Math-Net.Ru

Общероссийский математический портал

С. А. Степанов, Ф. Озбудак, Расслоенные произведения гиперэллиптических кривых и геометрические коды Гоппы, *Дискрет. матем.*, 1997, том 9, выпуск 3, 36–42

DOI: <https://doi.org/10.4213/dm490>

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: 34.229.108.108

26 апреля 2023 г., 12:03:37

Расслоенные произведения гиперэллиптических кривых и геометрические коды Гоппы

© 1997 г. С. А. Степанов, Ф. Озбудак

Цель этой работы перенести результаты первого автора [1] о построении достаточно длинных геометрических кодов Гоппы с хорошими значениями параметров над полем F_q , где $q = p^\nu$ и $\nu > 1$ четно, на случай конечных полей F_q с $q = p^\nu$ элементами, где $\nu > 1$ нечетно.

Работа выполнена при поддержке Университета в Билкенте, Анкара, Турция. Первый автор пользуется поддержкой Российского фонда фундаментальных исследований, грант 94-01-01206-а.

1. Введение

Напомним основные идеи предложенной Гоппой конструкции (см., например, [2] или [3]) линейных $[n, k, d]_q$ -кодов, связанных с гладкой проективной кривой X рода $g = g(X)$, определенной на конечном поле F_q . Пусть $\mathcal{P} = \{P_1, \dots, P_n\}$ — множество F_q -рациональных точек кривой X и

$$D_0 = P_1 + \dots + P_n.$$

Пусть D — F_q -рациональный дивизор на X , носитель которого не пересекается с D_0 . Рассмотрим векторное F_q -пространство рациональных функций на X

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

и обозначим $l(D)$ его размерность над F_q .

Линейный $[n, k, d]$ -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 код называется геометрическим кодом Гоппы. Если $\deg D < n$, то отображение Ev есть вложение и, следовательно, $k = \dim C = l(D)$ и согласно теореме Римана-Роха

$$k \geq \deg D - g + 1;$$

в частности, если $2g - 2 < \deg D < n$, то

$$k = \deg D - g + 1$$

Кроме того,

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

Теорема 1. Пусть $\nu > 1$ — нечетное число, F_q — конечное поле характеристики $p > 2$ с $q = p^\nu$ элементами и пусть s — целое число, удовлетворяющее неравенствам

$$1 \leq s < \frac{2p^\nu + 4}{p^{(\nu-1)/2}(p+1) - 2}.$$

Кроме того, пусть r — целое число, удовлетворяющее неравенствам

$$2^{s-2}((p^{(\nu-1)/2}(p+1) - 2)s - 4) < r < 2^s p^\nu.$$

Тогда существует линейный $[n, k, d]_q$ -код, для которого

$$\begin{aligned} r < n &\leq 2^s p^\nu, \\ k &= r - 2^{s-2}((p^{(\nu-1)/2}(p+1) - 2)s - 4), \\ d &\geq n - r. \end{aligned}$$

Следствие 1. Если выполнены условия теоремы 1, то существует линейный $[n, k, d]_q$ -код с относительными параметрами $R = k/n$ и $\delta = d/n$, удовлетворяющими неравенству

$$R \geq 1 - \delta - \frac{2^{s-2}((p^{(\nu-1)/2}(p+1) - 2)s - 4)}{n}.$$

В частности, если $n = 2^s p^\nu$, то

$$R \geq 1 - \delta - \frac{(p^{(\nu-1)/2}(p+1) - 2)s - 4}{4p^\nu}.$$

2. Обозначения и леммы

Пусть $\bar{F}_q$ — алгебраическое замыкание поля F_q и $\mathbb{A}^{s+1}$ — аффинное пространство размерности $s+1$ над $\bar{F}_q$.

Лемма 1. Пусть $f_1, f_2, \dots, f_s \in F_q[x]$ — попарно простые свободные от квадратов нормированные полиномы одной и той же степени $t \geq 3$ и Y — расслоенное произведение в $\mathbb{A}^{s+1}$ над полем $F_q[x]$ задаваемое уравнениями

$$\begin{aligned} z_1^2 &= f_1(x), \\ z_2^2 &= f_2(x), \\ &\dots \\ z_s^2 &= f_s(x). \end{aligned}$$

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

$$g = \begin{cases} (ms - 3)2^{s-2} + 1, & \text{если } t \text{ нечетно,} \\ (ms - 4)2^{s-2} + 1, & \text{если } t \text{ четно.} \end{cases}$$

Доказательство. Пусть I — идеал кривой Y в $\bar{F}_q[x, z_1, \dots, z_s]$ и $\bar{Y}$ — проективное замыкание Y в $\mathbb{P}^{s+1}$. Однородный идеал кривой $\bar{Y}$ в $\bar{F}_q[x_0, x, z_1, \dots, z_s]$ имеет вид $I_h = \{f_h \mid f \in I\}$, где

$$f_h(x_0, x, z_1, \dots, z_s) = f(x/x_0, z_1/x_0, \dots, z_s/x_0)x_0^{\deg f}.$$

Таким образом, как множество $\bar{Y} = Y \cup \{(0, 0, \pm 1, \pm 1, \dots, \pm 1)\}$, и кривая $\bar{Y}$ сингулярна в 2^{s-1} точках $P_i \in \{(0, 0, 1, \pm 1, \dots, \pm 1)\}$.

Пусть X — нормализация кривой $\bar{Y}$, которая в то же время есть неособая модель кривой $\bar{Y}$ (см., например, [4], Глава 2, §5.3). Существует конечный морфизм (регулярное отображение) $\varphi_1: X \rightarrow \bar{Y}$ и композиция φ_1 с φ_2 , где $\varphi_2: \bar{Y} \rightarrow \mathbb{P}^1$ такие, что $(x_0, x, z_1, \dots, z_s) \mapsto (x_0, x)$ определяет морфизм $\varphi: X \rightarrow \mathbb{P}^1$ степени 2^s (см., например, [4], Глава 2, §3.1). Так как $\bar{Y}$ имеет 2^{s-1} точек P_i , $1 \leq i \leq 2^{s-1}$, на гиперповерхности $x_0 = 0$, множество $\varphi^{-1}(0, 1)$ состоит из 2^s или из 2^{s-1} точек $\{Q_i\} \subseteq X$.

Пусть $\Omega[\bar{Y}]$ — пространство регулярных дифференциальных форм на $\bar{Y}$. Пространство $\Omega[\bar{Y}]$, рассматриваемое как $\bar{F}_q[x, z_1, \dots, z_s]$ -модуль, порождается элементами dx и dz_i , $1 \leq i \leq s$. Так как $z_i^2 = f_i(x)$, пространство $\Omega[\bar{Y}]$, рассматриваемое как $\bar{F}_q[x]$ -модуль, порождается элементами dx и $dx/(z_{i_1} \dots z_{i_\sigma})$, где $1 \leq i_1 < \dots < i_\sigma \leq s$. Далее, так как φ_1 есть морфизм, пространство $\Omega[X]$ есть подмодуль пространства $\Omega[\bar{Y}]$, откуда следует, что любая дифференциальная форма $\omega \in \Omega[X]$ имеет один из видов

$$\omega = F(x)dx, \quad \omega = \frac{F_{i_1, \dots, i_\sigma}(x)dx}{z_{i_1} \dots z_{i_\sigma}},$$

где $F, F_{i_1, \dots, i_\sigma} \in \bar{F}_q[x]$. Таким образом, произвольная регулярная дифференциальная форма из $\Omega[\bar{Y}]$ регулярна в любой точке кривой X , возможно за исключением $Q_i \in \varphi^{-1}(0, 1)$.

Пусть x есть координата на $\mathbb{P}^1$, тогда $u = x^{-1}$ есть локальный параметр в точке $(0, 1)$ на бесконечности. Так как x есть рациональная функция на $\mathbb{P}^1$, она определяет дивизор $(x) \in \text{Div}(\mathbb{P}^1)$. Обозначая $\varphi^{-1}(x) \in \bar{F}_q(X)$ через x и его дивизор через (x) , получаем дивизор поднятия $(x) \in \text{Div}(X)$.

Так как $\varphi^{-1}(0, 1)$ состоит из 2^s или 2^{s-1} точек Q_i , либо $v_{Q_i}(u) = 1$, либо $v_{Q_i}(u) = 2$ и поэтому либо $v_{Q_i}(x) = -1$, либо $v_{Q_i}(x) = -2$. Если $F(x)$ — регулярная функция на X , то соответственно $v_{Q_i}(F(x)dx) = -(\deg F(x) + 2)$ или $-(2 \deg F(x) + 3)$. Таким образом, $F(x)dx \notin \Omega[X]$ для любой $F(x) \in \bar{F}_q[X]$.

Если m чётно, то возможны два случая:

- (1) $v_{Q_i}(x) = -1$ and $v_{Q_i}(z_j) = -m/2$ для любого $j = 1, \dots, s$,
- (2) $v_{Q_i}(x) = -2$ и $v_{Q_i}(z_j) = -m$ для любого $j = 1, \dots, s$.

Поскольку

$$v_{Q_i} \left(\frac{F_{i_1, \dots, i_\sigma}(x)dx}{z_{i_1} \dots z_{i_\sigma}} \right) = v_{Q_i}(x) \deg F_{i_1, \dots, i_\sigma}(x) + (v_{Q_i}(x) - 1) - \sigma v_{Q_i}(z_j)$$

для любого $j = 1, \dots, s$, то соответственно

$$v_{Q_i} \left(\frac{F_{i_1, \dots, i_\sigma}(x)dx}{z_{i_1} \dots z_{i_\sigma}} \right) = \frac{m\sigma}{2} - \deg F_{i_1, \dots, i_\sigma}(x) - 2$$

или

$$v_{Q_i} \left(\frac{F_{i_1, \dots, i_\sigma}(x) dx}{z_{i_1} \dots z_{i_\sigma}} \right) = m\sigma - 2 \deg F_{i_1, \dots, i_\sigma}(x) - 3.$$

Таким образом,

$$\frac{F_{i_1, \dots, i_\sigma}(x) dx}{z_{i_1} \dots z_{i_\sigma}} \in \Omega[X]$$

тогда и только тогда, когда соответственно

$$\deg F_{i_1, \dots, i_\sigma}(x) \leq \frac{m\sigma}{2} - 2$$

или

$$\deg F_{i_1, \dots, i_\sigma}(x) \leq \frac{m\sigma}{2} - \frac{3}{2}$$

Так как m чётно, второе неравенство эквивалентно первому.

Если m нечётно и $v_{Q_i}(x) = -1$, то $v_{Q_i}(z_j^2) = 2v_{Q_i}(z_j) = -m$ и мы получаем противоречие. Таким образом, возможен только один случай, когда $v_{Q_i}(x) = -2$. В этом случае

$$\frac{F_{i_1, \dots, i_\sigma}(x) dx}{z_{i_1} \dots z_{i_\sigma}} \in \Omega[X],$$

только если

$$\deg F_{i_1, \dots, i_\sigma}(x) \leq \begin{cases} (m\sigma - 4)/2 & \text{если } \sigma \text{ чётно,} \\ (m\sigma - 3)/2 & \text{если } \sigma \text{ нечётно.} \end{cases}$$

Так как X — неособая кривая,

$$g = \dim_{\bar{F}_q} \Omega[X].$$

Таким образом, если m чётно, то

$$g = \frac{1}{2} \sum_{\sigma=1}^s \sum_{1 \leq i_1 < i_2, \dots, < i_\sigma \leq s} (m\sigma - 2) = (ms - 4)2^{s-2} + 1,$$

а если m нечётно, то

$$\begin{aligned} g &= \frac{1}{2} \sum_{\sigma=1}^s \sum_{1 \leq i_1 < i_2, \dots, < i_\sigma \leq s} (m\sigma - 2) + \frac{1}{2} \sum_{\sigma=1}^s \sum_{1 \leq i_1 < i_2, \dots, < i_\sigma \leq s} (m\sigma - 1) \\ &= (ms - 3)2^{s-2} + 1, \end{aligned}$$

где суммирование берётся только по нечётным σ .

Лемма доказана.

Лемма 2. Пусть $\nu > 1$ нечётно, F_q — конечное поле характеристики $p > 2$ с $q = p^\nu$ элементами и $f \in F_q[x]$ — полином вида

$$f(x) = (x + x^{p^{(\nu-1)/2}})(x + x^{p^{(\nu+1)/2}}).$$

Если c — ненулевой элемент поля F_q , то полиномы $f(x)$ и $f(x+c)$ взаимно просты.

Доказательство. Пусть $\mu = (\nu - 1)/2$ и $f'(x) = x^{p^\mu} + x$, $f''(x) = x^{p^{\mu+1}} + x$, так что $f'(x)f''(x) = f(x)$. Докажем, что $(f'(x), f'(x+c)) = (1)$ и $(f'(x), f''(x+c)) = (1)$ для любого $c \in F_{p^\nu}^*$. Отсюда будет следовать, что $(f(x), f(x+c)) = (1)$ для любого $c \in F_{p^\nu}^*$.

Заметим, что главный идеал I' , порождаемый полиномами $f'(x)$ и $f'(x+c)$, равен

$$I' = (x^{p^\mu} + x, x^{p^\mu} + x + c^{p^\mu} + c).$$

Уравнение

$$\alpha^{p^\mu} + \alpha = 0 \quad (1)$$

не имеет решения в $F_{p^\nu}^*$. Действительно, в противном случае $\alpha^{p^\mu-1} = -1$. Тогда $\alpha^{p^{2\mu}-1} = 1$, так как p нечетно и, следовательно, $2 \mid (p^\mu + 1)$. Таким образом, $\alpha \in F_{p^{\gcd(2\mu+1, 2\mu)}} = F_p$. Отсюда следует, что $\alpha^{p^\mu-1} = 1 \neq -1$, и мы получаем противоречие.

Используя алгоритм Евклида, нетрудно видеть, что если k, l , $k \geq l$, — положительные целые числа и $c \in F_{p^\nu}$, то главный идеал $(x^k + x + c, x^l + x)$ в $F_{p^\nu}[x]$ удовлетворяет соотношению

$$(x^k + x + c, x^l + x) = (x^l + x, -x^{k-l+1} + x + c).$$

Аналогично

$$(-x^k + x + c, x^l + x) = (x^l + x, x^{k-l+1} + x + c).$$

Объединяя эти соотношения, находим, что если $k \geq 2l - 1$ и k, l — положительные целые числа, то

$$(x^k + x + c, x^l + x) = (x^l + x, x^{k-2l+2} + x + c).$$

По индукции, если $l \mid k$ и $c \in F_{p^\nu}$, то

$$(x^k + x + c, x^l + x) = (x^l + x, (-1)^{k/l} x^{k/l} + x + c).$$

Используя это соотношение при $k = p^{\mu+1}$ и $l = p^\mu$, находим, что идеал $I'' = (f''(x+c), f'(x))$ представляется в виде

$$I'' = (x^{p^\mu} + x, -x^{p^\mu+1} + x + c^{p^{\mu+1}} + c).$$

Заметим теперь, что $(g'(x), g''(x)) \supset (g'(x), (g''(x))^p)$ для любых $h', h'' \in F_{p^\nu}[x]$. Поэтому

$$I'' \supset J = (x^{p^\mu} + x, -x^{p^{\mu+1}} + x^{p^\mu} + \gamma^{p^{\mu+1}} + \gamma)$$

где $\gamma = c^{p^\mu}$. Преобразуя порождающие элементы идеала J , получаем, что

$$\begin{aligned} J &= (x^{p^\mu} + x, -x^{p^{\mu+1}} - x + \gamma^{p^{\mu+1}} + \gamma) \\ &= (x^{p^\mu} + x, x^{p^{\mu+1}} + x - \gamma^{p^{\mu+1}} - \gamma). \end{aligned}$$

Покажем, что

$$c^{p^{\mu+1}} + c \neq -\gamma^{p^{\mu+1}} - \gamma. \quad (2)$$

Так как $\gamma = c^{p^\mu}$ и $c^{p^\nu} = c \in F_{p^\nu}^*$, неравенство (2) можно переписать в виде

$$c^{p^{\mu+1}} + c^{p^\mu} + 2c \neq 0. \quad (3)$$

Уравнение

$$\beta^{p^{\mu+1}} + \beta^{p^\mu} + 2\beta = 0 \quad (4)$$

не имеет решений в $F_{p^\nu}^*$. Действительно, возводя обе стороны (4) в степень p^μ , получаем равенства

$$\beta + \beta^{p^{2\mu}} + \beta^{p^\mu} + \beta^{p^\mu} = (\beta^{p^\mu} + \beta)^{p^\mu} + (\beta^{p^\mu} + \beta) = 0. \quad (5)$$

Поскольку (1) не имеет ненулевых решений, последнее уравнение также не имеет решений в $F_{p^\nu}^*$.

Теперь, поскольку $f''(x+c) = x^{p^{\mu+1}} + x + c^{p^{\mu+1}} + c \in I''$, $x^{p^{\mu+1}} + x - \gamma^{p^{\mu+1}} - \gamma \in J \subseteq I''$ и

$$c^{p^{\mu+1}} + c \neq -\gamma^{p^{\mu+1}} - \gamma,$$

заключаем, что $I'' = (1)$.

В силу симметрии $(f''(x), f''(x+c)) = (1)$ и $(f''(x), f'(x+c)) = (1)$. В силу однозначности факторизации в $F_{p^\nu}[x]$

$$(f'(x), f'(x+c)f''(x+c)) = (1), \quad (f''(x), f'(x+c)f''(x+c)) = (1),$$

откуда следует, что $(f(x), f(x+c)) = (1)$.

Пусть $\theta: F_q \rightarrow F_q$ — автоморфизм Фробениуса поля F_q над F_p , именно, $\theta(x) = x^p$. Пусть χ — мультипликативный характер F_p . Обозначим χ_ν характер поля F_q порожденный характером χ :

$$\chi_\nu(x) = \chi(\text{norm}_\nu(x)), \quad x \in F_q,$$

где

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

Легко видеть, что если p и ν нечетны, χ_ν порожден нетривиальным квадратичным характером поля F_p и $f(x) = (x + x^{p^{(\nu-1)/2}})(x + x^{p^{(\nu+1)/2}})$, то (см. [1], лемма 2)

$$\chi_\nu(f(x)) = \begin{cases} 1, & \text{если } x \in F_q^*, \\ 0, & \text{если } x = 0. \end{cases}$$

Положим

$$\tilde{f}(x) = \frac{f(x)}{x^2} = (1 + x^{p^{(\nu-1)/2-1}})(1 + x^{p^{(\nu+1)/2-1}}).$$

Тогда $\chi_\nu(\tilde{f}(x)) = 1$ для всех $x \in F_q$ и мы получили следующий результат.

Лемма 3. Пусть $\nu > 1$ нечетно, F_q — конечное поле характеристики $p > 2$ с $q = p^\nu$ элементами, $c_1, \dots, c_s$ — различные элементы поля F_q и N_q — число F_q -рациональных точек аффинной кривой Y , определяемой уравнениями

$$z_1^2 = f_1(x) = \tilde{f}(x + c_1),$$

$$z_2^2 = f_2(x) = \tilde{f}(x + c_2),$$

...

$$z_s^2 = f_s(x) = \tilde{f}(x + c_s).$$

Тогда

$$N_q = 2^s q.$$

Доказательство. Поскольку $\chi_\nu(f_i(x)) = \chi_\nu(\tilde{f}(x + c_i)) = 1$ для всех $x \in F_{p^\nu}$, $i = 1, \dots, s$,

$$N_q = \sum_{x \in F_{p^\nu}} (1 + \chi_\nu(f_1(x))) \dots (1 + \chi_\nu(f_s(x))) = \sum_{x \in F_{p^\nu}} 2^s = 2^s p^\nu.$$

3. Доказательство теоремы

Рассмотрим аффинную кривую

$$Y: z_i^2 = f_i(x) = \tilde{f}(x + c_i), \quad 1 \leq i \leq s,$$

где $c_1, \dots, c_s$ — различные элементы поля F_q . Число F_q -рациональных точек кривой Y в силу леммы 3 равно $N_q = 2^s q$. Кривая Y удовлетворяет условиям леммы 1, поэтому род $g = g(X)$ ее гладкой проективной модели X равен

$$g = 2^{s-2}((p^{\nu-1})^{1/2}(p+1) - 2)s - 4 + 1.$$

Пусть S — множество рациональных точек на Y и $S_1 \subset S$ — подмножество S . Применяя конструкцию Гоппы с

$$D_0 = \sum_{P \in S_1} P$$

и с

$$D = rP_\infty,$$

где $r < \deg D_0 = |S_1|$ и P_∞ — точка кривой X , соответствующая бесконечной точке проективизации $\tilde{Y}$ аффинной кривой Y , получаем, что $r < n \leq 2^s p^\nu$, $k \geq r + 1 - g$, $d \geq n - r$. Так как в рассматриваемом случае $2g - 2 < r = \deg D < n$, получаем, что $k = r + 1 - g$.

Список литературы

1. С. А. Степанов, Коды на расслоенных произведениях гиперэллиптических кривых. *Дискретная математика* (1997) **9**, №1, 83–94.
2. В. Г. Гоппа, Коды на алгебраических кривых. *Докл. АН СССР* (1981) **24**, 170–172.
3. И. Р. Шафаревич, *Основы алгебраической геометрии*. Наука, Москва.

Статья поступила 13.08.1996.