УДК 519.725

DOI: 10.21779/2542-0321-2021-36-2-15–19

Ю.С. Касаткина, А.С. Касаткина

Анализ структуры графа минимальных носителей одного класса рациональных кодов Гоппы

Российская академия народного хозяйства и государственной службы при Президенте РФ (Западный филиал); Россия, 236016, г. Калининград, ул. Артиллерийская, 18; yuliya_kasatkina@list.ru, kasatkina_ana@mail.ru

Алгебраические кривые с большим числом рациональных точек над конечным полем зачастую необходимы при решении задач, возникающих в теории помехоустойчивого кодирования. Некоторые методы построения алгебраических кривых над конечным полем основаны на использовании кодовых слов 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. Но такой способ построения алгебраической кривой над конечным полем требует знания не только весовой иерархии кода, но и структуры подкодов, на которых достигается минимальный вес. В свою очередь анализ минимальных слов кода позволяет изучить группу автоморфизмов этого линейного кода. Структура графа минимальных носителей линейного кода дает представление о группе автотопий этого линейного кода.

В нашей работе исследуется структура графа минимальных носителей одного геометрического кода Гоппы, ассоциированного с дивизорами поля рациональных функций. Для анализа весового спектра кода изучены основные характеристики этого кода. В работе получена оценка размерности и минимального расстояния исследуемого кода, что позволило сделать вывод о его принадлежности классу разделимых кодов с максимальным расстоянием над конечным полем. Кроме того, в работе исследовалось влияние параметра кода на структуру графа минимальных носителей. Получено описание структуры графа минимальных носителей кода для возможных случаев, возникающих при изменении параметра этого кода.

Ключевые слова: *код Гоппы, вес Хемминга, обобщенный вес Хемминга, граф минимальных носителей*.

Представление минимального веса Хемминга как некоторого минимального свойства одномерного подкода позволило получить обобщение этого понятия для подкодов большей размерности. Этот подход предложен в работе В.К. Вэй [1]. Обобщенные веса Хемминга характеризуют поведение линейного кода в WTC II. Такой канал передачи информации отличается отсутствием шума, и задача заключается в том, чтобы помешать третьему лицу получить слишком много информации. Кодер канала должен быть спроектирован так, чтобы максимизировать неопределенность третьего лица относительно данных в перехваченных им битах, при условии, что приемник может полностью восстановить исходное сообщение из битов полученного сообщения. Уста-

новлено, что изменение неопределенности третьего лица соответствует изменению обобщенного веса Хемминга.

В работе [2] на различных носителях ненулевых кодовых слов линейного кода вводится отношение частичного порядка. Минимальный носитель кода определяется как минимальный элемент по введенному порядку. Кодовое слово с минимальным носителем называется минимальным. На множестве минимальных носителей кода граф минимальных носителей определяется следующим образом: несовпадающие минимальные носители смежны в графе, если пересечение носителей не пусто. Аналогично вводится порядок на носителях подкодов. Линейный подкод U_1 размерности k называется минимальным, если для любого другого подкода U_2 размерности k из отношения $\mathrm{supp}\,(U_2) \subseteq \mathrm{supp}\,(U_1)$ следует *supp* (U_2) = *supp* (U_1).

Геометрический код Гоппы $C_L(D, G)$ длины n, определенный над полем F_p, является образом пространства $L(G)$ [3–5] при линейном отображении

$$ev_D: L(G) \longrightarrow F_p^n, \quad f \mapsto (f(P_1), \dots f(P_n)).$$

Различные точки $P_1, \dots, P_n$ функционального поля F/F_p степени один образуют носитель дивизора D, причем носители дивизоров D и G не пересекаются. Если степень дивизора G меньше n, то отображение $ev_D: L(G) \longrightarrow C_L(D, G)$ является инъекцией [6].

В нашей работе исследуется структура графа минимальных носителей рационального кода Гоппы $C_L(D, aP_\infty)$ ассоциированного с дивизорами поля рациональных функций $F_p(x)$. Предполагаем, что дивизор D является суммой всех различных рациональных точек поля $F_p(x)/F_p$, исключая бесконечно удаленную точку. Напомним, что в рациональном поле $F_p(x)/F_p$ нет других точек, кроме P_∞ и $P_{p(x)}$, где $p(x)$ – неприводимый многочлен из кольца многочленов $F_p(x)$. Единственными рациональными точками поля $F_p(x)/F_p$ являются точки P_∞ и $P_{(x-\beta)}$, где β – элемент конечного поля F_p.

Лемма. Пусть $C = C_L(D, aP_\infty)$ – рациональный код Гоппы над полем F_p длины n, размерности k и минимальным расстоянием d. Дивизор поля рациональных функций $D = P_0 + \dots + P_{p-1}$. Тогда

1) если $a < 0$, то $k = 0$;
2) если $a \geq p$, то $k = n$;
3) если $0 < a < p$, то $k = a + 1$ и $d = n - a$. Кроме того, в этом случае порождающая матрица кода имеет вид

$$\begin{pmatrix} 1(P_0) & 1(P_1) & \dots & 1(P_{p-1}) \\ x(P_0) & x(P_1) & \dots & x(P_{p-1}) \\ \vdots & \vdots & \dots & \vdots \\ x^a(P_0) & x^a(P_1) & \dots & x^a(P_{p-1}) \end{pmatrix}.$$

Доказательство. Отображение $ev_D: L(G) \longrightarrow C_L(D, G)$ является сюръективным линейным отображением пространства, ассоциированного с дивизором G, на пространство $C_L(D, G)$. Ядро этого отображения совпадает с векторным пространством, ассоциированным с дивизором $G - D$ [6]. Отсюда имеем

$$k = \dim C_L(D, G) = \dim L(G) - \dim L(G - D).$$

Если $a < 0$, то размерность пространства, ассоциированного с дивизором G, равна нулю, следовательно, равна нулю и размерность пространства, ассоциированного с дивизором $G - D$.

Если выполняется условие $a \geq p$, то, применяя теорему Римана–Роха, получаем $dim\ C_L\ (D,\ G) = n$.

Если $0 < a < p$, то отображение ev_D является инъективным отображением, а следовательно, $k = \deg G + 1$.

Минимальное расстояние кода имеет смысл только в случае, когда код $C_L(D, G) \neq 0$. Можно показать [6], что выполняется неравенство $d \geq n - deg\ G$. Учитывая это неравенство, имеем $k + d \geq n + 1$. Согласно границе Синглтона [7; 8] выполняется неравенство $k + d \leq n + 1$. Тогда $k + d = n + 1$. Отсюда получаем $d = n - deg\ G$.

Следствие. Рациональный код $C_L(D, aP_\infty)$ является разделимым кодом с максимальным расстоянием над конечным полем.

Утверждение 1. Если параметр a равен $p - 1$, то граф минимальных носителей кода несвязный и состоит из p изолированных вершин.

Действительно, количество кодовых слов минимального веса в таком коде равно $p\ (p - 1)$. Число кодовых слов минимального веса с различными носителями равно p, следовательно, граф минимальных носителей состоит из p вершин. Минимальное расстояние в этом случае равно 1, поэтому смежных вершин нет.

Утверждение 2. Если $1 \leq a < p - 1$, то граф минимальных носителей кода состоит из C_n^d вершин и является связным.

Для кода $C_L(D, aP_\infty)$ над конечным полем F_5 графы минимальных носителей представлены на рисунке

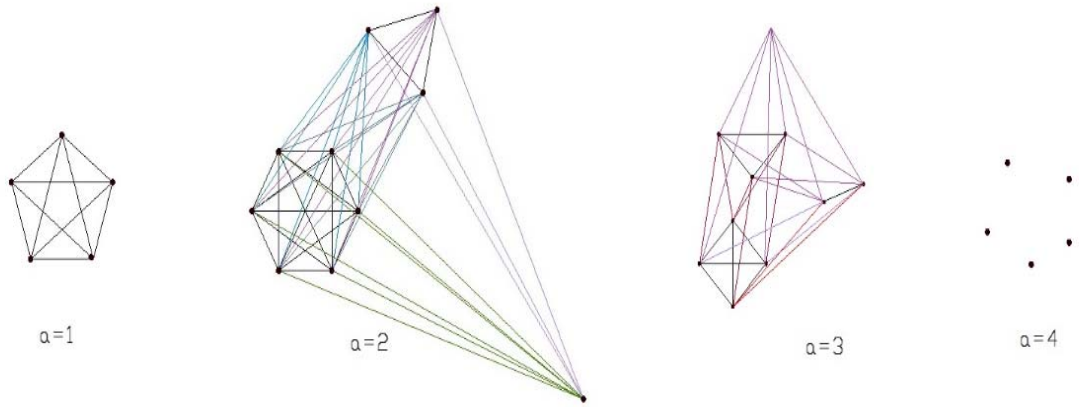

Рис. Графы минимальных носителей

Структура подкодов минимального веса анализируется в работах [9–10].

Литература

1. *Wei V.K.* Generalized Hemming Weights for Linear Codes // IEEE Trans. Inform. Theory. – 1991. – V. 37. – Pp. 1412–1418.

2. *Августинович С.В., Горкунов Е.В.* Об автоморфизмах линейных кодов над простым полем // Сиб. электрон. матем. изв. – 2017. – Т. 14. – С. 210–217.

3. *Гоппа В.Д.* Коды, ассоциированные с дивизорами // Пробл. передачи информ. – 1977. – Т. 13, вып. 1. – С. 33–39; Problems Inform. Transmission, – 1977. – iss. 1. – Vol. 13. – Pp. 22–27.

4. *Гоппа В.Д.* Коды на алгебраических кривых // Докл. АН СССР. – 1981. – Т. 259, вып. 6. – С. 1289–1290.

5. *Гоппа В.Д.* Алгебраико-геометрические коды // Известия АН СССР. Сер. матем. – 1982. – Т. 46, № 4. – С. 762–781.

6. Stichtenoth H. Algebraic Function fields and Codes // Springer. – 1993. – 260 p.

7. *Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А.* Теория кодов, исправляющих ошибки. – М.: Связь, 1979. – 744 с.

8. *Ling S., Xing C.* Coding theory: A first course. – Cambridge: Cambridge University Press, 2004. – 222 p.

9. *Касаткина Ю.С., Касаткина А.С.* О конструкции кривой, соответствующей подкоду наименьшего веса рационального кода Гоппы // Вестник Волгоградского государственного университета. Сер. 1: Математика. Физика. – 2016. – № 4 (35). – С. 75–83.

10. *Касаткина Ю.С., Касаткина А.С.* О представлении подкодов рационального кода Гоппы в виде след-кода // Алгебра, теория чисел и дискретная геометрия: современные проблемы и приложения. Материалы XIII Международной конференции, посвященной 85-летию со дня рождения профессора Сергея Сергеевича Рышкова / Тульский государственный педагогический университет им. Л.Н. Толстого. – Тула, 2015. – С. 195–199.

Поступила в редакцию 22 марта 2021 г.

UDC 519.725

DOI: 10.21779/2542-0321-2021-36-2-15–19

About the Structure of the Graph of Minimal Supports of One Class Rational Goppa Codes

Yu.S. Kasatkina, A.S. Kasatkina

Russian Presidential Academy of National Economy and Public Administration; Russia, 236016, Kaliningrad, Artilleriyskaya st., 18; yuliya_kasatkina@list.ru, kasatkina_ana@mail.ru

We often need algebraic curves over finite fields with many rational points to solve some problems of the coding theory. Some methods for constructing algebraic curves over a finite field are based on the use of low weight codewords. These codewords can be associated with the Artin-Schreier curves. The correspondence can be extended to subcodes and the fibred product of Artin-Schreier curves. But this method of constructing an algebraic curve over a finite field requires knowledge of not only the weight hierarchy of the code, but also the structure of the subcodes on which the mini-

mum weight is achieved. In turn, the analysis of the minimal words of the code allows one to study the group of automorphisms of this linear code.

In this paper we study the structure of the graph of minimal supports of the geometric Goppa code associated with the divisors of a rational function field. We studied the construction of this code to obtain the distribution of weights for this code. We got a description of the graph structure for possible cases arising when changing a code parameter. Besides, the influence of the code parameter on the graph structure of minimum codewords. As a result, the description of all possible graph structure minimum codewords arising under the transformations of the code parameters is given.

Keywords: *Goppa code, Hamming weight, generalized Hamming weight, graph of minimal supports.*

Received 22 March 2021