Math-Net.Ru

Общероссийский математический портал

С. А. Степанов, Коды на расслоенных произведениях гиперэллиптических кривых, *Дискрет. матем.*, 1997, том 9, выпуск 1, 83–94

DOI: <https://doi.org/10.4213/dm460>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 3.80.253.173

26 апреля 2023 г., 09:13:56

Коды на расслоенных произведениях гиперэллиптических кривых

© 1997 г. С. А. Степанов

Целью настоящей статьи является построение нового семейства гладких проективных кривых над полем F_q с большим числом F_q -рациональных точек. Род этого семейства существенно меньше, чем число рациональных точек, так что соответствующие геометрические коды Гоппы имеют хорошие параметры.

1. Введение

Пусть X — гладкая проективная кривая рода $g = g(X)$ над конечным полем $k' = F_q$. Напомним основные идеи предложенной Гоппой конструкции [3] линейных $[n, k, d]_q$ -кодов, связанных с кривой X . Пусть $\{x_1, \dots, x_n\}$ — множество k' -рациональных точек кривой X и

$$D_0 = x_1 + \dots + x_n.$$

Пусть D — k' -рациональный дивизор на X . Будем предполагать, что носитель D не пересекается с D_0 , то есть точки x_i , $i = 1, \dots, n$ входят в D с нулевой кратностью. Обозначим $k'(X)$ поле рациональных функций на X и рассмотрим векторное пространство над k'

$$L(D) = \{f \in k'(X)^* \mid (f) + D \geq 0\} \cup \{0\}.$$

Линейный $[n, k, d]_q$ -код $C = C(D_0, D)$, связанный с парой (D_0, D) , есть образ линейного отображения

$$\text{Ev}: L(D) \rightarrow F_q^n, \quad f \mapsto (f(x_1), \dots, f(x_n)).$$

Такой q -арный линейный код называется геометрическим кодом Гоппы. Если $\deg D < n$, то отображение Ev есть инъекция и $C \simeq L(D)$.

Рассмотрим двойственную конструкцию. Пусть $\Omega(X)$ обозначает $k'(X)$ -векторное пространство рациональных дифференциальных форм на X . Рассмотрим линейное пространство над k'

$$\Omega(D_0 - D) = \{\omega \in \Omega(X)^* \mid (\omega) + D_0 - D \geq 0\} \cup \{0\}.$$

Линейное отображение

$$\text{Res}: \Omega(D_0 - D) \rightarrow F_q^n, \quad \omega \mapsto (\text{Res}_{x_1}(\omega), \dots, \text{Res}_{x_n}(\omega))$$

определяет линейный $[n, k, d]_q$ -код $C^* = C^*(D_0, D)$, связанный с парой (D_0, D) . Если $\deg D > 2g - 2$, отображение Res является инъективным и $C^* \simeq \Omega(D_0 - D) \simeq L(K + D_0 - D)$, где K — канонический дивизор на X .

С каждым линейным $[n, k, d]_q$ -кодом C связана пара параметров (δ, R) , где $\delta = d/n$ — относительное минимальное расстояние и R — информационная скорость кода C . Точки (δ, R) образуют множество кодовых точек $V_q^{\text{lin}} \subseteq [0, 1]^2$. Пусть U_q^{lin} обозначает подмножество предельных точек V_q^{lin} . Другими словами, $(\delta, R) \in U_q^{\text{lin}}$ тогда и только тогда, когда существует бесконечная последовательность различных линейных кодов C_i с параметрами $\delta_i = \delta(C_i)$ и $R_i = R(C_i)$ такая, что

$$\lim_{i \rightarrow \infty} (\delta_i, R_i) = (\delta, R).$$

Если $\delta > 0$ и $R > 0$, то такое семейство кодов C_i называется асимптотически хорошим. Структуру множества U_q^{lin} можно описать следующим образом (см. [1, 4]): существует непрерывная функция $\alpha_q^{\text{lin}}(\delta)$ такая, что

$$U_q^{\text{lin}} = \{(\delta, R) \mid 0 \leq R \leq \alpha_q^{\text{lin}}(\delta)\},$$

и кроме того, $\alpha_q^{\text{lin}}(0) = 1$, $\alpha_q^{\text{lin}}(\delta) = 0$ при $(q-1)/q \leq \delta \leq 1$ и $\alpha_q^{\text{lin}}(\delta)$ убывает на интервале $[0, (q-1)/q]$.

Как следует из теоремы Римана–Роха, параметры $R = k/n$ и $\delta = d/n$, как для L так и для Ω конструкций удовлетворяют неравенству (см. [8, 10])

$$R \geq 1 - \delta - \frac{g-1}{n}. \quad (1)$$

Для того чтобы построить семейство асимптотически хороших геометрических кодов Гоппы, для которых $R + \delta$ лежит выше границы Варшавова–Гильберта

$$\alpha_q^{\text{lin}}(\delta) \geq 1 - H_q(\delta),$$

где

$$H_q(\delta) = \delta \log_q(q-1) - \delta \log_q \delta - (1-\delta) \log_q(1-\delta),$$

нужно иметь семейство гладких проективных кривых с большим числом k' -рациональных точек по сравнению с их родом. Примерами таких семейств служат классические модулярные кривые $X_0(N)$ и $X(N)$ (см. [9, 5]) и модулярные кривые Дринфельда [10, Гл. 4.1 и 4.2]). Так, если $q = p^\nu$ — четная степень простого числа p , то существует бесконечная последовательность геометрических кодов Гоппы C_i , для которой

$$\alpha_q^{\text{lin}} \geq 1 - \delta - (\sqrt{q} - 1)^{-1}.$$

Прямая $R = 1 - \delta - (\sqrt{q} - 1)^{-1}$ пересекает кривую $R = 1 - H_q(\delta)$ при $q \geq 49$. Значительно более простое доказательство этого результата, основанное на рассмотрении последовательности (модифицированных) накрытий Артина–Шрайера проективной прямой $P^1(\bar{k}')$, недавно предложено в [2].

В настоящей работе рассматривается новое семейство гладких проективных кривых X_s , задаваемых над $k' = F_q$ уравнениями

$$z_i^2 = f_i(u), \quad 1 \leq i \leq s, \quad (2)$$

где $f_i(u)$ — взаимно простые свободные от квадратов полиномы специального вида из $k'[u]$. Каждая такая кривая есть фактически расслоенное произведение гиперэллиптических кривых. Основное внимание в работе уделено вычислению рода $g(X_s)$ (лемма 1) и нахождению числа k' -рациональных точек $N_q(X_s)$ на кривой X_s (лемма 4). Доказывается, что отношение $g(X_s)/N_q(X_s)$ мало, и из (1) выводится, что соответствующие геометрические коды Гоппы $C(D, D_0)$ и $C^*(D, D_0)$ имеют достаточно хорошие параметры. При малых значениях s эти параметры сравнимы с параметрами введенных в [2] кодов на накрытиях Артина–Шрайера. В частности, если $s = 1$, то коды $C(D, D_0)$ и $C^*(D, D_0)$ имеют такие же параметры, как коды на Эрмитовых кривых (см. [8], Раздел VII.3). К сожалению, параметр s в наших построениях ограничен величиной $q^{1/2}$ и, следовательно, род $g(X_s)$ ограничен величиной

$$(q - 3)2^{(q^{1/2} - 2)} + 1.$$

Однако, поскольку при $q \geq q_0$ эта верхняя граница достаточно велика, кривые X_s дают довольно длинные геометрические коды Гоппы.

Аналогичная конструкция неособых проективных кривых с большим числом k' -рациональных точек, основанная на использовании расслоенных произведений некоторых кривых Артина–Шрайера, была независимо предложена в статье [11].

Род $g(X_s)$ можно легко вычислить, используя формулу Гурвица. Мы предпочли использовать несколько более сложный подход, позволяющий найти в явном виде базис пространства $\Omega(D_0 - D)$. Это дает возможность просто выписать порождающую матрицу кодов рассматриваемого семейства и указать быстрый алгоритм декодирования.

Применяя к кривым X_s конструкцию Гоппы, получаем следующие результаты.

Теорема 1. Пусть p — простое число, $p > 2$, ν — четное число, $\nu > 1$, и F_q — конечное поле с $q = p^\nu$ элементами.

Для любых положительных целых чисел $s \leq q^{1/2}$ и $l > (sq^{1/2} - 3)2^{s-2}$ существует геометрический $[n, k, d]_q$ -код Гоппы $C = C(D_0, D)$, для которого

$$\begin{aligned} l &< n \leq (2q^{1/2} - s)q^{1/2}2^{s-1}, \\ k &\geq l - (sq^{1/2} - 3)2^{s-2}, \\ d &\geq n - l. \end{aligned}$$

Теорема 2. Пусть p , q и s выбраны так же, как в предыдущей теореме, и $l > (sq^{1/2} - 3)2^{s-1}$.

Тогда существует геометрический $[n, k, d]_q$ -код Гоппы $C^* = C^*(D_0, D)$, для которого

$$\begin{aligned} l - (sq^{1/2} - 3)2^{s-2} &< n \leq (2q^{1/2} - s)q^{1/2}2^{s-1}, \\ k &\geq n - l + (sq^{1/2} - 3)2^{s-2}, \\ d &\geq l - (sq^{1/2} - 3)2^{s-1}. \end{aligned}$$

Следствие 1. Для параметров $R = k/n$ и $\delta = d/n$ кодов из теорем 1 и 2 справедливо неравенство

$$R \geq 1 - \delta - \frac{(sq^{1/2} - 3)2^{s-2}}{n}.$$

В частности, при $n = (2q^{1/2} - s)q^{1/2}2^{s-1}$

$$R \geq 1 - \delta - \frac{sq^{1/2} - 3}{2(2q^{1/2} - s)q^{1/2}}.$$

С помощью соответствующей конкатенации можно получить достаточно хорошие коды над F_p . Действительно, пусть k_0 — четное число, $k_0 > 1$, применяя линейный $[n_0, k_0, d_0]_p$ -код C_0 к $[n, k, d]_q$ -коду $C = C(D_0, D)$ над F_q , где $q = p^{k_0}$, получаем $[n', k', d']_p$ -код C' с параметрами

$$n' = n_0 n, \quad k' = k_0 k, \quad d' = d_0 d.$$

Обозначим $R_0 = k_0/n_0$ и $\delta_0 = d_0/n_0$ относительные параметры кода C_0 .

Следствие 2. Для любых положительных целых чисел $n_0 > 1$, $s \leq q^{1/2}$ и $l > (sq^{1/2} - 3)2^{s-2}$ существует линейный $[n', k', d']_p$ -код C' , для которого

$$\begin{aligned} n_0 l < n' = n_0 n &\leq n_0 (2q^{1/2} - s)q^{1/2}2^{s-1}, \\ k' &\geq k_0 (l - (sq^{1/2} - 3)2^{s-2}), \\ d' &\geq d_0 (n - l). \end{aligned}$$

Для относительных параметров $R' = k'/n'$ и $\delta' = d'/n'$ кода C' справедливо неравенство

$$R' + \delta' \geq R_0 \left(\frac{l}{n} - \frac{(sq^{1/2} - 3)2^{s-2}}{n} \right) + \delta_0 \left(1 - \frac{l}{n} \right).$$

Применяя $[n_0, k_0, d_0]_p$ -код C_0 к $[n, k, d]_q$ -коду $C^* = C_*(D_0, D)$, получаем следующее утверждение.

Следствие 3. Для любых положительных целых чисел $n_0 > 1$, $s \leq q^{1/2}$ и $l > (sq^{1/2} - 3)2^{s-2}$ существует линейный $[n'', k'', d'']_p$ -код C'' , для которого

$$\begin{aligned} n_0 (l - (sq^{1/2} - 3)) < n'' = n_0 n &\leq n_0 (2q^{1/2} - s)q^{1/2}2^{s-1}, \\ k'' &\geq k_0 (n - l + (sq^{1/2} - 3)2^{s-2}), \\ d'' &\leq d_0 (l - (sq^{1/2} - 3)2^{s-1}). \end{aligned}$$

Для относительных параметров $R'' = k''/n''$ и $\delta'' = d''/n''$ кода C'' справедливо неравенство

$$R'' + \delta'' \geq R_0 \left(1 - \frac{l}{n} + \frac{(sq^{1/2} - 3)2^{s-2}}{n} \right) + \delta_0 \left(\frac{l}{n} - \frac{(sq^{1/2} - 3)2^{s-1}}{n} \right).$$

Результаты этой статьи могут быть перенесены на случай расслоенных произведений более общего вида над произвольным конечным полем.

2. Обозначения и леммы

Пусть k'' — алгебраическое замыкание $k' = F_q$ и A^{s+1} — аффинное пространство размерности $(s+1)$ над k'' . Предположим, что $\text{char } k' > 2$.

Лемма 1. Пусть $f_1, \dots, f_s$ — попарно взаимно простые свободные от квадратов нормированные полиномы из $k'[u]$ одной и той же нечетной степени $m \geq 1$ и Y — расслоенное произведение в A^{s+1} над полем k' , задаваемое уравнениями

$$z_i^2 = f_i(u), \quad 1 \leq i \leq s. \quad (3)$$

Тогда род $g = g(X)$ гладкой проективной модели X равен

$$g = (ms - 3)2^{s-2} + 1.$$

Доказательство. Пусть X — гладкая проективная модель кривой Y . Обозначим v_x каноническое нормирование поля функций $k''(X)$ и $\Omega[X]$ — пространство регулярных дифференциальных форм на X . Легко видеть, что аффинная кривая Y является гладкой. Если $\bar{Y}$ — ее проективное замыкание, то X есть нормализация $\bar{Y}$, и мы имеем отображение $\psi: X \rightarrow \bar{Y}$, являющееся изоморфизмом между Y и $\psi^{-1}(\bar{Y})$. Отсюда следует, что $g = g(X) = g(Y)$.

Рациональное отображение $(u, z_1, \dots, z_s) \mapsto u$ кривой Y в A^1 определяет морфизм $\varphi: X \rightarrow P^1$ степени 2^s , поэтому для $u_0 \in A^1$ либо $\varphi^{-1}(u_0)$ состоит из 2^s точек вида $x' = (u_0, \pm z_1, \dots, \pm z_s)$, в каждой из которых $v_{x'}(t) = 1$ для локального параметра t в точке u_0 , либо $\varphi^{-1}(u_0)$ состоит из 2^{s-1} точек вида $x''_i = (u_0, \pm z_1, \dots, \pm z_{i-1}, 0, \pm z_{i+1}, \dots, \pm z_s)$ и $v_{x''_i}(t) = 2$.

Рассмотрим бесконечно удаленную точку $u_\infty \in P^1$. Если ее координата в A^1 обозначена u , то $t = u^{-1}$ есть локальный параметр в точке u_∞ . Если бы $\varphi^{-1}(u_\infty)$ состояла из 2^s точек $x_\infty^{(\tau)}$, то в каждой точке $x_\infty = x_\infty^{(\tau)}$ функция t была бы локальным параметром. Отсюда следовало бы, что $v_{x_\infty}(t) = 1$ и $v_{x_\infty}(f_i(t)) = -m$. Но так как m нечетно, это противоречит тому, что $v_{x_\infty}(f_i(u)) = 2v_{x_\infty}(z_i)$. Таким образом, $\varphi^{-1}(u_\infty)$ состоит из $r = 2^{s-1}$ точек $x_\infty^{(\tau)}$, $1 \leq \tau \leq r$, с проективными координатами $x_\infty^{(\tau)} = (0, 1, \pm 1, \dots, \pm 1, 0)$. Следовательно, $X = Y \cup \{x_\infty^{(1)}\} \cup \dots \cup \{x_\infty^{(r)}\}$. В каждой такой точке $x_\infty = x_\infty^{(\tau)}$ справедливы равенства $v_{x_\infty}(u) = -2$ и $v_{x_\infty}(z_i) = -m$.

Найдем теперь базис пространства $\Omega[X]$ над полем k'' . Произвольный элемент $\omega \in \Omega[Y]$ может быть записан как линейная комбинация над полем k'' дифференциальных форм $\omega_0 = P_0(u) du$ и

$$\omega_{i_1, \dots, i_\sigma} = \frac{P_{i_1, \dots, i_\sigma}(u) du}{z_{i_1} \dots z_{i_\sigma}},$$

где целые числа $i_1, \dots, i_\sigma$ такие, что $1 \leq i_1 < \dots < i_\sigma \leq s$ и $P_{i_1, \dots, i_\sigma}$ — полиномы из $k''[u]$. Действительно, дифференциальная форма

$$\omega'_{i_1, \dots, i_\sigma} = \frac{du}{z_{i_1} \dots z_{i_\sigma}}$$

регулярна в любой точке $u_0 \in A^1$, если $z_i(u_0) \neq 0$ для $i \in \{i_1, \dots, i_\sigma\}$. Если теперь $z_i(u_0) = 0$ в единственной точке $i \in \{i_1, \dots, i_\sigma\}$, то z_i есть локальный параметр в точке

$$x_i'' = (u_0, \pm z_1, \dots, \pm z_{i-1}, 0, \pm z_{i+1}, \dots, \pm z_s),$$

так что $v_{x_i''}(z_i) = 1$ и $v_{x_i''}(u - u_0) = 2$. Поэтому $v_{x_i''}(du) = 1$ и опять $\omega'_{i_1, \dots, i_\sigma}$ регулярна в точке u_0 . Форма $\omega'_0 = du$ также регулярна в любой точке $u_0 \in A^1$. Таким образом, дифференциальные формы $\omega'_0 = du$ и $\omega'_{i_1, \dots, i_\sigma}$ образуют базис $k''[u]$ -модуля $\Omega[Y]$.

Остается выяснить, какие из форм ω_0 и $\omega_{i_1, \dots, i_\sigma}$ регулярны в точках $x_\infty^{(1)}, \dots, x_\infty^{(r)}$. Пусть x_∞ — одна из этих точек. Если t — локальный параметр в точке x_∞ , то $u = t^{-2}u'$, $z_i = t^{-m}z'_i$, где u' и z'_i — единицы в локальном кольце $\mathcal{O}_{x_\infty}$. Поэтому $\omega'_{i_1, \dots, i_\sigma} = t^{m\sigma-3}\eta_{i_1, \dots, i_\sigma}dt$, где $\eta_{i_1, \dots, i_\sigma}$ есть единица в $\mathcal{O}_{x_\infty}$. Отсюда следует, что $(\omega'_{i_1, \dots, i_\sigma}) = (m\sigma - 3)x_\infty$. Таким образом, дифференциальная форма

$$\omega_{i_1, \dots, i_\sigma} = \frac{P_{i_1, \dots, i_\sigma}(u)du}{z_{i_1} \dots z_{i_\sigma}}$$

регулярна в точке x_∞ тогда и только тогда, когда

$$v_{x_\infty}(P_{i_1, \dots, i_\sigma}(u)) \geq -(m\sigma - 3).$$

Это значит, что $\deg P_{i_1, \dots, i_\sigma}(u) \leq (m\sigma - 3)/2$ и, следовательно,

$$\deg P_{i_1, \dots, i_\sigma}(u) \leq \begin{cases} (m\sigma - 4)/2, & \text{если } \sigma \equiv 0 \pmod{2}, \\ (m\sigma - 3)/2, & \text{если } \sigma \equiv 1 \pmod{2}. \end{cases}$$

Дифференциальная форма $\omega_0 = P_0 du$ не является регулярной в x_∞ ни при одном полиноме $P_0 \in k''[u]$, поэтому регулярные дифференциальные формы

$$\omega'_{i_1, \dots, i_\sigma}, \quad u\omega'_{i_1, \dots, i_\sigma}, \quad \dots, \quad u^n \omega'_{i_1, \dots, i_\sigma},$$

где $1 \leq i_1 < \dots < i_\sigma \leq s$ и

$$n = \begin{cases} (m\sigma - 4)/2, & \text{если } \sigma \equiv 0 \pmod{2}, \\ (m\sigma - 3)/2, & \text{если } \sigma \equiv 1 \pmod{2}, \end{cases}$$

образуют базис пространства $\Omega[X]$ над k'' . Поэтому

$$\begin{aligned} \dim_{k''} \Omega[X] &= \frac{1}{2} \sum_{\sigma \equiv 0 \pmod{2}} \sum_{1 \leq i_1 < \dots < i_\sigma \leq s} (m\sigma - 2) + \frac{1}{2} \sum_{\sigma \equiv 1 \pmod{2}} \sum_{1 \leq i_1 < \dots < i_\sigma \leq s} (m\sigma - 1) \\ &= \frac{m}{2} \sum_{\sigma=1}^s \sigma \binom{s}{\sigma} - \sum_{\sigma \equiv 0 \pmod{2}} \binom{s}{\sigma} - \frac{1}{2} \sum_{\sigma \equiv 1 \pmod{2}} \binom{s}{\sigma} \\ &= \frac{1}{2} (ms2^{s-1} - 2^s - 2^{s-1} + 2) \end{aligned}$$

и, следовательно,

$$g = g(X) = \dim_{k''} \Omega[X] = (ms - 3)2^{s-2} + 1.$$

Лемма доказана.

Пусть p — простое число, ν — положительное целое число и F_q — конечное поле с $q = p^\nu$ элементами. Поле F_q является расширением Галуа простого конечного поля F_p степени ν с циклической группой Галуа порядка ν . Действие порождающего элемента θ этой группы на элемент $x \in F_q$ задается равенством $\theta(x) = x^p$. Отображение

$$\text{norm}_\nu(x) = x\theta(x) \dots \theta^{\nu-1}(x) = xx^p \dots x^{p^{\nu-1}}$$

поля F_q на F_p является нормой элемента x .

Пусть χ — мультипликативный характер поля F_p и x — элемент поля F_q . Положим

$$\chi_\nu(x) = \chi(\text{norm}_\nu(x))$$

и назовем χ_ν мультипликативным характером поля F_q , индуцированным характером χ .

Пусть теперь f — свободный от квадратов полином степени m из кольца $F_q[u]$ и χ — нетривиальный квадратичный характер поля F_p . Рассмотрим сумму характеров

$$S_\nu(f) = \sum_{u \in F_q} \chi_\nu(f(u)) = \sum_{u \in F_q} \chi(\text{norm}_\nu(f(u))).$$

Согласно хорошо известной оценке Вейля [12] (см. также [7], Главы 1 и 5])

$$|S_\nu(f)| \leq 2 \left[\frac{m-1}{2} \right] q^{1/2}.$$

Следующий результат автора (см. [6], теорема 3) показывает, что граница Вейля не может быть сколько нибудь существенно улучшена в любом расширении F_q поля F_p .

Лемма 2. Пусть F_q — конечное поле характеристики $p > 2$ с $q = p^\nu$ элементами и χ_ν — характер поля F_q , индуцированный нетривиальным квадратичным характером χ поля F_p . Если $\nu > 1$, то для свободного от квадратов полинома $f \in F_p[u]$, задаваемого равенствами

$$f(u) = \begin{cases} u + u^{p^{\nu/2}}, & \text{если } \nu \equiv 0 \pmod{2}, \\ (u + u^{p^{(\nu-1)/2}})(u + u^{p^{(\nu+1)/2}}), & \text{если } \nu \equiv 1 \pmod{2} \end{cases}$$

справедливо равенство

$$\sum_{u \in F_q} \chi_\nu(f(u)) = \begin{cases} (q^{1/2} - 1)q^{1/2}, & \text{если } \nu \equiv 0 \pmod{2}, \\ q - 1, & \text{если } \nu \equiv 1 \pmod{2}. \end{cases}$$

Доказательство. Пусть ν — четное число, $\nu > 1$. Поскольку $u^{p^\nu} = u$ в F_q , для любого $u \in F_q$ справедливы равенства

$$\begin{aligned} \text{norm}_\nu(f(u)) &= \prod_{i=1}^{\nu} (u + u^{p^{\nu/2}})^{p^{i-1}} = \prod_{i=1}^{\nu} (u^{p^{i-1}} + u^{p^{\nu/2+i-1}}) \\ &= \prod_{i=1}^{\nu/2} (u^{p^{i-1}} + u^{p^{\nu/2+i-1}}) \prod_{j=1}^{\nu/2} (u^{p^{\nu/2+j-1}} + u^{p^{j-1}}) \\ &= \prod_{i=1}^{\nu/2} (u^{p^{i-1}} + u^{p^{\nu/2+i-1}})^2. \end{aligned}$$

Поэтому

$$\sum_{u \in F_q} \chi_\nu(f(u)) = \sum_{u \in F_q} \chi(\text{norm}_\nu(f(u))) = q - N,$$

где N — число элементов в множестве $A = \{u \in F_q \mid f(u) = 0\}$. Так как $f(u) = u(1 + u^{p^{\nu/2}-1})$, справедливо равенство $A = \{0\} \cup B$, где

$$B = \{u \in F_q \mid 1 + u^{p^{\nu/2}-1} = 0\}$$

есть множество корней полинома $1 + u^{p^{\nu/2}-1}$ в F_q . Учитывая, что наибольший общий делитель $p^{\nu/2} - 1$ и $p^\nu - 1$ равен $p^{\nu/2} - 1$, согласно критерию Эйлера находим, что число корней полинома $1 + u^{p^{\nu/2}-1}$ равно $p^{\nu/2} - 1$. В этом случае

$$N = |A| = 1 + |B| = 1 + (p^{\nu/2} - 1) = q^{1/2},$$

и следовательно,

$$\sum_{u \in F_q} \chi_\nu(f(u)) = (q^{1/2} - 1)q^{1/2}.$$

Таким образом, лемма доказана в случае, когда ν — четное положительное число.

Пусть теперь ν — нечетное положительное число. В этом случае для любого $u \in F_q$

$$\begin{aligned}
 \text{norm}_\nu(f(u)) &= \prod_{i=1}^{\nu} (u^{p^{i-1}} + u^{p^{(\nu-1)/2+i-1}})(u^{p^{i-1}} + u^{p^{(\nu+1)/2+i-1}}) \\
 &= \prod_{i=1}^{(\nu-1)/2} (u^{p^{i-1}} + u^{p^{(\nu-1)/2+i-1}}) \prod_{i=(\nu+1)/2}^{\nu} (u^{p^{i-1}} + u^{p^{(\nu+1)/2+i-1}}) \\
 &\quad \times \prod_{i=1}^{(\nu-1)/2} (u^{p^{i-1}} + u^{p^{(\nu+1)/2+i-1}}) \prod_{i=(\nu+1)/2}^{\nu} (u^{p^{i-1}} + u^{p^{(\nu+1)/2+i-1}}) \\
 &= \prod_{i=1}^{(\nu+1)/2} (u^{p^{i-1}} + u^{p^{(\nu-1)/2+i-1}}) \prod_{j=1}^{(\nu-1)/2} (u^{p^{(\nu+1)/2+j-1}} + u^{p^{j-1}}) \\
 &\quad \times \prod_{i=1}^{(\nu-1)/2} (u^{p^{i-1}} + u^{p^{(\nu+1)/2+i-1}}) \prod_{j=1}^{(\nu+1)/2} (u^{p^{(\nu-1)/2+j-1}} + u^{p^{j-1}}) \\
 &= \prod_{i=1}^{(\nu+1)/2} (u^{p^{i-1}} + u^{p^{(\nu-1)/2+i-1}})^2 \prod_{i=1}^{(\nu-1)/2} (u^{p^{i-1}} + u^{p^{(\nu+1)/2+i-1}})^2
 \end{aligned}$$

и следовательно,

$$\sum_{u \in F_q} \chi_\nu(f(u)) = \sum_{u \in F_q} \chi(\text{norm}_\nu(f(u))) = q - N',$$

где N' — мощность множества $A = \{u \in F_q \mid f(u) = 0\}$. Ясно, что $N' = 1$ и поэтому

$$\sum_{u \in F_q} \chi_\nu(f(u)) = q - 1.$$

Лемма доказана.

Лемма 3. Пусть F_p — простое конечное поле характеристики $p > 2$, $F_q = F_{p^\nu}$ — расширение F_p четной степени $\nu > 1$ и A — множество корней в F_q полинома

$$f(u) = u + u^{p^{\nu/2}}.$$

Тогда

- (1) A — подгруппа аддитивной группы F_q^+ поля F_q ;
- (2) если $\{A_1 = A, A_2, \dots, A_r\}$ — множество всех смежных классов в F_q^+/A и $\{\alpha_1, \alpha_2, \dots, \alpha_r\}$ — различные представители этих смежных классов, то полиномы

$$f_i(u) = (u + \alpha_i) + (u + \alpha_i)^{p^{\nu/2}}, \quad 1 \leq i \leq r, \quad (4)$$

попарно взаимно просты в $F_q[u]$;

$$(3) \quad r = |F_q^+ / A| = p^{\nu/2}.$$

Доказательство. Основным является утверждение (1). Прежде всего, заметим, что $f(0) = 0$. Теперь, если α и β — нули полинома $f(u)$, то

$$f(\alpha + \beta) = (\alpha + \beta) + (\alpha + \beta)^{p^{\nu/2}} = \alpha + \alpha^{p^{\nu/2}} + (\beta + \beta^{p^{\nu/2}}) = f(\alpha) + f(\beta) = 0,$$

так что $\alpha + \beta$ — также корень полинома $f(u)$. Таким образом, A — подгруппа группы F_q^+ .

Чтобы доказать (2), предположим, что $f_i(u)$ и $f_j(u)$ при $i \neq j$ имеют общий корень в F_q , скажем $u = \theta$. В этом случае

$$\theta + \alpha_i + (\theta + \alpha_i)^{p^{\nu/2}} = \theta + \alpha_j + (\theta + \alpha_j)^{p^{\nu/2}}$$

и следовательно,

$$\theta + \alpha_i + \theta^{p^{\nu/2}} + \alpha_i^{p^{\nu/2}} = \theta + \alpha_j + \theta^{p^{\nu/2}} + \alpha_j^{p^{\nu/2}}.$$

Отсюда следует, что

$$\alpha_i - \alpha_j + (\alpha_i - \alpha_j)^{p^{\nu/2}} = 0,$$

и $\alpha_i - \alpha_j$ — корень полинома $f(u)$, следовательно, $\alpha_i - \alpha_j \in A$. Мы пришли к противоречию, так как $\alpha_i - \alpha_j \notin A$ в силу выбора $\alpha_1, \dots, \alpha_r$.

Наконец, поскольку $|A| = p^{\nu/2}$, справедливо равенство

$$r = |F_q^+ / A| = p^{\nu} / p^{\nu/2} = p^{\nu/2}.$$

Лемма доказана.

Лемма 4. Пусть F_p — простое конечное поле характеристики $p > 2$, F_q — расширение поля F_p четной степени $\nu > 1$ и s — положительное целое число, $s \leq q^{1/2}$. Пусть N_q — число F_q -рациональных точек аффинной кривой Y , задаваемой уравнениями (2) с полиномами

$$f_i(x) = (u + \alpha_i) + (u + \alpha_i)^{p^{\nu/2}}, \quad 1 \leq i \leq s,$$

определяемыми равенствами (3).

Тогда

$$N_q = (2q^{1/2} - s)q^{1/2}2^{s-1}.$$

Доказательство. Ясно, что

$$\begin{aligned} N_q &= \sum_{u \in F_q} (1 + \chi_{\nu}(f_1(u))) \dots (1 + \chi_{\nu}(f_s(u))) \\ &= \sum_{u \in F_q} (1 + \sum_{\sigma=1}^s \sum_{1 \leq i_1 < \dots < i_{\sigma} \leq s} \chi_{\nu}(f_{i_1}(u)) \dots \chi_{\nu}(f_{i_{\sigma}}(u))), \end{aligned}$$

отсюда следует, что

$$N_q = p^\nu + \sum_{\sigma=1}^s \sum_{1 \leq i_1 < i_2 < \dots < i_\sigma \leq s} \sum_{u \in F_q} \chi_\nu(f_{i_1}(u)) \dots \chi_\nu(f_{i_\sigma}(u)).$$

Согласно леммам 2 и 3

$$\chi_\nu(f_i(u)) = \begin{cases} 0, & \text{если } u \in A_i, \\ 1, & \text{если } u \in F_q \setminus A_i, \end{cases}$$

и так как любые два различных множества A_i и A_j не имеют общих элементов,

$$\begin{aligned} N_q &= p^\nu + \sum_{\sigma=1}^s \binom{s}{\sigma} (p^\nu - \sigma p^{\nu/2}) = p^\nu + (2^s - 1)p^\nu - s 2^{s-1} p^{\nu/2} \\ &= (2p^{\nu/2} - s)p^{\nu/2} 2^{s-1} = (2q^{1/2} - s)q^{1/2} 2^{s-1}. \end{aligned}$$

Лемма доказана.

3. Доказательства теорем

Пусть $p > 2$ — простое число, $p > 2$, $k' = F_q$ — расширение простого конечного поля F_p четной степени $\nu > 1$ и s — положительное целое число, $s \leq q^{1/2}$. Пусть $f_1, \dots, f_s$ — попарно взаимно простые полиномы из $k'[u]$ одинаковой степени $q^{1/2}$, определенные равенствами (3), и $Y \subset A^{s+1}$ — аффинная кривая, задаваемая над k' равенствами (2). Пусть $\tilde{Y} \subset P^{s+1}$ — проективное замыкание Y и X — неособая проективная модель $\tilde{Y}$ над алгебраическим замыканием k'' поля k' .

Кривые $\tilde{Y}$ и X бирационально изоморфны, поэтому $g = g(Y) = g(X)$ и согласно лемме 1

$$g = (sq^{1/2} - 3)2^{s-2} + 1.$$

Далее, пусть N_q и M_q — числа k' -рациональных точек кривых Y и X соответственно. Ясно, что $M_q \geq N_q + 1$, и согласно лемме 4

$$M_q \geq (2q^{1/2} - s)q^{1/2} 2^{s-1} + 1.$$

Пусть n — положительное целое число, $n \leq N_q$, и $x_1, \dots, x_n$ — k' -рациональные точки кривой X на ее конечной части и x_∞ — бесконечно удаленная точка кривой X . Положим

$$D_0 = x_1 + \dots + x_n, \quad D = lx_\infty.$$

Применяя к X L -конструкцию при $l > (sq^{1/2} - 3)2^{s-2}$ и $n > l$, получаем геометрический $[n, k, d]_q$ -код Гоппы $C = C(D_0, D)$ с параметрами

$$\begin{aligned} l &< n \leq (2q^{1/2} - s)q^{1/2} 2^{s-1}, \\ k &\geq l - g + 1 = l - (sq^{1/2} - 3)2^{s-2}, \\ d &\geq n - l. \end{aligned}$$

Таким образом, теорема 1 доказана.

Применяя теперь к X Ω -конструкцию при $l > (sq^{1/2} - s)q^{1/2}2^{s-1}$ и $n > l - (sq^{1/2} - 3)2^{s-2}$, получаем геометрический $[n, k, d]_q$ -код Гоппы $C^* = C^*(D_0, D)$ с параметрами

$$\begin{aligned} l - (sq^{1/2} - 3)2^{s-2} < n &\leq (2q^{1/2} - s)q^{1/2}2^{s-1}, \\ k &\geq n - l + (sq^{1/2} - 3)2^{s-2}, \\ d &\geq l - (sq^{1/2} - 3)2^{s-1}. \end{aligned}$$

Теорема 2 также доказана.

Наконец, из (1) следует, что относительные параметры $R = k/n$ и $\delta = d/n$ кодов $C = C(D_0, D)$ и $C^* = C^*(D_0, D)$ удовлетворяют неравенству

$$R \geq 1 - \delta - \frac{(sq^{1/2} - 3)2^{s-2}}{n}.$$

Таким образом, следствие 1 также доказано.

Список литературы

1. Aaltonen M. J. Notes on the asymptotic behavior of the information rate of block codes. *IEEE Trans. Inform. Theory* (1984) **30**, 84–85.
2. Garcia A., Stichtenoth H. A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound. *Invent. Math.* (1995) **121**, 211–222.
3. Гоппа В. Г. Коды на алгебраических кривых. *Докл. АН СССР* (1981) **24**, 170–172.
4. Manin Yu. I. What is the maximum of points on a curve over F_2 ? *J. Fac. Sci. Tokyo* (1981) **28**, 715–720.
5. Moreno C. *Algebraic Curves over Finite Fields*. Cambr. Univ. Press, Cambridge, 1991.
6. Степанов С. А. О нижних оценках сумм характеров над конечными полями. *Дискретная математика* (1991) **3**, No. 2, 77–86.
7. Stepanov S.A. *Arithmetic of Algebraic Curves*. Plenum, New York, 1994.
8. Stichtenoth H. *Algebraic Function Fields and Codes*. Springer, Berlin, 1993.
9. Tsfasman M.A., Vladut S.G., Zink Th. Modular curves, Shimura curves, and Goppa codes, better than the Varshamov-Gilbert bound. *Math. Nachr.* (1982) **109**, 21–28.
10. Tsfasman M.A., Vladut S.G. *Algebraic-Geometric Codes*. Kluwer Acad. Publ., Dordrecht, 1991.
11. van der Geer, G., van der Vlugt, M. Fibre products of Artin-Schreier curves and generalized Hamming weights of codes. *J. Comb. Theory* (1995) **70**, 337–348.
12. Weil A. Number of solutions of equations in finite fields. *Bull. Amer. Math. Soc.* (1949) **55**, 497–508.

Статья поступила 12.05.1996.