www.volsu.ru

DOI: https://doi.org/10.15688/mpcm.jvolsu.2019.3.2

УДК 512.77
ББК 22.147

Дата поступления статьи: 01.03.2019
Дата принятия статьи: 10.06.2019

АНАЛИЗ СТРУКТУРЫ ПОДКОДОВ МАЛОГО ВЕСА ОДНОГО КЛАССА РАЦИОНАЛЬНЫХ КОДОВ ГОППЫ

Юлия Сергеевна Касаткина

Преподаватель кафедры экономики и информационных технологий,
Западный филиал Российской академии народного хозяйства и государственной службы
yuliya_kasatkina@list.ru
ул. Артиллерийская, 18, 236016 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. Сужение на простое подполе одного класса рациональных кодов Гоппы приводит к классическим кодам Гоппы. В работе исследуется структура подкодов малого веса таких рациональных кодов. Получено описание, в терминах дивизоров, элементов, порождающих подкоды малого веса.

Ключевые слова: геометрический код Гоппы, обобщенный вес кода, весовая иерархия, подкод наименьшего веса.

Понятия обобщенный вес Хемминга и весовая иерархия линейного кода введены Вэем для характеристики поведения кода в каналах II типа. С другой стороны, если рассматривать линейный код как проективную систему, а минимальное расстояние кода описывать через максимальное число точек, лежащих в гиперплоскости, то проблема построения весовой иерархии равносильна вопросу о максимальном числе точек системы, лежащих в подпространстве коразмерности большей, чем единица. Весовые иерархии некоторых семейств кодов, например, кодов Рида – -Маллера, кодов Голея, БЧХ-кодов, кодов Гоппы, уже изучены.

В данной работе исследуется структура подкодов малого веса одного класса рациональных кодов Гоппы. Вопрос нахождения таких подкодов возникает при конструировании кривых с большим числом рациональных точек [1; 2]. Кроме того, задача нахождения кодовых слов наименьшего веса тесно связана с проблемами декодирования.

Мы рассматриваем геометрические коды Гоппы $C_L(D,G)$ ассоциированные с дивизорами D и G поля рациональных функций $F_q(x)$. Такие коды называются рациональными кодами Гоппы. Как обычно, предполагаем, что дивизор D является суммой различных точек степени один $D = P_1 + \ldots + P_n$ и носители дивизоров D и G не пересекаются.

Напомним, что в рациональном поле $F_q(x)/F_q$ нет других точек, кроме P_∞ и $P_{p(x)}$, где $p(x)$ -- неприводимый многочлен из кольца многочленов $F_q[x]$. Единственными рациональными точками поля $F_q(x)/F_q$ являются точки P_∞ и $P_{(x-\alpha)}$, где α -- элемент конечного поля F_q. Таким образом, в поле рациональных функций $F_q(x)/F_q$ имеется всего $q+1$ рациональная точка.

Код Гоппы $C_L(D,G)$ является образом пространства $L(G)$ при линейном отображении

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

Если степень дивизора G меньше n, то отображение $ev_D : L(G) \to C_L(D,G)$ является инъекцией. Кроме того, для рационального кода Гоппы $C_L(D,G)$ длины n, размерности k и с минимальным расстоянием d выполняется:

1. $n \leq q+1$.
2. $k = 0 \Leftrightarrow \deg G < 0$ и $k = n \Leftrightarrow \deg G > n-2$.
3. Если $0 \leq \deg G \leq n$, то $k = 1 + \deg G$ и $d = n - \deg G$.
4. Если $\{x_1, ..., x_n\}$ базис пространства $L(G)$, тогда матрица

$$M = \begin{pmatrix} x_1(P_1) & x_1(P_2) & \ldots & x_1(P_n) \\ \vdots & \vdots & & \vdots \\ x_k(P_1) & x_k(P_2) & \ldots & x_k(P_n) \end{pmatrix}$$

является порождающей матрицей кода $C_L(D,G)$ [3].

Опишем конструкцию одного вида рациональных кодов Гоппы. Этот класс кодов имеет тесную связь с классическими кодами Гоппы.

Пусть L некоторое подмножество мощности n конечного поля F_{q^m}

$$L = \{\alpha_1, ..., \alpha_n\} \subseteq F_{q^m}, \quad |L| = n.$$

Многочлен $g(x) \in F_{q^m}[x]$ степени t, такой, что $1 \leq t \leq n-1$ и $g(\alpha_i) \neq 0$ для всех $\alpha_i \in L$. Обозначим P_i – нуль элемента $(x - \alpha_i)$ для всех $\alpha_i \in L$. Дивизор D_L есть сумма точек степени один

$$D_L = P_1 + P_2 + ... + P_n.$$

Положим P_∞ – полюс элемента x поля рациональных функций $F_{q^m}(x)$. Дивизор нулей элемента $g(x)$ будем обозначать $G_0 \in Div(F_{q^m}(x)/F_{q^m})$.

Рассмотрим рациональный код Гоппы $C_L(D_L, G_0 - P_\infty)$. Длина этого кода равна n, размерность

$$k = 1 + \deg G = 1 + (t-1) = t$$

и минимальное расстояние

$$d = n - \deg G = n - t + 1.$$

Элементы поля рациональных функций $g(x)^{-1}$, $xg(x)^{-1}$, ..., $x^{t-1}g(x)^{-1}$ принадлежат пространству $L(G_0 - P_\infty)$. Размерность этого векторного пространства равна t. Таким образом, элементы $\{x^j g(x)^{-1}\}_{0 \le j \le t-1}$ образуют базис пространства $L(G_0 - P_\infty)$, а порождающая матрица рационально кода Гоппы $C_L(D_L, G_0 - P_\infty)$ имеет вид:

$$\begin{pmatrix} g(\alpha_1)^{-1} & g(\alpha_2)^{-1} & \dots & g(\alpha_n)^{-1} \\ \alpha_1 g(\alpha_1)^{-1} & \alpha_2 g(\alpha_2)^{-1} & \dots & \alpha_n g(\alpha_n)^{-1} \\ \vdots & \vdots & & \vdots \\ \alpha_1^{t-1} g(\alpha_1)^{-1} & \alpha_2^{t-1} g(\alpha_2)^{-1} & \dots & \alpha_n^{t-1} g(\alpha_n)^{-1} \end{pmatrix}.$$

Весовая иерархия кода $C_L(D_L, G_0 - P_\infty)$, то есть набор обобщенных весов Хемминга, определяется по формуле [4]:

$$d_r(C_L(D_L, G_0 - P_\infty)) = n - k + r, \text{ где } 1 \le r \le k.$$

В работе исследуется структура подкодов кода $C_L(D_L, G_0 - P_\infty)$, носители которых χ удовлетворяют условию

$$|\chi| = d_r(C_L(D_L, G_0 - P_\infty)).$$

Пусть D_r – r-мерный подкод кода $C_L(D_L, G_0 - P_\infty)$, обладающий наименьшим весом. Код D_r порождается r кодовыми словами $ev_D(f_1), \dots, ev_D(f_r)$, где $f_1, \dots, f_r$ – линейно независимые над полем F_{q^m} элементы пространства ассоциированного с дивизором $G_0 - P_\infty$. Условие $|\chi(D_r)| = d_r(C_L(D_L, G_0 - P_\infty))$ определяет структуру главных дивизоров (f_i)

$$(f_i) = D + B_i - (G_0 - P_\infty),\ 1 \le i \le r.$$

При этом дивизоры D и B_i такие, что

$$0 \le D \le D_L,\ \deg D = t - r$$

и

$$B_i \ge 0,\ \deg B_i = r - 1 \text{ для } 1 \le i \le r.$$

Заметим, что в конструкции дивизоров B_i возможно использование рациональных точек.

Рассмотрим, в качестве примера, рациональный код Гоппы $C_L(D_L, G_0 - P_\infty)$ над конечным полем F_{2^3}. Дивизор $D_L = P_{\alpha_1} + P_{\alpha_2} + ... + P_{\alpha_n}$ состоит из рациональных точек $P_{\alpha_i} = P_{(x-\alpha_i)}$, $\alpha_i \in L$ для всех $1 \le i \le n$. Множество L совпадает с полем F_{2^3}. В качестве многочлена $g(x)$ выберем многочлен $x^5 + x^2 + 1$. Таким образом, получим рациональный код Гоппы $C_L(D_L, G_0 - P_\infty)$ длины 8, размерности 5 и с минимальным расстоянием 4. Порождающая матрица этого кода имеет вид

$$\begin{pmatrix} 1 & 1 & \alpha^6 & \alpha^5 & \alpha^3 & \alpha^3 & \alpha^5 & \alpha^6 \\ 0 & 1 & 1 & 1 & \alpha^6 & 1 & \alpha^3 & \alpha^5 \\ 0 & 1 & \alpha & \alpha^2 & \alpha^2 & \alpha^4 & \alpha & \alpha^4 \\ 0 & 1 & \alpha^2 & \alpha^4 & \alpha^5 & \alpha & \alpha^6 & \alpha^3 \\ 0 & 1 & \alpha^3 & \alpha^6 & \alpha & \alpha^5 & \alpha^4 & \alpha^2 \end{pmatrix}.$$

Одномерный подкод наименьшего веса порождается элементом $ev_{D_L}(f)$ таким, что

$$(f) = P_{\alpha_{i_1}} + P_{\alpha_{i_2}} + P_{\alpha_{i_3}} + P_{\alpha_{i_4}} - (G_0 - P_\infty), \text{ где } P_{\alpha_{i_j}} \in supp(D_L), 1 \le j \le \deg D$$

или

$$(f) = \left(\frac{(x - \alpha_{i_1})(x - \alpha_{i_2})(x - \alpha_{i_3})(x - \alpha_{i_4})}{g(x)} \right).$$

Если $D = P_0 + P_1 + P_\alpha + P_{\alpha^2}$, то одномерный подкод D_1 порождается кодовым словом минимального веса

$$c = (0, 0, 0, 0, \alpha^5, \alpha, \alpha^2, \alpha^5).$$

Заметим, что число кодовых слов минимального веса для разделимого кода с максимальным расстоянием, определенного над полем F_q, равно $(q-1)C_n^d$. В нашем случае таких кодовых слов 490.

Второй обобщенный вес кода $C_L(D_L, G_0 - P_\infty)$ равен пяти. Двумерный подкод, носитель которого удовлетворяет условию $|\chi(D_2)| = d_2(C_L(D_L, G_0 - P_\infty))$ порождается элементами

$$(f_i) = D + B_i - (G_0 - P_\infty),\ 1 \le i \le 2.$$

При этом дивизоры D и B_i такие, что

$$0 \le D \le D_L,\ \deg D = 3$$

и

$$B_i \ge 0,\ \deg B_i = 1 \text{ для } 1 \le i \le 2.$$

Если дивизоры D, B_1, B_2 такие, что

$$D = P_0 + P_1 + P_\alpha,\ B_1 = P_{\alpha^2},\ B_2 = P_{\alpha^3},$$

то двумерный подкод наименьшего веса порождается векторами

$$c_1 = (0, 0, 0, 0, \alpha^5, \alpha, \alpha^2, \alpha^5) \quad c_2 = (0, 0, 0, \alpha, 0, \alpha^6, \alpha, \alpha^2).$$

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. — DOI: 10.15688/jvolsu1.2014.4.1.

2. Касаткина, Ю. С. О конструкции кривой, соответствующей подкоду наименьшего веса рационального кода Гоппы / Ю. С. Касаткина, А. С. Касаткина // Вестник Волгоградского государственного университета. Серия 1, Математика. Физика. — 2016. — № 4 (35). — С. 75 – 83. — DOI: 10.15688/jvolsu1.2016.4.5.

3. Stichtenoth, H. Algebraic Function Fields and Codes / H. Stichtenoth. — Berlin, Heidelberg : Springer-Verlag, 2009. — XIV+360 p. — DOI: 10.1007/978-3-540-76878-4.

4. Yang, K. On the weight hierarchy of geometric Goppa Codes / K. Yang, P. V. Kumar, H. Stichtenoth // IEEE Trans. Inform. Theory. — 1994. — Vol. 40, № 3. — P. 913-–920.

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. DOI: 10.15688/jvolsu1.2014.4.1.

2. Kasatkina Yu.S., Kasatkina A.S. O konstruktsii 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], 2016, no. 4 (35), pp. 75-83. DOI: 10.15688/jvolsu1.2016.4.5.

3. Stichtenoth H. *Algebraic Function Fields and Codes*. Berlin, Heidelberg, Springer-Verlag, 2009. XIV+360 p. DOI: 10.1007/978-3-540-76878-4.

4. Yang K., Kumar P.V., Stichtenoth H. On the Weight Hierarchy of Geometric Goppa Codes. *IEEE Trans. Inform. Theory*, 1994, vol. 40, no. 3, pp. 913-–920.

ON THE CONSTUCTION OF SUBCODES OF LOW WEIGHT OF A RATIONAL GOPPA CODE

Yuliya Sergeevna Kasatkina

Lecturer, Department of Economics and Information Technology,
RANEPA (west branch)
yuliya_kasatkina@list.ru
ul. Artilleriyskaya, 18, 236016 Kaliningrad, Russian Federation

Anna Sergeevna Kasatkina

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

Abstract. We consider the class of rational Goppa codes which is closely related to classical Goppa codes. In this paper, we study structure of subcodes of low weight of such rational Goppa codes. Firstly, we review some properties of rational Goppa codes. Finally, we analyze, in the term of divisors, construction of subcodes of low weight. Our analysis is based on the knowledge of weight hierarchy of codes.

Key words: geometric Goppa code, generalized Hemming weight of the code, weight hierarchy, subcode of low weight.