DOI: https://doi.org/10.15688/jvolsu1.2016.4.5
УДК 512.77
ББК 22.147

О КОНСТРУКЦИИ КРИВОЙ, СООТВЕТСТВУЮЩЕЙ ПОДКОДУ НАИМЕНЬШЕГО ВЕСА РАЦИОНАЛЬНОГО КОДА ГОППЫ

Юлия Сергеевна Касаткина

Старший преподаватель кафедры компьютерной безопасности,
Балтийский федеральный университет им. И. Канта
yuliya_kasatkina@list.ru
ул. А. Невского, 14, 236041 г. Калининград, Российская Федерация

Анна Сергеевна Касаткина

Преподаватель кафедры экономики и информационных технологий,
Западный филиал Российской академии народного хозяйства
и государственной службы
kasatkina_ana@mail.ru
ул. Артиллерийская, 18, 236016 г. Калининград, Российская Федерация

Аннотация. Исследуется конструкция кривых, ассоциированных с геометрическими кодами Гоппы. Для построения этих кривых используются подкоды малого веса. В работе изложен способ построения кривых, ассоциированных с рациональными кодами Гоппы.

Ключевые слова: геометрический код Гоппы, обобщенный вес кода, подкод наименьшего веса, алгебраическая кривая, способ построения кривой.

Введение

При построении эффективной системы связи, для защиты сообщения от ошибок используют помехоустойчивое кодирование, поэтому проблема получения новых кодов с хорошими характеристиками представляется актуальной. Конструкция некоторых классов кодов требует кривые, обладающие достаточным числом рациональных точек. Для построения таких кривых возможно использовать кодовые слова малого веса. Этим кодовым словам можно поставить в соответствие кривые Артина — Шрайера. Соответствие, в свою очередь, может быть продолжено до подкодов, на которых достигается обобщенный вес Хемминга, и расслоенного произведения кривых Артина — Шрайера.

В работе приводятся некоторые результаты, полученные в процессе построения кривых, в конструкции которых участвуют геометрические коды Гоппы $C_L(D,G)$ над конечным полем F_p с параметрами $[n,k]$.

1. Весовая иерархия и конструкция подкодов наименьшего веса

Алгебро-геометрический подход к теории кодирования информации начал развиваться в начале 80-х гг. прошлого столетия. Идея построения кодов на точках алгебраических кривых принадлежит Валерию Денисовичу Гоппе. Линейный код Гоппы, связанный с гладкой проективной кривой C над конечным полем, определяется следующим образом. Пусть C – абсолютно неприводимая гладкая проективная кривая над полем F_p. Пусть $P_1,\ldots,P_n$ есть различные F_p-рациональные точки на C и дивизор $D = P_1 + \ldots + P_n$. Дивизор $G \in Div(C)$ такой, что носители G и D не пересекаются. Линейное пространство

$$L(G) = \{f \in F_p(C)^* \,|(f) + G \geq 0\} \cup \{0\}$$

порождает линейное отображение

$$Ev : L(G) \to F_p^n, \quad f \mapsto (f(P_1),\ldots,f(P_n)).$$

Образ этого отображения есть линейный $[n,k]$-код $C_L(D,G)$ над конечным полем F_p.

Если C — линейный код длины n и размерности k, то носитель подкода $D \subset C$ определяют как множество номеров координат, в которых по крайней мере одно кодовое слово имеет ненулевую координату [4]. Обозначим носитель $\chi(D)$. Тогда

$$\chi(D) = \{i \,|\exists x = (x_1,\ldots,x_n) \in D, x_i \neq 0\}.$$

Количество элементов в носителе определяет вес подкода D:

$$\omega(D) = |\chi(D)|\,.$$

r-й обобщенный вес Хемминга кода равен весу, оказавшемуся наименьшим среди весов подкодов кода C, размерности r, то есть

$$d_r(C) = \min\{\omega(D) \,|D \subseteq C, \dim D = r\}, \ 1 \leq r \leq k.$$

Весовой иерархией кода C называется набор:

$$\{d_r(C) \,|1 \leq r \leq k\}.$$

Известно, что r-й обобщенный вес Хемминга кода $C_L(D, aP_\infty)$ может быть вычислен по формуле

$$d_r(C_L(D, aP_\infty)) = n - k + r, 1 \leq r \leq k.$$

Но, кроме иерархии весов кода, требуется явная конструкция подкода, на котором достигается обобщенный вес Хемминга. В частности, для геометрических кодов Гоппы вида $C_L(D, aP_\infty)$ подкоды минимального веса можно построить следующим образом.

Пусть D_r — r-мерный подкод F_p-кода C, носитель которого удовлетворяет условию

$$|\chi(D_r)| = d_r(C).$$

Предположим, что этот подкод порождается элементами $Ev(f_1), \ldots, Ev(f_r)$. Выполнение условия для носителя говорит о том, что в базисе кода D_r все кодовые слова имеют точно $n - d_r$ различных координат, значения которых равны нулю для всех элементов базиса. Или, формулируя вышесказанное в терминах дивизоров, получим

$$(f_i) = A + B_i - aP_\infty, 1 \leq i \leq r,$$

где дивизоры A и B_i такие, что:

$$0 \leq A \leq D, \deg A = n - d_r, B_i \geq 0, 1 \leq i \leq r.$$

Причем, носитель дивизора B_i может состоять из рациональных точек. Построенные таким образом элементы f_i, $1 \leq i \leq r$ представимы в виде:

$$f_i(x) = \prod_{j=1}^{a} (x - \alpha_{ij}), \alpha_{ij} \in F_p, 1 \leq i \leq r.$$

Дальнейшая конструкция требует представления полученного кода в виде след-кода.

2. Представление подкода в виде след-кода

Для того чтобы представить подкод наименьшего веса в виде следа некоторого кода, определенного над полем F_{p^m}, потребуется расширить поле констант. Напомним, что алгебраическое расширение F'/K' поля F/K называется расширением поля констант, если $F' = FK'$.

Рассмотрим поле рациональных функций $F_p(x)/F_p$. Тогда расширение $F_{p^m}(x)/F_{p^m}$ является расширением поля констант. В поле рациональных функций $F_p(x)/F_p$ существует точно $p+1$ точка степени один. Выясним поведение рациональных точек при подъеме поля констант.

Лемма. *Если P — рациональная точка поля $F_p(x)/F_p$, то в расширении $F_{p^m}(x)/F_{p^m}$ существует единственная точка степени один, лежащая над точкой P.*

Доказательство. Пусть Q точка поля $F_{p^m}(x)/F_{p^m}$, лежащая над точкой P. Тогда из условия

$$f(Q\,|P) \cdot \deg P = \deg Q \cdot m$$

следует, что относительная степень

$$f(Q\,|P) = \deg Q \cdot m.$$

Так как $f(Q\,|P) \leq m$, следовательно $\deg Q = 1$. Таким образом, над точкой P будут лежать только рациональные точки поля $F_{p^m}(x)/F_{p^m}$. Известно, что расширение поля констант не разветвлено, то есть индекс ветвления $e(Q\,|P) = 1$, для всех точек $P \in \in \mathrm{P}_{F_p(x)}$ и всех точек $Q \in \mathrm{P}_{F_{p^m}(x)}$ таких, что $Q\,|P$. Если $Q_1, \ldots, Q_r$ — все точки поля $F_{p^m}(x)/F_{p^m}$, лежащие над P, тогда из условия

$$\sum_{i=1}^{r} e(Q_i\,|P) \cdot f(Q_i\,|P) = m$$

заключаем, что $r = 1$. Следовательно, над точкой P будет лежать одна точка поля $F_{p^m}(x)/F_{p^m}$. Лемма доказана.

Пусть F'/K' — алгебраическое расширение поля F/K. Для точки $P \in \mathrm{P}_F$ конорма определяется следующим образом:

$$\mathrm{Con}_{F'/F}(P) = \sum_{Q|P} e(Q\,|P) \cdot Q,$$

где сумма берется по всем точкам Q, лежащим над точкой P, а целое число $e(Q\,|P)$ — индекс ветвления точки Q над P.

Для элемента $x - \alpha \in F_p(x)$ обозначим $(x - \alpha_p)_0^F$ — дивизор нулей этого элемента. Имеем

$$(x - \alpha_p)_0^F = P_\alpha.$$

Рассмотрим дивизор нулей этого же элемента в поле $F_{p^m}(x) = F'$:

$$(x - \alpha)_0^{F'} = \mathrm{Con}_{F'/F}((x - \alpha)_0^F) = \mathrm{Con}_{_{F'/F}}(P_\alpha) = \sum_{Q|P} e(Q\,|P) \cdot Q = Q.$$

Таким образом, точка Q, лежащая над точкой P_α, является единственным нулем элемента $x - \alpha$.

Пусть f_i — элементы поля $F_p(x)$, причем

$$f_i(x) = \prod_{j=1}^{a} (x - \alpha_{ij}), \alpha_{ij} \in F_p, 1 \le i \le r.$$

Каждому элементу f_i поставим в соответствие элемент $R_{f_i(x)}$, определяемый следующим образом:

$$R_{f_i(x)} = (\sum_{s=0}^{m-1} (bx)^{p^s})^{a-1} bx - \sum_{j=1}^{a} \alpha_{ij} (\sum_{s=0}^{m-1} (bx)^{p^s})^{a-2} bx +$$

$$+ \sum_{j \ne k}^{a} \alpha_{ij}\alpha_{ik} (\sum_{s=0}^{m-1} (bx)^{p^s})^{a-3} bx - \cdots + (-1)^{a-2} \sum_{j_1 < \ldots < j_{a-2}}^{a} \alpha_{ij_1} \cdot \ldots \cdot \alpha_{ij_{a-2}} \sum_{s=0}^{m-1} (bx)^{p^s} bx +$$

$$+ (-1)^{a-1} \sum_{j_1 < \ldots < j_{a-1}}^{a} \alpha_{ij_1} \cdot \ldots \cdot \alpha_{ij_{a-1}} bx + (-1)^a \alpha_i,$$

где $\mathrm{Tr}(\alpha_i) = \prod_{j=1}^{a} \alpha_{ij}$. Здесь Tr — отображение следа:

$$\mathrm{Tr} : F_{p^m} \to F_p,\ m \in Z,\ m > 1.$$

Элемент $b \in F_{p^m}$ такой, что $\mathrm{Tr}(b) = 1$.

Теорема. *Пусть D_r — r-мерный подкод F_p-кода $C = C_L(D, aP_\infty)$, носитель которого удовлетворяет условию $|\chi(D_r)| = d_r(C)$. Для любого кодового слова $c \in D_r$ существует элемент $R \in F_{p^m}[x]$ такой, что*

$$\mathrm{Tr}_{\mathrm{Con}_D}(R) = c.$$

Доказательство. Пусть D_r — r-мерный подкод F_p-кода Гоппы $C = C_L(D, aP_\infty)$. Предположим, что код D_r порождается кодовыми словами $c_1, \ldots, c_r$, где $c_i = Ev(f_i),\ 1 \leq \leq i \leq r$. Элементы $f_1, \ldots, f_r \in L(aP_\infty)$ являются линейно независимыми над F_p. Осуществим выбор базиса кода D_r таким образом, чтобы элементы $f_i,\ 1 \leq i \leq r$ допускали представление в виде

$$f_i(x) = \prod_{j=1}^{a} (x - \alpha_{ij}),$$

где $\alpha_{ij} \in F_p,\ 1 \leq i \leq r$. Каждому элементу $f_i(x)$ поставим в соответствие $R_i \in F_{p^m}[x]$. Пусть точка $P_s \in \mathrm{supp}(\mathrm{Con}(D)),\ 1 \leq s \leq n$, тогда

$$P_s = P_{x-\gamma_s},\ \gamma_s \in F_p.$$

Для точек $P_s \in \mathrm{supp}(\mathrm{Con}(D)),\ 1 \leq s \leq n$ выполняется

$$\mathrm{Tr}(R_i(P_s)) = f_i(\gamma_s).$$

Тогда для $1 \leq i \leq r$ получим

$$\mathrm{Tr}_{\mathrm{Con}(D)}(R_i) = \mathrm{Tr}(R_i(P_1), \ldots, R_i(P_n)) = (f_i(\gamma_1), \ldots, f_i(\gamma_n)) = c_i.$$

Пусть c — кодовое слово, тогда $c = \sum\limits_{i=1}^{r} \beta_i c_i,\ \beta_i \in F_p$, следовательно, получим

$$c = \sum_{i=1}^{r} \beta_i c_i = \sum_{i=1}^{r} \beta_i \,\mathrm{Tr}_{\mathrm{Con}(D)}(R_i) = \mathrm{Tr}_{\mathrm{Con}(D)}(\sum_{i=1}^{r} \beta_i R_i).$$

Теорема доказана.

Таким образом, если D_r — r-мерный подкод F_p-кода $C = C_L(D, aP_\infty)$, носитель которого удовлетворяет условию

$$|\chi(D_r)| = d_r(C),$$

элементы $R_1, \ldots R_r \in F_{p^m}(x)$ такие, что $\mathrm{Tr}_{\mathrm{Con}(D)}(R_i) = c_i,\ 1 \leq i \leq r$, где $c_1, \ldots, c_r$ — базис кода D_r, то, обозначив $U = \langle R_1, \ldots, R_r \rangle$ — r-мерное векторное пространство над полем F_p, получим

$$\mathrm{Tr}_{\mathrm{Con}(D)}(U) = D_r.$$

3. Анализ явного вида кривой, соответствующей подкоду наименьшего веса рационального кода Гоппы

Пусть D_r — r-мерный подкод рационального кода Гоппы $C_L(D, aP_\infty)$, носитель которого удовлетворяет условию

$$|\chi(D_r)| = d_r(C_L(D, aP_\infty)).$$

Элементам базиса c_{R_i} этого подкода поставим в соответствие кривые Артина — Шрайера C_{R_i} с аффинным уравнением

$$y_i^p - y_i = R_i(x), 1 \le i \le r,$$

здесь элемент $R_i(x) \in U$ соответствует слову c_{R_i}. F_p-векторное пространство $U \subseteq \subseteq F_{p^m}(x)$ и подкод D_r связывает следующее соотношение:

$$\mathrm{Tr}_{\mathrm{Con}(D)}(U) = \left\{ \mathrm{Tr}_{\mathrm{Con}(D)}(R) \,|R \in U \right\} = D_r,$$

где Tr — отображение следа

$$\mathrm{Tr} : F_{p^m} \to F_p.$$

Для элемента $R \in U$ обозначим $\varphi_R(T) = T^p - T - R \in F[T]$. Пусть E_U — поле разложения всех многочленов $\varphi_R(T)$ над полем $F = F_{p^m}(x)$. Многочлен $\varphi_R(T)$, соответствующий элементу $0 \neq R \in U$, либо неприводим над полем F, либо разлагается в произведение линейных сомножителей. Предположим последнее, то есть существует элемент $z \in F$, являющийся корнем $\varphi_R(T)$. Тогда $z^p - z = R$ и, кроме того, $\nu_{p_i}(z) \ge 0$ для всех точек $P_i \in \mathrm{P}_F$. Вычислим

$$\mathrm{Tr}_{\mathrm{Con}\,D}(R) = (\mathrm{Tr}(z^p - z)(P_1), \ldots, \mathrm{Tr}(z^p - z)(P_n)).$$

Полагая $\beta_i = z(P_i) \in F_{p^m},\ 1 \le i \le n$, получим:

$$\mathrm{Tr}_{\mathrm{Con}\,D}(R) = (\mathrm{Tr}(\beta_1^p - \beta_1), \ldots, \mathrm{Tr}(\beta_n^p - \beta_n)).$$

Тогда $\mathrm{Tr}_{\mathrm{Con}\,D}(R) = 0$. С другой стороны, $0 \neq R \in U$, следовательно, существуют элементы $\alpha_i \in F_p$ такие, что $R = \sum\limits_{i=1}^{r} \alpha_i R_i$. Вычислим

$$\mathrm{Tr}_{\mathrm{Con}(D)}(R) = \mathrm{Tr}(\sum_{i=1}^{r} \alpha_i R_i) = \sum_{i=1}^{r} \alpha_i \,\mathrm{Tr}_{\mathrm{Con}(D)}(R_i) = \sum_{i=1}^{r} \alpha_i c_i,$$

где c_i — кодовое слово, ассоциированное с элементом $R_i \in U$. Таким образом, имеем $\sum\limits_{i=1}^{r} \alpha_i c_i = 0$, что возможно только в случае равенства нулю всех коэффициентов $\alpha_i \in F_p$. Но это противоречит выбору элемента $0 \neq R \in U$, следовательно, многочлен $\varphi_R(T)$ неприводим. Поле E_U является полем разложения сепарабельных многочленов $\varphi_R(T)$ над F и, следовательно, расширение E_U/F является расширением Галуа.

Рассмотрим элементы $y_1, ..., y_r \in E_U$ такие, что

$$y_i^p - y_i = R_i,$$

тогда $E_U = F(y_1, ..., y_n)$. Обозначим $Gal(E_U/F)$ — группа Галуа расширения E_U/F. Отображение $\sigma : F \to F$ определим следующим образом:

$$\sigma(y_i) = y_i + \alpha_i,\ \alpha_i \in F_p,\ 1 \le i \le r,$$

тогда $\sigma \in Gal(E_U/F)$. Имеем

$$p^r \le |Gal(E_U/F)| = [E_U : F] \le p^r.$$

Таким образом, $[E_U : F] = p^r$. Кроме того, для всех $\sigma \in Gal(E_U/F)$ выполняется $\sigma^p = id$. Тогда расширение E_U/F является элементарным абелевым p-расширением [2].

Существует точно $\frac{p^r-1}{p-1}$ промежуточных полей $F \subset E \subset E_U$ степени $[E:F]=p$, каждое из которых определяется следующим образом:

$$E = E_R = F(y),\ y^p - y = R \in U\backslash\{0\}.$$

Таким образом, имеем E_U/F — элементарное абелево расширение степени p^r. Основные параметры этого расширения исследуются в работе [1]. Тогда существует элемент $y \in E_U$ такой, что $E_U = F(y)$, при этом минимальный многочлен элемента y над полем F имеет вид

$$\varphi(T) = T^{p^r} - T - z,\ z = \sum_{j=1}^{r}\sum_{i=0}^{r-1} \alpha^{j-1} R_j^{p^i}.$$

Поле E_U — поле рациональных функций кривой C_{D_r}, которая соответствует подкоду D_r. Таким образом, подкоду наименьшего веса соответствует кривая над полем F_{p^m}, задаваемая уравнением

$$y^{p^r} - y = \sum_{j=1}^{r}\sum_{i=0}^{r-1} \alpha^{j-1} R_j^{p^i}.$$

СПИСОК ЛИТЕРАТУРЫ

1. Касаткина, Ю. С. Анализ рода кривой, соответствующей подкоду наименьшего веса рационального кода Гоппы / Ю. С. Касаткина, А. С. Касаткина // Вестник Волгоградского государственного университета. Серия 1, Математика. Физика. — 2014. — № 4 (23). — С. 6–10.

2. Garcia, A. Elementary Abelian p-Extensions of Algebraic Function Fields / A. Garcia, H. Stichtenoth // Manuscripta math. — 1991. — Vol. 72. — P. 67–79.

3. Stichtenoth, H. Generalized Hemming Weights of Trace Codes / H. Stichtenoth, V. Voss // IEEE Trans. Inform. Theory. — 1994. — Vol. 40. — P. 554–558.

4. Wei, V. K. Generalized Hemming Weights for Linear Codes / V. K. Wei // IEEE Trans. Inform. Theory. — 1991. — Vol. 37. — P. 1412–1418.

REFERENCES

1. Kasatkina Yu.S., Kasatkina A.S. Analiz roda krivoy, sootvetstvuyushchey podkodu naimenshego vesa ratsionalnogo koda Goppy [On the Genus of the Curve Corresponding to the Subcode of Low Weight of a Rational Goppa Code]. *Vestnik Volgogradskogo gosudarstvennogo universiteta. Seriya 1, Matematika. Fizika* [Science Journal of Volgograd State University. Mathematics. Physics], 2014, no. 4 (23), pp. 6-10.

2. Garcia A., Stichtenoth H. Elementary Abelian P-Extensions of Algebraic Function Fields. *Manuscripta math.*, 1991, vol. 72, pp. 67-79.

3. Stichtenoth H., Voss V. Generalized Hemming Weights of Trace Codes. *IEEE Trans. Inform. Theory*, 1994, vol. 40, pp. 554-558.

4. Wei V.K. Generalized Hemming Weights for Linear Codes. *IEEE Trans. Inform. Theory*, 1991, vol. 37, pp. 1412-1418.

ON CONSTRUCTION OF THE CURVE CORRESPONDING TO THE SUBCODE OF LOW WEIGHT OF A RATIONAL GOPPA CODE

Yuliya Sergeevna Kasatkina

Senior Lecturer, Department of Computer Security,
Immanuel Kant Baltic Federal University
yuliya_kasatkina@list.ru
A. Nevskogo St., 14, 236041 Kaliningrad, Russian Federation

Anna Sergeevna Kasatkina

Lecturer, Department of Economics and Information Technology,
RANEPA (west branch)
kasatkina_ana@mail.ru
Artilleriyskaya St., 18, 236016 Kaliningrad, Russian Federation

Abstract. The theory of codes derived from algebraic curves was initiated by the works of V.D. Goppa. Since that time this theory has received an active development. Construction of certain classes of codes is based on the curves with sufficient number of rational points. In this paper we study curves arising from the subcode of low weight of a rational Goppa code.

According to algorithm of construction, first of all, it is necessary to represent subcode of low weight as a trace code. Let $C_L(D, aP_\infty)$ be a rational Goppa code over F_p with parameters [n, k] and let D_r denote the r-dimensional subcode of this code such that

$$|\chi(D_r)| = d_r(C_L(D, aP_\infty)).$$

We need to represent subcode of low weight as follows

$$\mathrm{Tr}_{\mathrm{Con}(D)}(U) = \left\{\mathrm{Tr}_{\mathrm{Con}(D)}(R)\,|R \in U\right\} = D_r,$$

where U is r-dimensional F_p-vector space and Tr is trace map

$$\mathrm{Tr} : F_{p^m} \to F_p.$$

Vector space U can be constructed in the following way. Let $\{c_1, ..., c_r\}$ be a basis of subcode of low weight of a rational Goppa code. Elements $R_1, ..., R_r$ correspond to elements of basis and can be constructed as

$$R_{f_i(x)} = (\sum_{s=0}^{m-1}(bx)^{p^s})^{a-1}bx - \sum_{j=1}^{a}\alpha_{ij}(\sum_{s=0}^{m-1}(bx)^{p^s})^{a-2}bx + \\ + \sum_{j\neq k}^{a}\alpha_{ij}\alpha_{ik}(\sum_{s=0}^{m-1}(bx)^{p^s})^{a-3}bx - \\ \cdots + (-1)^{a-2}\sum_{j_1<\ldots<j_{a-2}}^{a}\alpha_{ij_1}\cdot\ldots\cdot\alpha_{ij_{a-2}}\sum_{s=0}^{m-1}(bx)^{p^s}bx + \\ + (-1)^{a-1}\sum_{j_1<\ldots<j_{a-1}}^{a}\alpha_{ij_1}\cdot\ldots\cdot\alpha_{ij_{a-1}}bx + (-1)^a\alpha_i.$$

Thus we obtain $R_1, ...R_r \in F_{p^m}(x)$ such that $\mathrm{Tr}_{\mathrm{Con}(D)}(R_i) = c_i,\ 1 \leq i \leq r$, where $\{c_1, ..., c_r\}$ is a basis of D_r.

We denote $U = \langle R_1, \ldots, R_r \rangle$. Then U is r-dimensional F_p-vector space and

$$\mathrm{Tr}_{\mathrm{Con}(D)}(U) = D_r.$$

Let E_U be the function field of curve C_{D_r}, corresponding to the subcode of low weight D_r. So, the curve over field F_{p^m} corresponds to the subcode of low weight. The equation of this curve is

$$y^{p^r} - y = \sum_{j=1}^{r} \sum_{i=0}^{r-1} \alpha^{j-1} R_j^{p^i}.$$

Key words: geometric Goppa code, generalized Hemming weight of the code, subcode of low weight, algebraic curve, algorithm for constructing a curve.