Математические заметки

Том 107 выпуск 2 февраль 2020

УДК 519.7

Связь кодов и идемпотентов в диэдральной групповой алгебре

К. В. Веденёв, В. М. Деундяк

Исследуются коды в диэдральной групповой алгебре $\mathbb{F}_q D_{2n}$, т.е. левые идеалы в этой алгебре. Для всякого кода в $\mathbb{F}_q D_{2n}$, заданного своим образом в разложении Веддербёрна этой алгебры, построен порождающий идемпотент. С помощью выделенного набора идемпотентов построено обратное преобразование Веддербёрна алгебры $\mathbb{F}_q D_{2n}$. Непосредственно по порождающим идемпотентам некоторых кодов удается описать их образ при разложении Веддербёрна. Рассмотрены примеры применения полученных результатов к индуцированным кодам.

Библиография: 11 названий.

Ключевые слова: диэдральная группа, групповые алгебры, идемпотенты, разложение Веддербёрна, некоммутативные коды.

DOI: https://doi.org/10.4213/mzm12194

Введение

В связи с развитием квантовых вычислений и уязвимостью традиционных асимметричных криптосистем к атакам с использованием квантовых компьютеров возникает необходимость в создании устойчивых постквантовых криптосистем. Одним из вариантов таких систем являются кодовые криптосистемы, впервые описанные Мак-Элисом в [1] для кодов Гоппы. Впоследствии были созданы криптосистемы, основаные на использовании других кодов, таких как коды Рида–Соломона или Рида–Малера, оказавшиеся менее стойкими, чем оригинальная криптосистема Мак-Элиса (см., например, обзоры в [2], [3]). Таким образом, представляется актуальной задача построения и изучения новых классов кодов, применимых в криптографии, в частности, групповых кодов, т.е. левых идеалов в групповых алгебрах (см. [4]–[7]). Ранее авторами в [8] решена задача описания всех кодов в диэдральной групповой алгебре $\mathbb{F}_q D_{2n}$ с использованием построенного Мартинесом в [9] разложения Веддербёрна для $\mathbb{F}_q D_{2n}$. В настоящей статье продолжается изучение кодов в алгебре $\mathbb{F}_q D_{2n}$, а именно установлена связь между кодами и идемпотентами, которая затем применяется для изучения индуцированных кодов (см. [7]). Полученные результаты могут найти применение в построении декодеров для описанных кодов, а также в криптографии [10].

Работа имеет следующую структуру. Раздел 1 содержит необходимые вспомогательные сведения об алгебре $\mathbb{F}_q D_{2n}$. В разделе 2 приведена конструкция обратного преобразования Веддербёрна в терминах фиксированного набора идемпотентов, а в разделе 3 доказана теорема о виде порождающего идемпотента для кода, заданного образом разложения Веддербёрна. В разделе 4 вычислен образ разложения Веддербёрна для некоторых кодов, заданных порождающими идемпотентами. Раздел 5 посвящен применению идемпотентов к индуцированным кодам.

1. Предварительные сведения

Диэдральной группой D_{2n}, $n \geqslant 2$, называется группа, заданная копредставлением $\langle a, b : a^n, b^2, (ba)^2\rangle$, т.е. группа D_{2n} порождается элементами a, b, для которых выполняются следующие соотношения:

$$a^n = e, \qquad b^2 = e, \qquad bab = a^{-1}, \tag{1.1}$$

где e – нейтральный элемент группы. Из (1.1) вытекает, что

$$a^i b = ba^{-i} \tag{1.2}$$

для произвольного целого i, поэтому

$$D_{2n} = \{e, a, a^2, \ldots, a^{n-1}, b, ba, ba^2, \ldots, ba^{n-1}\}. \tag{1.3}$$

Пусть G – конечная группа и $\mathbb{F}_q$ – поле Галуа мощности q. *Групповой алгеброй* $\mathbb{F}_q G$ называется множество формальных линейных комбинаций вида $\alpha = \sum_{g\in G} a_g g$, $a_g \in \mathbb{F}_q$, с покомпонентно определенными операциями сложения и умножения на скаляр и операцией умножения:

$$\Big(\sum_{g\in G} a_g g\Big)\Big(\sum_{g\in G} b_g g\Big) = \sum_{g\in G}\Big(\sum_{h\in G} a_h b_{h^{-1}g}\Big) g.$$

Всякий левый идеал $I \subset \mathbb{F}_q G$ называется *групповым G-кодом* над полем $\mathbb{F}_q$ (см. [4]). Например, множества вида $(\mathbb{F}_q G)t$, где t – произвольный элемент групповой алгебры, являются кодами.

Рассмотрим групповую алгебру $\mathbb{F}_q D_{2n}$. В силу (1.2), (1.3) любой элемент $u \in \mathbb{F}_q D_{2n}$ может быть представлен следующим образом:

$$u = P(a) + bQ(a) = P(a) + Q(a^{-1})b, \tag{1.4}$$

где P и Q – многочлены степени меньшей n. В [9] доказана важная для дальнейшего теорема о виде разложения Веддербёрна для $\mathbb{F}_q D_{2n}$; прежде чем сформулировать ее, приведем в удобном виде необходимые вспомогательные сведения из [9].

Для каждого многочлена $g \in \mathbb{F}_q[x]$ такого, что $g(0) \neq 0$, *возвратным многочленом* называется многочлен $g^*(x) = x^{\deg(g)} g(x^{-1})$. Говорят, что многочлен g самовозвратный, если g и g^* отличаются на постоянный ненулевой множитель.

Далее везде 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 [9; с. 205], запишем это разложение следующим образом:

$$x^n - 1 = (f_1 f_2 \cdots f_r)(f_{r+1} f_{r+1}^* f_{r+2} f_{r+2}^* \cdots f_{r+s} f_{r+s}^*), \tag{1.5}$$

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

Пусть h – неприводимый над полем $\mathbb{F}_q$ многочлен степени m, α – его корень в некотором расширении этого поля; через $\mathbb{F}_q[\alpha]$ обозначим расширение поля $\mathbb{F}_q$ элементом α. Известно, что поля $\mathbb{F}_q[\alpha]$ и $\mathbb{F}[\alpha^{-1}]$ совпадают и изоморфны полю $\mathbb{F}_{q^{\deg h}}$. Наборы

$$\{1, \alpha^1, \alpha^2, \ldots, \alpha^{n-1}\}, \qquad \{1, \alpha^{-1}, \alpha^{-2}, \ldots, \alpha^{-n+1}\}$$

образуют $\mathbb{F}_q$-базисы поля $\mathbb{F}_q[\alpha]$; таким образом, всякий элемент из поля $\mathbb{F}_q[\alpha]$ можно записать как $v(\alpha)$ или $w(\alpha^{-1})$, где $v(x), w(x) \in \mathbb{F}_q[x]$ и $\deg v < m$, $\deg w < m$. Многочлены $v(x)$ и $w(x)$ назовем *полиномиальной записью* числа $v(\alpha) = w(\alpha^{-1})$ относительно α и α^{-1} соответственно.

Обозначим через α_j корень многочлена f_j из (1.5). Пусть

$$\zeta(n) := \begin{cases} 1, & n \text{ – нечетное}, \\ 2, & n \text{ – четное}. \end{cases}$$

Пусть $\mathrm{M}_2[\mathbb{F}]$ – алгебра (2×2)-матриц над полем $\mathbb{F}$. Рассмотрим следующие гомоморфизмы τ_j алгебры $\mathbb{F}_q D_{2n}$:

a) $\tau_1 \colon \mathbb{F}_q D_{2n} \to \mathbb{F}_q \oplus \mathbb{F}_q$, где $\tau_1(P(a) + bQ(a)) = (P(1) + Q(1), P(1) - Q(1))$;

b) $\tau_2 \colon \mathbb{F}_q D_{2n} \to \mathbb{F}_q \oplus \mathbb{F}_q$, где $\tau_2(P(a) + bQ(a)) = (P(-1) + Q(-1), P(-1) - Q(-1))$ для четного n;

c) $\tau_j \colon \mathbb{F}_q D_{2n} \to \mathrm{M}_2(\mathbb{F}_q[\alpha_j])$, где

$$\tau_j(P(a) + bQ(a)) = \begin{pmatrix} P(\alpha_j) & Q(\alpha_j^{-1}) \\ Q(\alpha_j) & P(\alpha_j^{-1}) \end{pmatrix}, \qquad j \geqslant \zeta(n) + 1.$$

Для $j = \zeta(n) + 1, \ldots, r$ рассмотрим автоморфизмы σ_j алгебр $\mathrm{M}_2(\mathbb{F}_q[\alpha_j])$, определяемые формулой

$$\sigma_j(X) := Z_j^{-1} X Z_j, \qquad Z_j := \begin{pmatrix} 1 & -\alpha_j \\ 1 & -\alpha_j^{-1} \end{pmatrix}. \tag{1.6}$$

В [9; с. 208], установлено, что $\sigma_j(\mathrm{im}(\tau_j)) = \mathrm{M}_2(\mathbb{F}_q[\alpha_j + \alpha_j^{-1}])$ при $\zeta(n) + 1 \leqslant j \leqslant r$.

Теорема 1 [9]. *Пусть* $\gcd(q, 2n) = 1$. *Тогда имеет место следующий изоморфизм алгебр*:

$$p = \bigoplus_{j=1}^{r+s} p_j \colon \mathbb{F}_q D_{2n} \to \bigoplus_{j=1}^{r+s} A_j, \tag{1.7}$$

где

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

$$p_j := \begin{cases} \sigma_j \circ \tau_j, & \zeta(n) + 1 \leqslant j \leqslant r, \\ \tau_j, & 1 \leqslant j \leqslant \zeta(n),\ r + 1 \leqslant j \leqslant r + s. \end{cases}$$

Рассмотрим разложение (1.7) и обозначим

$$R_j := \begin{cases} \mathbb{F}_q, & 1 \leqslant j \leqslant \zeta(n), \\ \mathbb{F}_q[\alpha_j + \alpha_j^{-1}], & \zeta(n)+1 \leqslant j \leqslant r, \\ \mathbb{F}_q[\alpha_j], & r+1 \leqslant j \leqslant r+s. \end{cases} \tag{1.8}$$

Определим

$$I_j(x,y) := \begin{cases} \{kx, ty \mid k,t \in \mathbb{F}_q\}, & 1 \leqslant j \leqslant \zeta(n), \\ \left\{ \begin{pmatrix} ky & -kx \\ ty & -tx \end{pmatrix} \mid k,t \in R_j \right\}, & \zeta(n)+1 \leqslant j \leqslant r+s. \end{cases} \tag{1.9}$$

Замечание 1. Отметим, что $I_j(x,y) = I_j(\mu x, \mu y)$ для любого ненулевого $\mu \in R_j$. Таким образом, для $1 \leqslant j \leqslant \zeta(n)$ достаточно рассматривать $I_j(1,0)$, $I_j(0,1)$, а для $\zeta(n)+1 \leqslant j \leqslant r+s$ достаточно рассматривать $I_j(0,1)$, $I_j(q,1)$, где $q \in R_j$.

В [8] с помощью теоремы 1 доказана следующая теорема о структуре кодов в алгебре $\mathbb{F}_q D_{2n}$. Приведем ее в удобном для дальнейшего виде.

Теорема 2. *Пусть* $\gcd(q,2n) = 1$. *Рассмотрим разложение* (1.7) *групповой алгебры* $\mathbb{F}_q D_{2n}$. *Для любого кода* $I \subset \mathbb{F}_q D_{2n}$ *найдутся такие непересекающиеся множества* $J_1, J_2, J_3 \subset \{1, \ldots, r+s\}$ *и набор чисел* $\{q_j\}_{j \in J_2}$, *где* $q_j \in R_j$, *что*

$$p(I) = \bigoplus_{j=1}^{r+s} B_j, \tag{1.10}$$

$$B_j = \begin{cases} A_j, & j \in J_1, \\ I_j(-q_j, 1), & j \in J_2 \setminus \{1, \zeta(n)\}, \\ I_j(0,1), & j \in J_2 \cap \{1, \zeta(n)\}, \\ I_j(1,0), & j \in J_3, \\ 0, & j \notin J_1 \cup J_2 \cup J_3. \end{cases} \tag{1.11}$$

С другой стороны, для любых попарно непересекающихся множеств $J_1, J_2, J_3 \subset \{1, \ldots, r+s\}$ *и для любого набора чисел* $\{q_j\}_{j \in J_2}$, $q_j \in R_j$, *множество*

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

где B_j *определены равенством* (1.11), *является кодом в* $\mathbb{F}_q D_{2n}$.

Замечание 2. 1) Для $j \in J_2 \setminus \{1, \zeta(n)\}$ число q_j из набора $\{q_j\}_{j \in J_2}$ может быть равно 0.

2) Прямые слагаемые B_j с номерами $1 \leqslant j \leqslant r$ соответствуют самовозвратным многочленам из (1.5), а с номерами $r+1 \leqslant j \leqslant r+s$ – несамовозвратным.

2. Конструкция изоморфизма p^{-1} с помощью идемпотентов

Идемпотентом называется такой элемент i некоторого кольца K, что $i^2 = i$. Идемпотент i называется *центральным*, если i лежит в центре кольца; идемпотент i называется *неразложимым*, если его нельзя разложить в сумму нескольких отличных от нуля идемпотентов (см. [11; с. 75]). В этом разделе получена конструкция изоморфизма p^{-1} в терминах некоторого набора идемпотентов.

Известно, что если $\gcd(|G|, q) = 1$, то групповая алгебра $\mathbb{F}_q G$ в силу теоремы Машке (см. [11; с. 140]) является полупростой. Известно также, что всякий левый идеал I произвольной полупростой алгебры A имеет вид $I = Ai$, где i – идемпотент (см. [11; с. 95]). Элемент i называется *порождающим идемпотентом* кода I.

Пусть $\mathcal{R}_n = \mathbb{F}_q[x]/\langle x^n - 1\rangle$. В [9] доказано, что для нормированного многочлена $f(x)$, делителя $x^n - 1$, и нормированного многочлена $g(x) := (x^n - 1)/f(x)$ элемент

$$e_g(x) := -\frac{[(g(x)^*)']^*}{n} \cdot \frac{x^n - 1}{g(x)} \tag{2.1}$$

является идемпотентом, порождающим идеал $\mathcal{R}_n[f(x)]$, где $[f(x)] \in \mathcal{R}_n$. Отметим далее некоторые свойства идемпотентов алгебры $\mathcal{R}_n$.

Лемма 1. *Пусть* $\gcd(q, n) = 1$, $g(x) \in \mathcal{R}_n$ *– нормированный делитель многочлена* $x^n - 1$, $g(x) = g_1(x)g_2(x)$. *Тогда*

$$e_g(x) = e_{g_1}(x) + e_{g_2}(x).$$

Доказательство. Непосредственно вычисляется, что

$$\begin{aligned}((g^*)')^*(x) &= x^{\deg(g_1)+\deg(g_2)-1}((g_1^*)'g_2^* + g_1^*(g_2^*)')^*\left(\frac{1}{x}\right)\\ &= ((g_1^*)')^*(x)g_2(x) + g_1(x)((g_2^*)')^*(x).\end{aligned}$$

Таким образом, из (2.1) получаем

$$e_g(x) = \frac{x^n - 1}{ng_1(x)g_2(x)}[((g_1^*)')^*(x)g_2(x) + g_1(x)((g_2^*)')^*(x)] = e_{g_1}(x) + e_{g_2}(x).$$

Лемма 2. *Пусть* $\gcd(q, n) = 1$. *Тогда для всякого идеала в* $\mathcal{R}_n$ *существует ровно один порождающий идемпотент.*

Доказательство. *Существование* порождающего идемпотента вытекает из равенства (2.1).

Докажем *единственность*. Соответствие

$$\phi\colon P(x) \mapsto (P(x) \bmod f_1(x), \ldots, P(x) \bmod f_r^*(x))$$

в силу китайской теоремы об остатках задает изоморфизм

$$\phi\colon \mathcal{R}_n \to \bigoplus_{i=1}^{r+s} \frac{\mathbb{F}_q[x]}{\langle f_i(x)\rangle} \oplus \bigoplus_{i=r+1}^{r+s} \frac{\mathbb{F}_q[x]}{\langle f_i^*(x)\rangle}.$$

Из того, что многочлены $f_i(x)$, $f_i^*(x)$ неприводимы над $\mathbb{F}_q$, следует, что $\mathbb{F}_q[x]/\langle f_i(x)\rangle$, $\mathbb{F}_q[x]/\langle f_i^*(x)\rangle$ – поля. Таким образом, если $t(x)$ – идемпотент в $\mathcal{R}_n$, то для произвольного неприводимого делителя $p(x)$ многочлена x^n-1 должно выполняться одно из следующих равенств:

$$t(x)\equiv 0(\operatorname{mod} p(x)), \qquad t(x)\equiv 1(\operatorname{mod} p(x)).$$

Известно, что всякий идеал в прямой сумме алгебр является прямой суммой идеалов в соответствующих слагаемых. Поэтому, если $t_1(x)$, $t_2(x)$ – два идемпотента, порождающих один и тот же идеал в $\mathcal{R}_n$, то для всякого неприводимого делителя $p(x)$ многочлена x^n-1 справедливы соотношения $t_1(x)\equiv t_2(x)(\operatorname{mod} p(x))$, откуда $t_1(x)=t_2(x)$.

Отметим, что если $C_n=\langle h\rangle$ – циклическая группа порядка n, порожденная элементом h, то гомоморфизм $\Phi\colon \mathbb{F}_qC_n\to\mathcal{R}_n$, заданный равенством $\Phi(h)=[x]$, является изоморфизмом. Таким образом, элементы $e_g(a)\in\mathbb{F}_qD_{2n}$ являются идемпотентами в алгебре $\mathbb{F}_qD_{2n}$ (см. (2.1)).

Через $\delta_{i,j}$ обозначим единицу алгебры A_j из (1.7), если $i=j$, и нулевой элемент алгебры A_i, если $i\neq j$. В [9] выделен набор центральных неразложимых идемпотентов в $\mathbb{F}_qD_{2n}$; приведем этот результат в удобном виде.

Лемма 3 [9]. *Пусть* $\gcd(q,2n)=1$. *Рассмотрим разложение* (1.7) *групповой алгебры* $\mathbb{F}_qD_{2n}$. *Алгебра* $\mathbb{F}_qD_n$ *содержит следующие центральные неразложимые идемпотенты*:

(i) $2\zeta(n)$ *идемпотентов вида*

$$\frac{1+b}{2}\,e_{f_j}(a) \quad и \quad \frac{1-b}{2}\,e_{f_j}(a), \qquad где \quad 1\leqslant j\leqslant\zeta(n),$$

причем

$$p\left(\frac{1+b}{2}\,e_{f_j}(a)\right)=\bigoplus_{i=1}^{r+s}\delta_{i,j}(1,0), \qquad p\left(\frac{1-b}{2}\,e_{f_j}(a)\right)=\bigoplus_{i=1}^{r+s}\delta_{i,j}(0,1);$$

(ii) $r-\zeta(n)$ *идемпотентов вида* $e_{f_j}(a)$, *где* $j=\zeta(n)+1,\dots,r$, *причем*

$$p(e_{f_j}(a))=\bigoplus_{i=1}^{r+s}\delta_{i,j}\begin{pmatrix}1&0\\0&1\end{pmatrix};$$

(iii) s *идемпотентов вида* $e_{f_j}(a)+e_{f_j^*}(a)$, *где* $r+1\leqslant j\leqslant r+s$, *причем*

$$p(e_{f_j}(a))=\bigoplus_{i=1}^{r+s}\delta_{i,j}\begin{pmatrix}1&0\\0&0\end{pmatrix}, \qquad p(e_{f_j^*}(a))=\bigoplus_{i=1}^{r+s}\delta_{i,j}\begin{pmatrix}0&0\\0&1\end{pmatrix}.$$

Набор идемпотентов $e_{f_j}(a)$, $e_{f_j^*}(a)$ позволяет удобно описать обратный к изоморфизму p (см. (1.7)). С использованием обозначений из предыдущего раздела в следующей теореме получена конструкция p^{-1}.

Теорема 3. *Пусть* $\gcd(q,2n)=1$, *мономорфизмы* $\epsilon_j\colon A_j\to\mathbb{F}_qD_{2n}$ *заданы следующим образом*:

(i) *для* $1 \leqslant j \leqslant \zeta(n)$

$$\epsilon_j(w_1, w_2) := w_1 \frac{1+b}{2} e_{f_j}(a) + w_2 \frac{1-b}{2} e_{f_j}(a), \qquad w_1, w_2 \in \mathbb{F}_q,$$

(ii) *для* $r+1 \leqslant j \leqslant r+s$

$$\epsilon_j\left(\begin{pmatrix} M(\alpha_j) & P(\alpha_j^{-1}) \\ N(\alpha_j) & Q(\alpha_j^{-1}) \end{pmatrix}\right) := [M(a) + bN(a)]e_{f_j}(a) + [Q(a) + bP(a)]e_{f_j^*}(a),$$

(iii) $\epsilon_j := \gamma_j \sigma_j^{-1}$ *для* $\zeta(n)+1 \leqslant j \leqslant r$, *автоморфизм* σ_j *определен в* (1.6), *а мономорфизм* $\gamma_j \colon \mathrm{im}(\tau_\mathrm{j}) \to \mathbb{F}_\mathrm{q}\mathrm{D}_{2\mathrm{n}}$ *задан формулой*

$$\gamma_j\left(\begin{pmatrix} P(\alpha_j) & Q(\alpha_j^{-1}) \\ Q(\alpha_j) & P(\alpha_j^{-1}) \end{pmatrix}\right) := P(a)e_{f_j}(a) + bQ(a)e_{f_j}(a),$$

где в (ii), (iii) *при записи произвольного элемента из* A_j *используются полиномиальные записи элементов* $\mathbb{F}_q[\alpha_j]$ *относительно* α_j *и* α_j^{-1}. *Тогда* $p^{-1} = \sum_{j=1}^{r+s} \epsilon_j$.

Доказательство. Для $1 \leqslant j \leqslant \zeta(n)$ из утверждения (i) леммы 3 вытекает, что

$$p\epsilon_j(w_1, w_2) = \bigoplus_{i=1}^{r+s} \delta_{i,j}(w_1, w_2).$$

Из утверждений (ii), (iii) леммы 3 и равенства

$$\tau_j(b) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \zeta(n)+1 \leqslant j \leqslant r+s,$$

в силу определения (1.7) изоморфизма p следует, что для любого $X_j \in A_j$

$$p\epsilon_j(X_j) = \bigoplus_{i=1}^{r+s} \delta_{i,j} X_j, \qquad \zeta(n)+1 \leqslant j \leqslant r+s.$$

Таким образом, $p^{-1} = \sum_{j=1}^{r+s} \epsilon_j$.

3. Порождающий идемпотент кода, заданного разложением Веддербёрна

Ниже для произвольного кода в алгебре $\mathbb{F}_q D_{2n}$, заданного своим образом при разложении Веддербёрна, будет построен порождающий идемпотент. В связи с этим потребуются следующие вспомогательные леммы об идемпотентах.

Непосредственно из леммы 3 вытекает следующее утверждение.

Лемма 4. *Пусть* $\gcd(q, 2n) = 1$. *Рассмотрим разложение* (1.7) *групповой алгебры* $\mathbb{F}_q D_{2n}$. *Тогда при* $1 \leqslant j \leqslant \zeta(n)$

(i) *для идемпотента* $z_j := ((1+b)/2)e_{f_j}(a)$ *справедливо*

$$p(\mathbb{F}_q D_{2n} z_j) = \bigoplus_{i=1}^{r+s} \delta_{i,j} I_j(1, 0), \tag{3.1}$$

(ii) *для идемпотента* $t_{j,0} := ((1-b)/2)e_{f_j}(a)$ *справедливо*

$$p(\mathbb{F}_q D_{2n} t_{j,0}) = \bigoplus_{i=1}^{r+s} \delta_{i,j} I_j(0,1). \tag{3.2}$$

Лемма 5. *Пусть* $\gcd(q,2n)=1$. *Рассмотрим разложение* (1.7) *групповой алгебры* $\mathbb{F}_q D_{2n}$. *Тогда при* $r+1 \leqslant j \leqslant r+s$

(i) *для идемпотента* $z_j := e_{f_j^*}(a)$ *справедливо*

$$p(\mathbb{F}_q D_{2n} z_j) = \bigoplus_{i=1}^{r+s} \delta_{i,j} I_j(1,0). \tag{3.3}$$

(ii) *элемент* $t_{j,Q} := e_{f_j}(a) + bQ(a)e_{f_j^*}(a)$, *где* $Q(x) \in \mathbb{F}_q[x]$ – *произвольный многочлен, является идемпотентом в* $\mathbb{F}_q D_{2n}$, *причем*

$$p(\mathbb{F}_q D_{2n} t_{j,Q}) = \bigoplus_{i=1}^{r+s} \delta_{i,j} I_j(-Q(\alpha_j^{-1}),1). \tag{3.4}$$

Доказательство. В силу утверждения (iii) леммы 3

$$p(z_j) = p(e_{f_j^*}(a)) = \bigoplus_{i=1}^{r+s} \delta_{i,j} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \tag{3.5}$$

из которого с помощью (1.7), (1.9) получаем утверждение (i).

Докажем теперь утверждение (ii). Из (3.5), (1.7) вытекает

$$p(Q(a)e_{f_j^*}(a)) = \bigoplus_{i=1}^{r+s} \delta_{i,j} \begin{pmatrix} 0 & 0 \\ 0 & Q(\alpha_j^{-1}) \end{pmatrix}, \qquad p_j(b) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Следовательно,

$$p(bQ(a)e_{f_j^*}(a)) = \bigoplus_{i=1}^{r+s} \delta_{i,j} \begin{pmatrix} 0 & Q(\alpha_j^{-1}) \\ 0 & 0 \end{pmatrix}, \qquad p(t_{j,Q}) = \bigoplus_{i=1}^{r+s} \delta_{i,j} \begin{pmatrix} 1 & Q(\alpha_j^{-1}) \\ 0 & 0 \end{pmatrix}.$$

В силу равенства

$$\begin{pmatrix} 1 & Q(\alpha_j^{-1}) \\ 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 1 & Q(\alpha_j^{-1}) \\ 0 & 0 \end{pmatrix}$$

получаем $p(t_{j,Q}^2) = p(t_{j,Q})$, $t_{j,Q}^2 = t_{j,Q}$, т.е. $t_{j,Q}$ – идемпотент. Равенство (3.4) теперь вытекает из (1.9).

Лемма 6. *Пусть* $\gcd(q,2n)=1$. *Рассмотрим разложение* (1.7) *групповой алгебры* $\mathbb{F}_q D_{2n}$. *Тогда для* $\zeta(n)+1 \leqslant j \leqslant r$ *справедливы следующие утверждения.*

1. *Для идемпотента* $z_j := ((1-b)/2)e_{f_j}(a)$ *имеет место равенство*

$$p(\mathbb{F}_q D_{2n} z_j) = \bigoplus_{i=1}^{r+s} \delta_{i,j} I_j(1,0).$$

2. *Пусть*

$$(x-1)F_1(x)+f_j(x)F_2(x)=1,$$
$$(x+1)G_1(x)+f_j(x)G_2(x)=1$$

– *соотношения Безу для* $\gcd(f_j(x),x-1)$, $\gcd(f_j(x),x+1)$ *соответственно*;

$$u_{j,Q}(x):=(xQ(x+x^{n-1})-1)F_1(x)G_1(x),$$

где $Q(x)\in\mathbb{F}_q[x]$. *Тогда элемент* $t_{j,Q}:=u_{j,Q}(a)e_{f_j}(a)+bu_{j,Q}(a)e_{f_j}(a)$ *является идемпотентом в алгебре* $\mathbb{F}_qD_{2n}$, *причем*

$$p(\mathbb{F}_qD_{2n}t_{j,Q})=\bigoplus_{i=1}^{r+s}\delta_{i,j}I_j(-Q(\alpha_j+\alpha_j^{-1}),1).$$

Доказательство. Вычислим $p(z_j)$, используя (1.6), (1.7) и утверждение (ii) леммы 3:

$$p(z_j)=\bigoplus_{i=1}^{r+s}\delta_{i,j}Z_j^{-1}\tau_j(z_j)Z_j=\bigoplus_{i=1}^{r+s}\delta_{i,j}\begin{pmatrix}0 & \frac{1}{2}(\alpha_j+\alpha_j^{-1})\\ 0 & 1\end{pmatrix}.$$

Отсюда в силу (1.7), (1.9) следует справедливость пункта 1.

Теперь докажем пункт 2. Из равенств $f_j(\alpha_j)=0$, $f_j(\alpha_j^{-1})=0$ получаем, что

$$F_1(\alpha_j)=(\alpha_j-1)^{-1},\qquad F_1(\alpha_j^{-1})=(\alpha_j^{-1}-1)^{-1},$$
$$G_1(\alpha_j)=(\alpha_j+1)^{-1},\qquad G_1(\alpha_j^{-1})=(\alpha_j^{-1}+1)^{-1}.$$

Элемент α_j – корень многочлена x^n-1, поэтому $\alpha_j^{-1}=\alpha_j^{n-1}$. Тогда

$$u_{j,Q}(\alpha_j)=\frac{\alpha_jQ(\alpha_j+\alpha_j^{-1})-1}{(\alpha_j-1)(\alpha_j-1)}=\frac{Q(\alpha_j+\alpha_j^{-1})-\alpha_j^{-1}}{\alpha_j-\alpha_j^{-1}},$$
$$u_{j,Q}(\alpha_j^{-1})=-\frac{Q(\alpha_j+\alpha_j^{-1})-\alpha_j}{\alpha_j-\alpha_j^{-1}}.$$

Теперь вычислим $p(t_{j,Q})$. Имеем

$$p(t_{j,Q})=\bigoplus_{i=1}^{r+s}\delta_{i,j}Z_j^{-1}\tau_j(z_j)Z_j=\bigoplus_{i=1}^{r+s}\delta_{i,j}\begin{pmatrix}1 & Q(\alpha_j+\alpha_j^{-1})\\ 0 & 0\end{pmatrix},$$

что в силу (1.9) и доказывает пункт 2.

В леммах 3–6 описан набор идемпотентов, с помощью которых представим ниже порождающий идемпотент произвольного кода. Обозначим

$$\omega_j:=\begin{cases}e_{f_j}(a), & 1\leqslant j\leqslant r,\\ e_{f_j}(a)+e_{f_j^*}(a), & r+1\leqslant j\leqslant r+s.\end{cases}$$

ТЕОРЕМА 4. *Пусть* $\gcd(q, 2n) = 1$. *Рассмотрим произвольный код* $I \subset \mathbb{F}_q D_{2n}$, *который по теореме 2 имеет разложение*

$$p(I) = \bigoplus_{j=1}^{r+s} B_j, \qquad B_j = \begin{cases} A_j, & j \in J_1, \\ I_j(-q_j, 1), & j \in J_2, \\ I_j(1, 0), & j \in J_3, \\ 0, & j \notin J_1, J_2, J_3, \end{cases}$$

где

$$q_j = \begin{cases} -Q_j(\alpha_j + \alpha_j^{-1}), & \zeta(n) + 1 \leqslant j \leqslant r, \\ -Q_j(\alpha_j^{-1}), & 1 \leqslant j \leqslant \zeta(n),\ r + 1 \leqslant j \leqslant r + s, \end{cases} \qquad Q_j \in \mathbb{F}_q[x].$$

Тогда

$$e_I = \sum_{j \in J_1} \omega_j + \sum_{j \in J_2} t_{j,Q_j} + \sum_{j \in J_3} z_j$$

– *идемпотент, порождающий код* I.

ДОКАЗАТЕЛЬСТВО. Из определения e_I вытекает

$$p(\mathbb{F}_q D_{2n} e_I) = \sum_{j \in J_1} p(\mathbb{F}_q D_{2n} \omega_j) + \sum_{j \in J_2} p(\mathbb{F}_q D_{2n} t_{j,Q_j}) + \sum_{j \in J_3} p(\mathbb{F}_q D_{2n} z_j).$$

Отсюда в силу лемм 3–6 и определения B_j получаем

$$p(\mathbb{F}_q D_{2n} e_I) = \bigoplus_{i=1}^{r+s} \left(\sum_{j \in J_1} \delta_{i,j} A_j + \sum_{j \in J_2} \delta_{i,j} I_j(-q_j, 1) + \sum_{j \in J_3} \delta_{i,j} I_j(1, 0) \right) = \bigoplus_{j=1}^{r+s} B_j = p(I).$$

Таким образом, $I = (\mathbb{F}_q D_{2n}) e_I$, т.е. e_I – порождающий идемпотент кода I.

4. Образ разложения Веддербёрна для кода, заданного порождающим идемпотентом

В теореме 2 описана структура кодов в терминах их образов при разложении Веддербёрна. Следующая же теорема позволяет для некоторых кодов, заданных порождающими идемпотентами, вычислить явно образ разложения Веддербёрна.

ТЕОРЕМА 5. *Пусть* $\gcd(q, 2n) = 1$. *Рассмотрим произвольный код* $I \subset \mathbb{F}_q D_{2n}$, *порожденный идемпотентом* $\lambda \in \mathbb{F}_q D_{2n}$. *Обозначим*

$$\theta_j = \lambda e_{f_j}(a), \qquad 1 \leqslant j \leqslant r + s,$$
$$\widetilde{\theta}_j = \lambda e_{f_j^*}(a), \qquad r + 1 \leqslant j \leqslant r + s.$$

Рассмотрим образ разложения Веддербёрна для кода I

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

Тогда компоненты B_j *находятся по элементам* θ_j, $\widetilde{\theta}_j$ *следующим образом*:

(i) *при* $1 \leqslant j \leqslant \zeta(n)$:

$$\theta_j = 0 \quad \Longrightarrow \quad B_j = 0, \qquad \theta_j = \frac{1+b}{2} e_{f_j}(a) \quad \Longrightarrow \quad B_j = I_j(1,0),$$
$$\theta_j = e_{f_j}(a) \quad \Longrightarrow \quad B_j = A_j, \qquad \theta_j = \frac{1-b}{2} e_{f_j}(a) \quad \Longrightarrow \quad B_j = I_j(0,1),$$

других значений θ_j *принимать не может*;

(ii) *при* $\zeta(n)+1 \leqslant j \leqslant r$:

$$\theta_j = 0 \quad \Longrightarrow \quad B_j = 0, \qquad \theta_j = e_{f_j}(a) \quad \Longrightarrow \quad B_j = A_j.$$

(iii) *при* $r+1 \leqslant j \leqslant r+s$, *если* $\theta_j = e_{f_j}(a)$, $\widetilde{\theta}_j = e_{f_j^*}(a)$, *то* $B_j = A_j$; *в противном случае, если* $\theta_j = g_j(a) + bh_j(a)$, $\widetilde{\theta}_j = \widetilde{g}_j(a) + b\widetilde{h}_j(a)$, *где* $g_j, \widetilde{g}_j, h_j, \widetilde{h}_j \in \mathbb{F}_q[x]$ (*см.* (1.4)), *то*

$$B_j = \begin{cases} I_j(\widetilde{h}_j(\alpha_j^{-1}), -g_j(\alpha_j)), & \text{если } (\widetilde{h}_j(\alpha_j^{-1}), g_j(\alpha_j)) \neq (0,0), \\ I_j(\widetilde{g}_j(\alpha_j^{-1}), -h_j(\alpha_j)), & \\ \qquad \text{если } \widetilde{h}_j(\alpha_j^{-1}) = g_j(\alpha_j) = 0, \ (\widetilde{g}_j(\alpha_j^{-1}), h_j(\alpha_j)) \neq (0,0), & \\ 0, \qquad \text{если } \widetilde{h}_j(\alpha_j^{-1}) = g_j(\alpha_j) = \widetilde{g}_j(\alpha_j^{-1}) = h_j(\alpha_j) = 0. \end{cases}$$

Замечание 3. В пункте (iii) в случае $\theta_j = 0$, $\widetilde{\theta}_j = 0$ получается $B_j = I_j(0,0) = 0$.

Доказательство. Прежде чем приступить к доказательству утверждений теоремы, покажем, что компоненты B_j полностью определяются элементами θ_j, $\widetilde{\theta}_j$. Из равенств леммы 3 получаем, что

$$p(e_{f_j}(a)) = \bigoplus_{i=1}^{r+s} \delta_{i,j}, \qquad 1 \leqslant j \leqslant r,$$
$$p(e_{f_j}(a) + e_{f_j^*}(a)) = \bigoplus_{i=1}^{r+s} \delta_{i,j}, \qquad r+1 \leqslant j \leqslant r+s.$$

Отсюда вытекает

$$\sum_{j=1}^{r} e_{f_j}(a) + \sum_{j=r+1}^{r+s} (e_{f_j}(a) + e_{f_j^*}(a)) = 1.$$

Тогда

$$\lambda = \lambda 1 = \sum_{j=1}^{r} \theta_j + \sum_{j=r+1}^{r+s} (\theta_j + \widetilde{\theta}_j).$$

Пусть $p(\lambda) = \bigoplus_{j=1}^{r+s} \lambda_j$, $\lambda_j \in A_j$. Легко видеть, что при $1 \leqslant j \leqslant r$ выполняется

$$p(\theta_j) = p(\lambda e_{f_j}(a)) = p(\lambda) \bigoplus_{i=1}^{r+s} \delta_{i,j} = \bigoplus_{i=1}^{r+s} \delta_{i,j} \lambda_j, \tag{4.1}$$

аналогично при $r+1 \leqslant j \leqslant r+s$

$$p(\theta_j + \widetilde{\theta}_j) = \bigoplus_{i=1}^{r+s} \delta_{i,j} \lambda_j. \tag{4.2}$$

Таким образом, вид λ_j легко установить по θ_j, $\widetilde{\theta}_j$. В свою очередь, из того, что

$$p(I) = p(\mathbb{F}_q D_{2n}\lambda) = \bigoplus_{j=1}^{r+s} A_j\lambda_j,$$

получаем $B_j = A_j\lambda_j$.

Докажем утверждение (i). Идемпотент λ_j алгебры A_j $(= \mathbb{F}_q \oplus \mathbb{F}_q)$ может принимать только значения $(0,0)$, $(0,1)$, $(1,0)$, $(1,1)$; тогда в силу (4.1) выполняется одно из равенств

$$p(\theta_j) = \bigoplus_{i,j} \delta_{i,j}(0,0), \qquad p(\theta_j) = \bigoplus_{i,j} \delta_{i,j}(0,1),$$
$$p(\theta_j) = \bigoplus_{i,j} \delta_{i,j}(1,0), \qquad p(\theta_j) = \bigoplus_{i,j} \delta_{i,j}(1,1).$$

При этом лемма 3 однозначно устанавливает вид θ_j для каждого из вариантов λ_j.

Доказательство для случая (ii) немедленно следует из (4.1) и леммы 3.

Рассмотрим случай (iii). Из (1.7) и п. (iii) леммы 3, если $\theta_j = g_j(a) + bh_j(a)$, $\widetilde{\theta}_j = \widetilde{g}_j(a) + b\widetilde{h}_j(a)$, то

$$\lambda_j \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} g_j(\alpha_j) & 0 \\ h_j(\alpha_j) & 0 \end{pmatrix}, \qquad \lambda_j \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & \widetilde{h}_j(\alpha_j) \\ 0 & \widetilde{g}_j(\alpha_j) \end{pmatrix},$$

откуда

$$\lambda_j = \begin{pmatrix} g_j(\alpha_j) & \widetilde{h}_j(\alpha_j^{-1}) \\ h_j(\alpha_j) & \widetilde{g}_j(\alpha_j^{-1}) \end{pmatrix}.$$

Очевидно, что если $\theta_j = 0$, $\widetilde{\theta}_j = 0$, то $\lambda_j = 0$, откуда $B_j = 0$, а если $\theta_j = e_{f_j}(a)$, $\widetilde{\theta}_j = e_{f_j^*}(a)$, то λ_j – единичная матрица и $B_j = A_j$.

Отметим, что так как по определению λ_j – идемпотент, то из линейной независимости строк матрицы λ_j следует, что λ_j – единичная матрица. Поэтому в случае, когда $\theta_j \neq 0$, $\widetilde{\theta}_j \neq 0$ и $\theta_j \neq e_{f_j}(a)$, $\widetilde{\theta}_j \neq e_{f_j^*}(a)$, справедливо равенство

$$B_j = \begin{cases} I_j(\widetilde{h}_j(\alpha_j^{-1}), -g_j(\alpha_j)), & \text{если } (\widetilde{h}_j(\alpha_j^{-1}), g_j(\alpha_j)) \neq (0,0), \\ I_j(\widetilde{g}_j(\alpha_j^{-1}), -h_j(\alpha_j)), & \text{если } (\widetilde{g}_j(\alpha_j^{-1}), h_j(\alpha_j)) \neq (0,0), \\ 0, & \text{если } (\widetilde{h}_j(\alpha_j^{-1}), g_j(\alpha_j)) = (\widetilde{g}_j(\alpha_j^{-1}), h_j(\alpha_j)) = (0,0). \end{cases}$$

Замечание 4. В пункте (iii), если

$$(\widetilde{h}_j(\alpha_j^{-1}), g_j(\alpha_j)) \neq (0,0), \qquad (\widetilde{g}_j(\alpha_j^{-1}), h_j(\alpha_j)) \neq (0,0),$$

то

$$I_j(\widetilde{h}_j(\alpha_j^{-1}), -g_j(\alpha_j)) = I_j(\widetilde{g}_j(\alpha_j^{-1}), -h_j(\alpha_j)).$$

Замечание 5. В пункте (ii) в общем случае по θ_j явно установить вид B_j может быть затруднительно. Если $\theta_j \neq 0$ и $\theta_j \neq e_{f_j}(a)$, то B_j может принимать значения $I_j(1,0)$ или $I_j(q_j,1)$. Для нахождения B_j необходимо явно вычислить $p(\mathbb{F}_q D_{2n}\theta_j)$.

5. Применение идемпотентов к индуцированным кодам

В [7] рассмотрен способ переноса кода из групповой алгебры над подгруппой в групповую алгебру над всей группой. Пусть G – конечная группа, H – ее подгруппа, $\mathcal{T}$ – правая трансверсаль G по H. Напомним, что множество $\mathcal{T}$ называется *правой трансверсалью* группы G по подгруппе H, если всякий правый смежный класс по подгруппе H содержит ровно один элемент из $\mathcal{T}$. Множество $J = (\mathbb{F}_q G)I$ $(\subset \mathbb{F}_q G)$ назовем *кодом*, *индуцированным кодом* I $(\subset \mathbb{F}_q H)$. Отметим, что если элемент $i \in \mathbb{F}_q H$ порождает код I, т.е. $I = (\mathbb{F}_q H)i$, то в силу равенства

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

элемент i порождает и индуцированный код J.

В [8] описаны все подгруппы диэдральной группы и показано, что они изоморфны циклическим группам или диэдральным группам с меньшими параметрами. Ниже, применив результаты предыдущих разделов, рассмотрим примеры вычисления образов некоторых индуцированных кодов при разложении Веддербёрна (1.7).

5.1. Коды, индуцированные циклическими кодами. Пусть $\gcd(n, q) = 1$, k – натуральный делитель числа n. Рассмотрим алгебру $\widehat{\mathcal{R}}_{n/k} := \mathbb{F}_q[\widehat{x}]/\langle \widehat{x}^{\,n/k} - 1\rangle$ и аналогично (2.1) определим идемпотент

$$\widehat{e}_g(\widehat{x}) := -\frac{[(g(\widehat{x})^*)']^*}{n/k} \cdot \frac{\widehat{x}^{\,n/k} - 1}{g(\widehat{x})}$$

для нормированного делителя $g(\widehat{x}) \in \widehat{\mathcal{R}}_n$ многочлена $\widehat{x}^{\,n/k} - 1$.

Лемма 7. *Если $P(x)$ – неприводимый нормированный делитель $x^{n/k} - 1$, то*

$$\widehat{e}_P(x^k) = \left(\sum_{\substack{i=1 \\ f_i(x) | P(x^k)}}^{r+s} e_{f_i}(x) \right) + \left(\sum_{\substack{i=r+1 \\ f_i^*(x) | P(x^k)}}^{r+s} e_{f_i^*}(x) \right). \tag{5.1}$$

Доказательство. Рассмотрим алгебры $\mathcal{R}_n$ и $\widehat{\mathcal{R}}_{n/k}$ и вложение

$$\psi\colon \widehat{\mathcal{R}}_{n/k} \to \mathcal{R}_n, \qquad \widehat{x} \mapsto x^k.$$

В силу равенства $\widehat{e}_P(x^k) = \psi(\widehat{e}_P(\widehat{x}))$ получаем, что $\widehat{e}_P(x^k)$ – идемпотент в $\mathcal{R}_n$. По определению (2.1) идемпотент $\widehat{e}_P(\widehat{x})$ порождает идеал $\widehat{\mathcal{R}}_{n/k}(\widehat{x}^{\,n/k} - 1)/P(\widehat{x})$, т.е.

$$\widehat{\mathcal{R}}_{n/k} \frac{\widehat{x}^{\,n/k} - 1}{P(\widehat{x})} = \widehat{\mathcal{R}}_{n/k} \widehat{e}_P(\widehat{x}).$$

Откуда, учитывая равенство $\mathcal{R}_n \psi(\widehat{\mathcal{R}}_{n/k}) = \mathcal{R}_n$, получаем

$$\mathcal{R}_n \widehat{e}_P(x^k) = \mathcal{R}_n \psi(\widehat{\mathcal{R}}_{n/k} \widehat{e}_P(\widehat{x})) = \mathcal{R}_n \psi\left(\widehat{\mathcal{R}}_{n/k} \frac{\widehat{x}^{\,n/k} - 1}{P(\widehat{x})} \right) = \mathcal{R}_n \frac{x^n - 1}{P(x^k)}.$$

Тогда $e_P(x^k)$ – порождающий идемпотент идеала $\mathcal{R}_n(x^n - 1)/P(x^k)$ кольца $\mathcal{R}_n$, в силу леммы 2 этот идемпотент единственный, а в силу леммы 1 идемпотент $e_P(x^k)$ имеет вид (5.1).

Замечание 6. Отметим, что если многочлен $f(x)$ делит многочлен $g(x)$, то и возвратный многочлен $f^*(x)$ делит $g^*(x)$.

Ниже понадобится такое следствие из леммы 7.

Следствие 1. *Рассмотрим аналогичное* (1.5) *разложение многочлена* $\widehat{x}^{n/k}-1$ *на неприводимые множители*

$$\widehat{x}^{n/k}-1=(\widehat{f}_1(\widehat{x})\widehat{f}_2(\widehat{x})\cdots\widehat{f}_{\widehat{r}}(\widehat{x}))(\widehat{f}_{\widehat{r}+1}(\widehat{x})\widehat{f}^*_{\widehat{r}+1}(\widehat{x})\cdots\widehat{f}_{\widehat{r}+\widehat{s}}(\widehat{x})\widehat{f}^*_{\widehat{r}+\widehat{s}}(\widehat{x})), \tag{5.2}$$

где $\widehat{r}$ *– количество самовозвратных множителей, а* $2\widehat{s}$ *– несамовозвратных. Тогда*

(i) *при* $1\leqslant j\leqslant\widehat{r}$

$$\widehat{e}_{\widehat{f}_j}(x^k)=\left(\sum_{\substack{i=1\\ f_i(x)|\widehat{f}_j(x^k)}}^{r}e_{f_i}(x)\right)+\left(\sum_{\substack{i=r+1\\ f_i(x)|\widehat{f}_j(x^k)}}^{r+s}(e_{f_i}(x)+e_{f_i^*}(x))\right); \tag{5.3}$$

(ii) *при* $\widehat{r}+1\leqslant j\leqslant\widehat{r}+\widehat{s}$

$$\widehat{e}_{\widehat{f}_j}(x^k)=\left(\sum_{\substack{i=r+1\\ f_i(x)|\widehat{f}_j(x^k)}}^{r+s}e_{f_i}(x)\right)+\left(\sum_{\substack{i=r+1\\ f_i^*(x)|\widehat{f}_j(x^k)}}^{r+s}e_{f_i^*}(x)\right), \tag{5.4}$$

$$\widehat{e}_{\widehat{f}^*_j}(x^k)=\left(\sum_{\substack{i=r+1\\ f_i(x)|\widehat{f}_j(x^k)}}^{r+s}e_{f_i^*}(x)\right)+\left(\sum_{\substack{i=r+1\\ f_i^*(x)|\widehat{f}_j(x^k)}}^{r+s}e_{f_i}(x)\right). \tag{5.5}$$

Равенством $\Omega(\widehat{x})=a^k$, где k – натуральный делитель числа n, определим мономорфизм Ω алгебры $\widehat{\mathcal{R}}_{n/k}$ в $\mathbb{F}_qD_{2n}$. Легко видеть, что образ $\mathrm{im}(\Omega)$ равен $\mathbb{F}_q\langle a^k\rangle$.

Теорема 6. *Пусть* $\gcd(q,2n)=1$, k *– натуральный делитель числа* n. *Для циклического кода* $C_g\subset\widehat{\mathcal{R}}_{n/k}$, *порожденного нормированным многочленом* $g(\widehat{x})$, *делителем* $\widehat{x}^{n/k}-1$, *определим индуцированный код* $T_g=(\mathbb{F}_qD_{2n})\Omega(C_g)$. *Тогда образ кода* T_g *при разложении Веддербёрна* (1.7) *имеет следующий вид*:

$$p(T_g)=\left(\bigoplus_{j=1}^{r+s}B_j\right),\quad B_j=\begin{cases}A_j, & j\in J_1,\\ I_j(0,1), & j\in J_2,\\ I_j(1,0), & j\in J_3,\\ 0, & j\notin J_1,J_2,J_3,\end{cases} \tag{5.6}$$

где

$$J_1=\{j\in 1,\dots,r+s:(f_j(x)\nmid g(x^k))\wedge(f_j^*(x)\nmid g(x^k))\},$$
$$J_2=\{j\in\zeta(n)+1,\dots,r+s:(f_j(x)\nmid g(x^k))\wedge(f_j^*(x)\mid g(x^k))\},$$
$$J_3=\{j\in\zeta(n)+1,\dots,r+s:(f_j(x)\mid g(x^k))\wedge(f_j^*(x)\nmid g(x^k))\}.$$

Доказательство. В силу лемм 1, 2 порождающий идемпотент кода C_g имеет следующий вид:

$$e_{C_g}(\widehat{x}) = \left(\sum_{\substack{i=1 \\ \widehat{f}_i(\widehat{x}) \nmid g(\widehat{x})}}^{r+s} \widehat{e}_{\widehat{f}_i}(\widehat{x}) \right) + \left(\sum_{\substack{i=1 \\ f_i^*(\widehat{x}) \nmid g(\widehat{x})}}^{r+s} \widehat{e}_{\widehat{f}_i^*}(\widehat{x}) \right).$$

Это значит, что для кода T_g справедливо следующее равенство:

$$T_g = (\mathbb{F}_q D_{2n})\Omega(C_g) = (\mathbb{F}_q D_{2n})\Omega(\widehat{\mathcal{R}}_{n/k} e_{C_g}(\widehat{x})) = (\mathbb{F}_q D_{2n}) e_{C_g}(a^k).$$

Используя равенства (5.3)–(5.5) получаем

$$e_{C_g}(a^k) = \left(\sum_{\substack{i=1 \\ f_i(x) \nmid g(x^k)}}^{r+s} e_{f_i}(a) \right) + \left(\sum_{\substack{i=r+1 \\ f_i^*(\widehat{x}) \nmid g(x^k)}}^{r+s} e_{f_i^*}(a) \right),$$

откуда в силу теоремы 5 следует (5.6).

5.2. Коды, индуцированные диэдральными кодами. Рассмотрим диэдральную группу $D_{2n} = \langle a, b \rangle$ и ее подгруппу $H = \langle a^k, ba^t \rangle$, где k – произвольный делитель числа n и $t < k$. Пусть $D_{2(n/k)} = \langle \widehat{a}, \widehat{b} \rangle$ – диэдральная группа с параметром n/k. Отображение $\upsilon\colon D_{2(n/k)} \to H$, заданное равенствами $\upsilon(\widehat{a}) = a^k$, $\upsilon(\widehat{b}) = a^t b$, в силу теоремы 1 из [8] является изоморфизмом. Пусть $\Upsilon\colon \mathbb{F}_q D_{2(n/k)} \to \mathbb{F}_q \langle a^k, ba^t \rangle$ – продолжение υ до изоморфизма групповых алгебр.

По теореме 1 групповые алгебры $\mathbb{F}_q D_{2n}$ и $\mathbb{F}_q D_{2(n/k)}$ имеют разложения Веддербёрна; чтобы различать эти разложения, а также необходимые вспомогательные конструкции, для алгебры $\mathbb{F}_q D_{2(n/k)}$ будем добавлять “шапочку” к соответствующим обозначениям из раздела 1.

Рассмотрим разложение (5.2). Очевидно, что тогда

$$x^n - 1 = (\widehat{f}_1(x^k)\widehat{f}_2(x^k)\cdots\widehat{f}_{\widehat{r}}(x^k))(\widehat{f}_{\widehat{r}+1}(x^k)\widehat{f}^*_{\widehat{r}+1}(x^k)\cdots\widehat{f}_{\widehat{r}+\widehat{s}}(x^k)\widehat{f}^*_{\widehat{r}+\widehat{s}}(x^k)).$$

Разложив множители $\widehat{f}_j(x^k)$, $\widehat{f}^*_j(x^k)$ на неприводимые, можно получить разложение (1.5). В следующей теореме, учитывая замечание 6, без потери общности будем считать, что $\widehat{f}_{\widehat{r}+1}(x^k)\widehat{f}_{\widehat{r}+2}(x^k)\cdots\widehat{f}_{\widehat{r}+\widehat{s}}(x^k)$ делит $f_{r+1}(x)f_{r+2}(x)\cdots f_{r+s}(x)$.

Теорема 7. *Пусть* $\gcd(q, 2n) = 1$, *а* I *– такой код в алгебре* $\mathbb{F}_q D_{2(n/k)}$, *что*

$$\widehat{p}(I) = \bigoplus_{j=1}^{\widehat{r}+\widehat{s}} \widehat{B}_j,$$

причем при $1 \leqslant j \leqslant \widehat{r}$ *возможны только равенства* $\widehat{B}_j = 0$, $\widehat{B}_j = \widehat{A}_j$. *Рассмотрим образ разложения Веддербёрна для индуцированного кода* $T = (\mathbb{F}_q D_{2n})\Upsilon(I)$:

$$p(T) = \bigoplus_{i=1}^{r+s} B_i.$$

Тогда для всех $1 \leqslant j \leqslant \widehat{r}+\widehat{s}$

$$B_i = \begin{cases} A_i, & \text{если } (f_i(x) \mid f_j(x^k)) \wedge (\widehat{B}_j = \widehat{A}_j), \\ I_i(-\alpha_i^{-t} Q_j(\alpha_i^{-k}), 1), & \text{если } (f_i(x) \mid f_j(x^k)) \wedge (\widehat{B}_j = I_j(-Q_j(\alpha_j^{-1}, 1))), \\ I_i(1,0), & \text{если } (f_i(x) \mid f_j(x^k)) \wedge (\widehat{B}_j = \widehat{I}_j(1,0)), \\ 0, & \text{если } (f_i(x) \mid f_j(x^k)) \wedge (\widehat{B}_j = 0). \end{cases} \tag{5.7}$$

Доказательство. В силу теоремы 4 порождающий идемпотент w кода I имеет вид $w = \sum_{j=1}^{\widehat{r}+\widehat{s}} w_j$, где

$$w_j = \begin{cases} \widehat{e}_{\widehat{f}_j}(\widehat{a}), & (1 \leqslant j \leqslant \widehat{r}) \wedge (\widehat{B}_j = \widehat{A}_j), \\ \widehat{e}_{\widehat{f}_j}(\widehat{a}) + \widehat{e}_{\widehat{f}_j^*}(\widehat{a}), & (\widehat{r}+1 \leqslant j \leqslant \widehat{r}+\widehat{s}) \wedge (\widehat{B}_j = \widehat{A}_j), \\ \widehat{e}_{\widehat{f}_j^*}(\widehat{a}), & (\widehat{r}+1 \leqslant j \leqslant \widehat{r}+\widehat{s}) \wedge (\widehat{B}_j = \widehat{I}_j(1,0)), \\ \widehat{e}_{\widehat{f}_j}(\widehat{a}) + \widehat{b} Q_j(\widehat{a}) \widehat{e}_{\widehat{f}_j^*}(\widehat{a}), & (\widehat{r}+1 \leqslant j \leqslant \widehat{r}+\widehat{s}) \wedge (\widehat{B}_j = I_j(-Q_j(\alpha_j^{-1}, 1))), \\ 0, & \widehat{B}_j = 0. \end{cases}$$

Тогда $\Upsilon(w)$ – порождающий идемпотент индуцированного кода $T = (\mathbb{F}_q D_{2n})\Upsilon(I)$ и

$$\Upsilon(w) = \sum_{j=1}^{\widehat{r}+\widehat{s}} \Upsilon(w_j).$$

Воспользуемся теперь равенствами (5.3)–(5.5). Тогда если $1 \leqslant j \leqslant \widehat{r}$ и $\widehat{B}_j = \widehat{A}_j$, то

$$\Upsilon(w_j) = \left(\sum_{\substack{i=1 \\ f_i(a) \mid \widehat{f}_j(x^k)}}^{r} e_{f_i}(a) \right) + \left(\sum_{\substack{i=r+1 \\ f_i(a) \mid \widehat{f}_j(a^k)}}^{r+s} (e_{f_i}(a) + e_{f_i^*}(a)) \right).$$

Аналогично, если $\widehat{r}+1 \leqslant j \leqslant \widehat{r}+\widehat{s}$ и $\widehat{B}_j = \widehat{A}_j$, то

$$\Upsilon(w_j) = \left(\sum_{\substack{i=r+1 \\ f_i(x) \mid \widehat{f}_j(x^k)}}^{r+s} (e_{f_i}(a) + e_{f_i^*}(a)) \right);$$

если $\widehat{r}+1 \leqslant j \leqslant \widehat{r}+\widehat{s}$ и $\widehat{B}_j = \widehat{I}_j(1,0)$, то

$$\Upsilon(w_j) = \left(\sum_{\substack{i=r+1 \\ f_i(x) \mid \widehat{f}_j(x^k)}}^{r+s} e_{f_i^*}(a) \right);$$

а если $\widehat{r}+1 \leqslant j \leqslant \widehat{r}+\widehat{s}$ и $\widehat{B}_j = I_j(-Q_j(\alpha_j^{-1}, 1))$, то

$$\Upsilon(w_j) = \left(\sum_{\substack{i=r+1 \\ f_i(x) \mid \widehat{f}_j(x^k)}}^{r+s} (e_{f_i}(a) + b a^t Q(a^k) e_{f_i^*}(a)) \right).$$

Отсюда в силу теоремы 5 следует равенство (5.7).

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

[1] R. J. McEliece, *Public-Key Cryptosystem Based on Algebraic Coding Theory*, DSN Progress Report № 42-44, 1978.

[2] D. J. Bernstein, "Grover vs. McEliece", *Post-Quantum Cryptography*, Lecture Notes in Comput. Sci., **6061**, Springer, Berlin, 2010, 73–80.

[3] V. M. Deundyak, Yu. V. Kosolapov, "On the Berger–Loidreau cryptosystem on the tensor product of codes", *J. Comput. Eng. Math.*, **5**:2 (2018), 16–33.

[4] К. Гарсиа-Пильядо, С. Гонсалес, В. Т. Марков, К. Мартинес, "Неабелевы групповые коды над произвольным конечным полем", *Фундамент. и прикл. матем.*, **20**:1 (2015), 17–22.

[5] Е. Коусело, С. Гонсалес, В. Т. Марков, К. Мартинес, А. А. Нечаев, "Представления кодов Рида–Соломона и Рида–Маллера идеалами", *Алгебра и логика*, **51**:3 (2012), 297–320.

[6] C. Polcino Milies, F. D. de Melo, "On cyclic and Abelian codes", *IEEE Trans. Inform. Theory*, **59**:11 (2013), 7314–7319.

[7] В. М. Деундяк, Ю. В. Косолапов, "Алгоритмы для мажоритарного декодирования групповых кодов", *Модел. и анализ информ. систем*, **22**:4 (2015), 464–482.

[8] К. В. Веденёв, В. М. Деундяк, "Коды в диэдральной групповой алгебре", *Модел. и анализ информ. систем*, **25**:2 (2018), 232–245.

[9] F. E. Brochero Martínez, "Structure of finite dihedral group algebra", *Finite Fields Appl.*, **35** (2015), 204–214.

[10] В. М. Деундяк, Ю. В. Косолапов, "Криптосистема на индуцированных групповых кодах", *Модел. и анализ информ. систем*, **23**:2 (2016), 137–152.

[11] C. Polcino Milies, S. K. Sehgal, *An Inroduction to Group Rings*, Kluwer Acad. Publ., Dordrecht, 2002.

К. В. Веденёв
Южный Федеральный университет,
г. Ростов-на-Дону
E-mail: vedenevk@gmail.com

В. М. Деундяк
ФГАНУ НИИ "Спецвузавтоматика",
г. Ростов-на-Дону;
Южный Федеральный университет,
г. Ростов-на-Дону
E-mail: vl.deundyak@gmail.com

Поступило
17.09.2018
Принято к публикации
20.03.2019