*Моделирование и анализ информационных систем.* Т. 25, №2 (2018), с. 232–245
*Modeling and Analysis of Information Systems.* Vol. 25, No 2 (2018), pp. 232–245

Кодовые криптосистемы



**DOI:** 10.18255/1818-1015-2018-2-232-245

УДК 517.9

# Коды в диэдральной групповой алгебре

**Веденёв К. В., Деундяк В. М.**

*получена 2 декабря 2017*

**Аннотация.** В 1978 году Р. Мак-Элисом построена первая асимметричная кодовая криптосистема, основанная на применении помехоустойчивых кодов Гоппы, при этом эффективные атаки на секретный ключ этой криптосистемы до сих пор не найдены. К настоящему врмени известно достаточно много кодовых криптосистем, но их криптографическая стойкость уступает стойкости классической криптосистемы Мак-Элиса. В связи с развитием квантовых вычислений кодовые криптосистемы рассматриваются как альтернатива теоретико-числовым, поэтому актуальной представляется задача поиска перспективных классов кодов для построения новых стойких кодовых криптосистем. Для этого можно использовать некоммутативные коды, т.е. идеалы в групповых алгебрах $\mathbb{F}_q G$ над конечными некоммутативными группами $G$. Ранее изучалась стойкость криптосистем на кодах, индуцированных кодами на подгруппах. Важной для исследования некоммутативных кодов является теорема Веддерберна, доказывающая существование изоморфизма групповой алгебры на прямую сумму матричных алгебр, но конкретный вид слагаемых и конструкция изоморфизма этой теоремой не определены, и поэтому для каждой группы остается задача построения представления Веддерберна. Ф. Е. Б. Мартинесом получено полное представление Веддерберна для групповой алгебры $\mathbb{F}_q D_{2n}$ над диэдральной группой $D_{2n}$ в случае, когда мощность поля и порядок группы взаимно просты. С использованием этих результатов в настоящей работе исследуются коды в групповой алгебре $\mathbb{F}_q D_{2n}$. Решена задача о структуре всех кодов и описана структура кодов, которые индуцированы кодами над циклическими подгруппами группы $D_{2n}$, что представляет интерес для криптографических приложений.

**Ключевые слова:** некоммутативные группы, групповые алгебры, некоммутативные коды, кодовые криптосистемы

**Для цитирования:** Веденёв К. В., Деундяк В. М., "Коды в диэдральной групповой алгебре", *Моделирование и анализ информационных систем*, **25**:2 (2018), 232–245.

**Об авторах:**
Веденёв Кирилл Владимирович, orcid.org/0000-0002-7893-655X, студент,
Южный Федеральный Университет,
ул. Большая Садовая, 105/42, г. Ростов-на-Дону, 344006 Россия, e-mail: vedenev@sfedu.ru

Деундяк Владимир Михайлович, orcid.org/0000-0001-8258-2419, канд. физ.-мат. наук, доцент,
Южный Федеральный Университет,
ул. Большая Садовая, 105/42, г. Ростов-на-Дону, 344006 Россия,
ФГНУ НИИ "Спецвузавтоматика",
пер. Газетный, 51, г. Ростов-на-Дону, 344002, Россия, e-mail: vl.deundyak@gmail.com.

## Введение

В работе [1] Р. Мак-Элис предложил асимметричную криптосистему, основанную на применении помехоустойчивых кодов Гоппы, причем к настоящему времени эф-

фективные структурные атаки на эту криптосистему не известны. После пионерской работы Р. Мак-Элиса появилось много других кодовых криптосистем на различных кодах, в частности, на ранговых кодах, кодах Рида–Соломона, кодах Рида–Маллера, алгебро-геометрических кодах. Небольшой обзор работ по анализу стойкости кодовых криптосистем содержится в [2]. Представляется актуальной задача поиска перспективных классов кодов для построения новых стойких кодовых криптосистем. Одним из вариантов решения этой задачи является использование некоммутативных алгебраических структур и, в частности, некоммутативных кодов, являющихся идеалами в групповых алгебрах $\mathbb{F}_q G$ над конечными некоммутативными группами $G$. Например, в работах [2], [3], [4] рассмотрены криптосистемы на индуцированных некоммутативных групповых кодах и их тензорных произведениях, а также проведен анализ их стойкости как к структурным атакам, так и к атакам на шифрограмму.

Целью настоящей работы является исследование кодов в диэдральной групповой алгебре в случае, когда мощность группы взаимно проста, с мощностью поля Галуа. В статье решена задача о структуре кодов, описаны все подгруппы диэдральной группы, и на этой основе получена структура диэдральных кодов, индуцированных циклическими кодами.

Для полупростых групповых алгебр есть теорема Веддерберна (см. [5]), доказывающая существование изоморфизма групповой алгебры на прямую сумму некоторых матричных алгебр. Эта теорема является очень важной для исследования некоммутативных кодов. Однако конкретный вид матричных слагаемых и конструкция изоморфизма этой теоремой не определены, т.е. для каждой группы остается задача построения представления Веддерберна. Некоторые результаты о структуре диэдральной групповой алгебры содержатся в работе [6], а в работе [7] получено полное представление Веддерберна для диэдральной групповой алгебры в случае, когда мощность поля и порядок группы взаимно просты.

Структура работы. Раздел 1 содержит определения диэдральной группы и групповой алгеброй, а также необходимые вспомогательные результаты. Основные результаты статьи о виде кодов, в том числе и индуцированных, а также нижняя оценка кодовых расстояний приведены в разделе 2. В разделе 3 рассмотрен пример построения диэдральных кодов.

# 1. Предварительные сведения о диэдральной групповой алгебре

Диэдральной группой $D_{2n}$, где $n \geq 2$, называется группа симметрий правильного плоского n-угольника с центром в точке $O$, состоящая из поворотов вокруг точки $O$ на углы, кратные $\frac{2\pi}{n}$, и отражений относительно прямых, проходящих через $O$ и одну из вершин или середину одной из сторон. Группа $D_{2n}$ порождается поворотом $a$ на угол $\frac{2\pi}{n}$ и произвольным отражением $b$, при этом выполняются следующие соотношения:

$$a^n = e,\ b^2 = e,\ bab = a^{-1} \tag{1}$$

(см. [8] с. 171). Таким образом, $D_{2n}$ допускает копредставление $\langle a, b :\ a^n,\ b^2,\ (ba)^2\rangle$, при этом формально можно считать, что $n$ – произвольное натуральное число. Из

(1) вытекает, что для произвольного $i$

$$a^i b = ba^{-i}, \tag{2}$$

поэтому

$$D_{2n} = \{e, a, a^2, ..., a^{n-1}, b, ab, a^2b, ..., a^{n-1}b\}. \tag{3}$$

Следующая теорема о структуре подгрупп диэдральной группы, возможно, известна специалистам, однако, в доступных источниках её найти не удалось. Через $d(n)$ обозначим количество делителей натурального числа $n$.

**Теорема 1.** *В группе $D_{2n}$ ($n \geq 2$) имеются следующие собственные подгруппы:*

*а) $n$ различных подгрупп вида $\{e, a^k b\}$, где $0 \leq k < n$, каждая из которых изоморфна $\mathbb{Z}_2$;*

*б) $d(n)$ подгрупп вида $\langle a^k \rangle$, где $k$ – любой натуральный делитель $n$, каждая из которых изоморфна $\mathbb{Z}_{\frac{n}{k}}$;*

*в) для каждого собственного делителя $k$ числа $n$ существует $k-1$ различных подгрупп вида $\langle a^l b, a^k \rangle$, где $0 \leq l < k$, каждая из которых изоморфна $D_{2\frac{n}{k}}$.*

*Других собственных подгрупп нет. Подгруппы вида б) нормальны, подгруппы вида а) нормальны только при $n = 2$, а подгруппы вида в) нормальны только при $k = 2$.*

Пусть $G$ – конечная группа и $\mathbb{F}_q$ – поле Галуа мощности $q$. Групповой алгеброй $\mathbb{F}_q G$ называется множество формальных линейных комбинаций вида

$$\alpha = \sum_{g \in G} a_g g, \quad a_g \in \mathbb{F}_q$$

с покомпонентно определёнными операциям сложения и умножения на скаляр и операцией умножения по следующему правилу:

$$(\sum_{g \in G} a_g g)(\sum_{g \in G} b_g g) = \sum_{g \in G} (\sum_{h \in G} a_h b_{h^{-1}g}) g \; (= \sum_{g,h \in G} a_g b_h gh)$$

(см. [5], с.139). Определено естественное вложение группы $G$ в групповую алгебру $\mathbb{F}_q G$, переводящее элемент группы $g \in G$ в элемент групповой алгебры $1g \in \mathbb{F}_q G$. Аналогично определено вложение поля $\mathbb{F}_q$ в $\mathbb{F}_q G$, переводящее $\lambda \in \mathbb{F}_q$ в $\lambda e \in \mathbb{F}_q G$, где $e \in G$ – нейтральный элемент группы. В $\mathbb{F}_q G$ имеется естественная инволюция, индуцированная инверсией в группе $G$:

$$(\sum_{g \in G} a_g g)^* = \sum_{g \in G} a_g g^{-1},$$

которая устанавливает взаимно однозначное соответствие между левыми и правыми идеалами, поэтому в этой статье мы будем рассматривать только левые идеалы. Всякий левый идеал $I \subset \mathbb{F}_q G$ называется групповым $G$-кодом над полем $\mathbb{F}_q$ (см. [9]). Если идеал $I$ – двусторонний, то будем называть его центральным кодом.

Рассмотрим групповую алгебру $\mathbb{F}_q D_{2n}$. В силу (2), (3) любой элемент $u \in \mathbb{F}_q D_{2n}$ может быть представлен следующим образом:

$$u = P(a) + bQ(a) = P(a) + Q(a^{-1})b, \tag{4}$$

где $P$ и $Q$ – многочлены степени, не превосходящей $n$.

В работе [7] доказана теорема о виде разложения Веддерберна для $\mathbb{F}_q D_{2n}$, однако прежде чем сформулировать её в удобном для дальнейшего виде, приведём необходимые вспомогательные сведения. Для каждого многочлена $g \in \mathbb{F}_q[x]$ такого, что $g(0) \neq 0$, возвратным многочленом называется многочлен $g^*(x) := x^{\deg(g)} g(\frac{1}{x})$. Говорят, что многочлен $g$ самовозвратный, если $g$ и $g^*$ имеют одни и те же корни в своём поле разложения, т. е. эти многочлены отличаются на постоянный ненулевой множитель. Ниже будем полагать, что наибольший общий делитель $\gcd(2n, q)$ чисел $2n$ и $q$ равен единице.

Известно, что многочлен $x^n - 1 \in \mathbb{F}_q[x]$ разлагается на неприводимые над $\mathbb{F}_q$ множители; следуя [7], запишем это разложение следующим образом:

$$x^n - 1 = (f_1 f_2 \dots f_r)(f_{r+1} f^*_{r+1} f_{r+2} f^*_{r+2} \dots f_{r+s} f^*_{r+s}), \tag{5}$$

где $f_1 = x - 1$, при $1 < j \leq r$ выполнено равенство $f^*_j = f_j$ и $f_2 = x + 1$ в случае чётного $n$. Здесь $r$ — количество самовозвратных множителей в этом разложении, а $2s$ — несамовозвратных.

Всякий неприводимый над полем $\mathbb{F}_q$ многочлен $h$ степени $m$ имеет корень в расширении этого поля $F_{q^m}$, обозначим его через $\alpha$, при этом элементы

$$\alpha^0 = 1, \alpha^1, \alpha^2, \dots, \alpha^{m-1}$$

составляют базис расширения $F_{q^m}$ как векторного пространства над $\mathbb{F}_q$ (см. [8], с. 409). Поэтому

$$\mathbb{F}_q[\alpha] := \{\sum_{j=0}^{k} c_j \alpha^j \in F_{q^m} \mid k \in \mathbb{N} \cup \{0\},\ c_j \in \mathbb{F}_q\}$$

совпадает с полем $F_{q^m}$. Если $\deg(h) = 1$, то $\alpha \in \mathbb{F}_q$ и, следовательно, $F[\alpha] = \mathbb{F}_q$. Аналогично, элементы

$$1, \beta, \beta^2, \dots \beta^{n-1},$$

где $\beta = \alpha^{-1}$ — корень многочлена $h^*$, тоже образуют базис в $F_{q^n}$, поэтому

$$F_{q^m} = F[\alpha] = F[\alpha^{-1}].$$

Обозначим далее $\alpha_j$ — корень многочлена $f_j$ из (5),

$$\delta(n) := \begin{cases} 1, & n \text{ — нечётное}, \\ 2, & n \text{ — чётное}. \end{cases}$$

Рассмотрим гомоморфизмы $\tau_j$ алгебры $\mathbb{F}_q D_{2n}$, определяемые своими значениями на порождающих элементах $a$ и $b$:

a) $\tau_1 : \mathbb{F}_q D_{2n} \to \mathbb{F}_q \oplus \mathbb{F}_q, \quad \tau_1(a) = (1, 1),\ \tau_1(b) = (1, -1)$;

b) $\tau_2 : \mathbb{F}_q D_{2n} \to \mathbb{F}_q \oplus \mathbb{F}_q, \quad \tau_2(a) = (-1, -1),\ \tau_2(b) = (1, -1), \quad \delta(n) = 2$;

c) $\tau_j : \mathbb{F}_q D_{2n} \to \mathrm{M}_2(\mathbb{F}_q[\alpha_j]),\ \tau_j(a) = \begin{pmatrix} \alpha_j & 0 \\ 0 & \alpha_j^{-1} \end{pmatrix}, \tau_j(b) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad j \geq \delta(n) + 1.$

Для $j = \delta(n)+1, \ldots, r$ рассмотрим автоморфизмы $\sigma_j$ алгебр (2×2)-матриц $\mathrm{M}_2(\mathbb{F}_q[\alpha_j])$, определяемые формулой

$$\sigma_j(X) = Z_j^{-1} X Z_j, \quad Z_j := \begin{pmatrix} 1 & -\alpha_j \\ 1 & -\alpha_j^{-1} \end{pmatrix}. \tag{6}$$

Отметим, что $\mathbb{F}_q[\alpha_j + \alpha_j^{-1}] \subset \mathbb{F}_q[\alpha_j]$ и при $\delta(n) + 1 \le j \le r$

$$\sigma_j(\mathrm{im}(\tau_j)) = \mathrm{M}_2(\mathbb{F}_q[\alpha_j + \alpha_j^{-1}]) \simeq \mathrm{M}_2(F_{q^{\deg(f_j)/2}}).$$

***Замечание 1.*** В [7], с. 209, отмечено, что если $u := P(a) + Q(a)b \in \mathbb{F}_q D_{2n}$, $v := P(a) + bQ(a) \in \mathbb{F}_q D_{2n}$, то

$$\tau_j(u) = \begin{pmatrix} P(\alpha_j) & Q(\alpha_j) \\ Q(\alpha_j^{-1}) & P(\alpha_j^{-1}) \end{pmatrix}, \quad j > \delta(n),$$

$$\tau_j(v) = \begin{pmatrix} P(\alpha_j) & Q(\alpha_j^{-1}) \\ Q(\alpha_j) & P(\alpha_j^{-1}) \end{pmatrix}, \quad j > \delta(n),$$

$$\tau_1(u) = \tau_1(v) = (P(1) + Q(1), P(1) - Q(1)),$$

$$\tau_2(u) = \tau_2(v) = (P(-1) + Q(-1), P(-1) - Q(-1)), \quad \delta(n) = 2.$$

**Теорема 2.** *[7] Пусть* $\gcd(q, 2n) = 1$, *тогда имеет место изоморфизм:*

$$p : \mathbb{F}_q D_{2n} \to \bigoplus_{j=1}^{r+s} A_j, \tag{7}$$

*где*

$$A_j = \begin{cases} \mathbb{F}_q \oplus \mathbb{F}_q, & j \le \delta(n) \\ \mathrm{M}_2(\mathbb{F}_q[\alpha_j + \alpha_j^{-1}]), & \delta(n) + 1 \le j \le r \\ \mathrm{M}_2(\mathbb{F}_q[\alpha_j]), & r + 1 \le j \le r + s \end{cases},$$

$$p := \bigoplus_{j=1}^{r+s} p_j, \quad p_j := \begin{cases} \sigma_j \circ \tau_j, & \delta(n) + 1 \le j \le r \\ \tau_j, & 1 \le j \le \delta(n),\ r + 1 \le j \le r + s \end{cases},$$

$$\mathbb{F}_q[\alpha_j + \alpha_j^{-1}] \simeq F_{q^{\deg(f_j)/2}}, \quad \delta(n) + 1 \le j \le r,$$

$$\mathbb{F}_q[\alpha_j] \simeq F_{q^{\deg(f_j)}}, \quad r + 1 \le j \le r + s.$$

***Замечание 2.*** В случае, когда в разложении (5) все множители линейные, единственными самовозвратным многочленами первой степени являются $x + 1$ и $x - 1$, тогда $r = \delta(n)$ и поэтому

$$A_j = \begin{cases} \mathbb{F}_q \oplus \mathbb{F}_q, & j \le \delta(n) \\ \mathrm{M}_2(\mathbb{F}_q[\alpha_j]), & \delta(n) + 1 \le j \le \delta(n) + s \end{cases}.$$

## 2. Структура кодов в алгебре $\mathbb{F}_q D_{2n}$

По теореме 2 групповая алгебра $\mathbb{F}_q D_{2n}$ при $\gcd(2n, q) = 1$ изоморфна алгебре

$$\Delta := \bigoplus_{j=1}^{r+s} A_j$$

(см. (7)), поэтому изучение кодов в $\mathbb{F}_q D_{2n}$ сводится к изучению левых идеалов в $\Delta$. Пусть $F$ — произвольное поле Галуа, будем далее называть ненулевой вектор $(x, y) \in F^2$ нормированным, если $x = 1$ или $x = 0,\ y = 1$.

Для алгебры $A_1$ из разложения (7) и нормированного вектора $(x, y)$ положим

$$I_1(x, y) := \{\lambda x, \mu y \mid \lambda, \mu \in \mathbb{F}_q\}. \tag{8}$$

Отметим, что если $x = 1$ и $y \neq 0$, то $I_1(x, y) = A_1$. Для других нормированных векторов имеем

$$I_1(1, 0) = \mathbb{F}_q \oplus 0,\ I_1(0, 1) = 0 \oplus \mathbb{F}_q.$$

Легко видеть, что других собственных идеалов в алгебре $A_1$ нет. Аналогично при чётном $n$ определяются идеалы $I_2(x, y)$ в $A_2$.

Далее будем использовать следующий результат Н. Джекобсона: пусть $V$ – конечномерное векторное пространство над полем $F$, тогда всякий левый идеал в алгебре линейных эндоморфизмов $\mathcal{L}(V)$ имеет вид

$$I(K) = \{\theta \in \mathcal{L}(V) \mid K \subset \ker(\theta)\},$$

где $K$ — некоторое подпространство $V$ (см. [11], с. 93).

Рассмотрим разложение (7) и обозначим

$$R_j := \begin{cases} \mathbb{F}_q, & 1 \leq j \leq \delta(n), \\ \mathbb{F}_q[\alpha_j + \alpha_j^{-1}], & \delta(n) + 1 \leq j \leq r, \\ \mathbb{F}_q[\alpha_j], & r + 1 \leq j \leq r + s. \end{cases} \tag{9}$$

При $\delta(n) + 1 \leq j \leq r + s$ отождествим алгебру $A_j$ с алгеброй $\mathcal{L}(R_j^2)$. Всякое собственное подпространство $K_j$ пространства $R_j^2$ имеет размерность 1, т.е. является линейной оболочкой нормированного вектора $(x, y)$. Через $I_j(x, y)$ обозначим идеал $I(K_j)$ в соответствующей алгебре $A_j$.

**Лемма 1.** *Если $\delta(n) + 1 \leq j \leq r + s$, то*

$$I_j(x, y) = \{\begin{pmatrix} ky & -kx \\ ty & -tx \end{pmatrix} = k \begin{pmatrix} y & -x \\ 0 & 0 \end{pmatrix} + t \begin{pmatrix} 0 & 0 \\ y & -x \end{pmatrix} \mid k, t \in R_j\}.$$

*Доказательство.* Действительно, если

$$L = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in I_j(x, y),$$

то

$$L \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} Ax + By \\ Cx + Dy \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

Тогда найдутся такие $k, t \in R_j$, что

$$A = ky, B = -kx, C = ty, D = -tx.$$

С другой стороны, очевидно, что для любых $k, t \in R_j$ при $A = -ky, B = kx, C = -ty, D = tx$ получаем $L \in I_j(x, y)$. □

**Теорема 3.** *Пусть* $\gcd(q, 2n) = 1$. *Рассмотрим разложение (7) групповой алгебры* $F_pD_{2n}$. *Для любого кода* $I \subset \mathbb{F}_qD_{2n}$ *найдутся такие непересекающиеся множества* $J_1, J_2 \subset \{1, \ldots, r+s\}$ *и набор нормированных векторов* $\{(x_j, y_j)\}_{j\in J_2}$, *где* $x_j, y_j \in R_j$, *что*

$$p(I) = \bigoplus_{j=1}^{r+s} B_j, \tag{10}$$

$$B_j := \begin{cases} A_j, & j \in J_1 \\ I_j(x_j, y_j) & j \in J_2 \\ 0, & j \notin J_1 \cup J_2 \end{cases}. \tag{11}$$

*С другой стороны, для любых* $J_1, J_2 \subset \{1, \ldots, r+s\}$ *таких, что* $J_1 \cap J_2 = \varnothing$, *и для любого набора векторов* $\{(x_j, y_j)\}_{j\in J_2}$ *над соответствующими полями* $R_j$ *(см. (9)) множество*

$$p^{-1}(\bigoplus_{j=1}^{r+s} B_j),$$

*где* $B_j$ *определены равенством (11), является кодом в* $\mathbb{F}_qD_{2n}$.

*Доказательство.* В силу теоремы 2 при $\gcd(q, 2n) = 1$ алгебры $\mathbb{F}_qD_{2n}$ и $\Delta$ изоморфны, поэтому изоморфизм $p$ устанавливает взаимно однозначное соответствие между кодами в $\mathbb{F}_qD_{2n}$ и левыми идеалами в $\Delta$. Рассмотрим идеалы в алгебре $\Delta$. Известно, что всякий левый идеал в прямой сумме алгебр есть прямая сумма левых идеалов в слагаемых. Лемма 1 устанавливает вид собственных левых идеалов в матричных слагаемых, а собственные идеалы в $\mathbb{F}_q \oplus \mathbb{F}_q$ указаны ранее (см. (8)). Отсюда вытекают оба утверждения теоремы. □

***Замечание 3.*** Для построения кодов в $\mathbb{F}_qD_{2n}$ необходимой является конструкция обратного к $p$ изоморфизма $p^{-1}$. Чтобы получить её, рассмотрим несколько шагов. Ниже будем пользоваться представлением (4) элементов групповой алгебры $\mathbb{F}_qD_{2n}$ и конструкциями, использовавшимися для построения изоморфизма $p$, в частности (5), (6), (7). Введём также обозначения: $\mathrm{id}_X$ — тождественное отображение на множестве $X$ и $\xi := (1+1)^{-1} \in \mathbb{F}_q$.

1. Определим мономорфизм $\epsilon_1 : \mathbb{F}_q \oplus \mathbb{F}_q \to \mathbb{F}_qD_{2n}$ по формуле

$$\epsilon_1(w) := \xi[(w_1 + w_2) + (w_1 - w_2)b]M_1(a)M_1',$$

$$M_1(x) := \frac{x^n - 1}{x - 1} \in \mathbb{F}_q[x],\ M_1' := (M_1(1))^{-1}.$$

2. При чётном $n$ аналогично определим мономорфизм $\epsilon_2 : \mathbb{F}_q \oplus \mathbb{F}_q \to \mathbb{F}_qD_{2n}$ по формуле

$$\epsilon_2(w) := \xi[(w_1 + w_2) + (w_1 - w_2)b]M_2(a)M_2',$$

$$M_2(x) := \frac{x^n - 1}{x + 1},\ M_1' := (M_2(-1))^{-1}.$$

3. Для $r + 1 \le j \le r + s$ определим мономорфизмы $\epsilon_j : \mathrm{M}_2(\mathbb{F}_q[\alpha_j]) \to \mathbb{F}_q D_{2n}$ по формуле

$$\epsilon_j(\begin{pmatrix} A(\alpha_j) & C(\alpha_j^{-1}) \\ B(\alpha_j) & D(\alpha_j^{-1}) \end{pmatrix}) = [A(a) + bB(a)]M_j(a)M_j'(a) + [D(a) + bC(a)]N_j(a)N_j'(a),$$

$$M_j(x) := \frac{x^n - 1}{f_j(x)} \in \mathbb{F}_q[x], \quad M_j(\alpha_j)M_j'(\alpha_j) = 1,$$

$$N_j(x) := \frac{x^n - 1}{f_j^*(x)} \in \mathbb{F}_q[x], \quad N_j(\alpha_j^{-1})N_j'(\alpha_j^{-1}) = 1.$$

Из замечания 1 видно, что $\tau_j\epsilon_j = \mathrm{id}_{A_j}$ и для любого $i \ne j$ выполняется $\tau_i\epsilon_j = 0$.

4. Для $\delta(n) + 1 \le j \le r$ формулой $\gamma_j(X) = Z_j X Z_j^{-1}$ определим отображение

$$\gamma_j : M_2(\mathbb{F}_q[\alpha_j + \alpha_j^{-1}]) \to M_2(\mathbb{F}_q[\alpha_j]),$$

а формулой

$$\psi_j(\begin{pmatrix} P(\alpha_j) & Q(\alpha_j) \\ Q(\alpha_j^{-1}) & P(\alpha_j^{-1}) \end{pmatrix}) = M_j(a)M_j'(a)P(a) + M_j(a)M_j'(a)Q(a)b,$$

где

$$M_j(x) := \frac{x^n - 1}{f_j(x)} \in \mathbb{F}_q[x],\ M_j(\alpha_j)M_j'(\alpha_j) = 1,$$

отображение $\psi_j : \mathrm{im}(\gamma_j) \to \mathbb{F}_q D_{2n}$. Видно, что $\sigma_j\tau_i\psi_j\gamma_j = \mathrm{id}_{\mathrm{A_j}}$ и для любого $i \ne j$ выполняется $\tau_i \circ \psi_j = 0$.

Пусть

$$q := \sum_{j=1}^{\delta(n)} \epsilon_j + \sum_{j=\delta(n)+1}^{r} \psi_j\gamma_j + \sum_{j=r+1}^{r+s} \epsilon_j. \tag{12}$$

Тогда

$$pq = p(\sum_{j=1}^{\delta(n)} \epsilon_j + \sum_{j=\delta(n)+1}^{r} \psi_j\gamma_j + \sum_{j=r+1}^{r+s} \epsilon_j) = \bigoplus_{j=1}^{\delta(n)} \tau_j\epsilon_j \oplus \bigoplus_{j=\delta(n)+1}^{r} \sigma_j\tau_j\psi_j\gamma_j \oplus \bigoplus_{j=r+1}^{r+s} \tau_j\epsilon_j =$$

$$= \bigoplus_{j=1}^{r+s} \mathrm{id}_{A_j} = \mathrm{id}_\Delta.$$

Следовательно, $p^{-1} = q$. □

В [10] рассмотрен способ переноса код из групповой алгебры над подгруппой в групповую алгебру над всей группой. Пусть $G$ – конечная группа, $H$ – её подгруппа, $\mathcal{T}$ – правая трансверсаль $G$ по $H$, а $I$ – код в $\mathbb{F}_q H$. Индуцированным кодом называется код

$$J = (\mathbb{F}_q G)I,$$

при этом если $B(I) = \{n_1, n_2, ...n_k\}$ – $\mathbb{F}_q$-базис $I$, то $\mathbb{F}_q$-базисом $J$ будет

$$B(J) := \mathcal{T}B(I).$$

Если $[n, k, d]$ — параметры кода $I$ над подгруппой, то $[n|\mathcal{T}|, k|\mathcal{T}|, d]$ — параметры индуцированного кода $J$ (см. [10]).

Рассмотрим циклическую подгруппу $\langle a\rangle$ диэдральной группы $D_{2n}$; все идеалы в алгебре $\mathbb{F}_q\langle a\rangle$ — циклические коды (см. [12]). Ниже будем рассматривать коды в алгебре $\mathbb{F}_q D_n$, индуцированные циклическими кодами, что может иметь применение в задаче усиления кодовых криптосистем (см. [2], [3]).

Известно, что всякий код $C$ в $\mathbb{F}_q\langle a\rangle$ порождается многочленом $g(x)$, делителем $x^n - 1$ (см. [12]), при этом его $\mathbb{F}_q$-базисом является набор

$$\{g(a), ag(a), \ldots, a^{n-\deg(g)-1}g(a)\}.$$

Рассмотрим индуцированный код $T = (\mathbb{F}_q D_{2n})C$. Правая трансверсаль $\mathcal{T}$ группы $D_{2n}$ по подруппе $\langle a\rangle$ имеет вид

$$\mathcal{T} = \{e, b\},$$

поэтому базисом индуцированного кода $T$ является набор

$$\{g(a), ag(a), \ldots, a^{n-\deg(g)-1}g(a), bg(a), bag(a), \ldots, ba^{n-\deg(g)-1}g(a)\}. \tag{13}$$

**Теорема 4.** *Пусть* $\gcd(q, 2n) = 1$. *Рассмотрим разложение (7) групповой алгебры* $\mathbb{F}_q D_{2n}$. *Пусть* $C_g$ *— циклический код в* $\mathbb{F}_q\langle a\rangle$, *порождённый многочленом* $g(x)$. *Тогда для индуцированного этим циклическим кодом кода* $T_g = (\mathbb{F}_q D_{2n})C_g$ *разложение Веддерберна имеет следующий вид:*

$$p(T_g) = (\bigoplus_{j=1}^{r+s} B_j)$$

*где*

$$B_j = \begin{cases} A_j, & j \in J_1 \\ I_j(0,1) & j \in J_2 \\ I_j(1,0) & j \in J_3 \\ 0, & j \notin J_1, J_2, J_3 \end{cases}, \tag{14}$$

$$J_1 := \{j \in 1, \ldots, r+s \ : \ (f_j \not| g) \ \wedge \ (f_j^* \not| g)\},$$
$$J_2 := \{j \in \delta(n)+1, \ldots, r+s \ : \ (f_j \not| g) \wedge (f_j^* \mid g)\},$$
$$J_3 := \{j \in \delta(n)+1, \ldots, r+s \ : \ (f_j \mid g) \wedge (f_j^* \not| g)\}.$$

*Доказательство.* В силу (13) любой элемент из индуцированного кода $T_g$ представим в виде

$$u = P(a)g(a) + bQ(a)g(a).$$

В силу замечания 1 при $j \geq \delta(n) + 1$ получаем

$$\tau_j(u) = \begin{pmatrix} P(\alpha_j)g(\alpha_j) & Q(\alpha_j^{-1})g(\alpha_j^{-1}) \\ Q(\alpha_j)g(\alpha_j) & P(\alpha_j^{-1})g(\alpha_j^{-1}) \end{pmatrix}.$$

Если $f_j$ делит многочлен $g$, то нетрудно видеть, что левый столбец при любых $P$ и $Q$ обращается в 0; справедливо и обратное: если при любых $P$ и $Q$ левый столбец обращается в 0, то $f_j$ делит $g$. Действительно, положим $P(x) = Q(x) = 1$, тогда $g(\alpha_j) = 0$, т.е. $\alpha_j$ – корень многочлена $g$ и $f_j | g$. Аналогичные рассуждения справедливы для правых столбцов и возвратных многочленов $f_j^*$. Таким образом, при $j \leq \delta(n) + 1$:

$$\begin{array}{rcl} (f_j \not| g) \wedge (f_j^* \not| g) & \Rightarrow & \tau_j(T_g) = A_j, \\ (f_j | g) \wedge (f_j^* \not| g) & \Rightarrow & \tau_j(T_g) = I_j(0,1), \\ (f_j \not| g) \wedge (f_j^* | g) & \Rightarrow & \tau_j(T_g) = I_j(1,0), \\ (f_j | g) \wedge (f_j^* | g) & \Rightarrow & \tau_j(T_g) = 0. \end{array}$$

Далее, в силу замечания 1

$$\tau_1(u) = (P(1)g(1) - Q(1)g(1), P(1)g(1) + Q(1)g(1)).$$

Аналогично этот вектор обращается в 0 при любых $P$ и $Q$ тогда и только тогда, когда $g(1) = 0$. Аналогично при чётном $n$:

$$\tau_2(u) = (P(-1)g(-1) - Q(-1)g(-1), P(-1)g(-1) + Q(-1)g(-1))$$

обращается в 0 при любых $P$ и $Q$ тогда и только тогда, когда $g(-1) = 0$. А т.к. изоморфизм $p$ имеет вид (7), то теорема доказана. □

Введём линейное отображение $\mathrm{pr}_a : \mathbb{F}_q D_{2n} \to \mathbb{F}_q\langle a \rangle$, действующее по правилу

$$\mathrm{pr}_a(P(a) + bQ(a)) := P(a).$$

**Лемма 2.** *Если $I$ — левый идеал в алгебре $\mathbb{F}_q D_{2n}$, то $\mathrm{pr}_a(I)$ — идеал в $\mathbb{F}_q\langle a \rangle$, т.е. циклический код.*

*Доказательство.* Действительно, пусть $P(a) \in \mathrm{pr}_a(I)$, тогда существует такое $u = P(a) + bQ(a) \in I$. Тогда для любого $S(a) \in \mathbb{F}_q\langle a \rangle$ имеем

$$(S(a) + 0b)u = S(a)P(a) + bQ(a)S(a^{-1}) \in I,$$

т.е. $S(a)P(a) = \mathrm{pr}_a((S(a) + 0b)u) \in \mathrm{pr}_a(I)$. □

**Теорема 5.** *Для всякого кода $I \subset \mathbb{F}_q D_{2n}$ найдутся циклические коды $C_1, C_2 \subset \mathbb{F}_q\langle a \rangle$ такие, что $(\mathbb{F}_q D_{2n})C_1 \subset I \subset (\mathbb{F}_q D_{2n})C_2$.*

*Доказательство.* Положим $C_2 := \mathrm{pr}_a(I)$. Покажем, что $I \subset (\mathbb{F}_q D_{2n})C_2$, пусть $u = P(a) + bQ(a) \in I$, тогда

$$\mathrm{pr}_a(u) = P(a) \in \mathrm{pr}_a(I)$$
$$\mathrm{pr}_a(bu) = Q(a) \in \mathrm{pr}_a(I),$$

откуда $P(a), Q(a), bP(a), bQ(a) \in (\mathbb{F}_q D_{2n})C_2$, следовательно, $u \in (\mathbb{F}_q D_{2n})C_2$.

Положим $C_1 := I \cap \mathbb{F}_q\langle a \rangle$, очевидно, что это действительно циклический код и что $(\mathbb{F}_q D_{2n})C_1 \subset I$.

□

Через $\mathrm{dist}(I)$ обозначим минимальное кодовое расстояние кода $I$.

**Следствие 1.** *Пусть $I$ — код в $\mathbb{F}_q D_{2n}$, тогда* $\mathrm{dist}(I) \geq \mathrm{dist}(\mathrm{pr}_a(I))$.

Доказательство следует из того, что у индуцированных кодов наименьшее кодовое расстояние такое же, как и у кодов, которыми они индуцированы.

# 3. Пример

Рассмотрим пример диэдрального кода, который не входит в класс кодов, индуцированных циклическими.

Пусть $\mathbb{F}_q$ – конечное поле, $n$ – некоторый делитель числа $q-1$, $\omega \in \mathbb{F}_q$ – элемент порядка $n$. Выберем целый параметр $d \le \frac{n}{2} - 1$ и рассмотрим код Рида–Соломона (см. [12]) $C_g$ с порождающим многочленом

$$g(x) = \begin{cases} (x-\omega^{\frac{n}{2}})[(x-\omega^{\frac{n}{2}-1})(x-\omega^{\frac{n}{2}+1})]\dots[(x-\omega^{\frac{n}{2}-d})(x-\omega^{\frac{n}{2}+d})], & n \text{ — четное}, \\ [(x-\omega^{\lfloor\frac{n}{2}\rfloor})(x-\omega^{\lceil\frac{n}{2}\rceil})]\dots[(x-\omega^{\lfloor\frac{n}{2}\rfloor-d})(x-\omega^{\lceil\frac{n}{2}\rceil+d})], & n \text{ — нечетное}. \end{cases}$$

Отметим, что если многочлен $f$ — делитель многочлена $g$, то его возвратный многочлен $f^*$ тоже делит $g$. Длина кода $C_g$ равна $n$, минимальное кодовое расстояние – $(2d+1)$ при нечётном $n$ и $(2d+2)$ при чётном. Размерность кода $C_g$ равна $(n-2d)$ в случае чётного $n$ и $(n-2d-1)$ в случае нечётного. Рассмотрим индуцированный код $T_g = (\mathbb{F}_q D_{2n})C_g$. По теореме 4

$$p(T_g) = \bigoplus_{j=1}^{r+s} B_j,$$

где

$$B_j = \begin{cases} A_j, & j \in S_1 \\ 0, & j \in S_2 \end{cases}, \tag{15}$$

$$S_1 \subset \{1,\dots,r+s\}, \quad S_2 = \{1,\dots,r+s\} \setminus S_1.$$

Теперь построим новый код $T'$, вложенный в $T_g$. Для этого выберем произвольное непустое множество $S_3 \subset S_1 \setminus \{1, \delta(n)\}$ и набор таких нормированных векторов $\{(x_j, y_j)\}_{j\in S_3}$, что $x_j \neq 0$ и $y_j \neq 0$. Определим левый идеал $D = \bigoplus_{j=1}^{r+s} B'_j$ в алгебре $\Delta$, где

$$B'_j = \begin{cases} A_j, & j \in S_1 \setminus S_3 \\ I_j(x_j, y_j), & j \in S_3 \\ 0, & j \in S_2. \end{cases}. \tag{16}$$

Воспользуемся построенным в замечании 3 изоморфизмом $p^{-1}$ и определим код $T' = p^{-1}(D)$. Заметим, что этот код не является кодом, индуцированным циклическим. Действительно, если бы $T'$ был таким кодом, то по теореме 4 левый идеал $D$ имел бы вид (14), но по построению это не так.

Теперь рассмотрим коды $C_g$, $T_g$ и $T'$ для конкретных числовых параметров. Пусть $q = 11$, $n = 10$, $\omega = 2$ — примитивный элемент поля $\mathbb{F}_{11}$. Выпишем для многочлена $x^{10} - 1$ разложение (5) на неприводимые множители:

$$x^{10} - 1 = f_1 f_2 [f_3 f_3^* f_4 f_4^* f_5 f_5^* f_6 f_6^*],$$

где

$$f_1(x) = x - 1,\ f_2(x) = x + 1,$$

$$f_3(x) = x - 2,\ f_4(x) = x - 3,\ f_5(x) = x - 7,\ f_6(x) = x - 9,$$

$$f_3^*(x) = x - 6,\ f_4^*(x) = x - 4,\ f_5^*(x) = x - 8,\ f_6^*(x) = x - 5.$$

В нашем случае $r = 2$ — количество самовозвратных множителей в этом разложении, а $2s = 8$ — количество несамовозвратных. Положим $d = 2$. Тогда

$$g(x) = (x - \omega^5)[(x - \omega^4)(x - \omega^6)][(x - \omega^3)(x - \omega^7)],$$

$$g(x) = (x - 10)[(x - 5)(x - 9)][(x - 8)(x - 7)],$$

$$g(x) = f_2(x)f_6(x)f_6^*(x)f_5(x)f_5^*(x).$$

Код $C_g$ является $[10, 5, 6]$–кодом, индуцированный код $T_g = (\mathbb{F}_{11}D_{20})C_g$ является $[20, 10, 6]$–кодом. По теореме 4

$$p(T_g) = B_1 \oplus B_2 \oplus B_3 \oplus B_4 \oplus B_5 \oplus B_6$$

(см. (14), (16)), где

$$B_1 = \mathbb{F}_{11} \oplus \mathbb{F}_{11},\ B_2 = 0 \oplus 0,$$

$$B_3 = \mathrm{M}_2(\mathbb{F}_{11}[2]),\ B_4 = \mathrm{M}_2(\mathbb{F}_{11}[3]),\ B_5 = 0,\ B_6 = 0.$$

Теперь для наших параметров вычислим код $T'$. Пусть

$$D = B_1' \oplus B_2' \oplus B_3' \oplus B_4' \oplus B_5' \oplus B_6',$$

$$B_1' = \mathbb{F}_{11} \oplus \mathbb{F}_{11},\ B_2' = 0 \oplus 0,$$

$$B_3' = I_3(1, -1),\ B_4' = \mathrm{M}_2(\mathbb{F}_{11}[3]),\ B_5' = 0,\ B_6' = 0,$$

где

$$M_3(x) = \frac{x^{10} - 1}{x - 2}, \quad N_3(x) = \frac{x^{10} - 1}{x - 4}.$$

Лемма 1 устанавливает вид базиса в $I_3(1, -1)$, вид базисов в остальных слагаемых левого идеала $D$ известен, теперь с помощью замечания 3 построим $\mathbb{F}_q$-базис кода $T' = p^{-1}(D)$:

$$B_1 = e + a + a^2 + a^3 + a^4 + a^5 + a^6 + a^7 + a^8 + a^9,$$

$$B_3 = 6e + 3a + 7a^2 + 9a^3 + 10a^4 + 5a^5 + 8a^6 + 4a^7 + 2a^8 + 1a^9,$$

$$B_5 = 2e + 4a + 8a^2 + 5a^3 + 10a^4 + 9a^5 + 7a^6 + 3a^7 + 6a^8 + 1a^9,$$

$$B_7 = 3e + 9a + 5a^2 + 4a^3 + 1a^4 + 3a^5 + 9a^6 + 5a^7 + 4a^8 + 1a^9 +$$

$$+b(4e + 5a + 9a^2 + 3a^3 + 1a^4 + 4a^5 + 5a^6 + 9a^7 + 3a^8 + 1a^9),$$

$$B_2 = bB_1,\ B_4 = bB_3,\ B_6 = bB_5,\ B_8 = bB_7.$$

В результате прямой вычислительной проверки установлено, что кодовое расстояние данного кода равно 8, таким образом получен диэдральный $[20, 8, 8]$-код.

# Список литературы / References

[1] McEliece R.J., "A Public-Key Cryptosystem Based on Algebraic Coding Theory", *DSN Progress Report*, **42–44** (1978), 114–116.

[2] Деундяк В.М., Косолапов Ю.В., "Криптосистема на индуцированных групповых кодах", *Модел. и анализ информ. систем*, **23**:2 (2016), 137–152; [Deundyak V. M., Kosolapov Y. V., "Cryptosystem Based on Induced Group Codes", *Modeling and Analysis of Information Systems*, **23**:2 (2016), 137–152, (in Russian).]

[3] Деундяк В.М., Косолапов Ю.В., Лелюк Е.А., "Декодирование тензорного произведения MLD-кодов и приложения к кодовым криптосистемам", *Модел. и анализ информ. систем*, **24**:2 (2017), 239–252; [Deundyak V. M., Kosolapov Y. V., Lelyuk E. A., "Decoding the Tensor Product of MLD Codes and Applications for Code Cryptosystems", *Modeling and Analysis of Information Systems*, **24**:2 (2017), 239–252, (in Russian).]

[4] Деундяк В.М., Косолапов Ю.В., "Использование тензорного произведения кодов Рида–Маллера в асимметричной криптосистеме типа Мак-Элиса и анализ ее стойкости к атакам на шифрограмму", *Вычислительные технологии*, **22**:4 (2017), 43–60; [Deundyak V. M., Kosolapov Y. V., "The use of the tensor product of Reed–Muller codes in asymmetric McEliece type cryptosystem and analysis of its resistance to attacks on the cryptogram", *Computational Technologies*, **22**:4 (2017), 43–60, (in Russian).]

[5] Milies C. P., Sehgal S. K., *An inroduction to Group Rings*, Kluwer Academic Publishers, Boston, 2002.

[6] Сидельников В. М., Казарин Л. С., "О групповой алгебре группы диэдра и сложности умножения матриц второго порядка", *Тр. по дискр. матем.*, **11**:1 (2008), 109–118; [Sidel'nikov V. M., Kazarin L. S., "On a group algebra of a dihedral group and complexity of multiplication of second order matrices", *Tr. Diskr. Mat.*, **11**:1 (2008), 109–118, (in Russian).]

[7] Martinez F. E. B., "Structure of finite dihedral group algebra", *Finite Fields and Their Applications*, **35** (2015), 204–214.

[8] Винберг Э. Б., *Курс алгебры*, МЦНМО, М., 2013; [E. B. Vinberg, *Course in Algebra*, Moscow, 2013, (in Russian).]

[9] Циммерман К.-Х., *Методы теории модулярных представлений в алгебраической теории кодирования*, МЦНМО, М., 2011; [Tsimmerman K.-Kh, *Metody teorii modulyarnykh predstavleniy v algebraicheskoy teorii kodirovaniya*, Moscow, 2011, (in Russian).]

[10] Деундяк В. М., Косолапов Ю. В., "Алгоритмы для мажоритарного декодирования групповых кодов", *Модел. и анализ информ. систем*, **22**:4 (2015), 464–482; [Deundyak V. M., Kosolapov Y. V., "Algorithms for Majority Decoding of Group Codes", *Modeling and Analysis of Information Systems*, **22**:4 (2015), 464–482, (in Russian).]

[11] Jacobson N., *Structure of rings*, American Mathematical Soc., 1956.

[12] Сидельников В. М., *Теория кодирования*, Физматлит, М., 2011; [Sidelnikov V. M., *Teoriya kodirovaniya*, Fizmatlit, Moscow, 2011, (in Russian).]

---

**Vedenev K. V., Deundyak V. M.**, "Codes in Dihedral Group Algebra", *Modeling and Analysis of Information Systems*, **25**:2 (2018), 232–245.

**DOI:** 10.18255/1818-1015-2018-2-232-245

**Abstract.** Robert McEliece developed an asymmetric encryption algorithm based on the use of binary Goppa codes in 1978 and no effective key attacks has been described yet. Variants of this cryptosystem are known due to the use of different codes types, but most of them were proven to be less secure. Code cryptosystems are considered an alternate to number-theoretical ones in connection with the development of quantum computing. So, the new classes of error-correcting codes are required

for building new resistant code cryptosystems. Non-commutative codes, which simply are ideals of finite non-commutative group algebras, are an option. The Artin–Wedderburn theorem implies that a group algebra is isomorphic to a finite direct sum of matrix algebras, when the order of the group and the field characteristics are relatively prime. This theorem is important to study the structure of a non-commutative code, but it gives no information about summands and the isomorphism. In case of a dihedral group these summands and the isomorphism were found by F. E. Brochero Martinez. The purpose of the paper is to study codes in dihedral group algebras as and when the order of a group and a field characteristics are relatively prime. Using the result of F. E. Brochero Martinez, we consider a structure of all dihedral codes in this case and the codes induced by cyclic subgroup codes.

**Keywords:** non-commutative groups, group algebra, non-commutative codes, code cryptosystems

**On the authors:**
Kirill V. Vedenev, orcid.org/0000-0002-7893-655X, BSc student,
Southern Federal University
105/42 Bolshaya Sadovaya Str., Rostov-on-Don 344006, Russia, e-mail: vedenevk@gmail.com

Vladimir M. Deundyak, orcid.org/0000-0001-8258-2419, PhD,
Southern Federal University
105/42 Bolshaya Sadovaya Str., Rostov-on-Don 344006, Russia,
FGNU NII "Specvuzavtomatika"
51 Gazetniy lane, Rostov-on-Don 344002, Russia, e-mail: vl.deundyak@gmail.com