В.В. К а й з е р

СПЕЦИАЛЬНЫЕ РАСПРЕДЕЛЕНИЯ НА ГРАССМАНОВОМ МНОГООБРАЗИИ (III)

С помощью аналитического аппарата [1] выделены специальные неголономные конгруэнции и доказаны соответствующие результаты, сформулированные в 1-ой части работы [2].

УДК 512.7

ОБ ОДНОМ ПОДХОДЕ К ПОСТРОЕНИЮ АЛГЕБРАИЧЕСКИХ КРИВЫХ С БОЛЬШИМ ЧИСЛОМ РАЦИОНАЛЬНЫХ ТОЧЕК

Ю.С.К а с а т к и н а

(Калининградский государственный университет)

В настоящей работе ставится задача построения алгебраических кривых с большим числом рациональных точек, опираясь лишь на обобщенные веса Хемминга подкодов малой размерности. Рассмотрен пример, иллюстрирующий метод построения кривых, исходя из подкодов малых размерностей.

Вопрос построения алгебраических кривых с большим числом рациональных точек актуален как с теоретической, так и с практической точек зрения. В теории кодирования, например, такие кривые дают возможность построения кодов с хорошими характеристиками. Наличие большого числа рациональных точек на эллиптической кривой также значительно улучшает параметры криптосистемы. Для получения таких кривых используются различные подходы. Классический подход А.Вейля основан на расширении поля констант функционального поля. М.А.Цфасман и С.Г.Владут использовали для построения кодов так называемые модулярные кривые; F.Torres рассматривает этот вопрос с позиции алгебраической геометрии. Сравнительно недавно G.Geer и M.Vlugt [1] предложили новый подход к построению кривых с большим числом рациональных точек. Он основан на знании иерархии весов кода [2] и конструкции следов кодов [3], [4]. Однако, в общем случае, определение обобщенного веса Хемминга, следовательно, и весовой иерархии кода достаточно сложная задача. Распределение весов известно лишь для некоторых классов кодов.

Рассмотрим подробнее метод, предложенный в работе [1]. Пусть F_q - конечное поле, состоящее из $q = p^m$ элементов. Известно, что применяя отображение следа, можно коду C над полем F_q поставить в соответствие код над F_p, который называется следом кода C и обозначается Tr(C). Рассмотрим конечномерное над F_q подпространство L поля рациональных функций $F_q(x)$. Обозначим P - множе-

ство рациональных над F_q точек проективной прямой $P^1(F_q)$, которые являются полюсами для функций из L. Таким образом, код над полем F_q можно записать в виде:

$$\mathbf{C}=\{ f(x)_{x\in P^1(F_q)-P} \ : \ f \in L \}.$$

Тогда след кода Tr(C) является кодом над полем F_p:

$$Tr(C) = \{c_f = Tr(f(x))_{x\in P^1(F_q)-P} \ : \ f \in L\}.$$

Рассмотрим r-мерный подкод D кода Tr(C). Элементам базиса c_{f_i} этого подкода соответствуют элементы $f_i \in L, 1 \le i \le r$. Определим r-мерное подпространство пространства L над F_p (обозначим его L_D), порожденное элементами $f_1,\ldots,f_r$. Сопоставим кодовому слову c_{f_i} кривую Артина-Шрайера C_{f_i} с аффинным уравнением $y^p - y = f_i(x)$.

Пусть $\phi_i : C_{f_i} \to P^1$-отображение, задаваемое включением $F_q(x) \subset F_q(x,y)$. Рассмотрим кривую $C^{(D)}$, которая является нормализацией расслоенного произведения кривых C_{f_i} над $P^1(F_q)$. Известна формула [1] для определения веса подкода D:

$$W(D) = n - (\#C^{(D)}(F_q) - \sum_{Q\in P} p^{\varepsilon(Q)})/p^r,$$

где $\varepsilon(Q) = \dim_{F_P}\{f \in L_D : f - \text{регулярна в точке } Q\}$. Очевидно, что количество рациональных точек на кривой $C^{(D)}$ зависит от веса подкода D. Естественным образом можно предположить, что на подкодах малых весов будут получаться кривые с большим числом рациональных точек.

Рассмотрим пример, иллюстрирующий вышеизложенный метод. Пусть $\Gamma(L, g(x))$ - классический код Гоппы, где $L = F_8, g(x) = x^2 + x + 1$. Тогда $\Gamma(L, g(x))$ - код длины $n = 8$ над полем F_2. Известно [4], что код, дуальный к данному, можно представить как след. Обозначим:

$F = F_8(x)$-поле рациональных функций;

P_i-нуль элемента $(x - \alpha_i)$, $\alpha_i \in L$, $1 \le i \le 8$;

D-дивизор поля рациональных функций $F_8(x)$, $D = P_1 + \ldots + P_n$;

P_∞-полюс элемента x в поле рациональных функций $F_8(x)$;

G_0-дивизор нулей элемента $g(x)$.

Тогда $\Gamma(L, g(x))^\perp = Tr_D(V)$, где V-векторное пространство, ассоциированное с дивизором $(G_0 - P_\infty)$:

$$V = \{f(x) = \frac{h(x)}{g(x)} : h(x) \in F_8[x], \deg h(x) \le 1\}.$$

Нетрудно показать, что элементы $\frac{1}{g(x)}, \frac{x}{g(x)}$ îáðàçóþò базис векторного пространства V. С другой стороны, дуальный код $\Gamma(L, g(x))^\perp$ является кодом длины $n = 8$ размерности $k = 2$ над полем F_2. Выпишем все его кодовые слова:

(0,0,0,0,0,0,0,0); (1,1,0,0,0,0,0,0); (0,0,1,1,0,1,1,0); (1,1,1,1,0,1,1,0).

Рассмотрим всевозможные одномерные подкоды кода $\Gamma(L, g(x))^{\perp}$. Первый обобщенный вес Хемминга (в данном случае он равен двум) достигается на подкоде

$$D=\{(0,0,0,0,0,0,0,0);(1,1,0,0,0,0,0,0)\}.$$

Найдем элемент $f \in V$, который соответствует элементу базиса подкода D. Иначе говоря, такой элемент, который удовлетворяет соотношению:

$$(1,1,0,0,0,0,0,0) = (Tr(f(P_1)),\ldots,Tr(f(P_n))).$$

Получаем $f(x) = \frac{1}{g(x)} = \frac{1}{x^2 + x + 1}$. Рассмотрим кривую Артина-Шрайера C_f, задаваемую аффинным уравнением $y^2 - y = f(x)$. Подсчитаем количество рациональных точек кривой C_f. Над каждой точкой P_i из носителя дивизора D, для которой выполняется $Tr(f(P_i)) = 0$, лежат две различные точки степени один. В данном случае таких точек P_i шесть.

Для подсчета количества рациональных точек, лежащих над точкой P_∞, воспользуемся теоремой Куммера [3]. Получим, что над точкой P_∞ на кривой C_f лежат две различные рациональные точки. Таким образом, на кривой C_f лежат четырнадцать рациональных точек. Тем самым получена кривая над F_8 рода один с четырнадцатью рациональными точками. При этом использовались лишь одномерные подкоды. По данным таблицы [5] на кривой рода один над полем F_8 максимально возможное число рациональных точек равно четырнадцати, т.е. достигнуто максимальное значение.

Библиографический список

1. *Geer G., Vlugt M.* Fibre Products of Artin-Schreier cuvers and Generalized Hamming weight of codes // Journal of Combinatorial Theory. 1995. V.70. P.337-348.

2. *Wei V.K.* Generalized Hemming Weights of Linear Codes // IEEE Trans. Inform. 1991. V.37. P.1412-1418.

3. *Stichtenoth H.* Algebraic Function fields and Codes. Springer. 1993. 260 p.

4. *Stichtenoth H., Voss V.* Generalized Hemming Weights of Trace Codes // IEEE Trans. Inform. 1994. V.40. P.554-558.

5. *Geer G. , Vlugt M.* Tables for the function $N_q(g)$. http://www.wins. uva.nl/~geer.

J.S. K a s a t k i n a

ABOUT THE APPROACH TO THE CONSTRUCTION OF ALGEBRAIC CURVES WITH MANY RATIONAL POINTS

The problem of the construction of algebraic curves with many rational points, starting from generalized Hemming weight of subcodes, is discussed in this article. The example, which illustrates the method of construction this curves, is considered here.