УДК 621.39

КОНСТРУКЦИИ КОДОВ ПО КЛАССУ ДИВИЗОРА КРИВОЙ

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

Предлагается алгоритм построения алгебраико-геометрических кодов по классу произвольного дивизора кривой. Представлена группа однородных многочленов, отношение которых предлагается использовать в качестве генераторных функций порождающего базиса матрицы кода. Приведены примеры кодов, построенных по предложенному алгоритму.

Одним из центральных результатов теории алгебраических кривых является теорема Римана – Роха [1]. Пусть $\mathbf{L}$ – класс дивизоров на гладкой проективной алгебраической кривой $\mathbf{X}$ рода $\mathbf{g}$; $\mathbf{D}$ – некоторый дивизор класса $\mathbf{L}$; $\mathbf{L(D)}$ – $\mathbf{k}$ - мерное пространство функций, ассоциированное с $\mathbf{D}$. Пусть $\mathbf{f_1, f_2, ... f_k}$ – некоторый базис в $\mathbf{L(D)}$. Тогда $\mathbf{L}$ определяет отображение

$$\varphi : \mathbf{X} \to \mathbf{P^{k-1}},$$

где $\mathbf{L(D) = deg(D) - g + 1}$.

Если $\mathbf{X_1, X_2, ..., X_n}$ суть точки кривой $\mathbf{X}$, то набор $\mathbf{y_i = \varphi(x_i)}$ задает код $\mathbf{C}$ с конструктивными характеристиками $\mathbf{(n,k,d)}$, связанными соотношением

$$\mathbf{k + d \geq n - g + 1}. \qquad (1)$$

Анализ литературы [2 - 3] показал, что на сегодняшний день теоретически обоснована возможность построения кодов по алгебраическим кривым. В источниках [2 - 6] приведены примеры построения алгебраико-геометрических кодов. Предложенные алгоритмы предполагают построение кодов только по определенным кривым с известной структурой точек. Алгоритмов построения алгебраико - геометрических кодов по произвольной гладкой проективной кривой не существует. В статье кратко изложена суть разработанного алгоритма построения кодовых конструкций по алгебраико - геометрическим кривым, основанного на свойствах дивизоров кривой.

Алгебраико - геометрический код соответствует линейному пространству, полученному через рациональное отображение гладкой проективной кривой. Рациональное отображение может быть задано порождающим базисом генераторных функций $\mathbf{f_1, f_2, ..., f_k}$. Инвариантом по-

рождающего является пространство $\mathbf{L(D)}$, ассоциированное с классом произвольного дивизора $\mathbf{D}$ кривой $\mathbf{X}$.

Суть предложенного алгоритма состоит в следующем. Выбираем произвольный класс дивизоров на $\mathbf{X}$ и для любого дивизора $\mathbf{D}$ этого класса в пространстве $\mathbf{L(-D)}$ такое линейное конечномерное подпространство $\mathbf{M}$, что эффективные дивизоры $\mathbf{(f)-D}$ не имеют общих компонентов. Если $\mathbf{f_1, f_2, ... f_k}$ - его базис $\mathbf{M}$, то отображение задается формулой

$$\varphi : x \to \left(f_1(x), f_2(x), \ldots, f_k(x)\right). \qquad (2)$$

Так как умножение всех функций $\mathbf{f_i}$ из (2) на общий множитель $\mathbf{g \in k(X)}$ не изменит отображения φ, а дивизор $\mathbf{D}$ при этом изменится на эквивалентный дивизор $\mathbf{(g)+D}$, то инвариантом рационального отображения является класс дивизора $\mathbf{D}$. Может оказаться, что $\mathbf{L(-D)=0}$ или все дивизоры $\mathbf{(f)-D}$, $\mathbf{f \in L(D)}$ имеют общие компоненты. Тогда этот класс дивизоров не приводит ни к какому отображению.

Найдена группа многочленов, дающих малое число решений в $\mathbf{P^2}$ над $\mathbf{GF(2^m)}$. В табл.1 приведены некоторые из них, дающие одно решение.

Отношения этих многочленов могут быть использованы в качестве базиса рационального отображения, построенного по предложенному алгоритму.

Путем анализа полиномиальных форм, приведенных в табл. 1, сформулировано следующее предложение.

Предложение. Все алгебраические кривые, построенные на однородных многочленах, приведенных в табл. 1, имеют единственную точку в полях $\mathbf{GF(2^m)}$, степень расширения $\mathbf{m}$ которых не делится на степень многочлена $\mathbf{d}$.

Особенностью многочленов, приведенных в табл. 1, является число точек, равное единице над полями, степень расширения которых не делится на степень полиномов. Отношения таких многочленов дают рациональные функции, дивизор которых содержит небольшое число компонентов. Следовательно, можно выбрать такие рациональные функции, пересечение дивизоров которых конечное, по возможности, минимальное множество точек.

Далее, исключив из многообразия точек кривой это множество, получим необходимую нам конструкцию кодов по алгебраическим кривым. На практике вопрос выбора генераторных функций легко решаем при небольшом их числе. С увеличением числа генераторных функций выбор таковых затруднен или вообще невозможен без уменьшения длины кода.

Таблица 1

Однородные многочлены с малым числом точек над $\mathbf{GF(2^m)}$

d	**m**	Полиномиальная форма	Точки **XYZ**
3	2, 4, 5, 7, …	$y^3 + x^2y + x^3$	001
3	2, 4, 5, 7, …	$y^3 + xy^2 + x^3$	001
3	2, 4, 5, 7, …	$z^3 + x^2z + x^3$	010
3	2, 4, 5, 7, …	$z^3 + xz^2 + x^3$	010
3	2, 4, 5, 7, …	$z^3 + y^2z + y^3$	100
3	2, 4, 5, 7, …	$z^3 + yz^2 + y^3$	100
3	2, 4, 5, 7, …	$z^3 + xz^2 + y^2z + y^3 + x^2y + x^3$	111
3	2, 4, 5, 7, …	$z^3 + yz^2 + x^2z + y^3 + xy^2 + x^3$	111
3	2, 4, 5, 7, …	$z^3 + y^2z + x^2z + y^3 + xy^2 + x^2y + x^3$	110
3	2, 4, 5, 7, …	$z^3 + yz^2 + xz^2 + y^3 + xy^2 + x^2y + x^3$	110
3	2, 4, 5, 7, …	$z^3 + yz^2 + y^2z + x^2z + y^3 + x^2y + x^3$	011
3	2, 4, 5, 7, …	$z^3 + yz^2 + xz^2 + y^2z + y^3 + xy^2 + x^3$	011
3	2, 4, 5, 7, …	$z^3 + yz^2 + xz^2 + x^2z + y^3 + x^2y + x^3$	101
3	2, 4, 5, 7, …	$z^3 + xz^2 + y^2z + x^2z + y^3 + xy^2 + x^3$	101
2	3, 5, 7, 9, …	$y^2 + xy + x^2$	001
2	3, 5, 7, 9, …	$z^2 + xz + x^2$	010
2	3, 5, 7, 9, …	$z^2 + yz + y^2$	100
2	3, 5, 7, 9, …	$z^2 + xz + y^2 + xy + x^2$	011
2	3, 5, 7, 9, …	$z^2 + yz + y^2 + xy + x^2$	101
2	3, 5, 7, 9, …	$z^2 + yz + xz + y^2 + x^2$	110
2	3, 5, 7, 9, …	$z^2 + yz + xz + y^2 + xy + x^2$	111

На основе проведенного поиска однородных неприводимых многочленов [7] и исследования их характеристик выделены полиномиальные формы, дающие большое число решений в проективном пространстве над конечным полем. Эти исследования позволили получить необходимый объем алгебраико-геометрической информации для построения гладких проективных кривых с большим числом точек над фиксированным полем $\mathbf{GF(2^m)}$.

В качестве примера использования разработанного алгоритма построения алгебраико - геометрических кодов нами были построены коды на кривых с максимальным числом точек. Результаты этого построения сведены в таблицы кодовых характеристик, которые представлены в табл. 2 - 4.

В приведенных примерах по построению кодов в качестве теста проводился последовательный перебор всех комбинаций с одной, двумя и тремя единицами в информационной части, а также набор случайных последовательностей в количестве 100000 комбинаций.

Таблица 2

$$yz^3 + xz^3 + x^3z + xy^3 + x^2y^2 + x^3y + x^4,\ g = 3,\ GF(8),\ N = 24$$

GF(8)						
deg X	deg(f)	α	(G) (n, ≥ α − g + 1, ≥ n − α)		(H) (n, ≥ n − α + g − 1, ≥ α − 2g + 2)	
			теория	тест	теория	тест
4	2	8	(24, k ≥ 6, d ≥ 16)	(24,6,16)	(24, k ≥ 18, d ≥ 4)	(24,18,4)
4	4	16	(24, k ≥ 14, d ≥ 8)	(24,14,8)	(24, k ≥ 10, d ≥ 12)	(24,10,12)

Таблица 3

$$yz^2 + xyz + xy^2 + x^3,\ g = 1,\ GF(32),\ N = 44$$

GF(16)						
deg X	deg(f)	α	(G) (n, ≥ α − g + 1, ≥ n − α)		(H) (n, ≥ n − α + g − 1, ≥ α − 2g + 2)	
			теория	тест	теория	тест
3	2	6	(44, k ≥ 6, d ≥ 38)	(44,6,38)	(44, k ≥ 38, d ≥ 6)	(44,38,6)
3	4	12	(44, k ≥ 12, d ≥ 32)	(44,12,32)	(44, k ≥ 32, d ≥ 12)	(44,32,12)
3	6	18	(44, k ≥ 18, d ≥ 26)	(44,18,26)	(44, k ≥ 26, d ≥ 18)	(44,26,18)
3	8	24	(44, k ≥ 24, d ≥ 20)	(44,24,20)	(44, k ≥ 20, d ≥ 24)	(44,20,24)
3	10	30	(44, k ≥ 30, d ≥ 14)	(44,30,14)	(44, k ≥ 14, d ≥ 30)	(44,14,30)
3	12	36	(44, k ≥ 36, d ≥ 8)	(44,36,8)	(44, k ≥ 8, d ≥ 36)	(44,8,36)

Таблица 4

$z^4 + xz^3 + xy^2z + xy^3 + x^2y^2 + x^4$, $g = 3$, $GF(16)$, $N = 34$

GF(16)						
deg X	deg(f)	α	(G) $(n, \geq \alpha - g + 1, \geq n - \alpha)$		(H) $(n, \geq n - \alpha + g - 1, \geq \alpha - 2g + 2)$	
			теория	тест	теория	тест
4	3	12	**(34, $k \geq 10$, $d \geq 22$)**	**(34,10,22)**	**(34, $k \geq 24$, $d \geq 8$)**	**(34,24,8)**
4	6	24	**(34, $k \geq 22$, $d \geq 10$)**	**(34,22,11)**	**(34, $k \geq 12$, $d \geq 20$)**	**(34,12,20)**

Проведенный анализ показал, что разработанный алгоритм дает коды с характеристиками, соответствующими теоретическим характеристикам алгебраико - геометрических кодов (1). Этим подтверждается достоверность полученных результатов.

ЛИТЕРАТУРА

1. Шафаревич И.Р. Основы алгебраической геометрии. – М.: Наука, 1972. – 320 с.
2. Гоппа В.Д. Коды на алгебраических кривых // Докл. АН СССР. – 1981. – Т.259, № 6. – С. 1289 - 1290.
3. Влэдуц С. Г., Манин Ю. И. Линейные коды и модулярные кривые // Современные проблемы математики. – М.: ВИНИТИ. – 1984. – Т. 25. – С. 209 - 257.
4. Johan P. Hansen; Codes on the Klein quartic, ideals, and decoding (Corresp). – IEEE Trans. Info. Theory. – November 1987. – Vol. IT - 33. – P. 923 – 925.
5. Халимов Г.З. Алгеброгеометрическое обобщение кодов // Управление и связь. – Харьков: НАНУ, ПАНИ, ХВУ. – 1997. – С 56 - 59.
6. C. Voss, Tom Hoholdt; An explicit construction of a sequence of codes attaining the Tsfasman-Vladut-Zink bound. The first steps. – IEEE Trans. Info. Theory. – , January 1997. – Vol. IT – 43. – P. 128 – 135.
7. Кузнецов А. А., Ушно С. В. Поиск неприводимых алгебраических кривых малой степени в конечных полях // Системи обробки інформації. – Харків: НАНУ, ПАНМ, ХВУ. – 2000. – Вип. 3(9). – С 147 - 150.

Поступила в редколлегию 5.03.2001