С. А. Степанов, М. Х. Шалалфех, Коды на расслоенных произведениях кривых Артина–Шрейера, *Дискрет. матем.*, 2001, том 13, выпуск 2, 3–13

DOI: 10.4213/dm287

Дискретная математика

том 13 выпуск 2 * 2001

УДК 519.4

Коды на расслоенных произведениях кривых Артина–Шрейера

© 2001 г. С. А. Степанов, М. Х. Шалалфех

В статье с использованием расслоенного произведения кривых Артина–Шрейера построено новое семейство гладких проективных кривых над конечным полем F_q с большим числом F_q-рациональных точек. Показано, что для любой кривой X из этого семейства отношение $g(X)/N_q(X)$, где $g(X)$ — род и $N_q(X)$ — число F_q-рациональных точек, достаточно мало, чтобы получить геометрические коды Гоппы с хорошими параметрами. В статье обобщаются результаты С. А. Степанова и Ф. Озбудака о построении кодов большой длины.

1. Введение

Пусть p — простое число и F_q — конечное поле с $q = p^\nu$ элементами, ν — натуральное число. Линейный $[n, k, d]_q$-код C — это подпространство пространства F_q^n, где n — длина кода C, $k = \dim_{F_q} C$ — размерность C и d — кодовое расстояние, минимальное расстояние Хемминга между ненулевыми элементами C. Каждый линейный $[n, k, d]$-код C определяет пару относительных параметров (δ, R), где $\delta = d/n$ — относительное минимальное расстояние и $R = k/n$ — скорость передачи кода C.

Используя конструкцию Гоппы линейных кодов, связанную с гладкими проективными кривыми над конечными полями, можно доказать существование линейных кодов большой длины. Хотя геометрические коды Гоппы, связанные с максимальными кривыми, обладают хорошими относительными параметрами, длина этих кодов ограничена величиной $1+q^3$. Эта оценка является прямым следствием оценки Хассе–Вейля и того факта, что род максимальной кривой X удовлетворяет неравенству $g(X) \leqslant q(q-1)/2$ (см. [10]).

В статье [7] С. А. Степанов построил геометрические коды Гоппы большой длины с использованием расслоенного произведения гиперэллиптических кривых над конечным полем F_q, для которого $q = p^\nu$ и ν — четное число. В [8] С. А. Степановым и Ф. Озбудаком этот результат обобщен на случай, когда ν нечетно. В [4] Ф. Озбудак с использованием расслоенного произведения покрытий Куммера построил коды, длина которых больше длин кодов, построенных в [7] и [8]. В настоящей статье с использованием расслоенных произведений кривых Артина–Шрейера строятся геометрические коды Гоппы, длина которых значительно длиннее кодов из статей [6], [7], [8] и [4].

Далее $F_q[x]$ обозначает пространство рациональных функций проективной прямой P^1. Элемент $f(x) \in F_q[x]$ называется вырожденным если существует такой элемент $g(x) \in F_q[x]$, что $f = g^p - g + a$, где $a \in F_q$. В противном случае элемент f называется невырожденным.

Если C — код над F_q и $\mathrm{Tr}_\nu \colon F_q \to F_p$ обозначает функцию след из F_q в F_p, то

$$\mathrm{Tr}(C) = \{\mathrm{Tr}_\nu(c) \mid c \in C\}$$

— код над F_p, называемый след-кодом кода C.

Соотношение $\mathrm{Tr}_\nu(\alpha) = 0$, выполняемое тогда и только тогда, когда существует такое $\beta \in F_q$, что $\beta^p - \beta = \alpha$, связывает след-коды с кривыми Артина–Шрейера X_f с определяющим уравнением

$$y^p - y = f(x) \in F_q(x). \tag{1}$$

Кривая (1) абсолютно неприводима тогда и только тогда, когда кривая $f(x)$ невырождена (см. [3]). Известно, что если $f(x) \in F_q[x]$, $\deg f(x) = m$ и $(m, p) = 1$, то $f(x)$ невырождена (см. [5]).

Обозначим $N_q(X_f)$ число F_q-рациональных точек гладкой проективной модели кривой (1), это число равно

$$N_q(X_f) = pN + 1,$$

где $N = |\{x \in F_q \colon \mathrm{Tr}_\nu f(x) = 0\}|$.

Пусть A — F_q-линейное подпространство пространства $F_q[x]$, A называется невырожденным, если каждая функция $f(x) \in A$ невырождена. Если рассматривать A как векторное пространство над F_p, то ясно, что существует базис $\{f_1(x), \ldots, f_s(x)\}$ пространства A над F_p и

$$A = F_p f_1(x) + \ldots + F_p f_s(x).$$

Такой базис будем называть каноническим, если полиномы любого подмножества этого базиса, состоящего из полиномов одинаковых степеней, имеют F_p-линейно независимые коэффициенты при старшем члене. В таком случае система уравнений над $\bar{F}_q$

$$\begin{aligned} y_1^p - y_1 &= f_1(x), \\ y_2^p - y_2 &= f_2(x), \\ &\ldots \\ y_s^p - y_s &= f_s(x) \end{aligned} \tag{2}$$

определяет неприводимую кривую в $(s+1)$-мерном проективном пространстве P^{s+1} (см. [3]).

В [9] рассмвтривались расслоенные произведения

$$y_i^p - y_i = a_i x^{\sqrt{q}+1},$$

где $a_i \in F_q^*$ удовлетворяют равенству $a_i^{\sqrt{q}} + a_i = 0$, если $q = p^\nu$ и ν четно, и

$$y_i^p - y_i = a_i x^{p^{(\nu+1)/2}+1} - a_i^{(\nu-1)/2} x^{p^{(\nu-1)/2}+1},$$

где $a_i \in F_q^*$, если $q = p^\nu$ и ν нечетно.

В результате в [9] были получены гладкие проективные кривые X_r такие, что

$$g(X_r) = \begin{cases} (p^r - 1)\sqrt{q}/2, & 1 \leqslant r \leqslant \nu/2,\ \nu \text{ четно}, \\ (p^r - 1)\sqrt{pq}/2, & 1 \leqslant r \leqslant \nu,\ \nu \text{ нечетно}, \end{cases}$$

и число F_q-рациональных точек кривой X_r равно

$$N_q(X_r) = \begin{cases} p^r q + 1, & 1 \leqslant r \leqslant \nu/2,\ \nu \text{ четно}, \\ p^r q + 1, & 1 \leqslant r \leqslant \nu,\ \nu \text{ нечетно}. \end{cases}$$

Замечание 1. Для четного ν кривая X_r является максимальной кривой при любом r, $1 \leqslant r \leqslant \nu/2$.

В этой статье мы строим семейство невырожденных полиномов $f_i(x) \in F_q[x]$, образующих канонический базис линейного подпространства пространства $F_q[x]$, и к этому семейству полиномов применяем расслоенное произведение (2) для получения гладких проективных кривых над конечным полем, имеющих большое число рациональных точек и малое отношение $g(X)/N_q(X)$. Получены следующие результаты.

Теорема 1. *Пусть $q = p^\nu$ и F_{q^2} — конечное поле с q^2 элементами. Тогда для любого целого s, $1 \leqslant s < q$, $(s,p) = 1$, существует гладкая проективная кривая X_s, для которой род $g(X_s)$ и число F_{q^2}-рациональных точек $N_q(X_s)$ удовлетворяют соотношениям*

$$g(X_s) \leqslant \tfrac{1}{2}(q^{N_1(s)} - 1)(s(q+1) - 1), \qquad N_q(X_s) = q^{N_1(s)+2} + 1,$$

где $N_1(s) = s - [s/p] + 2[\log_p((s(q+1) - 1)/q)]$.

Теорема 2. *Пусть $q = p^{2\nu+1}$ и F_q — конечное поле с q элементами. Тогда для любого целого s, $1 \leqslant s < p^{\nu-1}$, $(s,p) = 1$, существует гладкая проективная кривая X_s, для которой род $g(X_s)$ и число F_q-рациональных точек удовлетворяют соотношениям*

$$g(X_s) < \tfrac{1}{2}(p^{N_2(s)} - 1)(s(p^{\nu+1} + 1) - 1), \qquad N_q(X_s) = qp^{N_2(s)} + 1,$$

где $N_2(s) = (2\nu + 1)(s - [s/p])$.

Применяя конструкцию Гоппы к семейству кривых, описанных в этих теоремах, получаем следующие результаты.

Следствие 1. *Пусть F_{q^2}, s, $N_1(s)$ — такие, как в теореме 1. Тогда для любого*

$$l > \tfrac{1}{2}(q^{N_1(s)} - 1)(s(q+1) - 1)$$

существует геометрический $[n,k,d]_{q^2}$-код Гоппы $C(D_0, D)$ с параметрами

$$\begin{aligned} & l < n \leqslant q^{N_1(s)+2}, \\ & k \geqslant l - \tfrac{1}{2}(q^{N_1(s)} - 1)(s(q+1) - 1) + 1, \\ & d \geqslant n - l. \end{aligned}$$

Следствие 2. *Пусть F_q, s, $N_2(s)$ — такие, как в теореме 2. Тогда для любого*

$$l > \tfrac{1}{2}(p^{N_2(s)} - 1)(s(p^{\nu+1} + 1) - 1)$$

существует геометрический $[n, k, d]_q$-код Гоппы $C(D_0, D)$ с параметрами

$$\begin{aligned} &l < n \leqslant qp^{N_2(s)}, \\ &k \geqslant l - \tfrac{1}{2}(p^{N_2(s)} - 1)(s(p^{\nu+1} + 1) - 1) + 1, \\ &d \geqslant n - l. \end{aligned}$$

Замечание 2. Самый длинный код из следствия 1 имеет длину $p^{2\nu}p^{\nu((p-1)p^{\nu-1}+\nu)}$, а длина самого длинного кода из теоремы 2 равна $p^{(2\nu+1)(p-1)p^{\nu-1}}$, эти коды значительно длиннее, чем коды из статьи [4], где улучшены результаты статей [7] и [8]. Самый длинный код, описанный в [4] имеет длину $(p-1)^{p^\nu}p^\nu$.

Замечание 3. Относительные параметры $R = k/n$ и $\delta = d/n$ кодов из следствий 1 и 2 удовлетворяют, соответственно, неравенствам

$$R \geqslant 1 - \delta - \frac{(q^{N_1(s)} - 1)(s(q+1) - 1) - 1}{q^{N_1(s)+2} + 1},$$

$$R \geqslant 1 - \delta - \frac{(p^{N_2(s)} - 1)(s(p^{\nu+1} + 1) - 1) - 1}{qp^{N_2(s)} + 1}.$$

Доказательство основных результатов этой статьи проводится следующим образом. В параграфе 2 приводится явное выражение для рода кривой (2). В параграфе 3 строится канонический базис невырожденного подпространства пространства $F_q[x]$ и находится число F_q-рациональных точек кривой, определенной системой (2) для этого канонического базиса. В последнем параграфе доказываются теоремы 1 и 2, а также их следствия.

2. Вычисление рода кривой

Пусть F_q — конечное поле характеристики p с $q = p^\nu$ элементами. Пусть $f(x) \in F_q[x]$ — полином степени m, $(m, p) = 1$. Тогда кривая X, определенная над $\bar{F}_q$ уравнением

$$y^p - y = f(x), \tag{3}$$

неприводима. Следующая лемма хорошо известна; мы приводим ее доказательство, поскольку его часть используется в доказательстве теоремы 3.

Лемма 1. *Род кривой X равен*

$$g(X) = \tfrac{1}{2}(p-1)(m-1).$$

Доказательство. Кривая X определяет покрытие $\phi\colon X \to P^1$ степени p проективной прямой P^1. Единственной точкой ветвления покрытия ϕ является точка на бесконечности. Пусть $p_\infty = [0:1]$ — точка на бесконечности и x — координата в A^1. Если взять $t = 1/x$ в качестве локального параметра в p_∞, то обратным образом p_∞ будет точка x_∞ на кривой X, которая соответствует дискретной оценке v_{x_∞} с

$v_{x_\infty}(x) = -p$ и $v_{x_\infty}(y) = -m$. Локальный параметр в x_∞ есть $s = 1/(x^a y^b)$, где $ap + bm = 1$. Так как $v_{x_\infty}(1/(x^a y^b)) = 1$,

$$v_{x_\infty}\left(d\left(\frac{1}{x^a y^b}\right)\right) = v_{x_\infty}\left(\frac{bx^a y^{b-1}dy + ax^{a-1}y^b dx}{x^{2a}y^{2b}}\right) = 0.$$

Используя равенство $d(y^p - y) = df(x)$, или эквивалентное равенство $dy = -f'(x)\,dx$, получаем, что

$$v_{x_\infty}\left(\frac{(bxf'(x) + ay)\,dx}{x^{a+1}y^{b+1}}\right) = 0.$$

Поскольку

$$\begin{aligned} v_{x_\infty}(bxf'(x) + ay) &= \min\{v_{x_\infty}(bxf'(x)), v_{x_\infty}(ay)\} \\ &= v_{x_\infty}(bxf'(x)) = -mp, \end{aligned}$$

находим, что степень канонического делителя равна

$$v_{x_\infty}(dx) = mp - m - p - 1.$$

Таким образом, $2g(X) - 2 = mp - m - p - 1$, что приводит к равенству

$$g(X) = \tfrac{1}{2}(p-1)(m-1).$$

Так как ϕ — покрытие степени p проективной прямой P^1, получаем, что

$$2g(X) - 2 = p(2g(P^1) - 2) + \deg R_\phi, \tag{4}$$

где R_ϕ — делитель ветвления покрытия ϕ.

Единственной точкой ветвления покрытия ϕ является точка x_∞, поэтому $R_\phi = a_{x_\infty} x_\infty$. Используя (4) и выражение для рода, находим, что $a_{x_\infty} = (p-1)(m+1)$.

Пусть теперь A — линейное подпространство пространства $F_q[x]$. Пусть $\{f_1, \ldots, f_s\}$ — канонический базис подпространства A такой, что $\deg f_i(x) = m_i$ и $(m_i, p) = 1$. Предположим, что m_i упорядочены так, что $m_1 \leqslant \ldots \leqslant m_s$. Пусть X_s — кривая, задаваемая над $\bar{F}_q$ расслоенным произведением

$$\begin{aligned} y_1^p - y_1 &= f_1(x), \\ y_2^p - y_2 &= f_2(x), \\ &\ldots \\ y_s^p - y_s &= f_s(x). \end{aligned} \tag{5}$$

Теорема 3. *Род кривой X_s, задаваемой* (5), *равен*

$$g(X_s) = p^{s-1}\frac{(p-1)(m_s-1)}{2} + \ldots + p\frac{(p-1)(m_2-1)}{2} + \frac{(p-1)(m_1-1)}{2}.$$

Доказательство. Для $1 \leqslant r \leqslant s$ пусть X_r — кривая в P^{s-r+1}, задаваемая системой (5) с удаленными первыми $r-1$ уравнениями. Тогда для любого r, $2 \leqslant r \leqslant s$, X_{r-1} есть покрытие X_r и X_s есть покрытие проективной прямой P^1, причем степень каждого из покрытий равна p. Таким образом, мы имеем цепочку покрытий

$$X_1 \to X_2 \to \ldots \to X_s \to P^1.$$

Доказательство формулы для рода проведем индукцией по s. Для $s = 1$ это утверждение содержится в лемме 1. Предположим что оно верно для $s-1$, тогда

$$g(X_2) = p^{s-2}\frac{(p-1)(m_{s-1}-1)}{2} + \ldots + p\frac{(p-1)(m_2-1)}{2} + \frac{(p-1)(m_1-1)}{2}.$$

Поскольку X_1 есть покрытие степени p для X_2, справедливо равенство

$$2g(X_1) - 2 = p(2g(X_2) - 2) + \deg R_{\phi_2} \tag{6}$$

где R_{ϕ_2} — делитель ветвления покрытия $\phi_2\colon X_1 \to X_2$. Имея в виду, что единственной точкой ветвления покрытия ϕ_2 является точка на бесконечности и гладкая проективная кривая X_2 вблизи точки на бесконечности ведет себя как проективная прямая P^1, с помощью рассуждений, использованных в доказательстве леммы 1, находим, что

$$\deg R_{\phi_2} = (p-1)(m_1+1).$$

Таким образом, из (6) следует, что

$$g(X_1) = pg(X_2) + \tfrac{1}{2}(p-1)(m_1-1),$$

и теорема доказана.

Подчеркнем, что упорядочение $m_1 \leqslant \ldots \leqslant m_s$ степеней полиномов $f_1(x), \ldots, f_s(x)$ существенно. Действительно, если рассматривать каждое уравнение $y_i^p - y_i = f_i(x)$ в (5) отдельно как покрытие проективной прямой и x_{i_∞} как обратный образ бесконечной точки $[0:1] \in P^1$, то x_{i_∞} будет соответствовать такой дискретной норме $v_{x_{i_\infty}}$, что $v_{x_{i_\infty}}(x) = -m_i$. Таким образом, сначала придется рассматривать покрытие с минимальной нормой x и ясно, что это есть покрытие с максимальной степенью m_i, скажем m_s. Проводя ту же операцию с заменой проективной прямой на кривую $y_s^p - y_s = f_s(x)$ и принимая во внимание, что гладкая проективная кривая вблизи точки на бесконечности ведет себя как проективная прямая, мы убеждаемся в необходимости упорядочения.

Следует отметить также, что для доказательства теоремы 3 можно было бы использовать формулу для рода элементарных абелевых p-расширений, приведенную в [1], или теорему 2.2 из [3], однако преимущества приведенного здесь доказательства заключаются в его простоте и замкнутости в смысле геометрии кривой X_s.

Замечание 4. Важно заметить, что значение рода, указанное в теореме 3 ограничено сверху величиной $(p^s-1)(m_s-1)/2$.

3. Число F_q-рациональных точек

Пусть p — простое число и F_q — конечное поле с $q = p^\nu$ элементами. Обозначим $\mathrm{Tr}_\nu\colon F_q \to F_p$ функцию след. Число N решений уравнения $y^p - y = f(x) \in F_q(x)$ в $F_q \times F_q$ задается формулой $N = p|\{x \in F_q\colon \mathrm{Tr}_\nu f(x) = 0\}|$. Используя этот хорошо известный факт, получаем следующее утверждение.

Лемма 2. *Пусть p — простое число, $q = p^\nu$, где ν — положительное целое число, и F_{q^2} — конечное поле с q^2 элементами. Тогда для любого $a \in F_{q^2}^*$ такого, что $a + a^q = 0$, и любого целого $j \geqslant 1$ число F_{q^2}-рациональных точек аффинной кривой $y^p - y = ax^{j(1+q)}$ равно q^2p.*

Доказательство. Ясно, что

$$\begin{aligned}\mathrm{Tr}_{2\nu}(ax^{j(1+q)}) &= \sum_{k=0}^{2\nu-1}(ax^{j(1+q)})^{p^k} = \sum_{k=0}^{\nu-1} a^{p^k}x^{jp^k(1+q)} + \sum_{k=\nu}^{2\nu-1} a^{p^k}x^{jp^k(1+q)}\\ &= \sum_{k=0}^{\nu-1} a^{p^k}x^{jp^k(1+q)} + \sum_{k=0}^{\nu-1} a^{p^{k+\nu}}x^{jp^{k+\nu}(1+q)}\\ &= \sum_{k=0}^{\nu-1} a^{p^k}x^{jp^k(1+q)} + \sum_{k=0}^{\nu-1} -a^{p^k}x^{jp^k(q+q^2)}.\end{aligned}$$

Для любого $x \in F_{q^2}$ справедливо равенство $x^{q^2} = x$, поэтому $\mathrm{Tr}_{2\nu}(ax^{j(1+q)}) = 0$ для любого $x \in F_{q^2}$. Отсюда следует утверждение леммы.

Лемма 3. *Пусть F_{q^2} — то же, что и в лемме 2. Тогда для любого $a \in F_{q^2}^*$ и любого целого j, $0 < j \leqslant \nu - 1$, число F_{q^2}-рациональных точек аффинной кривой*

$$y^p - y = ax^{1+p^{\nu+j}} - a^{p^{\nu-j}}x^{1+p^{\nu-j}}$$

равно q^2p.

Доказательство. Ясно, что

$$\begin{aligned}&\mathrm{Tr}_{2\nu}(ax^{1+p^{\nu+j}} - a^{p^{\nu-j}}x^{1+p^{\nu-j}})\\ &\quad= \sum_{k=0}^{2\nu-1}(ax^{1+p^{\nu+j}})^{p^k} - \sum_{k=0}^{2\nu-1}(a^{p^{\nu-j}}x^{1+p^{\nu-j}})^{p^k}\\ &\quad= \sum_{k=0}^{\nu-j-1}(ax^{1+p^{\nu+j}})^{p^k} + \sum_{k=\nu-j}^{2\nu-1}(ax^{1+p^{\nu+j}})^{p^k}\\ &\qquad- \sum_{k=0}^{\nu+j-1}(a^{p^{\nu-j}}x^{1+p^{\nu-j}})^{p^k} - \sum_{k=\nu+j}^{2\nu-1}(a^{p^{\nu-j}}x^{1+p^{\nu-j}})^{p^k}\\ &\quad= \sum_{k=0}^{\nu-j-1} a^{p^k}x^{p^k(1+p^{\nu+j})} + \sum_{k=0}^{\nu+j-1} a^{p^{\nu-j+k}}x^{p^k(p^{\nu-j}+q^2)}\\ &\qquad- \sum_{k=0}^{\nu+j-1} a^{p^{\nu-j+k}}x^{p^k(1+p^{\nu-j})} - \sum_{k=0}^{\nu-j-1} a^{p^{2\nu+k}}x^{p^k(p^{\nu+j}+q^2)}\\ &\quad= \sum_{k=0}^{\nu-j-1} a^{p^k}x^{p^k(1+p^{\nu+j})} - \sum_{k=0}^{\nu-j-1} a^{p^{2\nu+k}}x^{p^k(p^{\nu+j}+q^2)}\\ &\qquad+ \sum_{k=0}^{\nu+j-1} a^{p^{\nu-j+k}}x^{p^k(p^{\nu-j}+q^2)} - \sum_{k=0}^{\nu+j-1} a^{p^{\nu-j+k}}x^{p^k(1+p^{\nu-j})}.\end{aligned}$$

Используя то, что $a^{q^2} = a$ и $x^{q^2} = x$ для всех $x \in F_{q^2}$, получаем, что

$$\mathrm{Tr}_{2\nu}(ax^{1+p^{\nu+j}} - a^{p^{\nu-j}}x^{1+p^{\nu-j}}) = 0$$

для любого $x \in F_{q^2}$. Отсюда следует утверждение леммы.

Пусть $S_1, S_2 \subset F_q[x]$ — множества полиномов, соответственно, вида

$$f_1(x) = a_i x^{j(1+q)},$$

где $a_i \in F_{q^2}$ удовлетворяют соотношению $a_i^q + a_i = 0$ и F_p-линейно независимы и $1 \leqslant j < q$, $(j,p) = 1$; и

$$f_2(x) = a_i x^{1+p^{\nu+j}} - a_i^{p^{\nu-j}} x^{1+p^{\nu-j}},$$

где a_i принадлежат F_{q^2} и F_p-линейно независимы и $1 \leqslant j \leqslant \nu - 1$, $i = 1, 2$.

Используя эти множества и леммы 2 и 3, получаем следующий результат.

Лемма 4. *Пусть F_{q^2} — то же, что и в леммах 2, 3. Пусть s, $1 \leqslant s < q$, — целое число такое, что $(s,p) = 1$, и X_s — аффинная кривая, определенная над $\bar{F}_{q^2}$ расслоенным произведением*

$$\begin{aligned} y_1^p - y_1 &= f_1(x), \\ y_2^p - y_2 &= f_2(x), \\ &\dots \\ y_s^p - y_s &= f_s(x), \end{aligned}$$

где $f_i(x) \in S_1 \cup S_2$ имеют степени $\deg f_i(x) \leqslant s(q+1)$, $i = 1, \dots, s$.

Тогда число F_{q^2}-рациональных точек $N_{q^2}(X_s)$ кривой X_s равно

$$N_{q^2}(X_s) = q^{N_1(s)+2},$$

где $N_1(s) = s - [s/p] + 2[\log_p((s(q+1)-1)/q)]$.

Доказательство. Семейство полиномов $S_1 \cup S_2$ образует канонический базис невырожденного линейного подпространства пространства $F_q[x]$, так что данная система определяет кривую. В силу лемм 2 и 3 для любого $x \in F_{q^2}$ расслоение над x на кривой X_s содержит $p^{N(s)}$ F_{q^2}-рациональных точек, где $N(s)$ — число определяющих уравнений этой кривой. Записывая s в виде $s = np + r$, $1 \leqslant r \leqslant p-1$, видим, что число целых j таких, что $1 \leqslant j \leqslant s$ и $(j,p) = 1$, равно

$$n(p-1) + r = np + r - n = s - n = s - [s/p].$$

Таким образом, число определяющих уравнений для полиномов из S_1 равно $\nu(s - [s/p])$. Число определяющих уравнений для полиномов из S_2 равно $2\nu m$, где m — наибольшее целое число такое, что

$$p^{\nu+m} + 1 \leqslant s(p^\nu + 1).$$

Таким образом,

$$m = [\log_p((s(q+1)-1)/q)],$$

и, следовательно,

$$N(s) = \nu((s - [s/p]) + 2[\log_p((s(q+1)-1)/q)]) = \nu N_1(s),$$

что завершает доказательство.

Две следующие леммы относятся к случаю F_q, $q = p^{2\nu+1}$.

Лемма 5. *Пусть p — простое число, $q = p^{2\nu+1}$, где ν — положительное целое число, и F_q — конечное поле с q элементами. Тогда для любого $a_i \in F_q^*$ и любого целого $j \geqslant 1$ число F_q-рациональных точек аффинной кривой*

$$y^p - y = a_i x^{j(p^{\nu+1}+1)} - a_i^{p^\nu} x^{j(p^\nu+1)}$$

равно qp.

Доказательство. Ясно, что

$$\begin{aligned}
&\mathrm{Tr}_{2\nu+1}(ax^{j(p^{\nu+1}+1)} - a^{p^\nu} x^{j(p^\nu+1)}) \\
&\quad = \sum_{k=0}^{2\nu} (ax^{j(p^{\nu+1}+1)})^{p^k} - \sum_{k=0}^{2\nu} (a^{p^\nu} x^{j(p^\nu+1)})^{p^k} \\
&\quad = \sum_{k=0}^{\nu-1} a^{p^k} x^{jp^k(p^{\nu+1}+1)} + \sum_{k=\nu}^{2\nu} a^{p^k} x^{jp^k(p^{\nu+1}+1)} \\
&\qquad - \sum_{k=0}^{\nu} a^{p^{\nu+k}} x^{jp^k(p^\nu+1)} - \sum_{k=\nu+1}^{2\nu} a^{p^{\nu+k}} x^{jp^k(p^\nu+1)} \\
&\quad = \sum_{k=0}^{\nu-1} a^{p^k} x^{jp^k(p^{\nu+1}+1)} + \sum_{k=0}^{\nu} a^{p^{\nu+k}} x^{jp^{\nu+k}(p^{\nu+1}+1)} \\
&\qquad - \sum_{k=0}^{\nu} a^{p^{\nu+k}} x^{jp^k(p^\nu+1)} - \sum_{k=0}^{\nu-1} a^{p^{2\nu+k+1}} x^{jp^{\nu+k+1}(p^\nu+1)} \\
&\quad = \sum_{k=0}^{\nu-1} a^{p^k} x^{jp^k(p^{\nu+1}+1)} + \sum_{k=0}^{\nu} a^{p^{\nu+k}} x^{jp^k(p^{2\nu+1}+p^\nu)} \\
&\qquad - \sum_{k=0}^{\nu} a^{p^{\nu+k}} x^{jp^k(p^\nu+1)} - \sum_{k=0}^{\nu-1} a^{p^{2\nu+k+1}} x^{jp^k(p^{2\nu+1}+p^{\nu+1})}.
\end{aligned}$$

Используя то, что $a^q = a$ и $x^q = x$ для всех $x \in F_q$, получаем, что

$$\mathrm{Tr}_{2\nu+1}(ax^{j(p^{\nu+1}+1)} - a^{p^\nu} x^{j(p^\nu+1)}) = 0$$

для всех $x \in F_q$, что завершает доказательство.

Взяв a_i в предшествующей лемме так, что они образуют базис F_q над F_p и рассуждая так, как в доказательстве леммы 4, получаем следующее утверждение.

Лемма 6. *Пусть F_q — то же, что и в лемме 5. Тогда для любого целого s, $1 \leqslant s < p^{\nu-1}$, $(s,p) = 1$, расслоенное произведение*

$$y_{ij}^p - y_{ij} = a_i x^{j(p^{\nu+1}+1)} - a_i^{p^\nu} x^{j(p^\nu+1)}$$

где $1 \leqslant j \leqslant s$, $(j,p) = 1$, имеет

$$qp^{(2\nu+1)(s-[s/p])}$$

F_q-рациональных точек.

4. Доказательство теорем

В этом параграфе доказывается теорема 1 и следствие 1. Доказательства теоремы 2 и следствия 2 совершенно аналогичны.

Доказательство теоремы 1. Пусть F_{q^2} — конечное поле с $q^2 = p^{2\nu}$ элементами и $1 \leqslant s < q$, $(s,p) = 1$. Пусть X_s — аффинная кривая, определенная в лемме 4. Согласно этой лемме число F_{q^2}-рациональных точек в X_s равно $q^{N_1(s)+2}$, где

$$N_1(s) = s - [s/p] + 2[\log_p((s(q+1)-1)/q)].$$

Нормализуя кривую X_s, получаем несингулярную модель $\tilde{X}_s$ без нарушения F_{q^2}-рациональности этих точек. Принимая во внимание точку на бесконечности p_∞ кривой $\tilde{X}_s$, находим, что

$$N_{q^2}(\tilde{X}_s) = q^{N_1(s)+2} + 1.$$

Согласно теореме 3 и следствию 4 род кривой $\tilde{X}_s$ не превосходит

$$\tfrac{1}{2}(q^{N_1(s)} - 1)(s(q+1) - 1),$$

что и завершает доказательство.

Прежде чем приступить к доказательству следствия 1, напомним известную конструкцию линейных $[n,k,d]_q$-кодов Гоппы, связанных с гладкой проективной кривой X над конечным полем F_q, где $q = p^\nu$ (см. [2]).

Пусть X — абсолютно неприводимая гладкая проективная кривая рода g над F_q. Пусть $\{p_1, \ldots, p_n\}$ — множество различных F_q-рациональных точек на X и $D_0 = p_1 + \ldots + p_n$. Пусть D — F_q-рациональный делитель на X такой, что носители D и D_0 не пересекаются. Линейное пространство

$$L(D) = \{f \in F_q(X)^* \mid (f) + D \geqslant 0\} \cup \{0\}$$

порождает линейное отображение

$$Ev\colon L(D) \to F_q^n, \qquad f \to (f(p_1), \ldots, f(p_n)).$$

Образ этого отображения есть линейный $[n,k,d]_q$-код $C = C(D_0, D)$, называемый геометрическим кодом Гоппы, связанным с парой (D_0, D).

Если $\deg D < n$, то Ev есть вложение, поэтому $k = \dim C = l(D)$. По теореме Римана–Роха

$$k = l(D) \geqslant \deg D - g + 1.$$

В частности, если $2g - 2 < \deg D < n$, то $k = \deg D - g + 1$.

Минимальное расстояние d кода $C = C(D, D_0)$ удовлетворяет неравенству

$$d \geqslant n - \deg D.$$

Отсюда следует, что относительные параметры $R = k/n$ и $\delta = d/n$ линейного $[n,k,d]_q$-кода $C = C(D_0, D)$ удовлетворяют соотношению

$$R \geqslant 1 - \delta - \frac{g-1}{n}.$$

Теперь, применяя конструкцию Гоппы к кривым из теоремы 1, мы можем доказать следствие 1.

Доказательство следствия 1. Пусть X_s — гладкая проективная кривая, определенная в теореме 1. Пусть S — множество F_{q^2}-рациональных точек на конечной части кривой X_s и p_∞ — точка кривой X_s на бесконечности. Согласно лемме 4 $|S| = q^{N_1(s)+2}$. Пусть $n \leqslant q^{N_1(s)+2}$ и

$$D_0 = p_1 + \ldots + p_n, \qquad D = lp_\infty.$$

Применяя конструкцию Гоппы к этим F_{q^2}-делителям на X_s для каждого l такого, что

$$\tfrac{1}{2}(q^{N_1(s)} - 1)(s(q+1) - 1) < l < n,$$

мы получаем требуемый код.

Список литературы

1. Garcia A., Stichtenoth H., Elementary abelian p-extensions of algebraic function fields. *Manuscr. Math.* (1991) **72**, 67–79.
2. Goppa V. G., Codes on algebraic curves. *Soviet Math. Dokl.* (1981) **24**, 170–172.
3. Lachaud G., Artin–Schreier curves, exponential sums, and the Carlitz–Uchiyama bound for geometric codes. *J. Number Theory* (1991) **39**, 18–40.
4. Özbudak F., Codes on fibre products of some Kummer coverings. *Finite Fields and their Appl.* (1999) **5**, 188–205.
5. Степанов С. А., *Арифметика алгебраических кривых*. Наука, Москва, 1971.
6. Stepanov S. A., *Codes on Algebraic Curves.* Plenum, New York, 1999.
7. Степанов С. А., Коды на расслоенных произведениях гиперэллиптических кривых. *Дискретная математика* (1997) **9**, №1, 83–94.
8. Степанов С. А., Озбудак Ф., Расслоенные произведения гипергеометрических кривых и геометрические коды Гоппы. *Дискретная математика* (1997) **9**, №3, 36–42.
9. G. van der Geer, M. van der Vlugt, How to construct curves over finite fields with many points. *Algebraic Geometry E-prints*, alg-geom/9511005, 1995.
10. Xing C., Stichtenoth H., The genus of maximal function fields. *Manuscr. Math.* (1955) **86**, 217–224.

Статья поступила 02.02.2001.