Неабелевы групповые коды над произвольным конечным полем

К. ГАРСИА-ПИЛЬЯДО
Университет Овьедо, Испания

С. ГОНСАЛЕС
Университет Овьедо, Испания

В. Т. МАРКОВ
Московский государственный университет им. М. В. Ломоносова
e-mail: vtmarkov@yandex.ru

К. МАРТИНЕС
Университет Овьедо, Испания

УДК 519.725+512.552.7

Ключевые слова: групповой код, линейный код, групповое кольцо.

Аннотация

Доказано существование неабелева группового кода над произвольным конечным полем.

Abstract

C. García Pillado, S. González, V. T. Markov, C. Martínez, Non-Abelian group codes over an arbitrary finite field, Fundamentalnaya i prikladnaya matematika, vol. 20 (2015), no. 1, pp. 17—22.

We prove that there exist non-Abelian group codes over an arbitrary finite field.

1. Введение

Изучение групповых кодов было начато давно (см., например, [1]), но только в [6] было дано определение группового кода, не зависящее от упорядочивания элементов группы.

Пусть F — конечное поле, G — конечная группа, FG — групповое кольцо.

Определение 1. Линейный код $\mathcal{K}$ длины n над F называется (*левым*) *G-кодом*, если существует такое биективное отображение $\nu\colon \{1,\dots,n\} \to G$, что множество

$$I = \left\{ \sum_1^n a_i \nu(i) \colon (a_1, ..., a_n) \in \mathcal{K} \right\} -$$

Фундаментальная и прикладная математика, 2015, том 20, № 1, с. 17—22.

(левый) идеал кольца FG. Говорят также, что (левый) идеал I *определяет* код $\mathcal{K}$.

Код называется (*левым*) *групповым кодом*, если он является (левым) G-кодом для некоторой группы G. Код называется *абелевым* групповым кодом, если он является A-кодом для некоторой абелевой группы A.

Некоторый класс некоммутативных групп G, для которых все G-коды абелевы, даёт следующая теорема.

Теорема 2 [6]. *Если G — конечная группа и*

$$G = AB = \{ab\colon a \in A,\ b \in B\}$$

для некоторых абелевых подгрупп A, B группы G, то любой G-код является абелевым групповым кодом.

Из этой теоремы следует, что если порядок группы G меньше 24, то любой G-код является абелевым групповым кодом.

Легко убедиться, что количество идеалов групповой алгебры FG при условии $\operatorname{char} F \nmid |G|$ ограничено функцией $2^{C(G)}$, где $C(G)$ обозначает число классов сопряжённых элементов группы G. Поэтому, вообще говоря, групповая алгебра некоммутативной группы содержит меньше идеалов, чем групповая алгебра абелевой группы того же порядка над тем же полем. Для левых идеалов групповых алгебр ситуация иная: их число в случае некоммутативной группы неограниченно возрастает при росте мощности поля при фиксированной характеристике. Из этого замечания в [6] выведено существование неабелевых левых G-кодов над некоторым полем для произвольной некоммутативной группы G. Независимо примеры неабелевых левых групповых кодов были найдены в [4].

Первый пример неабелева группового кода был построен в [2, 7] с помощью компьютера; это был S_4-код размерности 9 над полем $\mathbb{F}_5$. Позже были построены примеры неабелевых S_4-кодов и $\mathrm{SL}_2(\mathbb{F}_3)$-кодов над полями $\mathbb{F}_3$ [3] и $\mathbb{F}_2$ [5]. В [5] была также высказана гипотеза о существовании неабелевых $\mathrm{SL}_2(\mathbb{F}_3)$-кодов размерности 4 над произвольным полем $\mathbb{F}_p$ при $p \geqslant 5$ (к тому моменту она была проверена с помощью компьютера для всех простых чисел p от 5 до 97).

Основной результат настоящей заметки — доказательство следующей теоремы, из которой, в частности следует справедливость упомянутой гипотезы.

Теорема 3. *Пусть $F = \mathbb{F}_p$, и пусть либо $G = \mathrm{SL}_2(\mathbb{F}_3)$ и $p \geqslant 5$, либо $G = S_4$ и $p \geqslant 3$. Тогда существует неабелев G-код над полем F, имеющий размерность* 9 *или* 4 *соответственно.*

Из теоремы 3, существования неабелевых групповых кодов над полями $\mathbb{F}_3$ и $\mathbb{F}_2$ и теоремы 5.1. из [8] о том, что если все G-коды над полем F абелевы, то и все G-коды над любым подполем поля F абелевы, вытекает следствие.

Следствие 4. *Над произвольным конечным полем существует неабелев групповой код длины* 24.

2. Подмодули и идеалы групповых колец

В этом разделе мы рассмотрим идеалы групповых колец конечных групп над, возможно, бесконечными кольцами с единицей.

Определение 5. Пусть R — кольцо, G — конечная группа. Для любого элемента

$$r = \sum_{g \in G} a_g g \in RG$$

определим его *носитель* и *вес*:

$$\operatorname{supp}(r) = \{g \in G \colon a_g \neq 0\}, \quad \|r\| = |\operatorname{supp}(r)|.$$

Назовём *минимальным расстоянием* произвольного ненулевого R-подмодуля $\mathcal{C} \subseteq RG$ число

$$d(\mathcal{C}) = \min\bigl\{\|x\| \colon x \in \mathcal{C} \setminus \{0\}\bigr\}.$$

Элементы веса $d(\mathcal{C})$ будем называть *элементами минимального веса* подмодуля $\mathcal{C}$. Элемент

$$r = \sum_{g \in G} a_g g \in RG$$

назовём *U-элементом*, если $a_g = 1$ или $a_g = -1$ для любого элемента $g \in \operatorname{supp}(r)$. Множество носителей U-элементом минимального веса подмодуля $\mathcal{C}$ обозначим через $S(\mathcal{C})$.

Определение 6. Пусть $f \colon R \to S$ — унитарный гомоморфизм колец, G — группа. Обозначим через $f \colon RG \to SG$ *продолжение* гомоморфизма f на групповое кольцо RG, заданное правилом

$$\hat{f}\biggl(\sum_{g \in G} a_g g\biggr) = \sum_{g \in G} f(a_g) g \quad \text{для всех} \quad \sum_{g \in G} a_g g \in RG.$$

Следующая лемма носит технический характер.

Лемма 7. *Пусть R, $\bar{R}$ — два кольца, G — конечная группа. Допустим, что R-подмодуль $\mathcal{C}$ группового кольца RG и сюръективный гомоморфизм колец $f \colon R \to \bar{R}$ удовлетворяют следующим условиям:*

- *модуль $\mathcal{C}$ порождён U-элементами минимального веса;*
- *$d\bigl(\hat{f}(\mathcal{C})\bigr) = d(\mathcal{C})$;*
- *$S\bigl(\hat{f}(\mathcal{C})\bigr) = S(\mathcal{C})$;*
- *$1 + 1 \neq 0$ in $\bar{R}$.*

Если $\hat{\pi}(\mathcal{C})$ — идеал кольца $\bar{R}G$, то $\mathcal{C}$ — идеал кольца RG.

Доказательство. Ввиду i) достаточно проверить, что если $r \in \mathcal{C}$ — U-элемент минимального веса в $\mathcal{C}$, то $gr \in \mathcal{C}$ и $rg \in \mathcal{C}$ для любого элемента $g \in G$.

Рассмотрим элемент gr. Его образ $\hat{f}(gr) = g\hat{f}(r)$ принадлежит $\hat{f}(\mathcal{C})$ и является U-элементом минимального веса в $\hat{f}(\mathcal{C})$. Согласно iii) существует U-элемент u из $\mathcal{C}$, для которого

$$\operatorname{supp}(u) = \operatorname{supp}\bigl(g\hat{f}(r)\bigr) = \operatorname{supp}(gr).$$

Положим

$$u = \sum_{h \in G} a_h h, \quad gr = \sum_{h \in G} b_h h,$$

где $a_h, b_h \in \{-1, 0, 1\}$ для всех $h \in G$. Выберем произвольный элемент $h \in$ $\in \operatorname{supp}(u)$. Тогда либо $a_h = b_h$, либо $a_h = -b_h$. В первом случае $\hat{f}(gr - u)$ — элемент модуля $\hat{\pi}(\mathcal{C})$ и $\|\hat{f}(gr - u)\| < \|(u)\| = d(\mathcal{C}) = d\big(\hat{f}(\mathcal{C})\big)$, откуда следует, что $\hat{f}(gr) = \hat{f}(u)$. Но тогда $gr = u$, так как и u и $rg - U$-элементы. Во втором случае применяем то же рассуждение к элементу $\hat{f}(gr + u)$. Итак, либо $gr = u$, либо $gr = -u$, значит, $gr \in \mathcal{C}$.

Включение $rg \in \mathcal{C}$ доказывается аналогично. □

3. Построение неабелевых групповых кодов

В этом разделе мы существенно используем результаты вычислений с помощью пакета GAP [9].

Доказательство теоремы 3. Сначала рассмотрим случай группы $G = S_4$. Функция `CentralIdempotentsOfAlgebra` пакета GAP, применённая к групповой алгебре $\mathbb{Q}G$, даёт список минимальных центральных идемпотентов этой алгебры. Учитывая результаты предыдущих экспериментов, выберем идемпотент

$$e = \frac{3}{8}\mathcal{E} - \frac{1}{8}s_2 - \frac{1}{8}s_{2,2} + \frac{1}{8}s_4 \in \mathbb{Q}G,$$

где s_α обозначает сумму всех перестановок, имеющих цикловой тип α.

Рассмотрим кольцо $R = \mathbb{Z}\left[\frac{1}{2}\right]$. Тогда $e \in RG$ и $RGe = RG \cap \mathbb{Q}Ge$, поскольку RGe — аннулятор элемента $\mathcal{E} - e$ в кольце RG.

Зафиксировав некоторую нумерацию элементов группы G, мы можем представлять элементы кольца $\mathbb{Q}G$ строками рациональных чисел. Применяя функцию `NullspaceIntMat` пакета GAP, получаем целочисленную матрицу M размера 9×24, строки которой образуют базис абелевой группы $\mathbb{Z}G \cap \mathbb{Q}Ge$. Очевидно, что эти же строки образуют R-базис модуля RGe и $\mathbb{Q}$-базис векторного пространства $\mathbb{Q}Ge$.

Перебирая все подматрицы M' матрицы M, имеющие размер 9×16, делаем следующее:

- проверяем, что $\operatorname{rk} M' = 9$ или $\operatorname{rk} M' = 8$;
- проверяем, что если $\operatorname{rk} M' = 8$ и v_0 — целочисленный вектор, порождающий группу $\{v \colon vM' = 0\}$, то $u_0 = v_0 M$ — целочисленный вектор веса 8 и $u_0 = ku$, где u представляет U-элемент и k — целое число, обратимое в R;
- подсчитывая количество матриц M', для которых $\operatorname{rk} M' = 8$, получаем, что $|S(RGe)| = 162$ и что U-элементы веса 8 порождают модуль RGe;
- применяя к каждой матрице M' функцию `ElementaryDivisorsMat`, проверяем, что $\operatorname{rk} M'$ не меняется при замене M' на $M' \pmod p$, если p — простое число и $p > 2$.

Пусть $p > 2$ — простое число. Тогда существует естественный гомоморфизм $\pi\colon R \to \mathbb{F}_p$. Из перечисленных свойств матрицы M вытекает, что расширение $\hat{\pi}_G$ удовлетворяет условиям леммы 7.

Теперь допустим, что $\hat{\pi}_G(RGe)$ определяет абелев групповой код. Тогда существуют абелева группа A и биективное отображение $\sigma\colon G \to A$, такие что $\tilde{\sigma}\big(\hat{\pi}(RGe)\big)$ — идеал кольца $\mathbb{F}_pA$, где $\tilde{\sigma}\colon \mathbb{F}_pG \to \mathbb{F}_pA$ обозначает естественное продолжение σ на групповые кольца (мы будем использовать это обозначение для различных колец коэффициентов).

Имеем коммутативную диаграмму

$$\begin{array}{ccc} RG & \xrightarrow{\ \tilde{\sigma}\ } & RA \\ {\scriptstyle\hat{\pi}_G}\downarrow & & \downarrow{\scriptstyle\hat{\pi}_A} \\ \mathbb{F}_pG & \xrightarrow[\ \tilde{\sigma}\ ]{} & \mathbb{F}_pA \end{array}.$$

Следовательно, гомоморфизм $\hat{\pi}_A$ также удовлетворяет условиям леммы 7. Таким образом, $I = \tilde{\sigma}(RGe)$ — идеал кольца RA и $\mathbb{Q}I$ — идеал кольца $\mathbb{Q}A$, причём

- $\dim \mathbb{Q}I = 9$;
- $d(\mathbb{Q}I) = 8$;
- существует базис $\mathbb{Q}I$, состоящий из U-элементов;
- все элементы минимального веса в $\mathbb{Q}I$ — это скалярные кратные U-элементов;
- $|S(\mathbb{Q}I)| = 162$.

Вычисления для каждого идеала размерности 9 в $\mathbb{Q}A$ для всех трёх абелевых групп A порядка 24 показывают, что идеалов, удовлетворяющих указанным условиям, не существует, что и доказывает теорему 3 для случая $G = S_4$.

Теперь положим $G = \mathrm{SL}(2, \mathbb{F}_3)$ и возьмём идемпотент $e \in \mathbb{Q}G$, такой что

$$\begin{aligned} 12e = {} & 2\begin{pmatrix}1&0\\0&1\end{pmatrix} - 2\begin{pmatrix}2&0\\0&2\end{pmatrix} + \begin{pmatrix}0&1\\2&1\end{pmatrix} - \begin{pmatrix}0&1\\2&2\end{pmatrix} - \begin{pmatrix}0&2\\1&2\end{pmatrix} + \begin{pmatrix}1&1\\2&0\end{pmatrix} + \\ & + \begin{pmatrix}0&2\\1&1\end{pmatrix} - \begin{pmatrix}1&0\\1&1\end{pmatrix} - \begin{pmatrix}1&0\\2&1\end{pmatrix} - \begin{pmatrix}1&1\\0&1\end{pmatrix} - \begin{pmatrix}1&2\\0&1\end{pmatrix} + \begin{pmatrix}1&2\\1&0\end{pmatrix} + \\ & + \begin{pmatrix}2&0\\1&2\end{pmatrix} + \begin{pmatrix}2&0\\2&2\end{pmatrix} + \begin{pmatrix}2&1\\0&2\end{pmatrix} - \begin{pmatrix}2&1\\2&0\end{pmatrix} + \begin{pmatrix}2&2\\0&2\end{pmatrix} - \begin{pmatrix}2&2\\1&0\end{pmatrix}. \end{aligned}$$

Легко убедиться, что коэффициенты e принадлежат кольцу $\mathbb{Z}\left[\frac{1}{6}\right]$, и доказательство для $p > 3$ проходит аналогично предыдущему случаю с единственным отличием. Мы заметили, что идеал $I = \mathbb{Q}Ge$ имеет важное дополнительное свойство: для любого элемента из $I \cap \mathbb{Z}G$ хотя бы один его коэффициент делится на 5. Это существенно уменьшает число подлежащих проверке идеалов в кольцах $\mathbb{Q}A$, где A — одна из трёх абелевых групп порядка 24, и среди них нет идеалов размерности $\dim I = 4$ с минимальным расстоянием $d(I) = 12$. Таким образом, теорема 3 доказана. □

Литература

[1] Берман С. Д. О теории групповых кодов // Кибернетика. — 1967. — Т. 3. — С. 31—39.

[2] Гарсиа-Пильядо К., Гонсалес С., Марков В. Т., Мартинес К., Нечаев А. А. Когда все групповые коды некоммутативной группы абелевы (вычислительный подход)? // Фундамент. и прикл. матем. — 2011/2012. — Т. 17, вып. 2. — С. 75—85.

[3] Гарсиа Пильядо К., Гонсалес С., Марков В. Т., Мартинес К., Нечаев А. А. Неабелевы групповые коды // Учёные записки Орловск. гос. ун-та. — 2012. — Т. 6, № 2. — С. 73—79.

[4] Коусело Е., Гонсалес С., Марков В., Нечаев А. Групповые коды и их неассоциативные обобщения // Дискрет. мат. — 2004. — Т. 16, № 1. — С. 146—156.

[5] Марков В. Т. Абелевы и неабелевы групповые коды над некоммутативными группами // Алгебра и теория чисел: современные проблемы и приложения: Материалы XII Международной конференции, посвящённой 80-летию профессора Виктора Николаевича Латышева. Тула, 21—25 апреля 2014 г. — Тула: Изд-во ТГПУ им. Л. Н. Толстого, 2014. — С. 200—203.

[6] Bernal J. J., del Río Á., Simón J. J. An intrinsical description of group codes // Designs, Codes and Cryptography. — 2009. — Vol. 51, no. 3. — P. 289—300.

[7] García Pillado C., González S., Markov V., Martínez C., Nechaev A. Group codes which are not Abelian group codes // Proc. of the Third Int. Castle Meeting on Coding Theory and Applications. — 2011. — P. 123—127.

[8] García Pillado C., González S., Markov V. T., Martínez C., Nechaev A. A. Group codes over non-Abelian groups // J. Algebra Its Appl. — 2013. — Vol. 12, no. 7. — P. 135037.

[9] http://www.gap-system.org/