\varphi)\sqrt{q^m \widetilde{d}/s} - 1.$$

Тогда список многочленов на выходе предложенного списочного алгоритма будет содержать $f(\boldsymbol{X})$.

Доказательство. Для всякого $\ell \in [t]$ рассмотрим базис

$$\boldsymbol{\alpha}_\ell = (\alpha_{\ell,1}, \ldots, \alpha_{\ell,m}) \in \mathbb{F}_{q^m}^m$$

и многочлен

$$g_\ell(T) := f \circ \gamma_{\boldsymbol{\alpha}_\ell}(T).$$

Используя предложение 9, имеем

$$g_\ell^{(i)}(x_0) = \sum_{\substack{\boldsymbol{e}\in\mathbb{N}^m \\ \deg(\boldsymbol{e})=i}} f^{(\boldsymbol{e})}(\gamma_{\boldsymbol{\alpha}_\ell}(x_0)) \prod_{j=1}^{m} \alpha_{\ell,j}^{e_j}, \quad \forall x_0 \in \mathbb{F}_{q^m},\ i \in [0, s-1].$$

Из условия утверждения существуют не менее $(1+3/\varphi)\sqrt{q^m\widetilde{d}/s}+1$ точек $\boldsymbol{y}_0 \in \mathbb{F}_q^m$, таких что $f^{(<s)}(\boldsymbol{y}_0) = r^{(<s)}(\boldsymbol{y}_0)$. Также отметим, что $\gamma_{\boldsymbol{\alpha}_\ell}$ является биекцией между $\mathbb{F}_{q^m}$ и $\mathbb{F}_q^m$. Тогда на втором шаге алгоритма найдется не менее $(1+3/\varphi)\sqrt{q^m\widetilde{d}/s}+1$ точек $x_0 \in \mathbb{F}_{q^m}$, для которых выполнено $g_\ell^{(i)}(x_0) = (h_\ell(x_0))_i$ для всех $i \in [0, s-1]$. Заметим, что степень $\deg(g_\ell(T)) \leqslant \widetilde{d}$ в силу леммы 3. Следовательно, множество $\mathcal{L}_\ell$, полученное на третьем шаге, будет содержать кодовое слово кода $\mathcal{C}_{q^m}^s(1, \widetilde{d}+1)$, соответствующее многочлену $g_\ell(T)$. Таким образом, на четвертом шаге будет рассмотрен набор, соответствующий $(g_1(T), \ldots, g_t(T))$, и многочлен $f(\boldsymbol{X}) \in V_q^s(m,d)$ будет найден при решении системы уравнений и включен в список на выходе алгоритма. ▲

Лемма 2. *Предположим, что существуют два многочлена* $\widetilde{f}_1(\boldsymbol{X}), \widetilde{f}_2(\boldsymbol{X}) \in V_q^s(m,d)$, *удовлетворяющие соотношению* (2). *Тогда* $\widetilde{f}_1(\boldsymbol{X}) = \widetilde{f}_2(\boldsymbol{X})$.

Доказательство. Определим $h(\boldsymbol{X}) := \widetilde{f}_1(\boldsymbol{X}) - \widetilde{f}_2(\boldsymbol{X})$. Рассмотрим некоторое число $\ell \in [t]$ и базис $\boldsymbol{\alpha}_\ell = (\alpha_{\ell,1}, \ldots, \alpha_{\ell,m}) \in \mathbb{F}_{q^m}^m$. Тогда выполнено соотношение

$$h \circ \gamma_{\boldsymbol{\alpha}_\ell}(T) \equiv_s 0.$$

В силу предложения 9 выполнено

$$\sum_{\substack{\boldsymbol{e}\in\mathbb{N}^m \\ \deg(\boldsymbol{e})=i}} h^{(\boldsymbol{e})}(\gamma_{\boldsymbol{\alpha}_\ell}(x_0)) \prod_{j=1}^{m} \alpha_{\ell,j}^{e_j} = 0, \quad \forall x_0 \in \mathbb{F}_{q^m},\ i \in [0, s-1],$$

где $\boldsymbol{e} = (e_1, \ldots, e_m)$. Поскольку отображение $\gamma_{\boldsymbol{\alpha}_\ell}$ задает биекцию между $\mathbb{F}_{q^m}$ и $\mathbb{F}_q^m$, мы можем заключить, что для всякой точки $\boldsymbol{y}_0 \in \mathbb{F}_q^m$ верно

$$\sum_{\substack{\boldsymbol{e}\in\mathbb{N}^m \\ \deg(\boldsymbol{e})=i}} h^{(\boldsymbol{e})}(\boldsymbol{y}_0) \prod_{j=1}^{m} \alpha_{\ell,j}^{e_j} = 0.$$

Мы можем думать о вышеуказанном выражении как о вычислении в точке $\boldsymbol{\alpha}_\ell$ значения многочлена

$$v(\boldsymbol{X}) := \sum_{\substack{\boldsymbol{e}\in\mathbb{N}^m \\ \deg(\boldsymbol{e})=i}} h^{(\boldsymbol{e})}(\boldsymbol{y}_0)\boldsymbol{X}^{\boldsymbol{e}}.$$

Степень данного многочлена меньше s. Поскольку набор базисов был выбран в s-общем положении, в силу определения 6 можно заключить, что $v(\boldsymbol{X})$ тождественно равен нулю. Отсюда следует, что $h^{(\boldsymbol{e})}(\boldsymbol{y}_0) = 0$ для всех $\boldsymbol{y}_0 \in \mathbb{F}_q^m$ и $\boldsymbol{e} \in \mathbb{N}^m$, $\deg(\boldsymbol{e}) < s$. Поскольку $h(\boldsymbol{X}) \in V_q^s(m,d)$, из первого утверждения в предложении 6 следует, что $h(\boldsymbol{X}) = 0$. Таким образом, требуемое утверждение доказано. ▲

Лемма 3. *Пусть даны числа q и s, являющиеся степенями простого числа p, а также положительные числа $m \geqslant 2$ и d, такие что*

$$d \leqslant sq - m - 2(s-1) \quad и \quad m + s \leqslant q.$$

Пусть вектор $\boldsymbol{\alpha} \in \mathbb{F}_{q^m}^m$ является базисом, и пусть $f(\boldsymbol{X}) \in V_q^s(m,d)$. Определим $g(T) := f \circ \gamma_{\boldsymbol{\alpha}}(T)$. Тогда существует единственный многочлен $r(T) \in \mathbb{F}_{q^m}[T]$, для которого верно $r(T) \equiv_s g(T)$ и $\deg(r(T)) \leqslant \widetilde{d}$, где

$$\widetilde{d} = q^{m-1}\left(s - 1 + \frac{q-1}{q}(m+d-1)\right).$$

Доказательство. Пусть $\lambda \in \mathbb{F}_q$, а $z(\boldsymbol{X}) \in V_q^s(d,m)$. В силу линейности

$$(f + \lambda z) \circ \gamma_{\boldsymbol{\alpha}}(T) = f \circ \gamma_{\boldsymbol{\alpha}}(T) + \lambda(z \circ \gamma_{\boldsymbol{\alpha}}(T))$$

достаточно рассматривать лишь многочлен $f(\boldsymbol{X})$, который является в точности $(m,d)_q^s$-хорошим мономом $\boldsymbol{X}^{\boldsymbol{v}}$, $\boldsymbol{v} = (v_1, \ldots, v_m) \in \mathbb{N}^m$. В дальнейшем будем использовать векторы $\boldsymbol{e}_j = (e_{j,0}, \ldots, e_{j,m-1})$, $j \in [m]$. Распишем получившийся многочлен $g(T)$ от одной переменной в таком случае:

$$g(T) = \prod_{j=1}^{m} \left(\mathrm{Tr}(\alpha_j T)\right)^{v_j} = \prod_{j=1}^{m} \left(\sum_{i=0}^{m-1} (\alpha_j T)^{q^i}\right)^{v_j} =$$

$$= \prod_{j=1}^{m} \left(\sum_{\substack{\boldsymbol{e}_j \in \mathbb{N}^m \\ \deg(\boldsymbol{e}_j) = v_j}} \binom{v_j}{e_{j,0}, \ldots, e_{j,m-1}} (\alpha_j T)^{\sum\limits_{i=0}^{m-1} e_{j,i} q^i} \right) =$$

$$= \sum_{\substack{\boldsymbol{e}_1 \in \mathbb{N}^m, \ldots, \boldsymbol{e}_m \in \mathbb{N}^m \\ \deg(\boldsymbol{e}_1) = v_1, \ldots, \deg(\boldsymbol{e}_m) = v_m}} T^{\sum\limits_{j=1}^{m} \sum\limits_{i=0}^{m-1} e_{j,i} q^i} \prod_{j=1}^{m} \binom{v_j}{e_{j,0}, \ldots, e_{j,m-1}} \alpha_j^{\sum\limits_{i=0}^{m-1} e_{j,i} q^i}.$$

Далее воспользуемся следствием 1, чтобы упростить данное выражение. Из этого утверждения следует, что если хотя бы для одного $i \in [0, m-1]$ не выполнено отношение порядка $e_{j,i} \leqslant_p v_j$, то соответствующий мультиномиальный коэффициент $\binom{v_j}{e_{j,0}, \ldots, e_{j,m-1}}$ равен нулю в поле характеристики p. В дальнейшем анализе будем рассматривать лишь слагаемые вышеуказанной суммы, для которых выполнено условие $\boldsymbol{e}_j \leqslant_p v_j$ для всех $j \in [m]$. В силу предложения 3 нас интересует многочлен $r(T)$ степени не выше $sq^m - 1$, для которого выполнено

$$r(T) \equiv g(T) \pmod{T^{sq^m} + (-T)^{q^m}}.$$

Для произвольного набора векторов $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_m \in \mathbb{N}^m$, для которых верно $\boldsymbol{e}_j \leqslant_p v_j$, $\deg(\boldsymbol{e}_j) = v_j$, $j \in [m]$, определим величину

$$\widetilde{e} := \sum_{j=1}^{m} \sum_{i=0}^{m-1} e_{j,i} q^i.$$

Таким образом, достаточно показать, что $\widetilde{e}$ удовлетворяет условию $\mathrm{Mod}_{q^m}^s(\widetilde{e}) \leqslant \widetilde{d}$.

Напомним, что моном $\boldsymbol{X}^{\boldsymbol{v}}$ является $(m,d)_q^s$-хорошим. Следовательно, из определения 4 имеем, что для произвольного $\boldsymbol{a} \in \mathbb{N}^m$, $a_j \leqslant_p v_j$, $j \in [m]$, выполнено неравенство $\mathrm{Mod}_q^s(\deg(\boldsymbol{a})) < d$. Возьмем в качестве $\boldsymbol{a} = (a_1, \ldots, a_m)$ вектор, j-я компонента

которого равна $a_j = e_{j,m-1}$. Тогда из определений хороших мономов и операции Mod_q^s получим, что

$$\sum_{j=1}^{m} e_{j,m-1} = \eta(qs - s) + \mu,$$

где целые числа удовлетворяют соотношениям $\eta \geqslant 0$ и $0 \leqslant \mu < d$. Более того, если $\eta > 0$, то $\mu \geqslant s$.

В дальнейшем мы получим верхнюю и нижнюю оценки на величину $\widetilde{e}$, что поможет доказать необходимое неравенство $\mathrm{Mod}_{q^m}^s(\widetilde{e}) \leqslant \widetilde{d}$. Начнем с верхней границы, при выводе которой воспользуемся соотношениями

$$v_j = \sum_{i=0}^{m-1} e_{j,i}, \quad j \in [m], \quad \text{и} \quad \sum_{j=1}^{m} v_j \leqslant q(s-1) + m(q-1)$$

(эквивалентно условию $\deg_q(\boldsymbol{v}) \leqslant s - 1$ в определении 4). Имеем

$$\widetilde{e} = \sum_{j=1}^{m}\sum_{i=0}^{m-1} e_{j,i}q^i \leqslant q^{m-1}\sum_{j=1}^{m} e_{j,m-1} + q^{m-2}\sum_{j=1}^{m}(v_j - e_{j,m-1}) \leqslant$$
$$\leqslant (q^{m-1} - q^{m-2})\sum_{j=1}^{m} e_{j,m-1} + q^{m-2}(q(s-1) + m(q-1)).$$

Напомним, что $\sum\limits_{j=1}^{m} e_{j,m-1} = \eta(qs - s) + \mu$. Продолжим вывод верхней оценки:

$$\widetilde{e} \leqslant (q^{m-1} - q^{m-2})(\eta(qs-s) + \mu) + q^{m-2}(qs - q + m(q-1)) =$$
$$= \eta(sq^m - s) + q^{m-1}(s - 1 + m + \mu - 2s\eta) + q^{m-2}(s\eta - \mu - m) + s\eta.$$

Теперь оценим $\widetilde{e}$ снизу:

$$\widetilde{e} = \sum_{j=1}^{m}\sum_{i=0}^{m-1} e_{j,i}q^i \geqslant \sum_{j=1}^{m} e_{j,m-1}q^{m-1} = q^{m-1}(\eta(qs-s) + \mu) \geqslant$$
$$\geqslant \eta(sq^m - s) + \eta s + (\mu - s\eta)q^{m-1}.$$

Заметим, что моном $\boldsymbol{X}^{\boldsymbol{a}}$ с $\boldsymbol{a} = (e_{1,m-1}, \ldots, e_{m,m-1})$ является также $(m,d)_q^s$-хорошим, поскольку $\boldsymbol{a} \leqslant_p \boldsymbol{v}$, и выполнено естественное свойство транзитивности для $(m,d)_q^s$-хороших мономов. Напоследок воспользуемся оценкой $\mu \geqslant s\eta$, которая следует из предложения 10, поскольку верно $d \leqslant sq - m - 2(s-1)$ по условию доказываемого утверждения. Таким образом, объединяя верхнюю и нижнюю границы для $\widetilde{e}$, получаем

$$\eta(sq^m - s) + \eta s \leqslant \widetilde{e} \leqslant \eta(sq^m - s) + d',$$

где

$$d' := q^{m-1}(s - 1 + m + \mu - 2s\eta) + q^{m-2}(s\eta - \mu - m) + s\eta.$$

Очевидно, что d' достигает максимального значения

$$\widetilde{d} = q^{m-1}\left(s - 1 + \frac{q-1}{q}(m + d - 1)\right)$$

при $\eta = 0$, $\mu = d - 1$. Если $\eta = 0$, то $\widetilde{e} \leqslant \widetilde{d}$ и $\mathrm{Mod}^s_{q^m}(\widetilde{e}) \leqslant \widetilde{d}$. Если $\eta > 0$, то $\widetilde{e} \geqslant \eta s$ и $\mathrm{Mod}^s_{q^m}(\widetilde{e}) = b$, где $b \in [\eta s, \widetilde{d}]$ и $b \equiv \widetilde{e} \pmod{sq^m - s}$. Эти рассуждения завершают доказательство. ▲

Предложение 10. *Пусть даны числа s и q, являющиеся степенями простого числа p, и положительное число $m \geqslant 2$, $m + s \leqslant q$. Предположим, что моном $\boldsymbol{X}^{\boldsymbol{v}}$ для некоторого вектора $\boldsymbol{v} = (v_1, \ldots, v_m) \in \mathbb{N}^m$ является $(m, sq - m - 2(s-1))^s_q$-хорошим. Тогда для целых чисел $\eta \geqslant 0$ и $0 \leqslant \mu < sq - m - 2(s-1)$ (причем $\mu \geqslant s$ при $\eta > 0$), удовлетворяющих соотношению*

$$\sum_{j=1}^{m} v_j = \eta s(q-1) + \mu,$$

выполнено неравенство $\eta s \leqslant \mu$.

Доказательство. Предположим противное, т.е. выполнено $\eta s > \mu$. Определим целые числа $h := \eta s$ и $k := p^\ell - h + \mu$, где $\ell \in \mathbb{N}$ – наименьшее число, при котором $p^\ell > h$. Заметим, что выполнено неравенство $q > h = \eta s$, так как

$$\deg(\boldsymbol{v}) = \eta s(q-1) + \mu \leqslant q(s-1) + m(q-1)$$

(из условия $\deg_q(\boldsymbol{v}) \leqslant s - 1$ в определении 4), и следовательно,

$$\eta s \leqslant m + \left\lfloor \frac{q}{q-1}(s-1) \right\rfloor = m + s - 1 < q. \tag{3}$$

Также отметим, что при таком выборе чисел имеет место следующее (частичное) p-ичное разложение:

$$\deg(\boldsymbol{v}) = \sum_{j=1}^{m} v_j = \eta s(q-1) + \mu = hq - h + \mu =$$
$$= (h-1)p^{\log_p q} + (p-1) \sum_{i=\ell}^{\log_p q - 1} p^i + k.$$

Тогда h, k, p и μ удовлетворяют условию предложения 12, так как $h = \eta s > \mu$ по предположению и $h < p^\ell$, $k = p^\ell - h + \mu$ по построению. Из этого утверждения следует, что существует число $\theta \in \mathbb{N}$, для которого верно $\theta \leqslant_p k$ и $\mu \leqslant \theta \leqslant h - 1$. Определим $e := \sum\limits_{j=1}^{m} v_j - \theta$. Поскольку $\theta \leqslant_p k$ и выполнено вышеуказанное (частичное) p-ичное разложение для суммы $\sum\limits_{j=1}^{m} v_j$, имеем $e \leqslant_p \sum\limits_{j=1}^{m} v_j$. Из предложения 11 следует, что существуют $e_1, \ldots, e_m \in \mathbb{N}$, такие что $\sum\limits_{j=1}^{m} e_j = e$ и $e_j \leqslant_p v_j$ для всех $j \in [m]$. Наконец, для получения противоречия посчитаем величину $\mathrm{Mod}^s_q(e)$. Поскольку

$$e = \sum_{j=1}^{m} v_j - \theta = \eta s(q-1) + \mu - \theta$$

и $\mu \leqslant \theta \leqslant s\eta - 1$, получаем, что

$$\mathrm{Mod}^s_q(e) \geqslant sq - s + (\mu - \theta) \geqslant sq - s - \eta s + 1.$$

Воспользуемся неравенством (3) и получим $\mathrm{Mod}^s_q(e) \geq sq - m - 2(s-1)$, что противоречит тому, что $\boldsymbol{X}^{\boldsymbol{v}}$ является $(sq - m - 2(s-1), m)^s_q$-хорошим. ▲

Следующие два технических утверждения необходимы для доказательства предложения 10.

Предложение 11. *Пусть даны числа* $v_1, \ldots, v_m, h \in \mathbb{N}$ *и простое число* p. *Предположим, что имеет место отношение порядка* $e \leqslant_p \sum\limits_{j=1}^{m} v_j$. *Тогда существуют* $e_1, \ldots, e_m \in \mathbb{N}$, *такие что* $\sum\limits_{j=1}^{m} e_j = e$ *и* $e_j \leqslant_p v_j$ *для всех* $j \in [m]$.

Доказательство. Рассмотрим многочлен $(1+T)^{\sum\limits_{j=1}^{m} v_j}$. Коэффициент при мономе T^e равен $\binom{\sum\limits_{j=1}^{m} v_j}{e}$. Из предложения 4 следует, что этот коэффициент удовлетворяет условию

$$\binom{\sum\limits_{j=1}^{m} v_j}{e} \not\equiv 0 \pmod{p},$$

так как справедливо отношение порядка $e \leqslant_p \sum\limits_{j=1}^{m} v_j$. С другой стороны, этот коэффициент при T^e равен

$$\sum_{\substack{\boldsymbol{e} \in \mathbb{N}^m \\ \deg(\boldsymbol{e}) = e}} \prod_{j=1}^{m} \binom{v_j}{e_j},$$

откуда получаем, что существуют хотя бы один выбор $e_1, \ldots, e_m \in \mathbb{N}$, такой что $\prod\limits_{j=1}^{m} \binom{v_j}{e_j} \not\equiv 0 \pmod{p}$. Если воспользоваться предложением 4 для e_j и v_j, то получим требуемое утверждение. ▲

Предложение 12. *Пусть даны числа* $h, k, \ell, \mu \in \mathbb{N}$ *и простое число* p. *Предположим, что выполнено* $k = p^\ell - h + \mu$ *и* $\mu < h < p^\ell$. *Тогда существует некоторое число* $\theta \in \mathbb{N}$, *для которого* $\theta \leqslant_p k$ *и* $\mu \leqslant \theta \leqslant h-1$.

Доказательство. Воспользуемся тождеством

$$\binom{p^\ell - 1}{\mu + p^\ell - k - 1} = \sum_{\theta=\mu}^{\min\{h-1,k\}} \binom{k}{\theta} \binom{p^\ell - k - 1}{\mu + p^\ell - k - 1 - \theta} =$$

$$= \sum_{\theta=\mu}^{\min\{h-1,k\}} \binom{k}{\theta} \binom{p^\ell - k - 1}{\theta - \mu}.$$

Действительно, левая часть равна числу способов выбрать $\mu + p^\ell - k - 1$ элементов из данного множества мощности $p^\ell - 1$. В средней части мы сначала выбираем среди первых k элементов некоторое подмножество из θ элементов, а затем из оставшихся $p^\ell - k - 1$ элементов некоторые $\mu + p^\ell - k - 1 - \theta$. Из предложения 4 следует, что левая часть по модулю p не равна нулю. Действительно, выполнено соотношение $a \leqslant_p p^\ell - 1$ для всякого $a \leqslant p^{\ell-1}$. Следовательно, существует хотя бы один выбор θ, при котором одно из слагаемых в правой части не равно нулю по модулю p. Используя снова предложение 4, получаем что для такого θ верно отношение порядка $\theta \leqslant_p k$. Более того, из ограничений суммы имеем $\mu \leqslant \theta \leqslant h-1$. ▲

2.3. Доказательство теоремы 2. Определим число $n_0 := \lfloor (d-1)/s \rfloor$ и произвольное подмножество $B \subseteq \mathbb{F}_q$ размера $|B| = n_0$. Для доказательства границы сверху на минимальное расстояние заметим, что ненулевой многочлен $f(X_1, \ldots, X_m) :=$

$:= \prod\limits_{\beta \in B} (X_1 - \beta)^s$ степени $\deg(f(\boldsymbol{X})) \leqslant d-1$ является $(m,d)_q^s$-хорошим. В силу предложения 2 и формулы для производной Хассе несложно видеть, что число позиций в кодовом слове $\mathrm{Ev}_{q,m}^s(f(\boldsymbol{X}))$, не равных $\mathbf{0}$, равно $\overline{d} = (q-n_0)q^{m-1}$.

Теперь докажем оценку снизу на минимальное расстояние. Пусть даны два различных многочлена $f_1(\boldsymbol{X}), f_2(\boldsymbol{X}) \in V_q^s(m,d)$. Определим $\widehat{f}(\boldsymbol{X}) := f_1(\boldsymbol{X}) - f_2(\boldsymbol{X}) \neq 0$. Для базиса $\boldsymbol{\alpha} \in \mathbb{F}_{q^m}^m$ определим $g(T) := \widehat{f} \circ \gamma_{\boldsymbol{\alpha}}(T)$. В силу леммы 3 можно заключить, что $g(T)$ является s-эквивалентным многочлену $r(T)$ степени не выше $\widetilde{d} = q^{m-1}\left(s - 1 + \dfrac{q-1}{q}(m+d-1)\right)$. Более того, используя формулу для подсчета производных из предложения 9, можно найти базис $\boldsymbol{\alpha} \in \mathbb{F}_{q^m}^m$, такой что соответствующий многочлен $r(T) \neq 0$. Действительно, для $x_0 \in \mathbb{F}_{q^m}$ и $i \in [0, s-1]$ верно соотношение

$$r^{(i)}(x_0) = \sum_{\substack{\boldsymbol{e} \in \mathbb{N}^m \\ \deg(\boldsymbol{e}) = i}} \widehat{f}^{(\boldsymbol{e})}(\gamma_{\boldsymbol{\alpha}}(x_0)) \prod_{j=1}^{m} \alpha_j^{e_j}.$$

Так как многочлен $\widehat{f}(\boldsymbol{X}) \in V_q^s(m,d)$ ненулевой, а отображение $\gamma_{\boldsymbol{\alpha}}$ задает биекцию между $\mathbb{F}_{q^m}$ и $\mathbb{F}_q^m$, то найдутся $y_0 \in \mathbb{F}_{q^m}$ и $\boldsymbol{w} \in \mathbb{N}^m$, $\deg(\boldsymbol{w}) < s$, такие что $\widehat{f}^{(\boldsymbol{w})}(\gamma_{\boldsymbol{\alpha}}(y_0)) \neq 0$. Из предложения 8 следует, что существует базис $\boldsymbol{\alpha}$, для которого $r^{(\deg(\boldsymbol{w}))}(y_0) \neq 0$. Значит, для этого же $\boldsymbol{\alpha}$ верно $r(T) \neq 0$. Тогда число точек $x_0 \in \mathbb{F}_{q^m}$, для которых выполнено $r^{(i)}(x_0) = 0$ для всех $i \in [0, s-1]$, не превосходит величины $\left\lfloor \dfrac{\widetilde{d}}{s} \right\rfloor$. Следовательно, число точек $x_0 \in \mathbb{F}_{q^m}$, для которых $r^{(<s)}(x_0) \neq \mathbf{0}$, не меньше $\underline{d} = q^m - \left\lfloor \dfrac{\widetilde{d}}{s} \right\rfloor$. Снова воспользовавшись формулой для подсчета производной $r^{(i)}(x_0)$, заключаем, что число точек $\boldsymbol{z}_0 \in \mathbb{F}_q^m$, для которых $\widehat{f}^{(<s)}(\boldsymbol{z}_0) \neq \mathbf{0}$, не меньше $\underline{d}$.

§ 3. Доказательства вспомогательных утверждений

Доказательство предложения 3. Сначала докажем существование такого многочлена. Рассмотрим многочлен $g(T)$, полученный из $f(T)$ в качестве остатка при делении на $(T^q - T)^s$. Его степень очевидно меньше sq. Отметим, что

$$g(T) = f(T) + h(T)(T^q - T)^s$$

для некоторого $h(T) \in \mathbb{F}_q[T]$. Из свойств производных Хассе (предложения 1 и 2) следует, что вычисление $g^{(i)}(t_0)$ в точке $t_0 \in \mathbb{F}_q$ для всякого $i \in [0, s-1]$ эквивалентно вычислению $f^{(i)}(t_0)$, поскольку $t_0^q = t_0$ для всех $t_0 \in \mathbb{F}_q$.

Предположим, что существует другой многочлен $\widehat{g}(t)$ степени не выше $sq-1$, такой что $\widehat{g}(T) \equiv_s f(T)$. Тогда рассмотрим многочлен $r(T) := \widehat{g}(T) - g(T)$, степень которого не выше $sq-1$. Из определения производной Хассе (см. определение 1) для всякого $t_0 \in \mathbb{F}_q$ имеем

$$r(T) = r(t_0 + (T - t_0)) = \sum_{i \in \mathbb{N}} r^{(i)}(t_0)(T - t_0)^i.$$

С другой стороны, из линейности производной Хассе (предложение 1) следует, что

$$r^{(i)}(t_0) = \widehat{g}^{(i)}(t_0) - g^{(i)}(t_0) = 0 \quad \text{для } i \in [0, s-1].$$

Следовательно, $(T-t_0)^s \mid r(T)$ для всякого $t_0 \in \mathbb{F}_q$, откуда $(T^q-T)^s \mid r(X)$, поскольку

$$\prod_{t_0 \in \mathbb{F}_q} (T - t_0) = T^q - T.$$

Наконец, пусть число s равно степени числа p. Тогда

$$(T^q - T)^s = \sum_{j=0}^{s} (-1)^{s-j} \binom{s}{j} T^{qj+(s-j)}.$$

В силу предложения 4 имеем, что $\binom{s}{j} \equiv 0 \pmod p$ для $j \in [1, s-1]$. Это означает, что $(T^q - T)^s = T^{qs} + (-T)^s$. ▲

Доказательство предложения 5. Пусть $\lambda \in \mathbb{F}_q$, а $z(\boldsymbol{X}) \in V_q^s(d, m)$. В силу линейности

$$(f + \lambda z) \circ \gamma(T) = f \circ \gamma(T) + \lambda(z \circ \gamma(T))$$

достаточно рассматривать лишь многочлен $f(\boldsymbol{X})$, который является в точности $(m, d)_q^s$-хорошим мономом $\boldsymbol{X}^{\boldsymbol{v}}$, $\boldsymbol{v} \in \mathbb{N}^m$. Распишем получившийся многочлен $g(T)$ от одной переменной в таком случае:

$$g(T) = \prod_{j=1}^{m} (a_j T + b_j)^{v_j} = \prod_{j=1}^{m} \sum_{e_j=0}^{v_j} \binom{v_j}{e_j} a_j^{e_j} b_j^{v_j - e_j} T^{e_j} =$$

$$= \sum_{e_1 \in [0, v_1], \ldots, e_m \in [0, v_m]} T^{\sum\limits_{j=1}^{m} e_j} \prod_{j=1}^{m} \binom{v_j}{e_j} \alpha_j^{e_j} b_j^{v_j - e_j}.$$

Далее воспользуемся предложением 4, из которого следует, что коэффициент при $T^{\sum\limits_{j=1}^{m} e_j}$ может быть отличен от нуля только в том случае, когда для вектора $\boldsymbol{e} = (e_1, \ldots, e_m)$ выполнено отношение порядка $\boldsymbol{e} \leqslant_p \boldsymbol{v}$. Поскольку моном $\boldsymbol{X}^{\boldsymbol{v}}$ является $(m, d)_q^s$-хорошим, то выполнено неравенство $\operatorname{Mod}_q^s(\deg(\boldsymbol{e})) < d$ для интересующих нас векторов $\boldsymbol{e}$. Наконец, воспользуемся наблюдением (1). Получаем, что многочлен $h(T)$, s-эквивалентный $g(T)$, имеет степень не выше $\operatorname{Mod}_q^s(\deg(\boldsymbol{e}))$, где $\boldsymbol{e} \leqslant_p \boldsymbol{v}$. ▲

СПИСОК ЛИТЕРАТУРЫ

1. *Hirschfeld J.W.P., Korchmáros G., Torres F.* Algebraic Curves over a Finite Field. Princeton: Princeton Univ. Press, 2008.
2. *Лидл Р., Нидеррайтер Г.* Конечные поля. Т. 1. М.: Мир, 1988.
3. *Lucas E.* Théorie des fonctions numériques simplement périodiques // Amer. J. Math. 1878. V. 1. № 4. P. 289–321. https://doi.org/10.2307/2369373
4. *Guo A., Kopparty S., Sudan M.* New Affine-Invariant Codes from Lifting // Proc. 4th Conf. on Innovations in Theoretical Computer Science (ITCS'13). Berkeley, CA, USA. Jan. 9–12, 2013. P. 529–540. https://doi.org/10.1145/2422436.2422494
5. *Розенблюм М.Ю., Цфасман М.А.* Коды для m-метрики // Пробл. передачи информ. 1997. Т. 33. № 1. С. 55–63. http://mi.mathnet.ru/ppi359
6. *Kopparty S., Saraf S., Yekhanin S.* High-Rate Codes with Sublinear-Time Decoding // J. ACM. 2014. V. 61. № 5. Art. 28. P. 1–20. https://doi.org/10.1145/2629416
7. *Holzbaur L., Polyanskaya R., Polyanskii N., Vorobyev I., Yaakobi E.* Lifted Reed–Solomon Codes and Lifted Multiplicity Codes // IEEE Trans. Inform. Theory. 2021. V. 67. № 12. P. 8051–8069. https://doi.org/10.1109/TIT.2021.3116520

8. *Wu L.* Revisiting the Multiplicity Codes: A New Class of High-Rate Locally Correctable Codes // Proc. 53rd Annu. Allerton Conf. on Communication, Control, and Computing. Monticello, IL, USA. Sept. 29 – Oct. 2, 2015. P. 509–513. https://doi.org/10.1109/ALLERTON.2015.7447047
9. *Li R., Wootters M.* Lifted Multiplicity Codes and the Disjoint Repair Group Property // IEEE Trans. Inform. Theory. 2021. V. 67. № 2. P. 716–725. https://doi.org/10.1109/TIT.2020.3034962
10. *Nielsen R.R.* List Decoding of Linear Block Codes. Ph.D. Thesis. Dept. Math., Tech. Univ. Denmark, Lyngby, Denmark, Sept. 2001. Available from https://orbit.dtu.dk/en/publications/list-decoding-of-linear-block-codes.
11. *Kopparty S.* List-Decoding Multiplicity Codes // Theory Comput. 2015. V. 11. Art. 5. P. 149–182. https://doi.org/10.4086/toc.2015.v011a005
12. *Guruswami V., Wang C.* Optimal Rate List Decoding via Derivative Codes // Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques (Proc. 14th Int. Workshop, APPROX'2011, and 15th Int. Workshop, RANDOM'2011. Princeton, NJ, USA. Aug. 17–19, 2011). Lect. Notes Comput. Sci. V. 6845. Berlin: Springer, 2011. P. 593–604. https://doi.org/10.1007/978-3-642-22935-0_50
13. *Guo A., Kopparty S.* List-Decoding Algorithms for Lifted Codes // IEEE Trans. Inform. Theory. 2016. V. 62. № 5. P. 2719–2725. https://doi.org/10.1109/TIT.2016.2538766
14. *Kopparty S.* Some Remarks on Multiplicity Codes // Discrete Geometry and Algebraic Combinatorics (AMS Special Session on Discrete Geometry and Algebraic Combinatorics. San Diego, CA, USA. Jan. 11, 2013). Providence, RI: Amer. Math. Soc., 2014. P. 155–176.

Полянский Никита Андреевич
Сколковский институт науки и технологий (Сколтех)
nikita.polyansky@gmail.com

Поступила в редакцию
05.03.2021
После доработки
17.11.2021
Принята к публикации
23.11.2021