УДК 621.39

ПОИСК НЕПРИВОДИМЫХ АЛГЕБРАИЧЕСКИХ КРИВЫХ МАЛОЙ СТЕПЕНИ В КОНЕЧНЫХ ПОЛЯХ

А.А. Кузнецов, С.В. Ушно
(представил д.т.н. проф. В.И. Долгов)

Рассмотрены одномерные алгебраические многообразия в конечных полях характеристики 2. Предложена методика поиска неприводимых алгебраических многообразий представленных многочленами малой степени. Представлены результаты поиска на ЭВМ. Приведено распределение полученных кривых по числу мономов.

Одним из центральных результатов теории алгебраических кривых является теорема Римана – Роха [1]. Пусть **L** – класс дивизоров на гладкой проективной алгебраической кривой **X** рода **g**, **D** – некоторый дивизор класса **L**, **L(D)** – **k**-мерное пространство функций, ассоциированное с **D**. Пусть $\mathbf{f_1, f_2, \ldots f_k}$ – некоторый базис в **L(D)**, тогда **L** определяет отображение $\boldsymbol{\varphi}\mathbf{: X \to P^k}$, где $\mathbf{L(D) = deg(D) - g + 1}$. Если $\mathbf{X_1, X_2, \ldots, X_n}$ суть $\mathbf{F_q}$ - точки кривой **X**, то набор $\mathbf{y_i = \varphi(x_i)}$ задает код **C** с конструктивными характеристиками **(n, k, d)** связанными соотношениями $\mathbf{d+k = N-g+1}$, где **N** – число точек кривой [2, 3].

Гладкая проективная алгебраическая кривая **X** в **n**-мерном проективном пространстве $\mathbf{P^n}$ над полем $\mathbf{F_q}$ – это одномерное алгебраическое многообразие без особенностей, т.е. совокупность решений системы однородных алгебраических уравнений от **(n + 1)** переменной с коэффициентами из $\mathbf{F_q}$ таких, что матрица производных в каждой точке задает уравнение прямой [4].

Верхнюю границу числа точек алгебраической кривой дает известное выражение Хассе-Вейля

$$\mathbf{N \le g\left[2\sqrt{q}\right] + q + 1}. \qquad (1)$$

Граница Хассе-Вейля, равно как и теорема Римана – Роха, справедлива только для неприводимых алгебраических кривых. Целью публикации является изложение материалов поиска неприводимых алгебраических кривых степени **d** в пространстве $\mathbf{P^n}$ над конечными полями характеристики 2.

Рассмотрим алгебраическую кривую степени **d** от **(n + 1)** переменных как множество нулей полиномиального многочлена общий вид которого представлен как

$$F(x_0, x_1, ..x_n) = \sum_{i=1}^{m} \prod_{j=0}^{n} a_{ij} x_j^{i_j}, \qquad (2)$$

где **m** – число мономов многочлена;

n+1 – число переменных;

$\sum_{j=0}^{n} i_j = d$ – степень многочлена.

Рассмотрим все однородные многочлены **F** степени **d** от **(n+1)** переменных. Они образуют линейное пространство, размерность которого равна

$$M = C\begin{pmatrix} d \\ n+d \end{pmatrix}. \qquad (3)$$

Отображение проективного пространства P^n в линейное пространство образованное всеми однородными многочленами степени **d**, обозначенное как $\vartheta: P^n \to P^M$ называется отображением Веронезе [1, 2].

По аналогии с отображением $\vartheta: P^n \to P^M$ приведем отображение $\upsilon: F(x_0, x_1, \dots, x_n) \to F(y_0, y_1, \dots, y_m)$.

Все точки кривой $F(x_0, x_1, \dots, x_n)$ из P^n отображаются в многообразие точек кривой $F(y_0, y_1, \dots, y_m)$ из P^M посредством базиса $y_0(x), y_1(x), \dots, y_m(x)$, где **m** – число мономов в выражении (2).

Число всех возможных кривых степени **d** от **(n + 1)** переменных равно числу гиперплоскостей $F(y_0, y_1, \dots, y_m)$ из проективного пространства P^M. Каждому значению **m** соответствует множество линейных подпространств, количество которых равно

$$\theta = C\begin{pmatrix} m \\ M \end{pmatrix}. \qquad (4)$$

Поскольку число мономов в кривой произвольного вида может быть любым, в пределах $1<m<M$, то число гиперплоскостей $F(y_0, y_1, \dots, y_m) \in P^M$ а, следовательно, и число всех возможных кривых $F(x_0, x_1, \dots, x_n) \in P^n$ степени **d** в конечных полях характеристики 2 равно

$$\Theta = \sum_{i=1}^{M} \theta_i = \sum_{i=1}^{M} C\begin{pmatrix} i \\ M \end{pmatrix} = 2^M - 1. \qquad (5)$$

Если многочлен $f(x_0, x_1, \dots, x_n)$ разлагается на два множителя: $f=g*h$, то множество точек кривой $f(x_0, x_1, \dots, x_n)$ является объединением множеств нулей алгебраических многочленов определенных уравнениями $g(x_0, x_1, \dots, x_n) = 0$ и $h(x_0, x_1, \dots, x_n) = 0$, соответственно.

Если многочлен **f** – неприводим, то и определенная им кривая называется неприводимой [2].

Все приводимые алгебраические кривые $\mathbf{f(x_0, x_1, \dots, x_n)}$ степени **d** можно представить как разложение на два, как минимум, сомножителя: **f=g*h**. Иными словами, любую приводимую кривую степени **d** можно записать в виде

$$\mathbf{F(x_0, x_1, x_2, \dots x_n) = \sum_{i=1}^{m} \prod_{j=0}^{n} a_{ij} x_j^{i_j} = \left(\sum_{i_1=1}^{m_1} \prod_{j=0}^{n} a_{ij} x_j^{i_{1j}} \right) \cdot \left(\sum_{i_1=1}^{m_2} \prod_{j=0}^{n} a_{ij} x_j^{i_{1j}} \right)}$$

где $\mathbf{m_1, m_2}$ – число мономов в каждом из многочленов разложения;

$\sum_{j=0}^{n} i_{1j} = d_1$, $\sum_{j=0}^{n} i_{2j} = d_2$ – степень многочленов разложения.

Число всех разложений степени **d** равно $\left\lfloor \frac{d}{2} \right\rfloor$. Следовательно, выражение для нахождения числа всех приводимых кривых степени **d** можно записать в виде

$$\Theta_{пр} \le \sum_{i=1}^{\left\lfloor \frac{d}{2} \right\rfloor} \Theta_{1i} \cdot \Theta_{2i} == \sum_{i=1}^{\left\lfloor \frac{d}{2} \right\rfloor} \left(2^{\frac{(i+n)!}{i! \cdot n!}} - 1 \right) \cdot \left(2^{\frac{(d-i+n)!}{(d-i)! \cdot n!}} - 1 \right). \qquad (6)$$

Знак «меньше или равно» говорит о том, что при перемножении различных сомножителей приводимых кривых могут образоваться мономы, сокращенные по некоторому модулю. Результатом подобных сокращений может стать разложение одной приводимой кривой на несколько пар сомножителей.

Выражение для числа неприводимых кривых степени **d** в пространстве $\mathbf{P^n}$ запишем в виде

$$\Theta_{нпр} = \Theta - \Theta_{пр} \ge 2^{\frac{(d+n)!}{d! \cdot n!}} - \sum_{i=1}^{\left\lfloor \frac{d}{2} \right\rfloor} \left(2^{\frac{(i+n)!}{i! \cdot n!}} - 1 \right) \cdot \left(2^{\frac{(d-i+n)!}{(d-i)! \cdot n!}} - 1 \right) - 1. \qquad (7)$$

Путем поиска на ЭВМ были получены все кривые малых степеней в малых полях характеристики 2, все разложения этих кривых, выделены все неприводимые кривые. Результаты поиска представлены в табл.1.

Таблица 1

Результаты поиска неприводимых кривых малой степени

Степень	Число всех кривых	Число разложений	Число неприводимых кривых (теория)	Число неприводимых кривых (практика)
2	63	≤ 49	≥ 14	35
3	1023	≤ 441	≥ 582	694
4	32767	≤ 8061	≥ 24704	26089

Интерес представляет распределение количества неприводимых кривых по числу мономов. Поведено исследование полученных неприводимых кривых распределение которых приведено в табл.2.

Таблица 2

Распределение числа кривых по количеству мономов

Число мономов	2-й степени	3-й степени	4-й степени
1	0	0	0
2	3	6	6
3	16	63	137
4	9	107	579
5	6	219	2184
6	1	143	3371
7	0	113	5763
8	0	33	5001
9	0	9	4765
10	0	1	2457
11	0	0	1308
12	0	0	400
13	0	0	102
14	0	0	15
15	0	0	1

ЛИТЕРАТУРА

1. Шафаревич И.Р. Основы алгебраической геометрии. – М.: Наука, 1972. – 568 с.

2. Грифитс Ф., Харрис Дж. Принципы алгебраической геометрии: Пер. с англ. – М.: Мир, 1982. – 366 с.

3. Халимов Г.З. Алгеброгеометрическое обобщение кодов. //Управление и связь. - Харьков: НАНУ, ПАНИ, ХВУ. - 1997. – С. 56-59.

4. Цфасман М.А. Коды Гоппы, лежащие выше границы Варшамова - Гилберта. // Пробл. передачи информации, - 1982,- № 3, - С. 3 - 6.