УДК 621.391

АЛГЕБРО-ГЕОМЕТРИЧЕСКИЕ КОДЫ НА ГРАНИЦЕ ГРАЙСМЕРА

С. В. Беззатеев
канд. техн. наук, доцент
М. В. Степанов
аспирант
Санкт-Петербургский государственный университет аэрокосмического приборостроения

В данной работе показывается существование класса алгебро-геометрических кодов, лежащих на границе Грайсмера. Этот класс выделяется среди алгебро-геометрических кодов рода один, которые иногда называют эллиптическими кодами.

The existence of class of algebro-geometrical codes laying on Graismer's border is shown in this paper. This class is distinguished among algebro-geometrical codes of genus one which are sometimes called elliptic codes.

Граница Грайсмера и ее связь с границей Синглтона

Рассмотрим $(n, k, d)_q$ коды, которые удовлетворяют верхним границам существования кодов, исправляющих ошибки [1], а именно границам Грайсмера и границам Синглтона. Покажем связь между этими границами.

Стандартный вид границы Грайсмера задается следующей формулой:

$$n=\sum_{i=0}^{k-1}\left\lceil\frac{d}{q^i}\right\rceil, \qquad (1)$$

где q – размер конечного поля F_q, над которым задан код. Округление до ближайшего целого, большего a. Коды, удовлетворяющие равенству (1), будем называть кодами Грайсмера. Граница Синглтона задана формулой

$$n=k+d-1. \qquad (2)$$

При $q > d$ равенство (1) эквивалентно (2), т. е. граница Синглтона частный случай границы Грайсмера. Известен только один класс линейных кодов, удовлетворяющих условию (2), – это коды МДР [1].

Необходимые сведения из алгебраической геометрии

Прежде всего, рассмотрим необходимые результаты алгебраической геометрии. К числу этих результатов отнесем границу, дающую верхнюю оценку количества точек на алгебраической кривой, а также теорему Римана–Роха, дающую оценку размерности пространства функций, заданных на некотором дивизоре.

Сначала дадим ряд определений. Для простоты изложения все определения, последующие ниже, будут справедливы только для гладких неприводимых плоских кривых.

Определение 1. Кривой назовем полиномиальную функцию $\aleph$.

Определение 2. Точкой на кривой назовем $P = (x, y)$, удовлетворяющую $\aleph(P)=0$, где $x,y\in F_q$.

Определение 3. Гладкая кривая – это кривая $\aleph$, у которой нет особых точек, т. е. не существует точки P: $\aleph(P)=\aleph_x(P)=\aleph_y(P)=0$.

Будем рассматривать только гладкие кривые.

Определение 4. Дивизор D – это формальная сумма точек кривой: $\sum_i \upsilon_i P_i$, $\upsilon_i \in Z$. Степень дивизора гладкой кривой $\deg(D) = \sum_i \upsilon_i$.

Рассмотрим поле рациональных алгебраических функций, в котором каждая функция может быть представлена в виде $f=\frac{g}{h}$, где g, h – полиномиальные функции, обращающиеся в ноль только в точках, лежащих на кривой. Множество таких функций будет полем функций, заданных на кривой [3].

Нулями рациональной функции назовем точки, в которых функция обращается в ноль, а *полюсами функции* – точки, в которых функция обращается в бесконечность.

Определение 5. Пространство функций, заданное на дивизоре $L(D)$, – это такое множество функций, в котором любая функция имеет полюс в тех же точках, что и дивизор D, и кратность конкретной точки меньше или равна коэффициенту υ_i. Количество нулей функции в каждой точке кривой должно быть больше или равно коэффициенту υ_i.

Определение 6 [3, следствие 2.2.8]. Род гладкой, неприводимой, плоской кривой g определяется величиной $g=\frac{(t-1)(t-2)}{2}$, где t – степень гладкой кривой $\aleph$.

Теорема 1 [3, 3.1.7]. Обозначим $N_q(g)$ максимальное количество точек на кривой. Тогда $N_q(g)\le q+1+g\lfloor 2\sqrt{q}\rfloor$.

Теорема 2 [3, теорема Римана–Роха]. Пусть $\aleph$ – гладкая кривая рода g, определенная над F_q, и пусть D – дивизор на кривой $\aleph$. Тогда $\dim L(D)\ge \deg(D)+1-g$.

Теорема Римана–Роха позволяет оценить базис векторов линейного пространства функций заданных на дивизоре кривой $\aleph$.

Теорема 3 [3, теорема 4.1.1]. Пусть $\aleph$ – кривая рода g, определенная над F_q. Пусть $P\subset\aleph(F_q)$ – подмножество n различных F_q – рациональных точек на $\aleph$ и пусть D – дивизор на $\aleph$: $0\le\deg(D)<n$ и $P\cap D=\varnothing$. Тогда алгебро-геометрический линейный код $C:=C(\aleph, P, D)$ длины n будет кодом с $k\ge\deg(D)+1-g$ и $d\ge n-\deg(D)$.

Следствие 1 [3, замечание 4.1.10]. Алгебро-геометрические $(n, k, d)_q$ коды удовлетворяют соотношению $k+d\ge n+1-g$.

Учитывая приведенный результат и оценку для верхней границы длины кода $N_q(q)$, можно сформулировать следующее следствие.

Следствие 2. Пусть $\aleph$ – гладкая проективная кривая рода g над F_q и пусть $k\ge 2$. Тогда расстояние линейного $(n, k, d)_q$ алгебро-геометрического кода удовлетворяет неравенству $d\le q-1+g\lfloor 2\sqrt{q}\rfloor$.

Доказательство. Из границы Синглтона получаем $n\ge k+d-1$. Согласно теореме 1, длина кода может быть оценена сверху как $n\le N_q(g)\Rightarrow n\le q+1+g\lfloor 2\sqrt{q}\rfloor$. Эту оценку можно уточнить, учитывая, что для построения кодов с $k\ge 2$ и $d < n$ необходимо, чтобы $\deg(D)\ne 0$ (теорема 3). Это означает, что длина кода будет, по крайней мере, на единицу меньше количества точек на кривой. Тогда $q+g\lfloor 2\sqrt{q}\rfloor\ge n\ge k+d-1$, откуда получим оценку $d\le q+1-k+g\lfloor 2\sqrt{q}\rfloor$ и, учитывая тот факт, что $k\ge 2$, получим $d\le q-1+g\lfloor 2\sqrt{q}\rfloor$.

Таким образом, все приведенные теоремы дают представление о параметрах линейного алгебро-геометрического $(n, k, d)_q$ кода.

Алгебро-геометрические коды, лежащие на границе Грайсмера

Для кодов с $k\ge 2$ рассмотрим случай с $d\ne 0 \bmod q$. Преобразуем равенство (1), применив формулу $\lceil a\rceil=\lfloor a\rfloor+1$:

$$n=\sum_{i=0}^{k-1}\left\lceil\frac{d}{q^i}\right\rceil=d+\sum_{i=1}^{k-1}\left\lceil\frac{d}{q^i}\right\rceil=d+k-1+\sum_{i=1}^{k-1}\left\lfloor\frac{d}{q^i}\right\rfloor,$$

следовательно,

$$n=d+k-1+\sum_{i=1}^{k-1}\left\lfloor\frac{d}{q^i}\right\rfloor. \qquad (3)$$

Лемма 1. Если g удовлетворяет соотношению $g\le\sum_{i=1}^{k-1}\left\lfloor\frac{d}{q^i}\right\rfloor$, то код лежит на границе Грайсмера.

Доказательство. Покажем, в каком случае алгебро-геометрический код будет иметь длину не более длины, определенной границей Грайсмера.

Длина кода, лежащего на границе Грайсмера, должна удовлетворять соотношению

$$n=d+k-1+\sum_{i=1}^{k-1}\left\lfloor\frac{d}{q^i}\right\rfloor. \qquad (4)$$

С другой стороны, длина алгебро-геометрического кода ограничена неравенством

$$n\le k+d-1+g, \qquad (5)$$

как следует из следствия 1.

Тогда условие, при котором правая часть неравенства (5) оказывается меньше правой части равенства (4), можно записать следующим образом:

$$k+d-1+g\le d+k-1+\sum_{i=1}^{k-1}\left\lfloor\frac{d}{q^i}\right\rfloor,$$

или

$$g\le\sum_{i=1}^{k-1}\left\lfloor\frac{d}{q^i}\right\rfloor, \qquad (6)$$

что и требовалось доказать.

Теорема 4. Любой алгебро-геометрический код с $d > q$ и $g = 1$ лежит на границе Грайсмера.

Доказательство. Воспользуемся результатом леммы 1 и докажем, что это условие выполняется. Перепишем неравенство (6) при $g = 1$. Тогда

$$1\le\sum_{i=1}^{k-1}\left\lfloor\frac{d}{q^i}\right\rfloor, \qquad (7)$$

но $q<d<q+\lfloor 2\sqrt{q}\rfloor-1<2q$ при $q\ge 2$, а следовательно, правая часть неравенства (7) превращается в единицу, что означает выполнение условия леммы.

Следствие 3. Параметры любого алгебро-геометрического кода с $d > q$ и $g = 1$ будут удовлетворять соотношению $n=k+d$.

Доказательство очевидно.

Пример. Построим поле F_{16} при помощи примитивного полинома $a^4 = a + 1$. Выберем кривую, например, $y^2 + xy = x^3 + \alpha^4 x + \alpha$. Тогда $g = 1$ согласно определению 6. Найдем точки на этой кривой, лежащие в поле F_{16}.

(1,0)	(a,a^3)	(a^14,a^9)
(a^6,0)	(a^10,a^4)	(a^4,a^11)
(a^13,0)	(a^11,a^4)	(a^5,a^12)
(1,1)	(a^14,a^4)	(a^4,a^13)
(a^7,1)	(a^6,a^6)	(a^11,a^13)
(a^9,1)	(a^9,a^7)	(a^13,a^13)
(0,a^2)	(a,a^9)	(a^5,a^14)
(a^10,a^2)	(a^7,a^9)	

Построим код с $k = 3$ и $n = 22$. Тогда, согласно доказанной теореме 4 и следствию 3, данный код имеет $d = 19$ и будет лежать на границе Грайсмера. Построим код (22, 3, 19) над F_{16}, используя базис $\{1, x, y\}$. Порождающая матрица такого кода

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & a^{10} & a^4 & 1 & a^6 & a^{13} & a & a^7 & a^{14} & a^4 & a^{11} & a^{13} & a^{10} & a^{11} & a^{14} & a^6 & 1 & a^7 & a^9 & a & a^5 & a^9 \\ a & a & a^3 & a^5 & a^5 & a^5 & a^6 & a^6 & a^6 & a^7 & a^7 & a^7 & a^8 & a^8 & a^8 & a^9 & a^{10} & a^{10} & a^{10} & a^{11} & a^{12} & a^{13} \end{bmatrix}.$$

Заключение

В данной работе доказано существование алгебро-геометрических кодов рода 1, лежащих на границе Грайсмера. Поскольку основными фактами при доказательстве утверждений стали теорема 3 и теорема 1, то полученные результаты справедливы для кодов, которые построены на произвольных кривых.

Литература

1. **Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А.** Теория кодов, исправляющих ошибки. – М.: Связь, 1979.
2. **Stichtenoth H.** Algebraic function fields and codes. – Berlin: Springer-Verlag, 1993.
3. **Влэдуц С. Г., Ногин Д. Ю., Цфасман М. А.** Алгебро-геометрические коды. Основные понятия. – М.: МЦНМО, 2003.
4. **Виноградов И. М.** Основы теории чисел. – М.: Наука, 1972.