УДК 621.391.26

АЛГЕБРО-ГЕОМЕТРИЧЕСКИЕ КОДЫ ПРОЕКТИВНЫХ И АФФИННЫХ ПРОСТРАНСТВ

В.В. ПАНЬКОВА, С.Б. САЛОМАТИН

Белорусский государственный университет информатики и радиоэлектроники
П. Бровки, 6, Минск, 220013, Беларусь

Поступила в редакцию 20 апреля 2016

Рассмотрены методы построения алгебро-геометрических кодов над конечными полями с нахождением всех аффинных точек и точек в бесконечности, которые определяются в результате применения стремящегося к нулю неприводимого сглаживания аффинной кривой. Проведен сравнительный анализ параметров алгебро-геометрических кодов различного вида.

Ключевые слова: алгебро-геометрический код, проективные и аффинные кривые.

Введение

Конструкция алгебро-геометрических (АГ) кодов требует множества точек, которые удовлетворяют неприводимым аффинным кривым и множеству рациональных функций на этих кривых. Проективное пространство является $(n+1)$-мерным, элементы в этом пространстве определяются над некоторым конечным полем. Такие элементы называются проективными точками и определяются как [1] $(c_1, c_2, c_3, ..., c_n, c_{n+1})$, где c_i, $i = 0,1, ..., n, n+1$ – элементы конечного поля.

Аффинное пространство является *n*-мерным, а элементы, определяемые в пространстве над некоторым конечным полем, называются аффинными точками и записываются в виде $(c_1, c_2, ..., c_n, 1)$.

Если точки задаются в форме $(c_1, c_2, ..., c_n, 0)$, то пространство называется гиперплоскостью в бесконечности [1-4]. Все точки, расположенные в гиперплоскости в бесконечности, называются точками в бесконечности. Для конструкции АГ-кодов представляет интерес нахождение всех аффинных точек и точек в бесконечности, которые определяются в результате применения стремящегося к нулю неприводимого сглаживания аффинной кривой.

Проективные и аффинные кривые

Проективная кривая является $(n+1)$-мерной кривой, определенной проективными точками, что позволяет получать *n*-мерные аффинные кривые в $(n+1)$ различных координатных системах.

Для 3-мерной проективной кривой $C(x, y, z)$ существуют три аффинные кривые $C(x, y, 1)$, $C(x, 1, z)$ и $C(1, y, z)$.

Алгебро-геометрические коды используют кривые, полученные путем неприводимого аффинного сглаживания. Например, кривая $C(x, y) = x^2 + y^2$ не является неприводимой над полем $GF(2)$, поскольку

$(x+y)(x+y) = (x^2 + xy + xy + y^2) = | xy + xy = 0 | = x^2 + y^2$.

С другой стороны кривая $C(x, y) = x^3 + y^3$ неприводима над $GF(2)$, но не является таковой над полем $GF(3)$, поскольку

$$(x+y)(x+y)(x+y) = (x^2 + 2xy + y^2)(x+y) = x^3 + x^2y + 2x^2y + 2xy^2 + xy^2 + y^3 =$$
$$= x^3 + 3x^2y + 3xy^2 + y^3 \equiv x^3 + y^3 \mod 3.$$

Точка на кривой называется несингулярной, если все частные производные кривой не сходятся к этой точке. Если все точки кривой являются несингулярными, то кривая носит название несингулярной или сглаженной [1, 2]. Важным является класс кривых Эрмита, определенных над квадратичным конечным полем $GF(w^2)$. Проективная кривая Эрмита определяется как

$$C(x, y, z) = x^{w+1} + y^w z + yz^w. \quad (1)$$

Кривая Эрмита является сглаженной. Действительно, три производные имеют вид

$$\frac{\partial C(x, y, z)}{\partial x} = (w+1)x^w = x^w, \quad \frac{\partial C(x, y, z)}{\partial y} = wy^{w-1}z + z^w = z^w,$$

$$\frac{\partial C(x, y, z)}{\partial z} = y^w + wyz^{w-1} = y^w.$$

Признаком сингулярности служат точки, имеющие производные, стремящиеся к (0, 0, 0). Но в рассматриваемом случае такие точки в проективном пространстве отсутствуют, следовательно, точки являются несингулярными, а кривая – сглаженной.

Нахождение точек на аффинной кривой

Проективные точки, которые удовлетворяют условию для проективной кривой $C(x, y, z) = 0$, представляются в виде формы (α, β, δ), где α, β, δ являются элементами конечного поля. Для построения АГ-кода используются только аффинные точки вида $(\alpha, \beta, 1)$, $z = 1$, а точки в бесконечности определяются формой $(\alpha, \beta, 0)$, $z = 0$. Для нахождения всех аффинных точек проективная кривая отображается в кривые аффинных компонент. Для каждой аффинной кривой находят точки $(\alpha, \beta, 1)$ и $(\alpha, \beta, 0)$.

Аффинная форма кривой Эрмита (1) в системе координат вида $(x - y)$ с $z = 1$, имеет вид

$$C(x, y, z) = x^{w+1} + y^w + y. \quad (2)$$

В $(x - z)$ системе координат, $y = 1$, кривая определяется как

$$C(x, 1, z) = x^{w+1} + z + z^w.$$

В $(y - z)$ системе координат, $x = 1$, имеем

$$C(1, y, z) = 1 + y^w z + yz^w.$$

Как известно, кривая Эрмита имеет $w^3 + 1$ точек. Для поля $GF(9)$ получаем $2^3 + 1 = 8 + 1 = 9$ точек и кривые вида:

$$C(x, y, z) = x^3 + y^2 z + yz^2.$$

Аффинная кривая в $(x - y)$ системе имеет вид $C(x, y) = x^3 + y^2 + y$.

Аффинные точки, удовлетворяющие условию $C(x, y, 1) = 0$, находятся подстановкой в последнее выражение всех возможных значений переменных x и y при $(z = 1)$ в поле $GF(2^2)$, где $\alpha^2 = \alpha + 1$. В результате получаем:

$C(0,0,1) = 0^3 + 0^2 + 0 = 0,\ \ C(0,1,1) = 0^3 + 1^2 + 1 = 0,$

$C(0,\alpha,1) = 0^3 + \alpha^2 + \alpha = \alpha(1+\alpha) = \alpha^3 = 1 \neq 0,$

$C(0,\alpha^2,1) = 0^3 + \alpha^4 + \alpha^2 = \alpha^2(1+\alpha^2) = \alpha^2\alpha = 1 \neq 0,$

$C(1,0,1) = 1^3 + 0^2 + 0 = 1 \neq 0,\ \ C(1,1,1) = 1^3 + 1^2 + 1 = 1 \neq 0,$

$C(1,\alpha,1) = 1^3 + \alpha^2 + \alpha = 1 + 1 = 0,$

$C(1,\alpha^2,1) = 1^3 + \alpha^4 + \alpha^2 = 1 + \alpha + \alpha^2 = 1 + 1 = 0,$

$C(\alpha,0,1) = \alpha^3 + 0^2 + 0 = \alpha^3 = 1 \neq 0,\ \ C(\alpha,1,1) = \alpha^3 + 1^2 + 1 = \alpha^3 = 1 \neq 0,$

$C(\alpha,\alpha,1) = \alpha^3 + \alpha^2 + \alpha = 1 + 1 = 0,$

$C(\alpha,\alpha^2,1) = \alpha^3 + \alpha^4 + \alpha^2 = \alpha^2(1 + \alpha + \alpha^2) = 0,$

$C(\alpha^2,0,1) = \alpha^6 + 0^2 + 0 = 1 \neq 0,\ \ C(\alpha^2,1,1) = \alpha^6 + 1^2 + 1 = 1 \neq 0,$

$C(\alpha^2,\alpha,1) = \alpha^6 + \alpha^2 + \alpha = \alpha^6 + 1 = 1 + 1 = 0,$

$C(\alpha^2,\alpha^2,1) = \alpha^6 + \alpha^4 + \alpha^2 = \alpha^6 + \alpha + \alpha^2 = 1 + 1 = 0.$

Аффинные точки, удовлетворяющие условию $C(x, y, 1) = 0$, приведены в табл. 1.

Таблица 1. **Восемь проективных точек кривой Эрмита в $(x - y)$ системе**

$P_1 = (0,0,1)$	$P_2 = (0,1,1)$	$P_3 = (1,\alpha,1)$	$P_4 = (1,\alpha^2,1)$
$P_5 = (\alpha,\alpha,1)$	$P_6 = (\alpha,\alpha^2,1)$	$P_7 = (\alpha^2,\alpha,1)$	$P_8 = (\alpha^2,\alpha^2,1)$

Аналогичным образом можно найти точки для двух других кривых

$C(x,1,z) = x^3 + z + z^2$ и $C(1,y,z) = 1 + y^2 z + yz^2$.

Восемь проективных точек, удовлетворяющих условию $C(x,1,z) = 0$, приведены в табл. 2. Точка P_2 является аффинной, она имеет форму $(x, y, 1)$ и также присутствует в табл. 2. Совпадают точка в бесконечности и точка $P_1 = (0,1,0)$.

Таблица 2. **Восемь проективных точек кривой Эрмита в $(x - z)$ системе**

$P_1 = (0,1,0)$	$P_2 = (0,1,1)$	$P_3 = (1,1,\alpha)$	$P_4 = (1,1,\alpha^2)$
$P_5 = (1,\alpha,1)$	$P_6 = (1,\alpha,\alpha^2)$	$P_7 = (1,\alpha^2,1)$	$P_8 = (1,\alpha^2,\alpha)$

Четыре проективные точки, удовлетворяющие условию $C(1,y,z) = 0$, приведены в табл. 3. В этом случае только точки P_1 и P_3 являются аффинными, так как они имеют форму $(x, y, 1)$ и также присутствуют в табл. 1.

Таблица 3. **Четыре проективные точки кривой Эрмита в $(y - z)$ системе**

$P_1 = (1,\alpha,1)$	$P_2 = (0,\alpha,\alpha^2)$	$P_3 = (1,\alpha^2,1)$	$P_4 = (1,\alpha^2,\alpha)$

Следовательно, проективная кривая Эрмита имеет восемь аффинных точек и одну точку в бесконечности $Q = (0,1,0)$.

Коды, получаемые с помощью кривых с одной точкой в бесконечности, называются АГ-кодами с одной точкой или кодами Гоппы [3]. Примерами кривых с одной точкой в бесконечности служат эллиптические и гиперэллиптические кривые.

Граничные соотношения

Верхняя граница, определяющая количество точек *N*, включая точку в бесконечности для кривых над полем $GF(q)$, носит название границы Хассе-Вейля и определяется как [1]:

$$| N | \le (m-1)(m-2)\sqrt{q} + 1 + q,$$

где *m* степень кривой.

Например, для рассмотренного выше примера кривой Эрмита степени $m = 3$ и $q = 4$, верхняя граница равна $| N | \le (3-1)(3-2)\sqrt{4} + 1 + 4$, $| N | \le 9$.

Максимальное количество точек кривой степени $m = 3$, определенной над $GF(2^2)$, равно 9. Для кривой Эрмита из примера было получено восемь аффинных точек и одна точка в бесконечности, что в сумме дает девять точек. Таким образом, кривая Эрмита лежит на границе Хассе-Вейля и является *максимальной* кривой. Такие кривые позволяют строить длинные коды.

Другой тип максимальных кривых дают эллиптические кривые над конечными полями. Например, эллиптическая кривая [2, 4]

$$C(x, y) = x^3 + x^2 + x + y^2 + y + 1$$

является максимальной кривой над полем $GF(2^4)$. Степень кривой $m = 3$, число ее точек – 25.

Кривая Эрмита над полем $GF(2^4)$ вида $C(x, y) = x^5 + y^4 + y$ имеет степень $m = 5$ и определяет 65 точек.

Коды, построенные над эллиптическими кривыми значительно короче, чем коды, построенные с помощью кривых Эрмита. Но коды, построенные по эллиптическим кривым, являются более длинными по сравнению с кодами Рида-Соломона, конструкция которых определяется аффинной линией $y = 0$ и имеет степень $m = 1$. Для конечного поля $GF(q)$ граница Хассе-Вейля упрощается и имеет вид $| N | \le q + 1$. Так, для $GF(2^4)$ наиболее длинный код Рида-Соломона имеет 16+1=17 точек, что меньше, чем у кода, построенного по эллиптической кривой.

Рациональные функции на кривых

Конструкции порождающих матриц АГ-кодов основываются на рациональных функциях соответствующих кривых. Каждая рациональная функция оценивается в каждой из *n* аффинных точек, формируя строку порождающей матрицы, где *n* – длина кода. Рациональную функцию $f(x, y, z)$ можно рассматривать как частное от деления двух функций $g(x, y, z)$ и $h(x, y, z)$, имеющих одинаковые степени $f(x, y, z) = \dfrac{g(x, y, z)}{h(x, y, z)}$. Разные формы представления функции позволяют более полно понять поведение кривых.

Например, функция $f(x, y) = \dfrac{x}{y+1}$, определенная над кубической кривой $C(x, y) = x^3 + y^3 + 1 = 0$ и полем $GF(2^2)$, может быть записана в виде

$$x^3 = y^3 + 1,\ x = \frac{y^3 + 1}{x^2} = \frac{(y+1)((y^2 + y + 1)}{x^2},\ \frac{x}{y+1} = \frac{y^2 + y + 1}{x^2}.$$

Кубическая кривая имеет 6 точек: $P_1 = (0,1)$, $P_2 = (0,\alpha)$, $P_3 = (0,\alpha^2)$, $P_4 = (1,0)$, $P_5 = (\alpha,0)$, $P_6 = (\alpha^2,0)$. В этом случае функция $f(x,y) = \dfrac{x}{y+1}$ определена для всех точек на кубической кривой, за исключением точки $P_1 = (0,1)$, так как $f(0,1) = \dfrac{0}{1+1} = \dfrac{0}{0}$.

Если функция не определяется на кривой, то она имеет в исследуемой точке ноль порядка 1 и полюс порядка 1.

Функция $f(x,y) = \dfrac{y^2 + y + 1}{x^2}$ в точке $(0,1)$ дает результат $f(0,1) = \dfrac{1^2 + 1 + 1}{0^2} = \dfrac{1}{0}$, не имеет нулей, но имеет полюс порядка 2.

Порядок функции обозначается как $v(f(x,y,z))$ и определяется путем суммирования порядков нулей и полюсов. Конструкция АГ-кодов на основе рациональных функций должна иметь полюс в точке бесконечности, но не должна иметь полюсов в любых других аффинных точках.

Последовательность рациональных функций на проективной линии имеет полюс только в точке бесконечности. Поэтому существует q аффинных точек и одна точка в бесконечности. Последовательность рациональных функций, имеющих полюс в точке бесконечности $Q = (1,0,0)$, может быть определена следующим образом. Последовательность рациональных функций вида $\left\{\dfrac{x^i}{y^i}\right\}$, $i > 0$ имеет полюс порядка i в Q, но не имеет полюсов в других аффинных точках. Рассматриваемый случай показывает, что число точек на проективной линии не может превышать кардинальность поля линии.

Коды, конструируемые из линии $y = 0$, известны как коды Рида-Соломона и представляют собой простейший вид алгебро-геометрических кодов. Малое количество точек на проективной линии показывает, почему коды Рида-Соломона имеют короткие длины, не превышающие размеры конечных полей.

Рациональные функции на кривой Эрмита

Последовательность рациональных функций на проективной кривой Эрмита может быть сформирована для элементов $\dfrac{x}{z}$ и $\dfrac{y}{z}$. Элемент $\dfrac{x}{z}$ можно переписать в виде выражений

$$x^{w+1} = y^w z + y z^w,\ \frac{x}{z} = \frac{y^w + y z^{w-1}}{x^w},$$

которые имеют порядок w в точке бесконечности $Q = (0,1,0)$.

Аналогично, для элемента $\dfrac{y}{z}$ можно записать

$$x^{w+1} = y^w z + y z^w,\ \frac{y^w z + y z^w}{x^{w+1}} = 1,\ \frac{1}{z} = \frac{y^w + y z^{w-1}}{x^{w+1}},\ \frac{y}{z} = \frac{y^{w+1} + y^2 z^{w-1}}{x^{w+1}}.$$

Элемент имеет порядок $w+1$ в точке бесконечности $Q = (0,1,0)$. Поэтому кривая Эрмита над полем $GF(2^2)$ имеет $r = 2$, $v\left(\dfrac{x}{z}\right) = 2$, $v\left(\dfrac{y}{z}\right) = 3$.

Другие рациональные функции на кривой формируются путем комбинации произведения различных степеней $\dfrac{x}{z}$ и $\dfrac{y}{z}$, и сложения их порядков. Например, произведение $\dfrac{x}{z} \cdot \dfrac{x}{z} = \dfrac{x^2}{z^2}$ име-

ет порядок равный $2+2=4$. Произведение $\frac{x}{z}\cdot\frac{y}{z}=\frac{xy}{z^2}$ имеет порядок $2+3=5$, а произведение $\frac{y}{z}\cdot\frac{y}{z}=\frac{y^2}{z^2}$ имеет порядок $3+3=6$. В общем случае порядок рациональной функции $\frac{x^i y^j}{z^{i+j}}$ на кривой Эрмита определяется выражением

$$v(\frac{x^i y^j}{z^{i+j}}) = iw + j(w+1).$$

Такая последовательность рациональных функций обозначается как $L(G)$, где G является дивизором кривой. Дивизор кривой определяется как целое значение каждой точки кривой. АГ-код имеет два дивизора D и G. Дивизор D определяется значением $D(P)=1$ для каждой аффинной точки и вычисляется через сумму всех аффинных точек

$$D=\sum_{i=1}^{n} D(P_i)P_i=\sum_{i=1}^{n} P_i.$$

Сумма $\sum_{i=1}^{n} D(P_i)$ называется степенью дивизора D, $d(D)$.

Аналогично дивизор G определяется как целое значение $G(Q)$ для каждой точки в бесконечности Q и вычисляется как сумма всех точек в бесконечности. Для кривых с одной точкой в бесконечности, дивизор G оценивается через произведение точки в бесконечности и степени G, $d(G)$:

$$G=\sum_{i} G(Q_i)Q_i = d(G)Q.$$

Пространство $L(G)$ содержит рациональные функции порядка $d(G)$. Для примера, рассмотренного выше, имеем, если $G=7Q$ и $d(G)=7$, тогда

$$L(7Q)=\left\{1,\frac{x}{z},\frac{y}{z},\frac{x^2}{z^2},\frac{xy}{z^2},\frac{y^2}{z^2},\frac{x^3}{z^3},\frac{x^2y}{z^3}\right\}.$$

Заметим, что порядки $\frac{x^3}{z^3}$ и $\frac{y^2}{z^2}$ совпадают и равны 6. В этом случае все функции, степени x в которых больше или равны 3, могут быть исключены из рассмотрения. Также можно исключить функции со степенями y большими 1. Поэтому, можно говорить только о семи функциях в $L(G)$:

$$L(7Q)=\left\{1,\frac{x}{z},\frac{y}{z},\frac{x^2}{z^2},\frac{xy}{z^2},\frac{y^2}{z^2},\frac{x^2y}{z^3}\right\}.$$

Теорема Римана-Роха используется для вычисления количества рациональных функций в $L(G)$ с учетом порядков и следовательно определяет размерность и минимальное расстояние кода. Число рациональных функций в $L(G)$ называется размерностью G, $l(G)$. Теорема утверждает, что существуют неотрицательные числа γ, для которых $l(G)-d(G)=1-\gamma$, при условии, что $d(G)>2\gamma-2$. Неотрицательное число γ называется *родом кривой* и определяется как

$$\gamma=\frac{(m-1)(m-2)}{2},$$

где m – степень кривой.

Род кривой играет важную роль в оценке размерности параметров кода.

Пример. Число рациональных функций кривой Эрмита нулевого порядка меньше или равно 21 с точкой в бесконечности $Q = (0,1,0)$. Действительно, рациональные функции $\frac{x}{z}$ и $\frac{y}{z}$ имеют порядки соответственно $w = 4$ и $w + 1 = 5$.

Поэтому последовательность функций имеет вид

$$L(21Q) = \left\{1, \frac{x}{z}, \frac{y}{z}, \frac{x^2}{z^2}, \frac{xy}{z^2}, \frac{y^2}{z^2}, \frac{x^3}{z^3}, \frac{x^2y}{z^3}, \frac{xy^2}{z^3}, \frac{y^3}{z^3}, \frac{x^4}{z^4}, \frac{x^3y}{z^4}, \frac{x^2y^2}{z^4}, \frac{xy^3}{z^4}, \frac{y^4}{z^4}, \frac{x^4y}{z^5}\right\}.$$

Все функции, содержащие степени x, большие, чем 4, должны быть исключены из рассмотрения как функции, порядки которых дублируют существующие порядки. Так, в последовательности отсутствует функция $\frac{x^5}{z^5}$, порядок которой такой же как порядок $v\left(\frac{x^4}{z^4}\right)$. Множество порядков полученных функций имеет вид

$$\{1,\ 4,\ 5,\ 8,\ 9,\ 10,\ 12,\ 13,\ 14,\ 15,\ 16,\ 17,\ 18,\ 19,\ 20,\ 21\}.$$

Соответственно получаем 16 функций в $L(G)$. Такое множество порядков известно, как множество *непустых* порядков. Порядки 0, 2, 3, 6, 7 и 11 отсутствуют в полученном множестве. Такие порядки называют *пустыми*. Число пустых порядков равно γ.

Степень кривой Эрмита равна $m = 5$, род кривой равен $\gamma = 6$ и $d(G) = 21$. Далее, из того факта, что $2\gamma - 2 = 10$ меньше, чем $d(G)$, следует возможность применения теоремы Римана-Роха $l(G) = d(G) + 1 - \gamma = 21 + 1 - 6 = 16$, что совпадает с числом функций в $L(G)$.

Заключение

Рассмотрены методы построения алгебро-геометрических кодовых структур с использованием проективных и аффинных пространств. Сравнительный анализ показывает, что наибольшим разнообразием обладают коды, поостренные на основе кривых Эрмита.

ALGEBRAIC GEOMETRICAL CODES OVER PROJECTIVE AND AFFINE SPACE

V.V. PANKOVA, S.B. SALOMATIN

Abstract

Methods of constructing of algebraic-geometric codes over finite fields with finding of all affine points and points at infinity, which are defined by the application of irreducible smoothing of an affine curve, which aspires to zero, are considered. The comparative analysis of the parameters of algebraic-geometric codes of various type is carried out.

Keywords: algebraic-geometric code, affine and projective curves.

Список литературы

1. *Carrasco R.A., Martin J.* Non-binary error control coding for wireless communication and data storage. John Wiley & Sons, Ltd. 2008.
2. *Lin S., Costello D.J.* Error Control Coding. New Jersey, 2004.
3. *Влэдуц С.Г., Ногин Д.Ю., Цфасман М.А.* Алгебро-геометрические коды. Основные понятия. М., 2003.
4. *Chaoping Xing, San Ling* // IEEE Transactions on Information Theory. 2000. Vol 46(4). P. 1527-1532.