

УДК 621.391.15

СПЕКТРЫ АЛГЕБРОГЕОМЕТРИЧЕСКИХ КОДОВ

Кацман Г. Л., Цфасман М. А.

Приводятся оценки на энумератор произвольного алгеброгеометрического кода. Полностью вычисляется весовой спектр кода, построенного по всем точкам эллиптической кривой. Оказывается, что весовой спектр (энумератор) зависит от группы точек этой кривой и от элемента этой группы. Число векторов минимального веса удается минимизировать как по элементам, так и по кривым. Изучается возможность для такого кода быть МДР-кодом.

§ 1. Введение

Фиксируем конечное поле F_q . Пусть X — некоторая алгебраическая кривая над F_q , $g=g(X)$ — ее род, $X(F_q)$ — множество ее F_q -точек, $N=|X(F_q)|$ — их число.

Приведем следующий вариант конструкции кода по алгебраической кривой, по существу совпадающий с конструкцией Ю. И. Манина [1] и обобщающий конструкцию В. Д. Гоппы [2].

Пусть имеется линейный $[n, k, d]$ -код, т. е. инъективное отображение $C: V \rightarrow F_q^n$ k -мерного линейного пространства V над полем F_q в n -мерное координатное пространство. Тогда i -я проекция $p_i: F_q^n \rightarrow F_q$ определяет элемент $z_i = p_i \circ C \in V^*$ — пространства линейных форм на V , т. е. коду C соответствует n -ка точек из V^* . Если код C имел минимальное расстояние d , то максимум числа точек z_i в гиперплоскости $H \subset V^*$ равен $(n-d)$. Наоборот, любая n -ка точек $\{z_i\}$ из V^* определяет отображение $C: V \rightarrow F_q^n$; если при этом максимум числа точек из набора $\{z_i\}$ в гиперплоскости $H \subset V^*$ равен $(n-d) < n$, то C будет инъективно и минимальное расстояние кода C будет равно d .

Пусть теперь имеется проективное пространство P^{k-1} над F_q и n -ка точек $y_i \in P^{k-1}$. Пространство P^{k-1} есть проективизация некоторого k -мерного линейного пространства, назовем его V^* . Пусть $\pi: V^* \rightarrow P^{k-1}$ — естественная проекция; выберем любой набор точек $z_i \in V^*$ такой, что $\pi(z_i) = y_i$. Тогда, согласно сказанному выше, набор z_i определит код C , параметры которого зависят только от набора y_i , а именно $(n-d)$ есть максимум числа точек y_i в гиперплоскости $H \subset P^{k-1}$.

Наконец, пусть X — гладкая алгебраическая кривая над F_q , \mathcal{L} — обратимый F_q -пучок на X (или, что то же самое, класс дивизоров на X , определенный над F_q) степени $a > g-1$. Тогда \mathcal{L} определяет отображение $\varphi: X \rightarrow P^{k-1}$, где (по теореме Римана — Роха) $k \geq a - g + 1$. Отображение φ можно определить, например, так: пусть D — некоторый дивизор класса \mathcal{L} , $L(D)$ — k -мерное пространство функций, ассоциированное с D , пусть f_0, \dots, f_{k-1} — некоторый базис в $L(D)$, тогда $\varphi: x \mapsto (f_0(x), \dots, f_{k-1}(x))$, если хотя бы для одного i $f_i(x) \neq 0$; можно доказать (см., например, [3]), что φ продолжается на всю кривую X . Если $\mathcal{S} = \{x_1, \dots, x_n\} \subseteq X(F_q)$, то набор $y_i = \varphi(x_i)$ задает код C . Число точек в пересечении $\varphi(X)$ с гиперплоскостью равно a , т. е. $n-d \leq a$. Заметим еще, что на любой кривой X ,

имеющей хотя бы одну F_q -точку, имеется обратимый F_q -пучок любой заданной степени.

Эта конструкция позволяет строить коды с параметрами $k+d \geq n-g+1$, длина n которых меньше либо равна числу F_q -точек на кривой X .

Пусть C — некоторый линейный $[n, k, d]_q$ -код, $A_r = A_r(C)$ — число векторов веса r , $W_C(x:y) = \sum A_r x^{n-r} y^r$ — весовой спектр (энумератор весов) кода C .

Мы будем изучать энумераторы алгеброгеометрических кодов. В § 2 будет доказана

Теорема 1. Пусть C — алгеброгеометрический код длины n по кривой рода g и дивизору степени a . Тогда

$$(1) \quad W_C(x:y) = x^n + y^{n-a} \sum_{i=0}^a B_i y^i (x-y)^{a-i},$$

где при $i \geq 2g-1$,

$$B_i = \binom{n}{a-i} (q^{i-g+1} - 1),$$

а при $i \leq 2g-2$,

$$\binom{n}{a-i} (q^{\lfloor i/2 \rfloor + 1} - 1) \geq B_i \geq \max \left\{ 0, \binom{n}{a-i} (q^{i-g+1} - 1) \right\}.$$

Вообще говоря, представление энумератора в виде (1) существует для любого кода с минимальным расстоянием $d \geq n-a$, поскольку многочлены $(x-y)^a, y(x-y)^{a-1}, \dots, y^a$ образуют базис в пространстве однородных многочленов от двух переменных степени a . Неотрицательность коэффициентов B_i следует из того, что если для кода C с минимальным расстоянием $d \geq n-a$

$$W_C(x:y) = \sum_{r=0}^n A_r x^{n-r} y^r = x^n + y^{n-a} \sum_{i=0}^a B_i y^i (x-y)^{a-i},$$

то

$$A_{l+n-a} = \sum_{j=0}^l (-1)^{l-j} \binom{a-j}{a-l} B_j \quad \text{и} \quad B_k = \sum_{l=0}^k \binom{a-l}{a-k} A_{l+n-a}.$$

Наличие точных формул для B_i при $i \geq 2g-1$ объясняется тем, что код, двойственный к алгеброгеометрическому коду, также является алгеброгеометрическим.

Пусть теперь X — эллиптическая кривая, т. е. кривая рода 1. Фиксируем точку $P_0 \in X(F_q)$, на кривой X имеется структура абелевой группы с нулем P_0 , $X(F_q)$ является конечной подгруппой группы всех точек X . Любому дивизору $D = \sum \alpha_i Q_i$ сопоставляется точка P_D , равная сумме всех Q_i с кратностями α_i , т. е. $P_D = \sum \alpha_i Q_i$ в группе X . Наличие на X такой сильной дополнительной структуры облегчает вычисление энумератора.

По теореме 1 для эллиптических кривых (т. е. при $g=1$) мы «почти знаем» $W_C(x:y)$: имеется ровно одно неизвестное B_0 , которое равно числу векторов минимального веса.

Оказывается, что для эллиптического кода (кода по кривой рода 1) B_0 , а следовательно, и $W_C(x:y)$, зависит лишь от группы $X(F_q)$, множества $\mathcal{P} = \{P_1, \dots, P_n\} \in X(F_q)$, степени a дивизора (пучка L) и элемента $P_D \in X(F_q)$. Точнее говоря, $B_0/(q-1)$ равно числу $M(X(F_q), \mathcal{P}, P_D, a)$ представлений P_D в виде суммы a различных элементов из множества \mathcal{P} .

При $\mathcal{P} = X(F_q)$, т. е. $n=N$, число $M(H, h, a)$ представлений элемента h конечной абелевой группы H в виде суммы a различных элементов вычис-

лено в работах [4, 5] в связи с вычислением энумераторов обобщенных кодов Варшавова — Тененгольца (называемых также кодами Константина — Рао) для асимметричного канала. Точную формулу мы приведем в конце § 3, она довольно громоздка.

Естественно постараться минимизировать число B_0 векторов минимального веса при фиксированном поле F_q и заданных параметрах кода (т. е. при заданном a). Это делается в два этапа. Сначала для заданной группы H вычисляется $M(H, a) = \min_{h \in H} M(H, h, a)$. Как ни странно, выраже-

ние для $M(H, a)$ много проще, чем для $M(H, h, a)$.

Теорема 2. Пусть H — абелева группа, r_H — максимальная степень такая, что $(\mathbb{Z}/2)^{r_H} \subseteq H$. Тогда

а) если $N \equiv 0 \pmod{4}$, $a \equiv 2 \pmod{4}$, то

$$M(H, a) = \frac{1}{N} \left[\sum_{m|(a, N)} \binom{N/m}{a/m} \mu(m) (-1)^{a/m} - 2^{r_H} \sum_{m|(a/2, N/2)} \binom{N/2m}{a/2m} \mu(m) \right];$$

б) в противном случае

$$M(H, a) = \frac{1}{N} \sum_{m|(a, N)} \binom{N/m}{a/m} \mu(m) (-1)^{a-a/m};$$

где $\mu(m)$ — функция Мёбиуса.

В частности, что впрочем много проще, если N и a взаимно просты, то

$$B_0 = (q-1) \binom{N}{a} / N.$$

Теперь надо минимизировать $M(H, a)$ по всем возможным группам $H = X(F_q)$ данного порядка N . Для этого следует знать, какие группы H реализуются в качестве $X(F_q)$ для эллиптических кривых X над данным конечным полем F_q .

Спектр возможных значений $N = |X(F_q)|$ дается теоремой Ватерхауза [6], а всевозможные группы $X(F_q)$ независимо перечислены в работах [7, 8] (точные формулировки см. в начале § 5). Эти результаты позволяют вычислить число $M(N, a)$, равное минимуму $M(X(F_q), a)$, по всем эллиптическим кривым X над полем F_q с $|X(F_q)| = N$.

Заметим, что возможна ситуация, когда $B_0 = 0$, т. е. эллиптический код является МДР-кодом (это было замечено Дринкуром и Мишоном (см. [9])). Для этого в группе $H = X(F_q)$ должен существовать элемент h , не представимый в виде суммы a различных элементов из подмножества $\mathcal{P} \subseteq X(F_q)$. Нетрудно показать, что при $\mathcal{P} = X(F_q)$ это возможно лишь при $X(F_q) = \mathbb{Z}/2$ или $(\mathbb{Z}/2)^2$, при этом код будет иметь длину 2 или 4, причем последнее невозможно над F_{2^m} . В случае $\mathcal{P} \subset X(F_q)$ также удастся показать, что эллиптический код может оказаться МДР-кодом лишь при длинах, не больших, чем у ранее известных кодов.

Доказательству теоремы 1 посвящен § 2; в § 3 после изложения необходимых сведений об эллиптических кривых доказывается, что $B_0 = (q-1)M(X(F_q), \mathcal{P}, P_D, a)$, и приводится формула для $M(H, h, a)$. Теорема 2 доказывается в § 4. В § 5 мы приводим результаты о структуре $X(F_q)$ и вычисляем $M(N, a)$. В § 6 доказывается несуществование длинных эллиптических кодов, являющихся МДР-кодами.

§ 2. Весовые спектры алгеброгеометрических кодов

В этом параграфе мы докажем теорему 1. Для удобства читателя, мало знакомого с понятием пучка, мы здесь и далее пользуемся определением алгеброгеометрического кода через $L(D)$. Однако все рассуждения проходят и для пучковой конструкции: достаточно всюду вместо D , $L(D)$, $L(D-P)$, f, \dots писать соответственно \mathcal{L} , $\Gamma(\mathcal{L})$, $\Gamma(\mathcal{L} \otimes \mathcal{O}(-P))$, s , и т. д.

Итак, фиксированы: гладкая алгебраическая кривая X рода g над F_q , набор точек $\mathcal{P} = \{P_1, \dots, P_n\} \subseteq X(F_q)$, эффективный дивизор D степени a , $g-1 \leq a \leq n$, причем $\text{Supp } D \cap \mathcal{P} = \emptyset$ (последнее требование не существенно и снимается использованием пучковой конструкции).

Положим $B'_{a-i} = B_i = \sum (q^{l(D-P_{j_1}-\dots-P_{j_{a-i}})} - 1)$, где суммирование ведется по всем поднаборам \mathcal{P} мощности $(a-i)$. Степень дивизора $D-P_{j_1}-\dots-P_{j_{a-i}}$ равна i и по теореме Римана-Роха $l(D-P_{j_1}-\dots-P_{j_{a-i}}) \geq i-g+1$, причем при $i \geq 2g-1$ имеет место равенство. С другой стороны, если дивизор $D-P_{j_1}-\dots-P_{j_{a-i}}$ специальный (т. е. $l(D-P_{j_1}-\dots-P_{j_{a-i}}) > i-g+1$), то имеет место теорема Клиффорда ([10, гл. 2, § 3], изложенное там доказательство проходит в произвольной характеристике), согласно которой

$$l(D-P_{j_1}-\dots-P_{j_{a-i}}) \leq [i/2] + 1.$$

Выразим теперь значения $A_{r'} = A_{n-r}$, $r \leq a$, весового спектра через величины B_i . Функция $f \in L(D)$ имеет ровно r нулей в \mathcal{P} в том и только том случае, когда $f \in L(D-P_{j_1}-\dots-P_{j_r})$ для некоторой r -ки $\{P_{j_1}, \dots, P_{j_r}\}$ и $f \notin L(D-P_{j_1}-\dots-P_{j_{r+1}})$ ни для какой $(r+1)$ -ки $\{P_{j_1}, \dots, P_{j_{r+1}}\} \subseteq \mathcal{P}$. Рассмотрим множество ненулевых векторов кода C и вычислим A_{n-r} , пользуясь принципом включения-исключения. Мы утверждаем, что

$$A_{n-r} = \sum_{i=0}^{a-r} (-1)^{a-r-i} \binom{a-i}{r} B_i,$$

т. е., что

$$(2) \quad A_{r'} = \sum_{i=r}^a (-1)^{i-r} \binom{i}{r} B'_i.$$

Пусть $j = (j_1, \dots, j_i) \subseteq \{1, 2, \dots, n\}$, $l(j) = i$; положим $X_j = \{v \in C \mid v \neq 0, v \in L(D-P_{j_1}-\dots-P_{j_i})\}$, пусть x_j — мощность X_j , тогда $B'_i = \sum_{l(j)=i} x_j$. Под-

считаем, сколько раз вектор $v \in L(D-P_{j_1}-\dots-P_{j_{r+s}})$ подсчитывается в правой части (2). Такой вектор входит в $\binom{r+s}{i}$ множеств X_j . Поэтому этот

вектор в правой части (2) подсчитан $\sum_{i=r}^a (-1)^{i-r} \binom{i}{r} \binom{r+s}{i}$ раз. При $s > 0$

эта величина равна 0 [11, 2.1.4], а при $s=0$ равна 1. Поэтому

$\sum_{i=r}^a (-1)^{i-r} \binom{i}{r} B'_i$ есть число векторов, входящих в X_j при $l(j)=r$ и не входящих

в X_j при $l(j) > r$, т. е. равно $A_{r'}$. Теорема 1 доказана.

При $2g-2 < a \leq n$ алгеброгеометрический код имеет параметры $[n, a-g+1, d]$, $d \geq n-a$, а двойственный к нему код также является алгеброгеометрическим и имеет параметры $[n, n-a+g-1, d^\perp]$, $d^\perp \geq a-2g+2$. Оказывается, что для доказательства большинства утверждений теоремы 1 достаточно этого неравенства на d^\perp . Лишь неравенство, получаемое с по-

мощью теоремы Клиффорда, имеет другую природу (см. пример в конце этого параграфа). Точнее говоря имеет место

Теорема 3. Пусть V — линейный q -ичный $[n, k, \geq d]$ код, с двойственным кодом, имеющим параметры $[n, n-k, \geq d^\perp]$.

Тогда

$$W_V(x, y) = x^n + y^d \sum_{i=0}^{n-d} B_i y^i (x-y)^{n-d-i}.$$

Причем при $n-d \geq i > n-d-d^\perp$

$$B_i = \binom{n}{d+i} (q^{k-n+d+i} - 1),$$

а при $n-d-d^\perp \geq i \geq 0$

$$\binom{n}{d+i} (q^{\min\{i+1, k-d^\perp+1\}} - 1) \geq B_i \geq \max \left\{ 0, \binom{n}{d+i} (q^{k-n+d+i} - 1) \right\}.$$

Доказательство. Положим $\{j_1, \dots, j_r\} = j \subseteq \{1, \dots, n\}$, $l(j) = r$ и $X_j = \{v \in V \mid v = (v_1, \dots, v_n) \neq 0, v_{j_1} = \dots = v_{j_r} = 0\}$. Положим $B_i = \sum_{l(j)=n-d-i} |X_j|$.

Тогда, как следует из рассуждений, проведенных при доказательстве теоремы 1, $W_V(x, y) = x^n + y^d \sum_{i=0}^{n-d} B_i y^i (x-y)^{n-d-i}$. Кроме того, из определения B_i следует, что $B_i \geq 0$.

Положим $L_j = \{v \in V \mid v = (v_1, \dots, v_n), v_{j_1} = \dots = v_{j_r} = 0\}$. Тогда $|X_j| = |L_j| - 1$ и L_j есть линейное подпространство, причем двойственное к L_j подпространство порождено строками матрицы $H_j = \begin{vmatrix} H \\ h_j \end{vmatrix}$, где H — проверочная матрица кода V , а h_j — матрица размера $l(j) \times n$, s -я строка имеет 1 в позиции с номером j_s и 0 в остальных позициях. Поэтому $|X_j| = |L_j| - 1 \geq \geq q^{n-l(n-k+l(j))} - 1 = q^{k-l(j)} - 1$. Поскольку число возможных выборов j таких, что $l(j) = n-d-i$ равно $\binom{n}{d+i}$, то $B_i \geq \binom{n}{d+i} (q^{k+d-n+i} - 1)$. При $n-d \geq$

$\geq i > n-d-d^\perp$, т. е. $0 \leq l(j) < d^\perp$, матрица H_j имеет ранг $n-k+l(j)$, поскольку в противном случае в двойственном коде V^\perp нашелся бы вектор веса $\leq l(j) < d^\perp$. Поэтому при $n-d \geq i > n-d-d^\perp$

$$B_i = \binom{n}{d+i} (q^{k+d-n+i} - 1).$$

Покажем теперь, что $\binom{n}{d+i} (q^{\min\{i+1, k-d^\perp+1\}} - 1) \geq B_i$ при $n-d-d^\perp \geq i \geq 0$. Обозначим $j^\perp = \{1, 2, \dots, n\} \setminus j$, $L_{j^\perp} = \{v \in V^\perp \mid v = (v_1, \dots, v_n), v_v = 0 \text{ при } v \in j^\perp\}$. Нетрудно показать, что $\dim L_j = k - l(j) + \dim L_{j^\perp}$. С другой стороны L_j и L_{j^\perp} суть линейные коды длины соответственно $n-l(j)$ и $l(j)$ с минимальными расстояниями $\geq d$ и $\geq d^\perp$. Поэтому при $0 \leq i \leq n-d-d^\perp$ для каждого из этих кодов может быть выписана граница Синглтона $\dim L_j = n-l(j)+1-d = i+1$; $\dim L_{j^\perp} \leq l(j)-d^\perp+1$, откуда $\dim L_j = k-l(j)+1 + \dim L_{j^\perp} \leq k-d^\perp+1$. Что и требовалось доказать.

Замечания. 1. При подстановке в условия теоремы 3 параметров алгеброгеометрического кода можно получить теорему 1 за исключением нера-

венства $B_i \leq \binom{n}{a-i} (q^{\lfloor i/2 \rfloor + 1} - 1)$. Это неравенство заменено на другое

$B_i \leq \binom{n}{a-i} (q^{\min\{i+1, k-d^\perp+1\}} - 1)$. Последнее неравенство лучше неравенства теоремы 1, если $2k - 2d^\perp < i \leq 2g - 2$. Такие i существуют, если для двойственного кода происходит «подскок минимального расстояния», т. е. $d^\perp > n - k^\perp - g + 1$.

2. Верхняя оценка для B_i может быть улучшена, если для оценки $\dim L_j$ и $\dim L_{j^\perp}$ использовать вместо границы Синглтона другие, более точные верхние оценки. Однако в этом случае формулировка соответствующего результата станет слишком громоздкой.

3. С другой стороны, из условий теоремы 3 не следует неравенство $B_i \leq \binom{n}{a-i} (q^{\lfloor i/2 \rfloor + 1} - 1)$, получаемое для алгеброгеометрических кодов из

теоремы Клиффорда. Приведем соответствующий пример.

Пусть V — линейный двоичный $[6, 4, 2]$ -код с порождающей матрицей

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

Для этого кода $d^\perp = 3$ и, как легко проверить, $B_0 = 6$, $B_1 = 24$, $B_2 = 45$, $B_3 = 42$, $B_4 = 15$. В то же время при $i = 1 = n - d - d^\perp$ оценка $\binom{n}{d+i} (q^{\lfloor i/2 \rfloor + 1} - 1)$ дает $B_1 \leq 20$.

§ 3. Эллиптические коды

Пусть X — эллиптическая кривая, т. е. гладкая алгебраическая кривая рода 1. Зафиксируем на X какую-нибудь F_q -точку P_0 (на эллиптической кривой над F_q всегда имеется F_q -точка). Тогда на кривой X имеется коммутативный групповой закон с нулем в P_0 , определяемый следующим образом. Пусть Q_1 и Q_2 — точки кривой X (с координатами, вообще говоря, не лежащими в F_q). Тогда дивизор $D = Q_1 + Q_2 - P_0$ имеет по теореме Римана — Роха $l(D) = 1$, т. е. существует единственная с точностью до константы функция f такая, что $D' = D + (f) \geq 0$, тем самым дивизор D' определен однозначно и, так как это эффективный дивизор степени 1, $D' = Q_3$ — некоторая точка, которая и называется суммой Q_1 и Q_2 . Обратный элемент определяется аналогично: пусть $Q_4 \sim 2P_0 - Q_1$, тогда Q_4 обратна к Q_1 . Сумма F_q -точек также определена над F_q , поэтому $X(F_q)$ является конечной абелевой группой. Можно точно описать все абелевы группы, которые могут реализоваться как $X(F_q)$ для эллиптической кривой X (см. теорему 6).

Пусть теперь $D = \sum \alpha_i Q_i$ — дивизор на X степени a . Определим точку $P_D = \sum \alpha_i Q_i$ (здесь сумма в смысле описанного выше группового закона). Если (f) — дивизор функции, то $P_{(f)} = P_0$, поэтому для эквивалентных дивизоров точки P_D совпадают, т. е. корректно определен элемент $P_{\mathcal{L}}$, где \mathcal{L} — класс дивизоров (обратимый пучок). Если D был определен над F_q , то $P_D \in X(F_q)$.

Заметим, что если в качестве нуля группового закона мы выберем другую F_q -точку, то P_D , вообще говоря, изменится. Однако легко видеть, что класс $[P_D]$ точки P_D в факторгруппе $X(F_q)/aX(F_q)$ остается прежним.

Еще заметим, что элемент $[P_D] \in X(F_q)/aX(F_q)$ определяет код однозначно с точностью до умножения всех кодовых слов на некоторый вектор, все компоненты которого отличны от нуля.

Пусть C — эллиптический код, построенный по эллиптической кривой X над \mathbf{F}_q , дивизору D степени a (или обратимому пучку \mathcal{L} степени a) и набору \mathbf{F}_q -точек $\mathcal{P} = \{P_1, \dots, P_n\} \subseteq X(\mathbf{F}_q)$. Код C — $[n, k, d]$ -код с $k=a$, $d \geq n-k$. Его спектр почти вычисляется по теореме 1, остается одна неизменная величина B_0 , равная числу векторов минимального веса.

Для произвольной абелевой группы H , подмножества $U \subseteq H$, элемента $h \in H$ и положительного целого числа a определим число $M(H, U, h, a)$ как количество различных представлений элемента h в виде суммы a различных элементов множества U .

Теорема 4. Число B_0 векторов минимального веса в эллиптическом коде равно $(q-1)M(X(\mathbf{F}_q), \mathcal{P}, P_D, a)$.

Доказательство. В предыдущем параграфе мы определили B_0 как сумму $\sum (q^{l(D-P_1-\dots-P_a)}-1)$ по всем поднаборам $\{P_{i_1}, \dots, P_{i_a}\} \subseteq \mathcal{P}$ мощности a . При этом $D' = D - P_{i_1} - \dots - P_{i_a}$ есть дивизор степени 0, поэтому либо он не эквивалентен никакому эффективному дивизору, тогда $l(D') = 0$, либо он эквивалентен нулевому дивизору и тогда $l(D') = 1$. Из определения P_D и группового закона видно, что $D' \sim P_D + (a-1)P_0 - P_{i_1} - \dots - P_{i_a}$; D' эквивалентен нулю тогда и только тогда, когда $P_D + (a-1)P_0 \sim P_{i_1} + \dots + P_{i_a}$, т. е. когда сумма $P_{i_1} + \dots + P_{i_a}$ в смысле группового закона на кривой есть P_D . Таким образом, B_0 имеет $M(X(\mathbf{F}_q), \mathcal{P}, P_D, a)$ ненулевых слагаемых, каждое из которых дает вклад, равный $(q-1)$, что и требовалось доказать.

Далее мы ограничиваемся случаем $\mathcal{P} = X(\mathbf{F}_q)$ и пишем $M(H, h, a)$ вместо $M(H, H, h, a)$, т. е. рассматриваем коды, построенные по всем \mathbf{F}_q -точкам эллиптической кривой.

Пусть $h = \sum_{i=1}^a h_i$, тогда $\sum_{i=1}^a (h_i + h_0) = h + ah_0$, т. е. каждому представлению h в виде суммы a различных слагаемых соответствует такое же представление $h + ah_0$ для любого h_0 . Тем самым доказано

Предложение 1. Пусть фиксирована абелева группа H порядка N и целое число a , тогда число $M(H, h, a)$ зависит только от класса h в факторгруппе H/aH .

Поскольку $aH = H$ при $(N, a) = 1$, имеем

Следствие. Если $(N, a) = 1$, то $M(H, h, a) = \binom{N}{a} / N$ для любого $h \in H$.

Общий случай сложнее. Пусть H — абелева группа порядка N ,

$H = \sum_{j=1}^r H_j$, $H_j = \mathbf{Z}/p_j^{\alpha_j}$ — ее разложение на примарные циклические подгруппы. Любой элемент $h \in H$ записывается в виде $h = (h_1, \dots, h_r)$, $0 \leq h_j \leq p_j^{\alpha_j} - 1$, $j = 1, \dots, r$.

Для любого $h = (h_1, \dots, h_r) \in H$, пусть $\varepsilon_j(h)$ — максимальная степень p_j , делящая h_j ; $\varepsilon_j(h) = \infty$, если $h_j = 0$. Для любого простого $p | N$ положим $J_p = \{j | p_j = p\}$,

и

$$e_p(h) = \begin{cases} \min_{j \in J_p} \varepsilon_j(h), & \text{если имеется } j \in J_p, \varepsilon_j(h) \neq \infty, \\ \sum_{j \in J_p} \alpha_j, & \text{если } \varepsilon_j(h) = \infty \text{ для всех } j \in J_p \end{cases}$$

и

$$\Delta(h) = \prod_{p|N} p^{e_p(h)}.$$

Наконец, пусть $t|N$ и $t = \prod_p p^{\delta_p}$. Определим $R_H(t) = \prod_{p|N} p^{\sum_{j \in J_p} \min(\delta_p, \alpha_j)}$.

В частности, $R_H(1) = 1$.

Ответ на вопрос о числе представлений заданного элемента конечной абелевой группы в виде суммы a различных элементов этой группы дается следующей теоремой.

Теорема 5 [4, 5]. Пусть $M(H, h, a)$ — число представлений элемента h конечной абелевой группы H в виде суммы a различных элементов. Тогда

$$M(H, h, a) = \frac{1}{N} \sum_{l|(N, a)} \binom{N/l}{a/l} (-1)^{a-a/l} \sum_{t|(l, \Delta(h))} \mu(l/t) R_H(t).$$

Здесь $\mu(m)$ — функция Мёбиуса

$$\mu(m) = \begin{cases} 0, & \text{если } m \text{ делится на квадрат простого числа,} \\ (-1)^n & \text{в противном случае, где } n \text{ — число простых} \\ & \text{сомножителей } m. \end{cases}$$

§ 4. Минимизация по дивизору

В этом параграфе мы докажем теорему 2. Положим $M(H, a) = \min_{h \in H} M(H, h, a)$. Доказательство основано на следующих леммах.

Лемма 1. Имеет место соотношение

$$M(H, h, a) = \frac{1}{N} \sum_{t|(N, a, \Delta(h))} R_H(t) \sum_{m|(a/t, N/t)} (-1)^{a-a/mt} \binom{N/mt}{a/mt} \mu(m).$$

Доказательство. По теореме 5

$$\begin{aligned} M(H, h, a) &= \frac{1}{N} \sum_{\substack{lu=a \\ lc=N}} \binom{c}{u} (-1)^{a-a/l} \sum_{\substack{mt=l \\ t|\Delta(h)}} \mu(m) R_H(t) = \\ &= \frac{1}{N} \sum_{\substack{mtu=a \\ mtc=N \\ t|\Delta(h)}} \binom{c}{u} (-1)^{a-a/mt} \mu(m) R_H(t) = \\ &= \frac{1}{N} \sum_{t|(N, a, \Delta(h))} R_H(t) \sum_{\substack{mu=a/t \\ mc=N/t}} (-1)^{a-a/mt} \binom{c}{u} \mu(m) = \\ &= \frac{1}{N} \sum_{t|(N, a, \Delta(h))} R_H(t) \sum_{m|(a/t, N/t)} (-1)^{a-a/mt} \binom{N/tm}{a/tm} \mu(m). \end{aligned}$$

Лемма 1 доказана.

При фиксированных N и a положим

$$A(t) = \sum_{m|(N/t, a/t)} (-1)^{a-a/mt} \binom{N/tm}{a/tm} \mu(m).$$

Для любого целого l положим, что $\tau(l)$ — максимальная степень 2, делящая l .

Лемма 2. 1. Если $\tau(a) > \tau(N)$, то $A(t) \geq 0$ для любого $t|(N, a)$.

2. Если $\tau(a) = 0$, то $A(t) \geq 0$ для любого $t|(N, a)$.

3. а. Если $0 < \tau(a) < \tau(N)$, то $A(t) \geq 0$ для любого $t | (N, a)$ такого, что $\tau(t) < \tau(a)$.

б. Если $0 < \tau(a) < \tau(N)$, то $A(t) \leq 0$ для любого $t | (N, a)$ такого, что $\tau(t) = \tau(a)$.

Доказательство. Пусть мы находимся в ситуации пп. 1, 2 или 3 а. Тогда $a \equiv a/t \pmod{2}$, поэтому

$$\begin{aligned} A(t) &= \sum_{m|(N/t, a/t)} (-1)^{a-a/mt} \left(\frac{N/mt}{a/mt} \right) \mu(m) = \\ &= \sum_{m|(N/t, a/t)} (-1)^{a/t-a/mt} \left(\frac{N/mt}{a/mt} \right) \mu(m). \end{aligned}$$

С другой стороны, пусть H' — произвольная абелева группа порядка N/t и $h' \in H'$, $h' = (1, \dots, 1)$. Тогда $\Delta(h') = 1$ и

$$M(H', h', a/t) = \frac{t}{N} \sum_{m|(N/t, a/t)} (-1)^{a/t-a/mt} \left(\frac{N/mt}{a/mt} \right) \mu(m).$$

Поскольку $M(H', h', a/t) \geq 0$, то $A(t) \geq 0$.

Предположим теперь (п. 3 б), что $0 < \tau(a) < \tau(N)$, $t | (N, a)$ и $\tau(t) = \tau(a)$, тогда

$$\begin{aligned} A(t) &= \sum_{m \cdot |(N/t, a/t)} (-1)^{a-a/mt} \left(\frac{N/mt}{a/mt} \right) \mu(m) = \\ &= - \sum_{m|(N/t, a/t)} (-1)^{a/t-a/mt} \left(\frac{N/mt}{a/mt} \right) \mu(m). \end{aligned}$$

Если определить теперь H' и h' так же, как выше, то получим

$$M(H', h', a/t) = \frac{t}{N} \sum_{m|(N/t, a/t)} (-1)^{a/t-a/mt} \left(\frac{N/mt}{a/mt} \right) \mu(m),$$

и поскольку $M(H', h', a/t) \geq 0$, то $A(t) \leq 0$.

Лемма 2 доказана.

Лемма 3. Пусть $\tau(N) > \tau(a) = \tau(t) > 0$. Тогда

$$\begin{aligned} C(t) &= R_H(t/2) \sum_{m|(2N/t, 2a/t)} (-1)^{a-2a/mt} \left(\frac{2N/mt}{2a/mt} \right) \mu(m) + \\ &+ R_H(t) \sum_{m|(N/t, a/t)} (-1)^{a-a/mt} \left(\frac{N/mt}{a/mt} \right) \mu(m) \geq 0. \end{aligned}$$

Доказательство. Из леммы 2 следует, что если $B \geq R_H(t)/R_H(t/2)$, то

$$\begin{aligned} C(t) &\geq R_H(t/2) \left[\sum_{m|(2N/t, 2a/t)} (-1)^{a-2a/mt} \left(\frac{2N/mt}{2a/mt} \right) \mu(m) + \right. \\ &+ B \sum_{m|(N/t, a/t)} (-1)^{a-a/mt} \left(\frac{N/mt}{a/mt} \right) \mu(m) \left. \right] = \\ &= R_H(t/2) \left[\sum_{m|(2N/t, 2a/t)} (-1)^{2a/t-2a/mt} \left(\frac{2N/mt}{2a/mt} \right) \mu(m) + \right. \\ &+ B \sum_{m|(N/t, a/t)} (-1)^{2a/t-a/mt} \left(\frac{N/mt}{a/mt} \right) \mu(m) \left. \right]. \end{aligned}$$

Последнее равенство справедливо, поскольку $a \equiv 0 \pmod{2}$.

Пусть H' — абелева группа, $H' = (\mathbf{Z}/2)^l \times \mathbf{Z}/\pi_1^{\beta_1} \times \dots \times \mathbf{Z}/\pi_s^{\beta_s}$, где $l = \tau(2N/t) = \tau(N) - \tau(t) + 1$, π_i — нечетные простые. При этом π_i и β_i выбраны так,

что $|H'| = 2^l \prod_{i=1}^s \pi_i^{\beta_i} = 2N/t$. Покажем, что $R_{H'}(2) \geq R_H(t)/R_H(t/2)$. Действи-

тельно, по определению функции $R_H(t)$ $R_{H'}(2) = 2^l = 2^{\tau(N) - \tau(t) + 1}$, $R_H(t)/R_H(t/2) = 2^{a_H(\delta_2)}$, где $a_H(\delta_2) = |\{j | \alpha_j > \delta_2, j \in J_2\}|$, $\delta_2 = \tau(t/2) = \tau(t) - 1$.

(Напомним, что $H = \prod_{j=1}^J \mathbf{Z}/p_j^{\alpha_j}$, а $J_p = \{j | p_j = p\}$.)

Легко видеть, что

$$\sum_{j \in J_2} \alpha_j = \tau(N).$$

С другой стороны,

$$\sum_{j \in J_2} \alpha_j \geq (\delta_2 + 1) a_H(\delta_2).$$

Поэтому

$$a_H(\delta_2) \leq \tau(N) / (\delta_2 + 1) = \tau(N) / \tau(t).$$

Теперь для доказательства неравенства $R_{H'}(2) \geq R_H(t)/R_H(t/2)$ достаточно доказать, что

$$\tau(N) / \tau(t) \leq \tau(N) - \tau(t) + 1.$$

Последнее неравенство равносильно $[\tau(N) - \tau(t)] [\tau(t) - 1] \geq 0$. Это неравенство справедливо, поскольку $\tau(N) \geq \tau(t) \geq 1$ по условию леммы. Таким образом,

$$C(t) \geq R_H(t/2) \left[\sum_{m | (2N/t; 2a/t)} \binom{2N/tm}{2a/tm} (-1)^{2a/t - 2a/tm} \mu(m) + \right. \\ \left. + R_{H'}(2) \sum_{m | (N/t; a/t)} \binom{N/tm}{a/tm} (-1)^{2a/t - a/tm} \mu(m) \right].$$

В определенной выше группе H' выберем элемент $h' = \underbrace{(0, \dots, 0, 1, \dots, 1)}_l$.

Тогда $\Delta(h') = 2^l$ и поскольку $\tau(a) = \tau(t)$, то

$$0 \leq M(H', h', 2a/t) = \frac{t}{2N} \left[\sum_{m | (2N/t; 2a/t)} \binom{2N/tm}{2a/tm} (-1)^{2a/t - 2a/tm} \mu(m) + \right. \\ \left. + R_{H'}(2) \sum_{m | (N/t; a/t)} \binom{N/tm}{a/tm} (-1)^{2a/t - a/tm} \mu(m) \right].$$

Отсюда следует, что $C(t) \geq 0$. Лемма 3 доказана.

Доказательство теоремы 2. Имеем

$$M(H, h, a) = \frac{1}{N} \sum_{t | (N, a, \Delta(h))} R_H(t) \sum_{m | (a/t, N/t)} \binom{N/tm}{a/tm} (-1)^{a - a/tm} \mu(m) = \\ = \frac{1}{N} \sum_{t | (N, a, \Delta(h))} R_H(t) A(t).$$

По лемме 2 при $\tau(N) < \tau(a)$ или при $\tau(a) = 0$, $A(t) \geq 0$, поэтому так как $R_H(t) > 0$, то

$$\begin{aligned} M(H, h, a) &\geq \frac{1}{N} R_H(1) A(1) = \\ &= \frac{1}{N} \sum_{m|(a, N)} \binom{N/m}{a/m} (-1)^{a-a/m} \mu(m) = M(H, h^*, a), \end{aligned}$$

где $h^* = (1, \dots, 1)$.

Поэтому при $\tau(N) < \tau(a)$ или $\tau(a) = 0$

$$\begin{aligned} M(H, a) &= \frac{1}{N} \sum_{m|(a, N)} \binom{N/m}{a/m} (-1)^{a-a/m} \mu(m) = \\ &= \frac{1}{N} \sum_{m|(a, N)} \binom{N/m}{a/m} \mu(m). \end{aligned}$$

Последнее равенство справедливо, так как при указанных условиях $a - a/m$ четно. Предположим теперь, что $\tau(N) = \tau(a) > 0$.

Обозначим $\tilde{H} = \{\tilde{h} \in H, o(\tilde{h}) = 2\}$, где $o(\tilde{h})$ — порядок элемента \tilde{h} . Очевидно $\sum_{h \in H} h = \sum_{\tilde{h} \in \tilde{H}} \tilde{h}$. Пусть $\sum_{\tilde{h} \in \tilde{H}} \tilde{h} = h_0$.

Тогда $M(H, h, a) = M(H, h_0 - h, N - a)$, так как $h_0 - h$ представляется дополнением до всей группы набора, представляющего h .

$$\text{Поэтому} \quad \min_{h \in H} M(H, h, a) = \min_{h \in H} M(H, h_0 - h, N - a) = \min_{h \in H} M(H, h, N - a).$$

Поскольку при $\tau(N) = \tau(a)$ $\tau(N) < \tau(N - a)$, то в этом случае

$$M(H, a) = \frac{1}{N} \sum_{m|(N, N-a)} \binom{N/m}{(N-a)/m} \mu(m) = \frac{1}{N} \sum_{m|(N, a)} \binom{N/m}{a/m} \mu(m).$$

Пусть теперь $\tau(N) > \tau(a) > 1$. Тогда по леммам 1–3

$$\begin{aligned} M(H, h, a) &= \frac{1}{N} \sum_{t|(H, a, \Delta(h))} R_H(t) \sum_{m|(N/t, a/t)} \binom{N/tm}{a/tm} (-1)^{a-a/tm} \mu(m) = \\ &= \frac{1}{N} \left\{ \sum_{\substack{t|(N, a, \Delta(h)) \\ a/2t \equiv 0 \pmod{2}}} R_H(t) \sum_{m|(N/t, a/t)} \binom{N/tm}{a/tm} (-1)^{a-a/tm} \mu(m) + \right. \\ &+ \sum_{\substack{t|(N, a, \Delta(h)) \\ a/t \equiv 1 \pmod{2}}} \left[R_H(t/2) \sum_{m|(2N/t, 2a/t)} \binom{2N/tm}{2a/tm} (-1)^{a-2a/tm} \mu(m) + \right. \\ &\left. \left. + R_H(t) \sum_{m|(N/t, a/t)} \binom{N/tm}{a/tm} (-1)^{a-a/tm} \mu(m) \right] \right\} = \\ &= \frac{1}{N} \left[\sum_{\substack{t|(N, a, \Delta(h)) \\ a/2t \equiv 0 \pmod{2}}} R_H(t) A(t) + \sum_{\substack{t|(N, a, \Delta(h)) \\ a/t \equiv 1 \pmod{2}}} C(t) \right] \geq \\ &\geq \frac{1}{N} R_H(1) A(1) = M(H, h^*, a), \end{aligned}$$

где $h^* = (1, \dots, 1)$.

Поэтому при $\tau(N) > \tau(a) > 1$

$$M(H, a) = \frac{1}{N} \sum_{m|(N, a)} \binom{N/m}{a/m} (-1)^{a-a/m} \mu(m).$$

Если $\tau(m) < \tau(a)$, то $a-a/m \equiv 0 \pmod{2}$, если же $\tau(m) = \tau(a)$, то $\mu(m) = 0$, так как $\tau(a) > 1$.

Поэтому при $\tau(N) > \tau(a) > 1$

$$M(H, a) = \frac{1}{N} \sum_{m|(N, a)} \binom{N/m}{a/m} \mu(m).$$

Пусть, наконец, $\tau(N) > \tau(a) = 1$. Тогда по леммам 1 и 3, если $\Delta(h) \equiv 0 \pmod{2}$,

$$\begin{aligned} M(H, h, a) &= \frac{1}{N} \sum_{t|(N, a, \Delta(h))} R_H(t) \sum_{m|(N/t; a/t)} \binom{N/tm}{a/tm} (-1)^{a-a/tm} \mu(m) = \\ &= \frac{1}{N} \sum_{\substack{t|(N, a, \Delta(h)) \\ t \equiv 0 \pmod{2}}} \left[R_H(t/2) \sum_{m|(2N/t; 2a/t)} \binom{2N/tm}{2a/tm} (-1)^{a-2a/tm} \mu(m) + \right. \\ &+ \left. R_H(t) \sum_{m|(N/t; a/t)} \binom{N/tm}{a/tm} (-1)^{a-a/tm} \mu(m) \right] = \\ &= \frac{1}{N} \sum_{\substack{t|(N, a, \Delta(h)) \\ t \equiv 0 \pmod{2}}} C(t) \geq \frac{1}{N} C(2) = M(H, h^*, a), \end{aligned}$$

где $h^* = (0, 1, \dots, 1)$, если $H = \mathbf{Z}/2^{\alpha_1} \times \mathbf{Z}/p_2^{\alpha_2} \times \dots \times \mathbf{Z}/p_r^{\alpha_r}$. Если же $\tau(N) > \tau(a) = 1$ и $\Delta(h) \equiv 1 \pmod{2}$, то по леммам 1 и 2

$$\begin{aligned} M(H, h, a) &= \frac{1}{N} \sum_{t|(N, a, \Delta(h))} R_H(t) \sum_{m|(N/t; a/t)} \binom{N/tm}{a/tm} (-1)^{a-a/tm} \mu(m) = \\ &= \frac{1}{N} \sum_{t|(N, a, \Delta(h))} R_H(t) A(t) \geq \frac{1}{N} R_H(1) A(1). \end{aligned}$$

Но $C(2) = R_H(1)A(1) + R_H(2)A(2)$. По лемме 2 при $\tau(N) > \tau(a) = 1$ $A(2) \leq 0$. Поэтому

$$M(H, h^*, a) = \frac{1}{N} C(2) \leq \frac{1}{N} R_H(1) A(1).$$

Таким образом, при $\tau(N) > \tau(a) = 1$

$$\begin{aligned} M(H, a) &= \frac{1}{N} \left[\sum_{m|(N, a)} \binom{N/m}{a/m} (-1)^{a-a/m} \mu(m) + \right. \\ &+ \left. R_H(2) \sum_{m|(N/2; a/2)} \binom{N/2m}{a/2m} (-1)^{a-a/2m} \mu(m) \right]. \end{aligned}$$

Поскольку $\tau(a) = 1$, то $a-a/2m \equiv 1 \pmod{2}$. Следовательно,

$$\begin{aligned} M(H, a) &= \frac{1}{N} \left[\sum_{m|(N, a)} \binom{N/m}{a/m} (-1)^{a-a/m} \mu(m) - \right. \\ &- \left. R_H(2) \sum_{m|(N/2; a/2)} \binom{N/2m}{a/2m} \mu(m) \right]. \end{aligned}$$

Что и требовалось доказать.

§ 5. Минимизация по кривым

Для того чтобы минимизировать число векторов минимального веса в эллиптическом коде с данными параметрами, надо знать структуру группы точек $X(\mathbb{F}_q)$. Ее возможный порядок полностью описывается теоремой Ватерхауза ([6, теорема 4.1]). Заметим, что в работе [12], где также изучались эллиптические коды, число \mathbb{F}_{2^m} -точек на эллиптической кривой оценивается непосредственно по ее уравнению. Следующая теорема [7, 8] отвечает на вопрос о том, какова может быть группа $X(\mathbb{F}_q)$. Теорема Ватерхауза включена в ее формулировку.

Теорема 6. *Группа G порядка N изоморфна группе \mathbb{F}_q -точек некоторой эллиптической кривой X над \mathbb{F}_q тогда и только тогда, когда выполнено одно из следующих условий (полагаем $t=N-q-1$, $q=p^e$):*

1) $(q, t)=1$, $|t| \leq 2\sqrt{q}$, $G=\mathbb{Z}/A \times \mathbb{Z}/B$, причем $B|A$ и $B|(t-2)$;

2) q является квадратом, $t=\pm 2\sqrt{q}$, $G=(\mathbb{Z}/A)^2$;

3) q является квадратом, $p \neq 1 \pmod{3}$, $t=\pm\sqrt{q}$, $G=\mathbb{Z}/N$.

4) q не является квадратом, $p=2$ или 3 , $t=\pm\sqrt{pq}$, $G=\mathbb{Z}/N$;

5а) (i) q не является квадратом и $p \neq 3 \pmod{4}$ или (ii) q является квадратом и $p \neq 1 \pmod{4}$, $t=0$, $G=\mathbb{Z}/N$;

5б) q не является квадратом, $p=3 \pmod{4}$, $t=0$, $G=\mathbb{Z}/N$ или $\mathbb{Z}/2 \times \mathbb{Z}/A$.

Теперь мы переходим к вычислению числа $M(N, a)$, равного по определению минимуму $M(X(\mathbb{F}_q), a)$ по всем эллиптическим кривым X над \mathbb{F}_q , имеющим ровно N , \mathbb{F}_q -точек.

Прежде всего заметим, что не при любом N имеются такие кривые (см. теорему 6). Далее мы считаем, что N именно таково и $M(N, a)$ имеет смысл. Согласно теореме 2, структура группы $H=X(\mathbb{F}_q)$ влияет на $M(X(\mathbb{F}_q), a)$ лишь при $N \equiv 0 \pmod{4}$, $a \equiv 2 \pmod{4}$. Обозначим $\log_2 R_H(2) = r_H$. Из теоремы 6 видно, что при $N \equiv 0 \pmod{4}$ $r_H=1$ или 2 , причем $r_H=2$ в следующих трех случаях: а) $N \not\equiv 1 \pmod{p}$ и q нечетно (в этом случае $G=\mathbb{Z}/A \times \mathbb{Z}/2$, $(q, t)=1$, $2|(t-2)$);

б) q является квадратом, $N=(\sqrt{q} \pm 1)^2$, q — нечетно;

в) $q=p^e$ не является квадратом, $p \equiv 3 \pmod{4}$, $N=q+1$.

По лемме 2 вторая сумма в формуле п. а) теоремы 2 положительна. Поэтому если $r_H=2$ реализуется, то именно такая группа H дает искомый минимум. Это доказывает следующую теорему.

Теорема 7. *Пусть существует эллиптическая кривая X над \mathbb{F}_q , $q=p^e$, имеющая ровно N точек. Тогда*

а) *если $N \equiv 0 \pmod{4}$, $a \equiv 2 \pmod{4}$, q нечетно и, кроме того, либо $N \not\equiv 1 \pmod{p}$, либо q является квадратом и $N=(\sqrt{q} \pm 1)^2$, либо q не является квадратом, $p \equiv 3 \pmod{4}$ и $N=q+1$, то*

$$M(N, a) = \frac{1}{N} \left[\sum_{m|(a, N)} \binom{N/m}{a/m} \mu(m) (-1)^{a-a/m} - 4 \sum_{m|(a/2, N/2)} \binom{N/2m}{a/2m} \mu(m) \right];$$

б) *если $N \equiv 0 \pmod{4}$, $a \equiv 2 \pmod{4}$, но либо q четно, либо ни одно из дополнительных условий предыдущего пункта не выполнено, то*

$$M(N, a) = \frac{1}{N} \left[\sum_{m|(a, N)} \binom{N/m}{a/m} \mu(m) (-1)^{a-a/m} - 2 \sum_{m|(a/2, N/2)} \binom{N/2m}{a/2m} \mu(m) \right];$$

в) если $N \not\equiv 0 \pmod{4}$ или $a \not\equiv 2 \pmod{4}$, то

$$M(N, a) = \frac{1}{N} \sum_{m|(a, N)} \binom{N/m}{a/m} \mu(m).$$

Интерес, конечно, представляет не столько формулировка теоремы 7, сколько сам факт, что число $M(N, a)$ может быть полностью вычислено.

§ 6. Эллиптические МДР-коды

Когда эллиптический код может иметь параметры $k+d=n+1$? Особенно интересно выяснить, бывают ли такие коды при длине большей, чем у ранее известных кодов [см. 13, § 11.7]. Как мы уже говорили во введении, для этого необходимо и достаточно, чтобы $M(X(\mathbb{F}_q), \mathcal{P}, P_D, a) = 0$.

Пусть $h_0 \in H$, $\mathcal{P} \subseteq H = X(\mathbb{F}_q)$, $a = s + 2t$, $|\mathcal{P}| = n$, $|H| = N$. Равенство $h_0 = h_1 + \dots + h_s + h_{s+1} + \dots + h_{s+t} + \dots + h_{s+2t}$ будем называть (a, s, \mathcal{P}) -представлением h_0 , если $h_i \neq h_j$ при $i \neq j$, $i = 1, \dots, s + 2t$, $j = 1, \dots, s + 2t$ и $h_{s+i} = -h_{s+i+t}$, $i = 1, \dots, t$.

Лемма 4. Пусть h_0 имеет (a, s, \mathcal{P}) -представление и $s + a \leq 2n - 5 - N$. Тогда h_0 имеет $(a + 2, s, \mathcal{P})$ -представление.

Доказательство. Положим $\mathcal{P}_{h_0}^* = \{h \in \mathcal{P} \mid h \neq -h, -h \in \mathcal{P}\}$. Поскольку $H = X(\mathbb{F}_q)$, то в H существует не более четырех элементов h (один из которых 0) таких, что $h = -h$. Поэтому $|\mathcal{P}_{h_0}^*| \geq 2n - 4 - N$.

Пусть $h_0 = h_1 + \dots + h_{s+2t}$ — (a, s, \mathcal{P}) -представление h_0 . Предположим, что множество

$$R = \mathcal{P}_{h_0}^* \setminus \{\pm h_1, \pm h_2, \dots, \pm h_s, h_{s+1}, \dots, h_{s+2t}\}$$

не пусто. Тогда если $h^* \in R$, то и $-h^* \in R$ и $h_0 = h_1 + \dots + h_{s+2t} + h^* + (-h^*)$ есть $(a + 2, s, \mathcal{P})$ -представление h_0 . Множество R не пусто, если $2n - 4 - N - 2t - 2s \geq 1$ или $s + a \geq 2n - N - 5$.

Лемма 5. Пусть $N - n < \lfloor (N - 2)/3 - 2/3(N - 1) \rfloor$, где $\lfloor x \rfloor$ — наименьшее целое не меньшее x . Тогда для любого $h_0 \in H$ существует $(3, 3, \mathcal{P})$ -представление.

Доказательство. По теореме 2 $M(H, h_0, 3) \geq \frac{1}{N} \left[\binom{N}{3} - N/3 \right]$.

Пусть фиксировано $h \in H$. Тогда число представлений h_0 в виде $h_0 = h + h_1 + h_2$, $h \neq h_1 \neq h_2 \neq h$ не превосходит $(N - 1)/2$. Поэтому если $N - n < \lfloor \frac{2}{N} \times$

$\times \left[\binom{N}{3} - N/3 \right] / (N - 1) \rfloor = \lfloor (N - 2)/3 - 2/3(N - 1) \rfloor$, то существует по крайней мере одно $(3, 3, \mathcal{P})$ -представление h_0 .

Аналогично доказывается

Лемма 6. Пусть $N - n < \lfloor (N - 4)/2 \rfloor$. Тогда для любого $h_0 \in H$ существует $(2, 2, \mathcal{P})$ -представление.

Из лемм 4–6 индукцией по a легко получить следующую лемму.

Лемма 7. Для любого $h_0 \in H$ и $a \leq 2n - 6 - N$ при $n > N - \min \{ \lfloor (N - 4)/2 \rfloor, \lfloor (N - 2)/3 - 2/3(N - 1) \rfloor \}$ существует представление элемента h_0 в виде a различных слагаемых из \mathcal{P} .

Поскольку, как известно, при $q < 13$ не существует МДР-кодов с длиной, большей чем у ранее известных, то лемма 7 нам необходима при $N > 14$. Поэтому последнее неравенство превращается в

$$n > N - \lfloor (N - 2)/3 - 2/3(N - 1) \rfloor.$$

Из леммы 7 (используя ее для кода или его двойственного) выводится

Предложение 2. При $q \geq 27$ не существует нетривиальных эллиптических МДР-кодов с длиной $n > q + 1$.

На самом деле можно показать, что не существует нетривиальных эллиптических МДР-кодов с длиной $n > q + 1$ при $q \geq 13$. Для доказательства этого требуется более тщательный анализ.

Приведем пример такого анализа при $q = 13$. Если $q = 13$, то максимальная длина эллиптического кода равна $N = 21$. В этом случае $H = \mathbf{Z}/21$. Пусть $n = |\mathcal{P}| = 15$. В случае $b = 2$ существование представления в виде суммы двух слагаемых из \mathcal{P} следует из леммы 6.

Пусть $b = 3$, тогда число представлений элемента из $\mathbf{Z}/21$ в виде суммы трех слагаемых из всей группы $\mathbf{Z}/21$ не меньше $\frac{1}{21} \left[\binom{21}{3} - \binom{7}{1} \right] = 63$.

Число таких представлений, содержащих один фиксированный элемент, не более десяти. Поэтому существует по крайней мере $63 - (21 - 15) \cdot 10 = 3$ представлений элемента в виде трех слагаемых из \mathcal{P} .

Пусть теперь $b = 4$ или 6. Обозначим $X = H \setminus \mathcal{P} = \{x_1, x_2, x_3, x_4, x_5, x_6\}$, $X^- = \{-x_1, \dots, -x_6\}$, $|\mathcal{P} \setminus X^-| \geq 9$.

Пусть $h_0 \in \mathcal{P}$, тогда существует представление $h_0 = h_1 + h_2$, $h_1 \neq 0$, $h_2 \neq 0$, $h_1, h_2 \in \mathcal{P}$. Тогда $|(\mathcal{P} \setminus X^-) \setminus \{h_1, h_2, -h_1, -h_2\}| \geq 5$. Множество $(\mathcal{P} \setminus X^-) \setminus \{h_1, h_2, -h_1, -h_2\}$ состоит из попарно взаимно обратных элементов и возможно нули. Следовательно, будет существовать представление h_0 в виде четырех и шести слагаемых из \mathcal{P} . При этом если $0 \in \mathcal{P}$, могут быть выбраны представления в виде четырех и шести слагаемых, не содержащих 0. Поэтому если $0 \in \mathcal{P}$, то будут существовать представления в виде пяти и семи слагаемых из \mathcal{P} .

Пусть $0 \notin \mathcal{P}$, тогда $0 \in X$ и $|\mathcal{P} \setminus X^-| = 10$. Пусть $h_0 = h_1 + h_2 + h_3$, $h_1, h_2, h_3 \in \mathcal{P}$. Тогда $|(\mathcal{P} \setminus X^-) \setminus \{h_1, h_2, h_3, -h_1, -h_2, -h_3\}| = 4$. Это множество состоит из пар взаимно обратных элементов. Следовательно, будет существовать представление h_0 в виде суммы пяти и семи слагаемых из \mathcal{P} . Отсюда следует, что в случае $p = 13$ и $N = 21$ не существует эллиптических МДР-кодов длины $n \geq 15$.

Пусть $q = 13$, $N = 20$, $n = 15$. Самый сложный случай $H = \mathbf{Z}/2 \times \mathbf{Z}/2 \times \mathbf{Z}/5$.

Так же, как и ранее, случай $b = 2$ очевиден. В случае $b = 3$ общее число представлений $h_0 \in H$ в виде трех слагаемых из H равно $\frac{1}{20} \binom{20}{3} = 57$.

Число таких представлений, содержащих фиксированный элемент, не превосходит девять. Поэтому будет существовать не менее $57 - (20 - 15) \cdot 9 = 12$ представлений h_0 в виде суммы трех слагаемых из \mathcal{P} .

Пусть $b = 4$, $\alpha, \beta, \gamma \in H$, $\alpha = -\alpha \neq 0$, $\beta = -\beta \neq 0$, $\gamma = -\gamma \neq 0$. Пусть $h_0 = h_1 + h_2$. Тогда $|(((\mathcal{P} \setminus X^-) \setminus \{h_1, h_2, -h_1, -h_2\}) \setminus \{0, \alpha, \beta, \gamma\})| \geq 2$. Это множество состоит из пар взаимно обратных элементов. Следовательно, существует представление h_0 в виде суммы четырех слагаемых из \mathcal{P} .

Пусть теперь $b = 5$ или 7. Нетрудно показать, что число представлений h_0 в виде суммы трех слагаемых, по крайней мере один из которых не принадлежит \mathcal{P} , оценивается сверху как $\lfloor \frac{19}{2} \rfloor + \lfloor \frac{18}{2} \rfloor + \lfloor \frac{17}{2} \rfloor + \lfloor \frac{16}{2} \rfloor + \lfloor \frac{15}{2} \rfloor = 41$. Пусть $R \subseteq (\mathcal{P} \setminus X^-) \setminus \{0, \alpha, \beta, \gamma\}$, $|R| = 6$ (такое подмножество существует, так как $|(\mathcal{P} \setminus X^-) \setminus \{0, \alpha, \beta, \gamma\}| \geq 6$). Число представлений h_0 в виде трех слагаемых, не менее два из которых принадлежат R , оценивается сверху как $\binom{6}{2} = 15$. Поэтому существует по крайней мере $57 - 41 - 15 = 1$ представление $h_0 = h_1 + h_2 + h_3$ в виде суммы трех слагаемых из \mathcal{P} , причем не более одного из этих слагаемых принадлежит R .

Легко видеть, что R может быть выбрано так, что если $h \in R$, то $-h \in R$. Тогда $|R \setminus \{h_1, h_2, h_3, -h_1, -h_2, -h_3\}| \geq 4$, и это множество состоит из пар взаимно обратных элементов. Поэтому существует представление h_0 в виде суммы пяти и семи слагаемых из \mathcal{P} .

Пусть $b = 6$. Предположим, что $0, \alpha, \beta, \gamma \in \mathcal{P}$, тогда существует представление $h_0 = h_1 + h_2$, $h_1, h_2 \in \mathcal{P}$, $h_1, h_2 \notin \{0, \alpha, \beta, \gamma\}$. Поскольку $0 + \alpha + \beta + \gamma = 0$, то $h_0 = h_1 + h_2 + 0 + \alpha + \beta + \gamma$. Если же по крайней мере один из элементов 0,

α, β, γ не принадлежит \mathcal{P} , то

$$|((\mathcal{P} \setminus X^-) \setminus \{h_1, h_2, -h_1, -h_2\}) \setminus \{0, \alpha, \beta, \gamma\}| \geq 3,$$

но поскольку это множество состоит из пар взаимно обратных элементов, то его мощность четна и поэтому не меньше четырех. Отсюда следует, что и в этом случае будет существовать представление h_0 в виде суммы шести элементов из \mathcal{P} .

Таким образом, в случае $q=13, N=20, H=\mathbf{Z}/2 \times \mathbf{Z}/2 \times \mathbf{Z}/5$ не существует эллиптических МДР-кодов длины больше либо равной 15.

При $q=13$ остальные случаи с $N=20$, и $N \leq 19$ доказательство производится полностью аналогично. Случаи $q=16, 17, 19, 23, 25$ проще случая $q=13$ и разбираются аналогично.

ЛИТЕРАТУРА

1. Влэдуц С. Г., Манин Ю. И. Линейные коды и модулярные кривые // Современные проблемы математики. М.: ВИНТИ, 1984. Т. 25. С. 209–257.
2. Гонна В. Д. Коды на алгебраических кривых // Докл. АН СССР. 1981. Т. 259. № 6. С. 1289–1290.
3. Шафаревич И. П. Основы алгебраической геометрии. М.: Наука, 1972.
4. Helleseth T., Klove T. On Group-Theoretic Codes for Asymmetric Channels // Inform. and Control. 1981. V. 49. № 1. P. 1–9.
5. Delsarte P., Piret P. Spectral Enumerators for Certain Additive Error-Correcting Codes over Integer Alphabets // Inform. and Control. 1981. V. 48. № 3. P. 193–210.
6. Waterhouse W. C. Abelian Varieties Over Finite Fields // Ann. Sci. Norm. Sup. 1969. Ser. 4. V. 2. P. 521–560.
7. Цфасман М. А. Группа точек эллиптической кривой над конечным полем // Тр. Всесоюз. конф. по теории чисел и ее приложениям. Тез. докл. Тбилиси, 1985. С. 286–287.
8. Schoof R. Nonsingular Plane Cubic Curves over Finite Fields (to appear).
9. Driencourt Y., Michon J.-F. Remarques sur les Codes Geometriques // C. R. Acad. Paris. 1985. V. 301. № 1. P. 15–17.
10. Гриффитс Ф., Харрис Дж. Принципы алгебраической геометрии. М.: Мир, 1982.
11. Холл М. Комбинаторика. М.: Мир, 1970.
12. Крачковский В. Ю. О кодах Гоппы, определяемых кубическими уравнениями // Тр. VIII Всесоюз. симпоз. по проблеме избыточности в информационных системах. Тез. докл. Ленинград, 1983. Ч. 1. С. 147–149.
13. Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки. М.: Связь, 1979.

Поступила в редакцию
5.IX.1985