ТРУДЫ II МЕЖДУНАРОДНОЙ КОНФЕРЕНЦИИ «ГЕОМЕТРИЧЕСКИЙ АНАЛИЗ И ЕГО ПРИЛОЖЕНИЯ»

УДК 512.77
ББК 22.147

АНАЛИЗ РОДА КРИВОЙ, СООТВЕТСТВУЮЩЕЙ ПОДКОДУ НАИМЕНЬШЕГО ВЕСА РАЦИОНАЛЬНОГО КОДА ГОППЫ

Касаткина Юлия Сергеевна

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

Касаткина Анна Сергеевна

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. Исследуются характеристики кривых, ассоциированных с геометрическими кодами Гоппы. Для построения этих кривых используются подкоды малого веса рационального кода Гоппы. В работе получена формула для рода кривой, соответствующей подкоду наименьшего веса.

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

Введение

Естественное направление развития теории кодирования связано с исследованием методов построения новых кодов. Конструкция Гоппы линейных кодов на гладких проективных кривых над конечными полями позволяет строить новые кривые, а следовательно, и линейные коды большей длины. 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 $[n,k]$.

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 $P_1,\ldots,P_n$ — различные F_p-рациональные точки на C и дивизор $D=P_1+\ldots+P_n$. Дивизор G 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.

1. Анализ рода 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

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

здесь элемент $R_i(x)\in U$ соответствует слову c_{R_i} [1]. F_p-векторное пространство $U\subseteq$ $\subseteq F_{p^m}(x)$ и подкод D_r связывает следующее соотношение:

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

где Tr — отображение следа

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

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, $\nu_{p_i}(z)\geq 0$, для всех точек $P_i\in \mathrm{P}_F$. Вычислим

$$Tr_{ConD}(R) = (Tr(z^p - z)(P_1), \ldots, Tr(z^p - z)(P_n)).$$

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

$$Tr_{ConD}(R) = (Tr(\beta_1^p - \beta_1), \ldots, Tr(\beta_n^p - \beta_n)).$$

Тогда $Tr_{ConD}(R) = 0$. 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

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

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. 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:

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

Тогда

$$g(E_U) = \sum_{i=1}^{t} g(E_i),\ t = \tfrac{p^r-1}{p-1},$$

здесь $g(E_i)$ — род промежуточного поля E_i такого, что

$$F_{p^m}(x) \subseteq E_i \subseteq E_U \text{ и } [E_i : F_{p^m}(x)] = p.$$

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}. Род этой кривой равен

$$g(C_{D_r}) = \sum_{i=1}^{t} g(E_i),\ t = \tfrac{p^r-1}{p-1},$$

СПИСОК ЛИТЕРАТУРЫ

1. Касаткина, Ю. С. Алгоритм построения элементарных абелевых кривых / Ю. С. Касаткина // Вестник Российского государственного университета им. И. Канта. Серия «Физико-математические науки». — 2006. — Вып. 10. — С. 109–112.

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. — 1994. — Vol. 40. — P. 554–558.

REFERENCES

1. Kasatkina Yu.S. Algoritm postroeniya elementarnykh abelevykh krivykh [On constraction of elementary abelian curves]. *Vestnik Rossiyskogo gosudarstvennogo universiteta im. I. Kanta. Seriya «Fiziko-matematicheskie nauki»*. 2006, iss. 10, pp. 109–112.

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.* 1994, vol. 40, pp. 554–558.

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

Kasatkina Yuliya Sergeevna

Senior Lecturer, Department of Computer Security,
Institute of Applied Mathematics and Information Technologies, Immanuel Kant Baltic Federal University
yuliya_kasatkina@list.ru
A.Nevskogo st., 14, 236041 Kaliningrad, Russian Federation

Kasatkina Anna Sergeevna

Lecturer, Department of Economics and Information Technology,
Russian Presidential Academy of National Economy and Public Administration (west branch)
kasatkina_ana@mail.ru
Artilleriyskaya st., 18, 236016 Kaliningrad, Russian Federation

Abstract. One of the main ways to provide correctness of information transmission via communication channels is the use of error-correcting codes. Construction of certain classes of codes is based on the curves with sufficient number of rational points. In this paper we study abelian curves.

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

$$Tr_{Con(D)}(U) = \{Tr_{Con(D)}(R) \,|R \in U\} = D_r,$$

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

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

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 genus of this curve is

$$g(C_{D_r}) = \sum_{i=1}^{t} g(E_i),\ t = \frac{p^r-1}{p-1},$$

Key words: geometric Goppa code, generalized Hemming weight of the code, subcode of low weight, algebraic curve, genus of an algebraic curve.