Math-Net.Ru

Общероссийский математический портал

Б. А. Погорелов, М. А. Пудовкина, Надгруппы аддитивных регулярных групп порядка 2^n кольца вычетов и векторного пространства, *Дискрет. матем.*, 2015, том 27, выпуск 3, 74–94

DOI: <https://doi.org/10.4213/dm1336>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением <http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 3.93.64.190

26 апреля 2023 г., 14:09:09

Надгруппы аддитивных регулярных групп порядка 2^n кольца вычетов и векторного пространства

© 2015 г. Б. А. Погорелов*, М. А. Пудовкина**

Аддитивные группы кольца вычетов $\mathbb{Z}_{2^n}$ и векторного пространства V_n над полем $GF(2)$, а также порождённая ими группа G_n , имеют общие системы импримитивности и являются подгруппами силовой 2-подгруппы симметрической группы $S(\mathbb{Z}_{2^n})$. Данные группы возникают в криптографии при использовании в качестве способа наложения ключа относительно операций сложения из V_n и $\mathbb{Z}_{2^n}$. В данной работе приведено подстановочное строение подгрупп группы G_n . Описаны ядра гомоморфизмов, соответствующих различным системам импримитивности, нормальные делители, а также некоторые модулярные представления группы G_n над полем $GF(2)$.

Ключевые слова: сплетение групп подстановок, импримитивная группа, силовая 2-подгруппа, аддитивная группа кольца вычетов, аддитивная группа векторного пространства.

1. Введение

В дискретной математике традиционное понятие производной для функций $f: \mathbb{Z}_q^n \rightarrow \mathbb{Z}_q$, рассматриваемых над кольцами вычетов, существенно различается в случаях $q = 2$ и $q > 2$. В первом случае значение производной $\Delta_\beta f(x) = f(x + \beta) + f(x)$ от функции f по элементу $v \in \mathbb{Z}_q^n$ в точке x равно сумме значений на орбите $\{x, x + v\}$ группы, порожденной сдвигом $\delta_\beta: x \mapsto x + \beta$ векторного пространства V_n . Во втором случае рассматривается разность значений $\Delta_v f(x) = f(x + v) - f(x)$, и на орбите соответствующего сдвига в общем случае производная принимает разные значения. Поэтому естественно рассмотрение другой производной — орбитальной, когда значение в точке x определяется как сумма значений функции во всех точках, составляющих орбиту соответствующей циклической группы сдвигов. Получающаяся производная содержит эту группу сдвигов в группе инерции. В [2, 3] начато исследование свойств таких производных функций над кольцом вычетов $\mathbb{Z}_{2^n}$.

*Место работы: Академия криптографии Российской Федерации,
e-mail: pogorelow.b@yandex.ru

**Место работы: Национальный исследовательский ядерный университет
(МИФИ), e-mail: maricap@rambler.ru

Заметим, что функция след над конечными полями получается суммированием элементов поля, лежащих на одном цикле автоморфизма Фробениуса. Так же получаются и производные двоичных функций. Орбиту x^H группы подстановок H , содержащей точку x , можно трактовать как ее H -окрестность. В криптографии производные дискретных отображений также играют важную роль. Они используются в методах криптографического анализа; через их свойства задаются криптографические параметры и вводятся целые классы отображений. Производные раундовых функций, имея более простое строение, отражают свойства этих функций и могут обладать дополнительными полезными свойствами. Например, производные раундовых функций и функции зашифрования могут быть инвариантными относительно группы наложения ключа, например, в XSL блочных шифрсистемах.

В работе предлагается понятие орбитальной производной, обобщающее случай $q = 2$ и случай, рассмотренный в [2], [3]. Оно также основано на суммировании значений функции на орбитах ряда вложенных подгрупп группы G_n , порожденной группами сдвигов векторного пространства V_n и кольца вычетов $\mathbb{Z}_{2^n}$. Заметим, что в криптографии группа G_n возникает в блочных шифрсистемах, использующих в качестве наложения ключа операции сложения в кольце вычетов и в векторном пространстве, например, в ARX системах.

Далее рассмотрены подстановочные свойства группы G_n . В частности, описаны ядра гомоморфизмов, соответствующих различным системам импримитивности, нормальные делители. Как следствие возникают некоторые модулярные представления группы G_n над полем $GF(2)$.

2. Основные обозначения

Пусть $\mathbb{N}$ — множество всех натуральных чисел, $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$; $\mathbb{Z}$ — кольцо целых чисел; $Z_m = \{0, \dots, m-1\} \subset \mathbb{Z}$; $\mathbb{Z}_{2^n}$ — кольцо вычетов по модулю 2^n , элементы которого обозначаются числами $0, \dots, 2^n - 1$; при $d \leq n$ для $\alpha \in \mathbb{Z}_{2^n}$ через $\alpha_{(d)}$ обозначаем такой элемент $\alpha_{(d)} \in \mathbb{Z}_{2^d}$, что $\alpha_{(d)} \equiv \alpha \pmod{2^d}$, при этом $\alpha_{(0)} = 0$, $x \mapsto x_{(d)}$ — соответствующее отображение; $A_{(d)} = \{\alpha_{(d)} | \alpha \in A\}$ для $A \subset \mathbb{Z}$; V_n — пространство n -мерных векторов над полем $GF(2)$, т.е. $V_n = (GF(2))^n$; $\oplus$ — операция покомпонентного сложения векторов в пространстве V_n .

Каждый вектор $\alpha = (\alpha_{n-1}, \dots, \alpha_1, \alpha_0) \in V_n$ можно рассматривать и как двоичную запись числа $\tilde{\alpha} = 2^{n-1}\alpha_{n-1} + \dots + 2\alpha_1 + \alpha_0$. Поэтому вектор α будем отождествлять с числом $\tilde{\alpha}$. При этом на V_n можно определить операции сложения и умножения по модулю 2^n , а над кольцом $\mathbb{Z}_{2^n}$ — операцию $\oplus$ покомпонентного сложения векторов. Эти операции будем обозначать теми же знаками, что и соответствующие операции над числами или векторами. Из контекста всегда будет ясно, об операциях в каких алгебраических структурах идет речь.

Пусть также $\mathbb{Z}_{2^n}^+$ и V_n^+ — аддитивные группы кольца $\mathbb{Z}_{2^n}$ и векторного пространства V_n ; $H \leq R$ — H -подгруппа группы R ; $S(X)$ — симметрическая группа на множестве X , $S_{2^n} = S(X)$ при $|X| = 2^n$; $G_n = \langle V_n^+, \mathbb{Z}_{2^n}^+ \rangle \leq S_{2^n}$; P_n — силовская 2-подгруппа группы S_{2^n} , содержащая группу G_n ; e — тождественная подстановка; e_n — тождественная подстановка группы G_n ; $\alpha^g = \alpha g = g(\alpha)$ — образ элемента $\alpha \in X$ при действии на него подстановкой $g \in S(X)$; $\alpha^G = \{\alpha^g | g \in G\}$,

$G \leq S(X)$; $X^\times = X \setminus \{0\}$, если 0 — нейтральный элемент относительно заданной на X бинарной операции; $A * B = \{\alpha * \beta \mid (\alpha, \beta) \in A \times B\}$ для группы X с бинарной операцией $*$, $A, B \subseteq X$, B^c — c -я декартова степень множества B ; $\langle \beta_1, \dots, \beta_t \rangle$ — группа, порождённая элементами $\beta_1, \dots, \beta_t$; $F_{n,m}^+ = \{f \mid f: \mathbb{Z}_{2^n} \rightarrow \mathbb{Z}_{2^m}\}$, $F_{n,m}^\oplus = \{f \mid f: V_n \rightarrow V_m\}$ при $1 \leq m \leq n$; $a(x) \cdot b(x) \equiv_{2^m} c(x)$ есть сокращённая запись условия $a(x) \cdot b(x) \equiv c(x) \pmod{2^m}$ для всех $x \in \mathbb{Z}_{2^n}$, где $a, b, c \in F_{n,m}^+$; « $\cdot$ » — бинарная операция над числами в кольце $\mathbb{Z}$, представляющими соответствующие классы вычетов; запись $a *_{2^n} A$ означает, что элемент $a_{(n)}$ и множество $A_{(n)}$ находятся в отношении $*$ $\in \{\in, \notin\}$, $a \in \mathbb{Z}$, $A \subset \mathbb{Z}$; запись $B *_{2^n} C$ означает, что множества $B_{(n)}$ и $C_{(n)}$ находятся в отношении $*$ $\in \{\subseteq, \not\subseteq, =, \equiv\}$, $B, C \subset \mathbb{Z}$ и B, C могут быть одноэлементными множествами; $\varphi_i^{(R)}$ — естественный гомоморфизм подгруппы R импримитивной группы P_n в группу, действующую на множестве $W^{(i,n)} = \{W_0^{(i,n)}, \dots, W_{2^i-1}^{(i,n)}\}$ блоков импримитивности i -й системы импримитивности, определяемой группой $\mathbb{Z}_{2^n}^+$, т.е. $W_t^{(i,n)} = \{j \in \mathbb{Z}_{2^n} \mid j \equiv_{2^i} t\}$, $i = 1, \dots, n-1$; $\text{Кег } \varphi_0^{(R)} = R$ для $R \leq P_n$; $u_{r,n} = (r, 2^{n-1} + r) \cdot (2^{n-2} + r, 2^{n-1} + 2^{n-2} + r)$ — произведение транспозиций для $r \in \{0, \dots, 2^{n-2} - 1\}$; $\delta_{r,n}^{(j)} = \prod_{t=0}^{2^{n-2}-j} u_{r+2^j t \pmod{2^{n-2}}, n}$ для $r \in \{0, \dots, 2^j - 1\}$, $j \in \{0, \dots, n-2\}$; $\varepsilon_{j,n} = (0, \dots, 0, 1, \underbrace{0, \dots, 0}_{j-1})$, $c_{j,n}: \alpha \mapsto \alpha \oplus \varepsilon_{j,n}$, $j = 0, \dots, n-1$; $X =_{2^n} Y$, если $X = Y_{(n)}$, $Y, X \subseteq \mathbb{Z}_{2^n}$; $\alpha =_{2^n} \beta$, если $\alpha = \beta_{(n)}$ для $\alpha, \beta \in \mathbb{Z}_{2^n}$;

$$\sum_{\alpha \in W} * = \begin{cases} \sum_{\alpha \in W} \oplus = \bigoplus_{\alpha \in W}, & \text{если } * = \oplus, \\ \sum_{\alpha \in W} 2^m, & \text{если } * - \text{операция } + \text{ сложения в кольце } \mathbb{Z}_{2^m}. \end{cases}$$

Всюду ниже предполагается, что $n, m \in \mathbb{N}$, $m \leq n$, $n \geq 2$.

Пусть X, Y — конечные абелевы группы, H — подгруппа симметрической группы $S(X)$.

Определение 2.1. Орбитальной производной отображения $f: X \rightarrow Y$ по группе H , или H -производной, называется оператор Δ_H , задаваемый формулой

$$\Delta_H f(x) = \sum_{\beta \in x^H} f(\beta).$$

Если $H = \langle a \rangle$, то H -производную также будем называть производной по элементу $a \in H$.

Пусть $n, m \in \mathbb{N}$, $m \leq n$. Для $X = \mathbb{Z}_{2^n}^+$, $Y = \mathbb{Z}_{2^m}^+$ назовем G^+ -производной оператор

$$\Delta_G^+: f(x) \mapsto \sum_{\alpha \in x^G} f(\alpha),$$

а для $X = V_n^+$, $Y = V_m^+$ назовем $G^\oplus$ -производной оператор

$$\Delta_G^\oplus: f(x) \mapsto \bigoplus_{\alpha \in x^G} f(\alpha).$$

Если δ_β — сдвиг на вектор $\beta \in V_n$, т.е. $\delta_\beta : x \mapsto x \oplus \beta$, то $\{\{\lambda, \lambda \oplus \beta\} | \lambda \in V_n\}$ — множество всех орбит подгруппы $\langle \delta_\beta \rangle$ и $\langle \delta_\beta \rangle^\oplus$ -производная функции $f \in F_{n,m}^\oplus$, определяемая условием $\Delta_{\langle \delta_\beta \rangle}^\oplus f : x \mapsto f(x) \oplus f(x \oplus \beta)$ совпадает с традиционным определением производной по направлению вектора β (см., например, [1]).

Положим $h_n = (0, 1, 2, \dots, 2^n - 1)$. Так как для $t \in \{1, \dots, n-1\}$ орбита группы $G = \langle h_n^{2^t} \rangle$, содержащая элемент $\alpha \in \mathbb{Z}_{2^n}$, равна

$$\left\{ (\alpha + 2^t c)_{(n)} | c \in \{0, \dots, 2^{n-t} - 1\} \right\},$$

то G^+ -производная отображения $f \in F_{n,m}^+$ задаётся оператором Δ_G^+ , где

$$\Delta_G^+ f(x) = \sum_{\beta \in \langle 2^t \rangle} f(x + \beta),$$

и совпадает с определением $(n-t)$ -й орбитальной производной [2].

3. Свойства группы G_n , порождённой аддитивными группами кольца вычетов $\mathbb{Z}_{2^n}$ и векторного пространства V_n

Группа $G_n = \langle V_n^+, \mathbb{Z}_{2^n}^+ \rangle$ импримитивна, и $W_t^{(i,n)} = \{j \in \mathbb{Z}_{2^n} | j \equiv_{2^i} t\}$ — t -й блок импримитивности i -й системы импримитивности $W^{(i,n)}$, $|W_t^{(i,n)}| = 2^{n-i}$, $t \in \{0, \dots, 2^i - 1\}$, $i \in \{1, \dots, n\}$. Другими словами, системы импримитивности групп G_n и $\mathbb{Z}_{2^n}^+$ совпадают. Нетрудно убедиться, что центр $Z(G_n)$ группы G_n равен

$$Z(G_n) = \langle (1, 1 + 2^{n-1}) \cdot \dots \cdot (2^{n-1} - 1, 2^n - 1) \rangle = V_n^+ \cap \mathbb{Z}_{2^n}^+.$$

Напомним, что силовская 2-подгруппа $P_n \in \text{Syl}_2(S_{2^n})$, содержащая группу G_n , описывается операцией сплетения $P_n = P_2 \wr P_{n-1}$.

Приведём подстановочное строение подгрупп группы G_n , из описания которого, в частности, следует известный порядок группы G_n , полученный ранее в [5].

Пусть

$$\varepsilon_{j,n} = (0, \dots, 0, 1, \underbrace{0, \dots, 0}_{j-1}), \quad c_{j,n} : \alpha \mapsto \alpha \oplus \varepsilon_{j,n}, \quad j = 0, \dots, n-1.$$

Теорема 3.1. Пусть $n \geq 2$. Тогда:

1. Если $\varphi_{n-1}^{(G_n)}$ — естественный гомоморфизм импримитивной группы G_n в группу, действующую на множестве блоков импримитивности $\{\{0, 2^{n-1}\}, \dots, \{2^{n-1} - 1, 2^n - 1\}\}$, то $\text{Im } \varphi_{n-1}^{(G_n)} \cong G_{n-1}$ и

$$\begin{aligned} \text{Ker } \varphi_{n-1}^{(G_n)} &= \\ &= \left\langle \{(r, 2^{n-1} + r) \cdot (2^{n-2} + r, 2^{n-1} + 2^{n-2} + r) | r = 0, \dots, 2^{n-2} - 1\}, \right. \\ &\quad \left. \prod_{t=0}^{2^{n-2}-1} (2^{n-2} + t, 2^{n-1} + 2^{n-2} + t) \right\rangle. \end{aligned}$$

2. Справедливы равенства $\left| \text{Кер } \varphi_{n-1}^{(G_n)} \right| = 2^{2^{n-2}+1}, |G_n| = 2^{2^{n-1}+n-1}.$

Доказательство. 1. Положим $v_{n-2} = h_n^{2^{n-2}} c_{n-2,n}.$

Группа $G_n = \langle c_{0,n}, \dots, c_{n-1,n}, h_n \rangle$ является импримитивной и имеет систему импримитивности $\{0, 2^{n-1}\}, \dots, \{2^{n-1} - 1, 2^n - 1\}.$ Рассмотрим естественный гомоморфизм $\varphi_{n-1}^{(G_n)}$ группы G_n в группу, действующую на множестве блоков импримитивности $\{\{0, 2^{n-1}\}, \dots, \{2^{n-1} - 1, 2^n - 1\}\}.$ Так как

$$\varphi_{n-1}^{(G_n)}(c_{j,n}) : \{i, i + 2^{n-1}\} \mapsto \{i \oplus \varepsilon_{j,n}, i \oplus \varepsilon_{j,n} \oplus \varepsilon_{n-1,n}\}, \quad j = 0, \dots, n-2,$$

$$\varphi_{n-1}^{(G_n)}(h_n) : \{i, i + 2^{n-1}\} \mapsto \{i + 1, i + 1 + 2^{n-1}\}, \quad i = 0, \dots, 2^{n-1} - 1,$$

то $\text{Im } \varphi_{n-1}^{(G_n)} \cong G_{n-1}.$

Опишем $\text{Кер } \varphi_{n-1}^{(G_n)}.$ Отметим, что

$$\begin{aligned} v_{n-2} &= \prod_{i=0}^{2^{n-2}-1} (i, 2^{n-2} + i, 2^{n-1} + i, 2^{n-1} + 2^{n-2} + i) \cdot \prod_{j=0}^{2^{n-2}-1} (j, 2^{n-2} + j) \cdot \\ &\cdot \prod_{j=2^{n-2}}^{2^{n-1}-1} (j, j - 2^{n-2}) \cdot \prod_{j=2^{n-1}}^{2^{n-1}+2^{n-2}-1} (j, j + 2^{n-2}) \cdot \prod_{j=2^{n-1}+2^{n-2}}^{2^n-1} (j, j - 2^{n-2}) = \\ &= \prod_{i=0}^{2^{n-2}-1} (2^{n-2} + i, 2^{n-1} + 2^{n-2} + i). \end{aligned}$$

Для $r = 0, \dots, 2^{n-2} - 1$ рассмотрим коммутатор $v_{n-2,r} = h_n^{-r} v_{n-2} h_n^r v_{n-2}.$ Так как

$$\begin{aligned} h_n^{-r} v_{n-2} h_n^r &= \prod_{i=0}^{2^{n-2}-1} (2^{n-2} + i + r, 2^{n-1} + 2^{n-2} + i + r) = \\ &= \prod_{i=0}^{r-1} (t, 2^{n-1} + t) \cdot \prod_{t=r}^{2^{n-2}-1} (2^{n-2} + t, 2^{n-1} + 2^{n-2} + t), \end{aligned}$$

то

$$v_{n-2,r} = \prod_{i=0}^{r-1} (t, 2^{n-1} + t) \cdot \prod_{t=0}^{r-1} (2^{n-2} + t, 2^{n-1} + 2^{n-2} + t).$$

Заметим, что $v_{n-2,1}$ — произведение двух независимых транспозиций, т.е.

$$v_{n-2,1} = (0, 2^{n-1}) \cdot (2^{n-2}, 2^{n-1} + 2^{n-2}).$$

Сопрягая $v_{n-2,1}$ преобразованием $h_n^r,$ получаем

$$b_{n,r} = h_n^{-r} v_{n-2,1} h_n^r = (r, 2^{n-1}+r) \cdot (2^{n-2}+r, 2^{n-1}+2^{n-2}+r), \quad r = 0, \dots, 2^{n-2}-1.$$

Множество $\{b_{n,r} \mid r = 0, \dots, 2^{n-2} - 1\}$ порождает подмножество $B_n = \langle b_{n,r} \mid r = 0, \dots, 2^{n-2} - 1 \rangle$ из ядра $\text{Кер } \varphi_{n-1}^{(G_n)}.$ Нетрудно убедиться в том, что $|B_n| = 2^{2^{n-2}}$ и $h_n^{-r} B_n h_n^r = B_n$ для каждого $r \in \{0, \dots, 2^{n-1} - 1\}.$

Рассмотрим элемент

$$\begin{aligned} u &= h_n^{-1} v_{n-2} h_n \cdot (0, 2^{n-1}) \cdot (2^{n-2}, 2^{n-1} + 2^{n-2}) = \\ &= \prod_{t=0}^{2^{n-2}-1} (2^{n-2} + t, 2^{n-1} + 2^{n-2} + t). \end{aligned}$$

Ясно, что $u \in \text{Ker } \varphi_{n-1}^{(G_n)}$. Так как разложение u в виде произведения независимых циклов содержит транспозиции вида $(2^{n-2} + j, 2^{n-1} + 2^{n-2} + j)$ и не содержит транспозицию $(j, 2^{n-1} + j)$ для каждого $j \in \{0, \dots, 2^{n-2} - 1\}$, то из способа задания множества B_n следует, что $u \notin B_n$. Таким образом, множество uB_n является смежным классом группы $\text{Ker } \varphi_{n-1}^{(G_n)}$ по подгруппе B_n . Значит, $|\text{Ker } \varphi_{n-1}^{(G_n)}| \geq 2^{2^{n-2}+1}$.

Покажем, что $|\text{Ker } \varphi_{n-1}^{(G_n)}| \leq |\text{Ker } \varphi_{n-2}^{(G_{n-1})}|^2$. Рассмотрим множества $W_{0,n} = \{2i \mid i = 0, \dots, 2^{n-1} - 1\}$, $W_{1,n} = \{2i + 1 \mid i = 0, \dots, 2^{n-1} - 1\}$. Произвольный элемент $g \in \text{Ker } \varphi_{n-1}^{(G_n)}$ представим в виде произведения таких двух элементов $g_1 \in S(W_{0,n})$, $g_2 \in S(W_{1,n})$, что g_1 сохраняет блок $\{2j, 2(j + 2^{n-2})\}$, а g_2 — блок $\{2j + 1, 2(j + 2^{n-2}) + 1\}$ для всех $j \in \{0, \dots, 2^{n-1} - 1\}$. Другими словами, $g_1 = \prod_{i \in T_1} (2t, 2t + 2^{n-1})$, $g_2 = \prod_{i \in T_2} (2t + 1, 2(t + 2^{n-2}) + 1)$ для некоторых множеств $T_1, T_2 \subseteq \{0, \dots, 2^{n-1} - 1\}$. Значит, элементу $g_1 = \prod_{i \in T_1} (2t, 2t + 2^{n-1})$ однозначно соответствует элемент $g'_1 = \prod_{i \in T_1} (t, t + 2^{n-2})$ из $\text{Ker } \varphi_{n-2}^{(G_{n-1})}$, а элементу $g_2 = \prod_{i \in T_2} (2t + 1, 2(t + 2^{n-2}) + 1)$ — элемент $g'_2 = \prod_{i \in T_2} (t, t + 2^{n-2})$ из $\text{Ker } \varphi_{n-2}^{(G_{n-1})}$. Поэтому

$$|\text{Ker } \varphi_{n-1}^{(G_n)}| \leq |\text{Ker } \varphi_{n-2}^{(G_{n-1})}|^2. \quad (3.1)$$

Так как элемент $w \in B_n$ представим в виде

$$w = \prod_{j \in T} (j, j + 2^{n-1})(j + 2^{n-2}, j + 2^{n-2} + 2^{n-1})$$

для некоторого подмножества $T \subseteq \{0, \dots, 2^{n-2} - 1\}$, то

$$wu = \prod_{i \in T} (i, i + 2^{n-1}) \cdot \prod_{j \in \overline{T}} (j + 2^{n-2}, j + 2^{n-2} + 2^{n-1}).$$

Таким образом,

$$uB_n = \left\{ \prod_{i \in T} (i, i + 2^{n-1}) \cdot \prod_{j \in \overline{T}} (j + 2^{n-2}, j + 2^{n-2} + 2^{n-1}) \mid T \subseteq \{0, \dots, 2^{n-2} - 1\} \right\}.$$

Отметим, что каждый элемент смежного класса uB_n представим в виде произведения 2^{n-2} независимых транспозиций, причём среди них нет пар транспозиций вида

$$(j, j + 2^{n-1})(j + 2^{n-2}, j + 2^{n-2} + 2^{n-1}), \quad j \in \{0, \dots, 2^{n-2} - 1\}.$$

Так как для любого $r \in \{0, \dots, 2^{n-1} - 1\}$ существует такое подмножество $T' \subseteq \{0, \dots, 2^{n-2} - 1\}$, что

$$\begin{aligned} h_n^{-r} u B_n h_n^r &= \prod_{i \in T} (i + r, i + t + 2^{n-1}) \cdot \prod_{j \in \overline{T}} (j + r + 2^{n-2}, j + r + 2^{n-2} + 2^{n-1}) = \\ &= \prod_{i \in T'} (i, i + 2^{n-1}) \cdot \prod_{j \in \overline{T'}} (j + 2^{n-2}, j + 2^{n-2} + 2^{n-1}), \end{aligned}$$

то $h_n^{-r} u B_n h_n^r = u B_n$.

Индукцией по n докажем равенство $|\text{Кер } \varphi_{n-1}^{(G_n)}| = 2^{2^{n-2}+1}$. Непосредственные вычисления показали, что $|\text{Кер } \varphi_{n-1}^{(G_n)}| = 2^{2^{n-2}+1}$ для $n \in \{3, 4, 5\}$. Пусть $|\text{Кер } \varphi_{n-2}^{(G_{n-1})}| = 2^{2^{n-3}+1}$. Тогда из неравенства (3.1) следует, что

$$|\text{Кер } \varphi_{n-1}^{(G_n)}| \leq 2^{2^{n-2}+2}. \quad (3.2)$$

Пусть $2^{2^{n-2}+1} < |\text{Кер } \varphi_{n-1}^{(G_n)}|$. Тогда существует такая подстановка $s \in \text{Кер } \varphi_{n-1}^{(G_n)} \setminus (B_n \cup u B_n)$, что $s = \prod_{j \in J} (j, j + 2^{n-1})$ для некоторого подмножества $J \subset \{0, \dots, 2^{n-1} - 1\}$, элементы которого удовлетворяют условию $j_1 - j_2 \not\equiv_{2^{n-2}} 0$ для любых различных элементов $j_1, j_2 \in J$. Очевидно, что $|J| \leq 2^{n-2}$. Из неравенства (3.2) следует, что $\text{Кер } \varphi_{n-1}^{(G_n)} = B_n \cup u B_n \cup s B_n \cup s u B_n$.

Справедливость включения $sh_n^{-r} s B_n h_n^r \subseteq B_n \cup u B_n$ для каждого $r \in \{0, \dots, 2^{n-1} - 1\}$ следует из равенств $h_n^{-r} u B_n h_n^r = u B_n$ и $h_n^{-r} B_n h_n^r = B_n$. Значит,

$$h_n^{-r} u B_n h_n^r = u B_n = \prod_{j \in J} (j, j + 2^{n-1}) \cdot \prod_{t \in J} (t + r, t + r + 2^{n-1}) \in B_n \cup u B_n.$$

Пусть $U(v)$ — множество всех циклов длины 2 в цикловой структуре инволюции $v \in \text{Кер } \varphi_{n-1}^{(G_n)}$; $J + t =_{2^n} \{j + t \mid j \in J\}$, $J^{(t)} = J \setminus (J \cap (J + t))$ для $J \subset \{0, \dots, 2^n - 1\}$, $t \in \{0, \dots, 2^n - 1\}$.

Пусть $sh_n^{-t} sh_n^t \in B_n$ для некоторого $t \in \{1, \dots, 2^{n-2} - 1\}$ и $j \in J^{(t)}$. Так как $(j, j + 2^{n-1}) \in U(s)$, то $(j + t, j + 2^{n-1} + t) \in U(h_n^{-t} sh_n^t)$. Из включения $sh_n^{-t} sh_n^t \in B_n$ следует, что

$$(j + 2^{n-2} + t, j + 2^{n-1} + 2^{n-2} + t) \in U(s)$$

и

$$\left((j - t + 2^{n-2})_{(n)}, (j + 2^{n-1} - t + 2^{n-2})_{(n)} \right) \in U(s),$$

так как

$$\begin{aligned} &\left(j, (j + 2^{n-1})_{(n)} \right) h_n^{-t} \left((j - t + 2^{n-2})_{(n)}, (j + 2^{n-1} - t + 2^{n-2})_{(n)} \right) h_n^t = \\ &= \left(j, (j + 2^{n-1})_{(n)} \right) \left(j, (j + 2^{n-1} + 2^{n-2})_{(n)} \right) \in B_n, \\ &h_n^{-t} (j, j + 2^{n-1}) h_n^t (j + 2^{n-2} + t, j + 2^{n-1} + 2^{n-2} + t) = \\ &= \left((j + t)_{(n)}, (j + 2^{n-1} + t)_{(n)} \right) \left((j + 2^{n-2} + t)_{(n)}, (j + 2^{n-1} + 2^{n-2} + t)_{(n)} \right) \in B_n. \end{aligned}$$

Таким образом,

$$\left\{ (2^{n-2} - t + j)_{(n-1)}, (2^{n-2} + t + j)_{(n-1)} \right\} \subseteq J^{(t)}. \quad (3.3)$$

Из включения (3.3) следует, что $\left\{ ((2^{n-2} + t)p + j)_{(n-1)} \right\} \in J^{(t)}$ для любого $p \in \{0, \dots, 2^{n-1} - 1\}$. Значит, существует такое наименьшее число $\tilde{p} \in \{0, \dots, 2^{n-1} - 1\}$, что справедливы соотношения $(2^{n-2} + t)\tilde{p} + j \equiv_{2^{n-2}} j$ и $(2^{n-2} + t)\tilde{p} + j \not\equiv_{2^{n-1}} j$, которые невозможны согласно заданию подстановки s , а именно, условию $j_1 - j_2 \not\equiv_{2^{n-2}} 0$ для любых различных элементов $j_1, j_2 \in J$. Следовательно, $2^{2^{n-2}+1} = |\text{Ker } \varphi_{n-1}^{(G_n)}|$.

Все элементы ядра $\text{Ker } \varphi_{n-1}^{(G_n)}$ являются произведением транспозиций вида $(i, i + 2^{n-1})$, $i \in \{0, \dots, 2^n - 1\}$. Поэтому, если $sh_n^{-i}sh_n^i \in B_n$ для некоторого $i \in \{2^{n-2} - 1, \dots, 2^n - 1\}$, то должно выполняться также включение $sh_n^{i-2^{n-1}}sh_n^{i-2^{n-1}} \in B_n$. Последнее невозможно. Таким образом, если существует такое число $\tilde{t} \in \{1, \dots, 2^{n-2} - 1\} \cup \{2^{n-2} + 1, \dots, 2^{n-1} - 1\}$, что $sh_n^{-\tilde{t}}sh_n^{\tilde{t}} \in B_n$, то $2^{2^{n-2}+1} = |\text{Ker } \varphi_{n-1}^{(G_n)}|$.

Обозначим $\tilde{J}^{(t)} = J \cup (J + t) \setminus (J \cap (J + t))$ для $t = 1, \dots, 2^{n-2} - 1$.

Предположим теперь, что $sh_n^{-t}sh_n^t \in uB_n$ для всех $t \in \{1, \dots, 2^{n-2} - 1\} \cup \{2^{n-2} + 1, \dots, 2^{n-1} - 1\}$. Тогда $|U(sh_n^{-t}sh_n^t)| = 2^{n-2}$, а значит, $|\tilde{J}^{(t)}| = 2^{n-2}$ для каждого $t \in \{1, \dots, 2^{n-2} - 1\} \cup \{2^{n-2} + 1, \dots, 2^{n-1} - 1\}$. Кроме того, $a \geq 2^{n-3}$ и для каждого $t \in \{1, \dots, 2^{n-2} - 1\} \cup \{2^{n-2} + 1, \dots, 2^{n-1} - 1\}$ выполняется равенство

$$|J \cap (J + t)| = a - 2^{n-3}. \quad (3.4)$$

Пусть $J \cap (J + \tilde{t}) = \emptyset$ для некоторого элемента $\tilde{t} \in \{1, \dots, 2^{n-2} - 1\} \cup \{2^{n-2} + 1, \dots, 2^{n-1} - 1\}$. Зафиксируем два произвольных различных числа $j_1, j_2 \in J$ и положим $t \equiv_{2^{n-1}} j_2 - j_1$. Тогда $|J| = 2^{n-3}$ и $J \cap (J + t) \neq \emptyset$. Значит, $|J \cap (J + \tilde{t})| \neq |J \cap (J + t)|$, что невозможно согласно равенству (3.4).

Предположим, что $J \cap (J + t) \neq \emptyset$ для всех элементов $t \in \{1, \dots, 2^{n-2} - 1\} \cup \{2^{n-2} + 1, \dots, 2^{n-1} - 1\}$.

Так как все элементы ядра $\text{Ker } \varphi_{n-1}^{(G_n)}$ являются произведениями транспозиций вида $(i, i + 2^{n-1})$, $i \in \{0, \dots, 2^n - 1\}$, то из включения $\left\{ (j_1, (j_1 + 2^{n-1})_{(n)}), (j_2, (j_2 + 2^{n-1})_{(n)}) \right\} \subseteq U(s)$ следует, что равенство

$$h_n^{-r} \left(j_1, (j_1 + 2^{n-1})_{(n)} \right) h_n^r = \left(j_2, (j_2 + 2^{n-1})_{(n)} \right)$$

выполняется тогда и только тогда, когда $r \in_{2^n} \{j_2 - j_1, j_2 - j_1 + 2^{n-1}\}$. Аналогично, равенство

$$h_n^{-r'} (j_2, j_2 + 2^{n-1}) h_n^{r'} =_{2^n} (j_1, j_1 + 2^{n-1})$$

выполняется тогда и только тогда, когда $r' \in_{2^n} \{j_1 - j_2, j_1 - j_2 + 2^{n-1}\}$. Таким образом, достаточно рассматривать разности между элементами j_1, j_2 , входящими в транспозиции $(j_1, j_1 + 2^{n-1})$, $(j_2, j_2 + 2^{n-1})$ соответственно, только по модулю 2^{n-1} .

Пусть $\Lambda = \{\{\lambda_0, \dots, \lambda_{p-1}\}\}$ — мультимножество из p элементов, а первичная спецификация (см., например, [4]) $[\theta_0^{t_1}, \dots, \theta_{c-1}^{t_c}]$ мультимножества Λ означает, что

элемент θ_i встречается в мультимножестве Λ равно t_i раз, $t_0 + \dots + t_{c-1} = n$, $|\Lambda| = t_0 + \dots + t_{c-1} = n$.

Положим

$$T(J) = {}_{2^{n-1}} \{ \{j_2 - j_1 \mid j_2, j_1 \in J, j_2 \neq j_1\} \}.$$

Ясно, что

$$\sum_{i \in T(J)} i = 2^{n-1} \cdot |T(J)|/2 = 2^{n-2} \cdot a(a-1), \quad (3.5)$$

где $|T(J)| = 2C_a^2 = a(a-1)$, 2^{n-1} появляется за счёт того, что если $i \in T(J)$, $i < 2^{n-1}$, то $2^{n-1} - i \in {}_{2^{n-1}} T(J)$, число пар $(i, 2^{n-1} - i)$ равно $|T(J)|/2$, а их сумма равна 2^{n-1} .

Отметим, что для элемента $t \in \{1, \dots, 2^{n-2} - 1\} \cup \{2^{n-2} + 1, \dots, 2^{n-1} - 1\}$ выполняется равенство

$$\left| J \cap (J + t) \right| = \left| \{ (j_2, j_1) \in J^2 \mid j_2 \neq j_1, j_2 - j_1 = {}_{2^{n-1}} t \} \right|.$$

Поэтому

$$\sum_{i \in T(J)} i = \sum_{t \in \{1, \dots, 2^{n-1} - 1\} \setminus \{2^{n-2}\}} \left| J \cap (J + t) \right| = 2(2^{n-2} - 1) \cdot (a - 2^{n-3}). \quad (3.6)$$

Из равенств (3.5) и (3.6) получаем, что

$$2^{n-2} \cdot a(a-1) = 2(2^{n-2} - 1) \cdot (a - 2^{n-3}). \quad (3.7)$$

Уравнение (3.7) не имеет натуральных решений при $n \geq 6$. Следовательно, не существует такой подстановки s , что $sh_n^{-t} sh_n^t \in uB_n$ для каждого $t \in \{1, \dots, 2^{n-2} - 1\} \cup \{2^{n-2} + 1, \dots, 2^{n-1} - 1\}$. Таким образом, $\left| \text{Ker } \varphi_{n-1}^{(G_n)} \right| = 2^{2^{n-2}+1}$.

2. Найдём $|G_n|$. Так как

$$|G_n| = |\text{Im } \varphi_{n-1}^{(G_n)}| \cdot |\text{Ker } \varphi_{n-1}^{(G_n)}| = |G_{n-1}| \cdot 2^{2^{n-2}+1} \quad \text{и} \quad |G_2| = |P_2| = 2^3,$$

то

$$|G_n| = |G_{n-1}| \cdot 2^{2^{n-2}+1} = |G_2| \cdot 2^{n-2+\sum_{i=3}^n 2^{i-2}} = 2^{n+2^{n-1}-1}.$$

Теорема доказана.

Заметим, что последовательность подгрупп

$$\text{Ker } \varphi_{n-1}^{(G_n)}, \text{Ker } \varphi_{n-2}^{(G_n)}, \dots, \text{Ker } \varphi_1^{(G_n)}, G_n$$

позволяет ввести упорядочение на базисных векторах $\varepsilon_{0,n}, \varepsilon_{1,n}, \dots, \varepsilon_{n-1,n}$ пространства V_n .

Пусть $O(G)$ — множество всех орбит неединичной длины группы G , $\bar{O}(G)$ — множество всех орбит неединичной длины всех подгрупп группы G , т.е. $\bar{O}(G) = \bigcup_{B \leq G} O(B)$. Очевидно, что $\bar{O}(V_n^+) \subset \bar{O}(G_n)$, $\bar{O}(\mathbb{Z}_{2n}^+) \subset \bar{O}(G_n)$, $\bar{O}(G_n) = \bar{O}(P_n)$. Далее

нам понадобится описание строения элементов множеств $O(G_n)$, $O(P_n)$, $\bar{O}(G_n)$ и $\bar{O}(P_n)$.

Утверждение 3.2. При $n \geq 2$ для каждого элемента $\alpha \in \mathbb{Z}_{2^n}$ существуют такие элементы $r, i_1, \dots, i_r$, $0 \leq i_1 < \dots < i_r \leq n-1$, что

$$\alpha^{P_n} = \alpha \oplus \{\varepsilon_{i_1, n} u_1 \oplus \dots \oplus \varepsilon_{i_r, n} u_r \mid u_1, \dots, u_r \in \{0, 1\}\}.$$

Доказательство. Очевидно, что произвольная подгруппа группы V_n^+ представима в виде $\langle \varepsilon_{i_1, n} \oplus \dots \oplus \varepsilon_{i_r, n} \rangle$, где $0 \leq i_1 < i_2 < \dots < i_r \leq n-1$, а произвольная подгруппа группы $\mathbb{Z}_{2^n}^+$ – в виде $\langle h_n^t \rangle$, $t \in \{0, \dots, 2^n - 1\}$. Орбита произвольного элемента $\alpha \in V_n$ относительно группы $\langle \varepsilon_{i_1, n} \oplus \dots \oplus \varepsilon_{i_r, n} \rangle$ равна $\alpha \oplus \langle \varepsilon_{i_1, n} \oplus \dots \oplus \varepsilon_{i_r, n} \rangle$, а относительно $\langle h_n^{2^t} \rangle$ равна $\{\alpha + 2^t \cdot i \mid i \in \{0, \dots, 2^{n-t} - 1\}\}$.

Рассмотрим взаимно однозначное отображение

$$\psi^{(i)} : \text{Ker } \varphi_{i-1}^{(P_n)} \rightarrow X_i^{(n)} \times \text{Ker } \varphi_i^{(P_n)},$$

где $X_i^{(n)} = \text{Im } \varphi_i^{(P_n)} \cap \text{Ker } \varphi_{i-1}^{(P_n)}$, $i \in \{2, \dots, n\}$.

Произвольный элемент $g \in P_n$ представим в виде пары $(g^{(1)}, g'^{(1)}) \in \text{Im } \varphi_1^{(P_n)} \times \text{Ker } \varphi_1^{(P_n)}$, где $\varphi_1^{(P_n)}(g) = g^{(1)}$, $g^{(1)} \in S(\{W_0^{(1)}, W_1^{(1)}\})$. Для $i \in \{2, \dots, n\}$ элемент $g'^{(i-1)}$ также задаётся парой $(g^{(i)}, g'^{(i)})$, где $\psi^{(i)}(g'^{(i-1)}) = (g^{(i)}, g'^{(i)})$. Причём выполняется равенство $g^{(i)} = \prod_{j=0}^{2^{i-1}-1} g_j^{(i)}$, где $g_t^{(i)} \in S(\{W_t^{(i)}, W_{t+2^{i-1}}^{(i)}\})$, $t \in \{0, \dots, 2^{i-1} - 1\}$.

Существуют такие инъективные отображения $\phi_{i,t} : S(\{W_t^{(i)}, W_{t+2^{i-1}}^{(i)}\}) \rightarrow S(\mathbb{Z}_{2^n})$, $t = 0, \dots, 2^{i-1} - 1$, $i = 1, \dots, n-1$, что

$$g = \prod_{i=1}^{n-1} \prod_{j=0}^{2^{i-1}-1} \phi_{i,j}(g_j^{(i)}). \quad (3.8)$$

Отметим, что для всех $\alpha \in W_t^{(i)} \cup W_{t+2^{i-1}}^{(i)}$ имеет место точно один из двух случаев: $\phi_{i,j}(g_j^{(i)}) : \alpha \mapsto \alpha \oplus \varepsilon_{i-1, n}$ или $\phi_{i,j}(g_j^{(i)}) : \alpha \mapsto \alpha$.

Из равенства (3.8) следует, что орбита $U(\alpha)$ элемента $\alpha \in \mathbb{Z}_{2^n}$ относительно подгруппы группы P_n имеет вид

$$U(\alpha) = \alpha \oplus \{\varepsilon_{i_1, n} u_1 \oplus \dots \oplus \varepsilon_{i_r, n} u_r \mid u_1, \dots, u_r \in \{0, 1\}\}, \quad (3.9)$$

где $0 \leq i_1 < \dots < i_r \leq n-1$. Заметим, что

$$\alpha + \langle 2^t \rangle = \alpha \oplus \{\varepsilon_{t, n} u_1 \oplus \varepsilon_{t+1, n} u_2 \oplus \dots \oplus \varepsilon_{n-t-1, n} u_{n-t} \mid u_1, \dots, u_{n-t} \in \{0, 1\}\},$$

т.е. орбиты подгруппы $\langle h_n^{2^t} \rangle$ также имеют представление (3.9).

Из теоремы 3.1 следует, что $G_n = G_n^{(n-1)} \dots G_n^{(2)}$, где $G_n^{(n-1)} \cong \text{Ker } \varphi_{n-1}^{(G_n)}, \dots, G_n^{(3)} \cong \text{Ker } \varphi_2^{(G_3)}, G_n^{(2)} \cong G_2$. Поэтому орбита элемента $\alpha \in \mathbb{Z}_{2^n}$ имеет вид

$$\alpha^{G_n} = U'(\alpha) = \alpha \oplus \{\varepsilon_{i_1, n} u_1 \oplus \dots \oplus \varepsilon_{i_r, n} u_r \mid u_1, \dots, u_r \in \{0, 1\}\},$$

где $0 \leq i_1 < \dots < i_r \leq n-1$. Следовательно, $\bar{O}(G_n) = \bar{O}(P_n)$. Утверждение доказано.

Из доказательства утверждения 3.2 следует, что если $\alpha^{H_1} \subset \alpha^{H_2}$, то существуют такие числа $0 \leq j_1 < \dots < j_d < n-1$, что

$$\alpha^{H_2} = \alpha^{H_1} \oplus \{\varepsilon_{j_1,n}u_1 \oplus \dots \oplus \varepsilon_{j_d,n}u_d \mid u_1, \dots, u_d \in \{0, 1\}\}.$$

Нетрудно убедиться в справедливости следующих свойств для любого $\alpha \in \mathbb{Z}_{2^n}$.

(1) Если $H \leq \text{Ker } \varphi_t^{(P_n)}$ и

$$\alpha^H = \alpha \oplus \{\varepsilon_{i_1,n}u_1 \oplus \dots \oplus \varepsilon_{i_r,n}u_r \mid u_1, \dots, u_r \in \{0, 1\}\},$$

то $r \leq n-t$ и $t \leq i_1 < i_2 < \dots < i_r \leq n-1$.

(2) Если $\text{Ker } \varphi_t^{(P_n)} \leq H < \text{Ker } \varphi_{t-1}^{(P_n)}$, то

$$\alpha^H \in \{\alpha \oplus \langle \varepsilon_{t,n}, \dots, \varepsilon_{n-1,n} \rangle, \alpha \oplus \langle \varepsilon_{t-1,n}, \varepsilon_{t,n}, \dots, \varepsilon_{n-1,n} \rangle\}.$$

Опишем строение множеств, элементами которого являются все орбиты некоторой подгруппы группы P_n .

Утверждение 3.3. Пусть $n \geq 2$, $H < P_n$ и орбита элемента $\alpha \in \mathbb{Z}_{2^n}$ равна

$$\alpha^H = \alpha \oplus \{\varepsilon_{p_1,n}u_1 \oplus \dots \oplus \varepsilon_{p_r,n}u_r \mid u_1, \dots, u_r \in \{0, 1\}\},$$

$$0 \leq p_1 < p_2 < \dots < p_r, r < n.$$

Тогда множество всех орбит группы H на $\alpha \oplus \langle \varepsilon_{p_1,n}, \dots, \varepsilon_{n-1,n} \rangle$ равно

$$\{\beta \oplus \langle \varepsilon_{p_1,n}, \dots, \varepsilon_{p_r,n} \rangle \mid \beta \in \alpha \oplus \langle \varepsilon_{p_1,n}, \dots, \varepsilon_{n-1,n} \rangle\}.$$

Кроме того, H при любом $c \in \{0, \dots, p_1-1\}$ стабилизирует в целом множество $\alpha \oplus \langle \varepsilon_{c,n}, \dots, \varepsilon_{n-1,n} \rangle$.

Доказательство. Доказательство проведём индукцией по размерности c подпространства $\langle \varepsilon_{n-c,n}, \dots, \varepsilon_{n-1,n} \rangle$.

Так как $\alpha \oplus \varepsilon_{c,n} \notin \alpha^H$ для каждого $c \in \{n-1, \dots, p_r+1\}$, то ядро $\text{Ker } \varphi_{p_r+1}^{(H)}$ стабилизирует поточно множество $\alpha \oplus \langle \varepsilon_{p_r+1,n}, \dots, \varepsilon_{n-1,n} \rangle$ и существует элемент из ядра $\text{Ker } \varphi_{p_r}^{(H)}$, отображающий каждый элемент $\beta^{(1)} \in \alpha \oplus \langle \varepsilon_{p_r+1,n}, \dots, \varepsilon_{n-1,n} \rangle$ в элемент $\beta^{(1)} \oplus \varepsilon_{p_r,n}$. Таким образом, при ограничении группы $\text{Ker } \varphi_{p_r+1}^{(H)}$ на множество $\alpha \oplus \langle \varepsilon_{p_r,n}, \dots, \varepsilon_{n-1,n} \rangle$ множество всех её орбит равно

$$\{\beta^{(1)} \oplus \langle \varepsilon_{p_r,n} \rangle \mid \beta^{(1)} \in \alpha \oplus \langle \varepsilon_{p_r,n}, \dots, \varepsilon_{n-1,n} \rangle\}.$$

Пусть для ядра $\text{Ker } \varphi_{p_t}^{(H)}$ при его ограничении на множество $\alpha \oplus \langle \varepsilon_{p_t,n}, \dots, \varepsilon_{n-1,n} \rangle$ доказано, что множество всех орбит равно

$$\{\beta^{(t)} \oplus \langle \varepsilon_{p_t,n}, \dots, \varepsilon_{p_r,n} \rangle \mid \beta^{(t)} \in \alpha \oplus \langle \varepsilon_{p_t,n}, \dots, \varepsilon_{n-1,n} \rangle\}, \quad 1 < t \leq r.$$

Тогда $\text{Ker } \varphi_c^{(H)}$ стабилизирует в целом множество $\beta \oplus \langle \varepsilon_{p_t,n}, \dots, \varepsilon_{p_r,n} \rangle$ для каждого $\beta \in \alpha \oplus \langle \varepsilon_{c,n}, \dots, \varepsilon_{n-1,n} \rangle$, $c \in \{p_{t-1}+1, \dots, p_t-1\}$, в противном случае элемент $\alpha \oplus \varepsilon_{c,n}$ принадлежал бы орбите α^H .

Так как $\alpha \oplus \varepsilon_{p_{t-1},n} \in \alpha^H$, то существует элемент из ядра $\text{Ker } \varphi_{p_{t-1}}^{(H)}$, отображающий каждый элемент $\beta^{(t-1)} \in \alpha \oplus \langle \varepsilon_{p_{t-1}+1,n}, \dots, \varepsilon_{n-1,n} \rangle$ в элемент $\beta^{(t-1)} \oplus \varepsilon_{p_{t-1},n}$. Поэтому при ограничении действия группы $\text{Ker } \varphi_{p_{t-1}}^{(H)}$ на множество $\alpha \oplus \langle \varepsilon_{p_{t-1},n}, \dots, \varepsilon_{n-1,n} \rangle$ множество всех её орбит равно

$$\left\{ \beta^{(t-1)} \oplus \langle \varepsilon_{p_{t-1},n}, \dots, \varepsilon_{p_r,n} \rangle \mid \beta^{(t-1)} \in \alpha \oplus \langle \varepsilon_{p_{t-1},n}, \dots, \varepsilon_{n-1,n} \rangle \right\}.$$

Следовательно, множество всех орбит группы H на множестве $\alpha \oplus \langle \varepsilon_{p_1,n}, \dots, \varepsilon_{n-1,n} \rangle$ равно

$$\{ \beta \oplus \langle \varepsilon_{p_1,n}, \dots, \varepsilon_{p_r,n} \rangle \mid \beta \in \alpha \oplus \langle \varepsilon_{p_1,n}, \dots, \varepsilon_{n-1,n} \rangle \}.$$

Если бы группа H не стабилизировала в целом множество $\alpha \oplus \langle \varepsilon_{c,n}, \dots, \varepsilon_{n-1,n} \rangle$ для каждого $c \in \{0, \dots, p_1 - 1\}$, то элемент $\alpha \oplus \varepsilon_{c,n}$ принадлежал бы орбите α^H . Утверждение доказано.

Следствие 3.4. Пусть $n \geq 2$, $t \in \{1, \dots, n-1\}$.

1. Если $\text{Ker } \varphi_t^{(G_n)} \leq H \leq \text{Ker } \varphi_t^{(P_n)}$, то $\alpha^H = \alpha \oplus \langle \varepsilon_{t,n}, \dots, \varepsilon_{n-1,n} \rangle$ для каждого $\alpha \in \mathbb{Z}_{2^n}$ и $W^{(t,n)}$ – множество всех орбит группы H .
2. Если $R \in \{G_n, P_n\}$ и $\text{Ker } \varphi_t^{(R)} < H < \text{Ker } \varphi_{t-1}^{(R)}$, то для каждого элемента $\alpha \in \mathbb{Z}_{2^n}$ имеет место один из двух случаев:

$$2.1) \alpha^H = \alpha \oplus \langle \varepsilon_{t-1,n}, \varepsilon_{t,n}, \dots, \varepsilon_{n-1,n} \rangle;$$

$$2.2) \alpha^H = \alpha \oplus \langle \varepsilon_{t,n}, \dots, \varepsilon_{n-1,n} \rangle \text{ и } (\alpha \oplus \varepsilon_{t-1,n})^H = \alpha \oplus \langle \varepsilon_{t,n}, \dots, \varepsilon_{n-1,n} \rangle \oplus \varepsilon_{t-1,n}.$$

Доказательство. 1. Из теоремы 3.1 следует, что множество всех орбит группы $\text{Ker } \varphi_{n-1}^{(G_n)}$ есть $\{ \{ \alpha, \alpha + 2^{n-1} \} \mid \alpha \in \{0, \dots, 2^{n-1} - 1\} \}$. Так как $G_n = G_n^{(n-1)} \dots G_n^{(2)}$, где $G_n^{(n-1)} \cong \text{Ker } \varphi_{n-1}^{(G_n)}, \dots, G_n^{(3)} \cong \text{Ker } \varphi_2^{(G_3)}, G_n^{(2)} \cong G_2$, то множество всех орбит группы G_n есть

$$O(G_n) = \{ \alpha \oplus \langle \varepsilon_{t,n}, \dots, \varepsilon_{n-1,n} \rangle \mid \alpha \in \{0, \dots, 2^t - 1\} \}.$$

Так как $\text{Ker } \varphi_{n-1}^{(P_n)} = \{ (\alpha, \alpha + 2^{n-1}) \mid \alpha \in \{0, \dots, 2^{n-1} - 1\} \}$ и $P_n^{(n-1)} \cong \text{Ker } \varphi_{n-1}^{(P_n)}, \dots, P_n^{(3)} \cong \text{Ker } \varphi_2^{(P_3)}, P_n^{(2)} \cong P_2$, то $O(G_n) = O(P_n)$.

П. 2 следует из доказательства п.1. Следствие доказано.

Следствие 3.5. Если $n \geq 2$, $t \in \{1, \dots, n-1\}$, то $V_{n-t}^+ \times \mathbb{Z}_{2^t}^+ \not\leq G_n$, $\mathbb{Z}_{2^t}^+ \times V_{n-t}^+ \not\leq G_n$.

Доказательство. Очевидно, что $\langle \varepsilon_{t-1,n}, \dots, \varepsilon_{0,n} \rangle \leq G_n$ и $\langle \varepsilon_{n-1}, \dots, \varepsilon_{n/2} \rangle \leq G_n$. Если $\mathbb{Z}_{2^t}^+ \times V_{n-t}^+ \leq G_n$, то

$$(0, 2^{n-t}, 2^{n-t+1}, \dots, 2^n - 2^{n-t}) \in G_n \text{ и } (0, 2^{n-t}, 2^{n-t+1}, \dots, 2^n - 2^{n-t}) \in \text{Ker } \varphi_{n-t}^{(G_n)}.$$

Значит,

$$\begin{aligned} & \{ h_n^{-a}(0, 2^{n-t}, 2^{n-t+1}, \dots, 2^n - 2^{n-t}) h_n^a \mid a \in \{0, \dots, 2^{n-t} - 1\} \} = \\ & = \{ ((a, (a+2^{n-t})_{(n)}), (a+2^{n-t+1})_{(n)}, \dots, (a+2^n-2^{n-t})_{(n)}) \mid a \in \{0, \dots, 2^{n-t}-1\} \} \subseteq \\ & \subseteq \text{Ker } \varphi_{n-t}^{(G_n)}. \end{aligned}$$

Однако из теоремы 3.1 следует, что

$$\left(a, (a + 2^{n-t})_{(n)}, (a + 2^{n-t+1})_{(n)}, \dots, (a + 2^n - 2^{n-t})_{(n)} \right) \notin \text{Ker } \varphi_{n-t}^{(G_n)},$$

$$a \in \{0, \dots, 2^{n-t} - 1\}.$$

Поэтому $\mathbb{Z}_{2^t}^+ \times V_{n-t}^+ \not\leq G_n$.

Пусть $g = (0, 1, 2, \dots, 2^t - 1)$. Если $V_{n-t}^+ \times \mathbb{Z}_{2^t}^+ \leq G_n$, то $g \in G_n$. Заметим, что $\{0, 2^{n-1}\}^g \in W^{(n-1, n)}$, но $\{0, 2^{n-1}\}^g = \{1, 2^{n-1}\}$ и $\{0, 2^{n-1}\}^g \cap \{1, 2^{n-1}\} = \{2^{n-1}\}$. Значит, $g \notin G_n$ и $V_{n-t}^+ \times \mathbb{Z}_{2^t}^+ \not\leq G_n$.

Следствие доказано.

4. Свойства нормальных подгрупп группы G_n

Опишем нормальные подгруппы группы G_n . Для $n \geq 2$ положим

$$R_n^{(j)} = \left\langle \prod_{t=0}^{2^{n-2-j}} u_{r+2^j t \pmod{2^{n-2}}, n} \mid r \in \{0, \dots, 2^j - 1\} \right\rangle, \quad j = 0, \dots, n-2,$$

$$c_{J,n} : \alpha \mapsto \alpha \oplus \bigoplus_{j \in J} \varepsilon_{j,n}, \quad J \subseteq \{0, \dots, n-1\}.$$

Заметим, что из теоремы 3.1 следует, что все элементы $u_{0,n}, \dots, u_{2^{n-2}-1,n}$ порождают подгруппу ядра $\text{Ker } \varphi_{n-1}^{(G_n)}$. При этом

$$R_n^{(0)} = Z(G_n), \quad \langle e_n \rangle < R_n^{(0)} < R_n^{(1)} < \dots < R_n^{(n-2)} < \text{Ker } \varphi_{n-1}^{(G_n)},$$

$$|R_n^{(j)}| = 2^{2^j}, \quad j = 0, \dots, n-2.$$

Утверждение 4.1. Если $n \geq 2$, то $R_n^{(m)} \triangleleft G_n$ для произвольного $m \in \{0, \dots, n-2\}$.

Доказательство. Из доказательства теоремы 3.1 следует, что нормальными подгруппами $\text{Ker } \varphi_{n-1}^{(G_n)}$ являются группы $R_n^{(0)} = Z(G_n)$ и $R_n^{(n-2)}$. Так как элемент $u_{r,n}$ можно представить в виде $\prod_{t \in W_r^{(m, n-1)}} (t, t + 2^{n-1})$ для $r \in \{0, \dots, 2^m - 1\}$, то для нормальности $R_n^{(m)}$ в G_n достаточно, чтобы каждый элемент группы G_n действовал как подстановка на множестве $U^{(m, n-1)} = \{U_0^{(m, n-1)}, \dots, U_{2^m-1}^{(m, n-1)}\}$, где

$$U_r^{(m, n-1)} = \left\{ \{t_{(n)}, (t + 2^{n-1})_{(n)}\} \mid t \in W_r^{(m, n-1)} \right\}, \quad r = 0, \dots, 2^m - 1.$$

Из справедливости для произвольных $i \in \{0, \dots, 2^n - 1\}$, $j \in \{0, \dots, n-1\}$ равенств

$$\left(U_r^{(m, n-1)} \right)^{h_n^i} = \left\{ \{ (t+i)_{(n)}, (t+i+2^{n-1})_{(n)} \} \mid t \in W_r^{(m, n-1)} \right\} = U_{r+i \pmod{2^m}}^{(m, n-1)},$$

$$\left(U_r^{(m, n-1)} \right)^{c_{j,n}} = {}_{2^n} \{ t \oplus \varepsilon_{j,n}, t \oplus \varepsilon_{j,n} \oplus \varepsilon_{n-1,n} \mid t \in W_r^{(m, n-1)} \} = U_{r \oplus \varepsilon_{j,n} \pmod{2^m}}^{(m, n-1)}$$

следует, что $U^g \in U^{(m, n-1)}$ и $(U^g \cap U) \in \{\emptyset, U\}$ для всех $U \in U^{(m, n-1)}$, $g \in G_n$. Таким образом, $R_n^{(m)} \triangleleft G_n$.

Утверждение доказано.

Каждому элементу $g \in \text{Ker } \varphi_{n-1}^{(G_n)}$ однозначно соответствует такое множество $J_n(g) \subseteq \{0, \dots, 2^{n-1} - 1\}$, что $g = \prod_{t \in J_n(g)} u_{t,n}$. Заметим, что $J_n(e_n) = \emptyset$.

Для $g \in R_n^{(n-2)}$ положим

$$J'_n(g) = \bigcup_{t \in J_n(g)} \{\{t, t + 2^{n-1}\}, \{t + 2^{n-2}, t + 2^{n-2} + 2^{n-1}\}\}.$$

Элемент $u_{t,n}$ однозначно определяется подмножеством

$$\{\{t, t + 2^{n-1}\}, \{t + 2^{n-2}, t + 2^{n-2} + 2^{n-1}\}\}, \quad t \in \{0, \dots, 2^{n-2} - 1\}.$$

Поэтому каждое из множеств $\{t, t + 2^{n-1}\}$, $\{t + 2^{n-2}, t + 2^{n-2} + 2^{n-1}\}$ однозначно соответствует элементу g .

Заметим, что для $j \in \{0, \dots, n-2\}$, $r \in \{0, \dots, 2^j - 1\}$ выполняются равенства

$$\delta_{r,n}^{(j)} = \prod_{t=0}^{2^{n-2-j}} u_{r+2^j t \pmod{2^{n-2}}, n} = h_n^{-r} \delta_{0,n}^{(j)} h_n^r,$$

$$J'_n(\delta_{r,n}^{(t)}) = J'_n(\delta_{r,n}^{(t)})^{h_n^{2^t}}, \quad r = 0, \dots, 2^t - 1.$$

Утверждение 4.2. Пусть $n \geq 2$. Группа $R_n^{(1)}$ является единственной нормальной подгруппой группы G_n , удовлетворяющей одновременно условиям $|R_n^{(1)}| = 4$, $Z(G_n) < R_n^{(1)} < \text{Ker } \varphi_{n-1}^{(G_n)}$.

Доказательство. Предположим, что существует другая такая нормальная подгруппа $B_n^{(1)}$ группы G_n , что $|B_n^{(1)}| = 4$, $R_n^{(0)} < B_n^{(1)}$ и $B_n^{(1)} < \text{Ker } \varphi_{n-1}^{(G_n)}$. Тогда $B_n^{(1)} = \langle g_1, g_2 \rangle$, причем $g_1 g_2 = u_{0,n} \dots u_{2^{n-2}-1,n}$, $g_1, g_2 \notin R_n^{(0)}$ и $J_n(g_1) \cap J_n(g_2) = \emptyset$. Очевидно, что $h_n^{-i} g_1 h_n^i h_n^{-i} g_2 h_n^i = u_{0,n} \dots u_{2^{n-2}-1,n}$ для каждого $i \in \{0, \dots, 2^n - 1\}$. Так как $|B_n^{(1)}| = 4$, то $\{h_n^{-i} g_1 h_n^i, h_n^{-i} g_2 h_n^i\} = \{g_1, g_2\}$ для каждого $i \in \{0, \dots, 2^n - 1\}$. Поэтому возможны два случая: 1) $J'_n(g_1)^{h_n} = J'_n(g_1)$, $J'_n(g_2)^{h_n} = J'_n(g_2)$; 2) $J'_n(g_1)^{h_n} = J'_n(g_2)$, $J'_n(g_2)^{h_n} = J'_n(g_1)$.

- (1) Ясно, что равенство $J'_n(g_1)^{h_n} = J'_n(g_1)$ выполняется тогда и только тогда, когда $J_n(g_1) \in \{\emptyset, \{0, \dots, 2^{n-2} - 1\}\}$, т.е. $g_1 = e$ или $g_1 = u_{0,n} \dots u_{2^{n-2}-1,n}$.
- (2) Без ограничения общности предположим, что $0 \in J_n(g_1)$. Так как $J'_n(g_1)^{h_n} = J'_n(g_2)$, $J'_n(g_2)^{h_n} = J'_n(g_1)$, то из описания блоков импримитивности группы G_n следует, что такие множества $J_n(g_1)$, $J_n(g_2)$ определяются однозначно и равны

$$J_n(g_1) = \{2i \mid i = 0, \dots, 2^{n-3} - 1\}, \quad J_n(g_2) = \{2i + 1 \mid i = 0, \dots, 2^{n-3} - 1\}.$$

Значит, $g_1 = \delta_{0,n}^{(1)}$, $g_2 = \delta_{1,n}^{(1)}$ и $B_n^{(1)} = R_n^{(1)}$.

Утверждение доказано.

Очевидно, что $R_n^{(1)}$ является наименьшей нормальной в G_n надгруппой группы $R_n^{(0)}$.

Для $g \in \text{Ker } \varphi_{n-1}^{(G_n)}$ положим

$$D_n(g) = \langle h_n^{-r} g h_n^r \mid r = 0, \dots, 2^n - 1 \rangle.$$

Заметим, что $R_n^{(j)} = D_n(\delta_{0,n}^{(j)})$.

Утверждение 4.3. Пусть $n \geq 2$. Тогда:

- (1) Группа $R_n^{(n-2)}$ является максимальной нормальной подгруппой группы G_n в $\text{Ker } \varphi_{n-1}^{(G_n)}$.
- (2) Для каждой нормальной подгруппы B_n группы G_n в $\text{Ker } \varphi_{n-1}^{(G_n)}$ существует такое наименьшее число $t_0 \in \{1, \dots, n-2\}$, что $B_n \leq R_n^{(t_0)}$ и $B_n \cap R_n^{(j)} \neq \emptyset$, $B_n \leq R_n^{(t_0)}$ при $j = 1, \dots, t_0$.

Доказательство. Пусть $g = \prod_{t=0}^{2^{n-2}-1} (2^{n-2} + t, 2^{n-1} + 2^{n-2} + t)$.

1. Из теоремы 3.1 следует, что $g \notin R_n^{(n-2)}$ и $\text{Ker } \varphi_{n-1}^{(G_n)} = \langle g, u_{0,n}, \dots, u_{2^{n-2}-1,n} \rangle$. Заметим, что

$$R_n^{(n-2)} = \langle h_n^{-i} u_{0,n} h_n^i \mid i \in \{0, \dots, 2^n - 1\} \rangle.$$

Предположим, что существует нормальная в G_n подгруппа $B_n \leq \text{Ker } \varphi_{n-1}^{(G_n)}$ большей мощности, чем $R_n^{(n-2)}$. Тогда $B_n \cap R_n^{(n-2)} \neq \emptyset$.

Рассмотрим группу

$$C_n(g) = \langle h_n^{-i} g h_n^i \mid i \in \{0, \dots, 2^n - 1\} \rangle.$$

Так как

$$u_{r,n} = h_n^{-r} g h_n^r h_n^{-(r+1)} g h_n^{r+1}, \quad r = 0, \dots, 2^{n-2} - 1, \quad (4.2)$$

то $C_n(g) = \text{Ker } \varphi_{n-1}^{(G_n)}$. Группа B_n нормальна в G_n , поэтому

$$\langle h_n^{-i} b h_n^i \mid i \in \{0, \dots, 2^n - 1\} \rangle \subseteq B_n$$

для каждого $b \in B$.

Пусть $g' = gu \in B_n \cap gR_n^{(n-2)}$ для некоторого $u \in R_n^{(n-2)}$. Тогда

$$h_n^{-r} g' h_n^r h_n^{-(r+1)} g' h_n^{r+1} = u_{r,n} h_n^{-r} u h_n^{-1} u h_n^{r+1}.$$

Следовательно, для каждого $r \in \{0, \dots, 2^{n-2} - 1\}$ справедливы включения

$$\begin{aligned} u h_n^{-(r+1)} u_{r,n} h_n^{-r} u h_n^{-1} &\in B_n, \\ g h_n^{-(r+1)} u_{r,n} h_n^{-r} u h_n^{-1} &\in B_n, \\ g u_{2r+1 \pmod{2^{n-2}}, n} h_n^{-1} u h_n^{-1} &\in B_n. \end{aligned} \quad (4.3)$$

Из включений (4.3) следует, что

$$u_{2r_0+1 \pmod{2^{n-2}}, n} u_{2r_1+1 \pmod{2^{n-2}}, n} \in B_n, \quad u_{2r_0 \pmod{2^{n-2}}, n} u_{2r_1 \pmod{2^{n-2}}, n} \in B_n$$

для произвольных чисел $r_0, r_1 \in \{0, \dots, 2^{n-3} - 1\}$. Значит, $B'_n \leq B_n$, где

$$B'_n = \langle u_j u_{j'} \mid j, j' \in \{0, \dots, 2^{n-2} - 1\} \rangle.$$

Следовательно, возможны два случая: $u \in B'_n$ или $u = u_{c,n}u'$ для некоторых $u' \in B'_n$, $c \in \{0, \dots, 2^{n-2} - 1\}$.

Если $u \in B'_n$, то $g \in B_n$. Значит, $B_n = C_n(g) = \text{Кер } \varphi_{n-1}^{(G_n)}$. Если же $u = u_{c,n}u'$ для некоторых $u' \in B'_n$, $c \in \{0, \dots, 2^{n-2} - 1\}$, то $gu_{c,n} \in B_n$. Таким образом, $ss' \in B_n$ для любых $s, s' \in \{h_n^{-i}gh_n^i \mid i \in \{0, \dots, 2^n - 1\}\}$. Из равенств (4.2) следует, что $u_{0,n} = \tilde{s}\tilde{s}'$ для некоторых $\tilde{s}, \tilde{s}' \in \{h_n^{-i}gh_n^i \mid i \in \{0, \dots, 2^n - 1\}\}$, а значит, $B_n = \text{Кер } \varphi_{n-1}^{(G_n)}$. Таким образом, $R_n^{(n-2)}$ – максимальная нормальная подгруппа группы G_n в $\text{Кер } \varphi_{n-1}^{(G_n)}$.

2. Пусть $C_n, C_n \leq \text{Кер } \varphi_{n-1}^{(G_n)}$, – произвольная нормальная подгруппа группы G_n , $C_n \notin \{R_n^{(j)} \mid j = 0, \dots, n-2\} \cup \{\text{Кер } \varphi_{n-1}^{(G_n)}\}$. Покажем, что $C_n \triangleleft R_n^{(n-2)}$.

Рассмотрим последовательность

$$C_n \leq C_n R_n^{(0)} \leq C_n R_n^{(1)} \leq \dots \leq C_n R_n^{(n-2)} \leq \text{Кер } \varphi_{n-1}^{(G_n)},$$

где $C_n R_n^{(j)} \triangleleft G_n$, $j = 0, \dots, n-2$. Согласно п.1 $R_n^{(n-2)}$ – максимальная подгруппа группы $\text{Кер } \varphi_{n-1}^{(G_n)}$, нормальная в G_n . Поэтому либо $C_n R_n^{(n-2)} = R_n^{(n-2)}$, либо $C_n R_n^{(n-2)} = \text{Кер } \varphi_{n-1}^{(G_n)}$. Если $C_n R_n^{(n-2)} = R_n^{(n-2)}$, то $C_n \leq R_n^{(n-2)}$. Если же $C_n R_n^{(n-2)} = \text{Кер } \varphi_{n-1}^{(G_n)}$, то $C_n \cap g R_n^{(n-2)} \neq \emptyset$. Аналогично доказательству п. 1 легко показать, что $C_n = \text{Кер } \varphi_{n-1}^{(G_n)}$. Значит, $C_n \leq R_n^{(n-2)}$.

Зафиксируем наибольшее число $p \in \{1, 2, \dots, n-3\}$ со свойством $C_n \setminus R_n^{(p)} \neq \emptyset$ и $C_n \setminus R_n^{(p+1)} = \emptyset$. Оно существует, так как $C_n < R_n^{(n-2)}$.

Докажем включение $R_n^{(p-1)} < C_n < R_n^{(p)}$. Рассмотрим произвольный элемент $b \in C_n \setminus R_n^{(p)}$. Для элементов $i \in \{0, \dots, 2^t - 1\}$, $t \in \{1, 2, \dots, n-2\}$ и множества $A \subseteq \{0, \dots, 2^{n-2} - 1\}$ положим

$$X_{i,t}^{(n)} = \{j \in \{0, 1, \dots, 2^{n-2} - 1\} \mid j \equiv_{2^t} i\}, \quad b_{t,n} = \prod_{j=0}^{2^{n-2}-t} h_n^{-j2^t} b h_n^{j2^t},$$

$$q_{i,t}^{(n)} \equiv_2 |\{a \in A \mid a \equiv_{2^t} i\}|, \quad A^{[0]} = \emptyset, \quad A^{[1]} = A.$$

Нетрудно убедиться в том, что

$$J_n(b_{t,n}) = \bigcup_{j=0}^{2^t-1} \left(X_{j,t}^{(n)} \right)^{[q_{j,t}^{(n)}]}.$$

Из равенства (4.1) следует, что $b_{t,n} \in R_n^{(t)}$.

Лемма 4.4. Пусть $n \geq 2$. Тогда и только тогда $b \in R_n^{(t)} \setminus R_n^{(t-1)}$, когда $b_{t,n} = e_n$, $b_{t-1,n} \neq e_n$.

Доказательство. Пусть $b \in R_n^{(t)} \setminus R_n^{(t-1)}$. Из равенства (4.1) следует, что $q_{i,t}^{(n)} = 0$ для $i = 0, \dots, 2^t - 1$, и $q_{j,t-1}^{(n)} = 1$ для некоторого $j \in \{0, \dots, 2^t - 1\}$. Таким образом, $J_n(b_{t,n}) = \emptyset$, $J_n(b_{t-1,n}) \neq \emptyset$, т.е. $b_{t,n} = e_n$, $b_{t-1,n} \neq e_n$. Аналогичным образом показывается, что $b \in R_n^{(t)} \setminus R_n^{(t-1)}$, если $b_{t,n} = e_n$, $b_{t-1,n} \neq e_n$.

Лемма доказана.

Из условий $b \in C_n \setminus R_n^{(p)}$, $C_n \setminus R_n^{(p+1)} = \emptyset$ и леммы 4.4 следует, что $b \in R_n^{(p+1)} \setminus R_n^{(p)}$ и $C_n \cap R_n^{(j)} \neq \emptyset$ для $j = 1, \dots, p$. Кроме того, в силу произвольности элемента b справедливо включение $C_n < R_n^{(p+1)}$.

Значит, существует такое наименьшее число $t_0 \in \{1, \dots, n-2\}$, что $C_n \leq R_n^{(t_0)}$ и $C_n \cap R_n^{(j)} \neq \emptyset$, $C_n \leq R_n^{(t_0)}$ при $j = 1, \dots, t_0$. Утверждение 4.3 доказано.

Укажем связь между нормальными подгруппами группы G_n , являющимися подгруппами ядер $\text{Ker } \varphi_{n-1}^{(G_n)}$ и $\text{Ker } \varphi_{n-i}^{(G_n)}$, и опишем орбиты нормальных подгрупп, содержащих центр группы G_n .

Пусть $\text{Ker } \varphi_n^{(G_n)} = \langle e_n \rangle$, $\text{Ker } \varphi_0^{(G_n)} = G_n$ и $H_{n-i}^{(0)}, H_{n-i}^{(1)}, \dots, H_{n-i}^{(d_{n-i,n})}$ — такие нормальные подгруппы группы G_n , что

$$\text{Ker } \varphi_{n-i}^{(G_n)} \triangleleft H_{n-i,n}^{(0)} \triangleleft H_{n-i,n}^{(1)} \triangleleft \dots \triangleleft H_{n-i,n}^{(d_{n-i,n})} \triangleleft \text{Ker } \varphi_{n-i-1}^{(G_n)}, \quad i \in \{0, 1, \dots, n-1\},$$

и не существует других нормальных подгрупп группы G_n , являющихся надгруппами группы $\text{Ker } \varphi_{n-i}^{(G_n)}$ и подгруппами группы $\text{Ker } \varphi_{n-i-1}^{(G_n)}$. Пусть $d_{n-i,n} + 1$ — число таких нормальных подгрупп.

Для $i \in \{1, \dots, n-1\}$ имеем

$$\begin{aligned} \text{Ker } \varphi_{n-i}^{(G_n)} / \text{Ker } \varphi_{n-1}^{(G_n)} &\triangleleft H_{n-i}^{(0)} / \text{Ker } \varphi_{n-1}^{(G_n)} \triangleleft H_{n-i}^{(1)} / \text{Ker } \varphi_{n-1}^{(G_n)} \triangleleft \dots \\ &\dots \triangleleft H_{n-i}^{(d_{n-i,n})} / \text{Ker } \varphi_{n-1}^{(G_n)} \triangleleft \text{Ker } \varphi_{n-i-1}^{(G_n)} / \text{Ker } \varphi_{n-1}^{(G_n)}. \end{aligned}$$

Из теоремы 3.1 следует, что $H_{n-i}^{(j)} / \text{Ker } \varphi_{n-1}^{(G_n)} \cong H_{n-i}^{(j,1)}$, где $H_{n-i}^{(j,1)} \leq G_{n-1}$, $j = 0, \dots, d_{n-i,n}$.

Так как $H_{n-i}^{(j)} \triangleleft G_{n-1}$, то $H_{n-i}^{(j,1)} \triangleleft G_{n-1}$. При этом $e_{n-1} \in G_{n-1}$, $\langle e_{n-1} \rangle \cong \text{Ker } \varphi_{n-1}^{(G_n)} / \text{Ker } \varphi_{n-1}^{(G_n)}$; $\text{Ker } \varphi_{n-i-1}^{(G_n)} / \text{Ker } \varphi_{n-1}^{(G_n)} \cong \text{Ker } \varphi_{n-i-1}^{(G_{n-1})}$; $H_{n-i}^{(j_1,1)} \neq H_{n-i}^{(j_2,1)}$ при $j_1, j_2 \in \{0, \dots, d_{n-i,n}\}$, $j_1 \neq j_2$. Поэтому

$$\text{Ker } \varphi_{n-i}^{(G_{n-1})} \triangleleft H_{n-i,n}^{(0,1)} \triangleleft H_{n-i,n}^{(1,1)} \triangleleft \dots \triangleleft H_{n-i,n}^{(d_{n-i,n},1)} \triangleleft \text{Ker } \varphi_{n-i-1}^{(G_{n-1})}$$

и $d_{n-i,n} \leq d_{n-i,n-1}$ для $i = 1, \dots, n-1$.

Очевидно, что

$$\begin{aligned} d_{n-j,n} &\geq d_{n-j-1,n-1}, \quad j = 0, \dots, n-1, \\ H_{n-1,n}^{(0,1)} &= Z(G_{n-1}), \quad H_{n-1,n}^{(d_{n-1,n},1)} = R_{n-1}^{(n-3)}. \end{aligned}$$

Заметим, что если $B_n \triangleleft G_n$, $B_n \leq \text{Ker } \varphi_{n-1}^{(G_n)}$, то

$$\text{O}(B_n) = \text{O} \left(\text{Ker } \varphi_{n-1}^{(G_n)} \right) = \{ \{ \alpha, \alpha + 2^{n-1} \}, \alpha \in \{0, \dots, 2^{n-1} - 1\} \} = W^{(n-1,n)}.$$

Если $\{ \alpha, \alpha + 2^{n-1} \} \in \text{O}(B_n)$ для некоторого $\alpha \in \{0, \dots, 2^{n-1} - 1\}$, то из условия $B_n \leq G_n$ следует включение $\{ \alpha^{h_n^j}, (\alpha + 2^{n-1})^{h_n^j} \} \in \text{O}(B_n)$ для каждого $j \in \{0, \dots, 2^n - 1\}$, т.е.

$$\text{O}(B_n) = \text{O}(Z(G_{n-1})) = \text{O} \left(\text{Ker } \varphi_{n-1}^{(G_n)} \right).$$

Зафиксируем произвольные числа $i \in \{1, \dots, n-1\}$, $j \in \{1, \dots, d_{n-i,n}\}$ и положим $H_{n-i}^{(j,0)} = H_{n-i}^{(j)}$, $H_{n-i}^{(j,c)} / \text{Ker } \varphi_{n-c}^{(G_n)} \cong H_{n-i}^{(j,1+c)}$, $c = 0, \dots, i+1$. Так как $\text{Ker } \varphi_{n-i-1}^{(G_{n-c})} / \text{Ker } \varphi_{n-c}^{(G_{n-c})} \cong \text{Ker } \varphi_{n-i-1}^{(G_{n-c-1})}$, то $H_{n-i}^{(j,1+c)} \triangleleft G_{n-c-1}$ и

$$\text{Ker } \varphi_{n-i}^{(G_{n-c-1})} \triangleleft H_{n-i,n}^{(0,1+c)} \triangleleft H_{n-i,n}^{(1,1+c)} \triangleleft \dots \triangleleft H_{n-i,n}^{(d_{n-i,n},1+c)} \triangleleft \text{Ker } \varphi_{n-i-1}^{(G_{n-1-c})}. \quad (4.4)$$

Если $H_{n-i-1,n}^{(0,1+i)} = Z(G_{n-i-1})$, то

$$O(H_{n-i-1,n}^{(j,1+i)}) = O(Z(G_{n-i-1})) = O(\text{Ker } \varphi_{n-i-2}^{(G_{n-i-1})}) = W^{(n-i-2, n-i-1)}. \quad (4.5)$$

Применяя соотношения (4.4), (4.5), индукцией по i несложно показать, что

$$O(H_{n-i,n}^{(j)}) = O(\text{Ker } \varphi_{n-i-1}^{(G_n)}) = W^{(n-i-1, n)}. \quad (4.6)$$

5. Модулярные представления группы G_n

Пусть $GL_n(2)$ — полная линейная группа над $GF(2)$; $\mathbf{0}_{d,m}$ — нулевая $(d \times m)$ -матрица, $\mathbf{e}_m$ — единичная $(m \times m)$ -матрица. Зафиксируем число $t \in \{1, \dots, n-2\}$. Пусть $\pi_n^{(t)}$ — гомоморфизм группы G_n в группу $GL_{2^t}(2)$, заданный действием группы G_n сопряжением на нормальной подгруппе $R_n^{(t)}$, и $\rho_n^{(t)}$ — такой изоморфизм группы $R_n^{(t)}$ в группу $V_{2^t}^+$, что $\rho_n^{(t)}(\delta_{r,n}^{(t)}) = \varepsilon_{r,2^t}$ для всех $r \in \{0, \dots, 2^t - 1\}$.

Заметим, что гомоморфизм $\pi_n^{(t)}$ является модулярным представлением группы G_n степени 2^t , а $\pi_n^{(t)}(h_n)$, $\pi_n^{(t)}(c_{0,n}), \dots, \pi_n^{(t)}(c_{t-1,n})$ — подстановочные матрицы. Для $r \in \{0, \dots, 2^t - 1\}$ имеем

$$\begin{aligned} \pi_n^{(t)}(h_n) &: \varepsilon_{r,2^t} \mapsto \varepsilon_{r+1 \pmod{2^t}, 2^t}, \\ \pi_n^{(t)}(c_{j,n}) &: \varepsilon_{r,2^t} \mapsto \varepsilon_{r \oplus 2^j, 2^t}, \quad j \in \{0, \dots, t-1\}. \end{aligned}$$

Матрица $\pi_n^{(t)}(h_n)$ действует на векторах из V_{2^t} циклическим сдвигом на одну координату вправо.

Тогда и только тогда $g \in \text{Ker}(\pi_n^{(t)}(h_n))$, когда

$$g^{-1} \delta_{r,n}^{(t)} g = \delta_{r,n}^{(t)}, \quad r = 0, \dots, 2^t - 1. \quad (5.1)$$

Равенства (5.1) равносильны тому, что

$$\begin{aligned} \left\{ \{t, t + 2^{n-1}\} \mid t \in W_r^{(t, n-1)} \right\}^g &= \left\{ \left\{ (t^g)_{(n)}, \left((t + 2^{n-1})^g \right)_{(n)} \right\} \mid t \in W_r^{(t, n-1)} \right\} = \\ &= \left\{ \left\{ t, (t + 2^{n-1})_{(n)} \right\} \mid t \in W_r^{(t, n-1)} \right\} \end{aligned}$$

для $r = 0, \dots, 2^t - 1$, т.е. $(W_r^{(t, n)})^g = W_r^{(t, n)}$. Значит, $\text{Ker}(\pi_n^{(t)}) = \text{Ker}(\varphi_t^{(G_n)})$ и $\text{Im}(\pi_n^{(t)}) \cong \text{Im}(\varphi_t^{(G_n)}) \cong G_t$.

Прямыми вычислениями несложно убедиться в том, что

$$\begin{aligned}\tilde{\mathbf{e}}_2 &= \pi_n^{(1)}(c_{0,n}) = \pi_n^{(1)}(h_n) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \\ \pi_n^{(2)}(c_{0,n}) &= \mathbf{e}_2 \otimes \pi_n^{(1)}(c_{0,n}) = \mathbf{e}_2 \otimes \tilde{\mathbf{e}}_2 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \\ \pi_n^{(2)}(c_{1,n}) &= \pi_n^{(1)}(c_{0,n}) \otimes \mathbf{e}_2 = \tilde{\mathbf{e}}_2 \otimes \mathbf{e}_2 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \\ \pi_n^{(1)}(h_n) &= \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix},\end{aligned}$$

$$\begin{aligned}\pi_n^{(3)}(c_{0,n}) &= \mathbf{e}_2 \otimes \tilde{\mathbf{e}}_2 = \mathbf{e}_2 \otimes \mathbf{e}_2 \otimes \tilde{\mathbf{e}}_2 = \mathbf{e}_4 \otimes \tilde{\mathbf{e}}_2, \\ \pi_n^{(3)}(c_{1,n}) &= \mathbf{e}_2 \otimes \pi_n^{(2)}(c_{1,n}) = \mathbf{e}_2 \otimes \tilde{\mathbf{e}}_2 \otimes \mathbf{e}_2, \\ \pi_n^{(3)}(c_{2,n}) &= \pi_n^{(2)}(c_{2,n}) \otimes \mathbf{e}_2 = \tilde{\mathbf{e}}_2 \otimes \mathbf{e}_2 \otimes \mathbf{e}_2 = \tilde{\mathbf{e}}_2 \otimes \mathbf{e}_4.\end{aligned}$$

Найдем тензорное представление матрицы $\pi_n^{(t)}(c_{j,n})$. Так как для $j \in \{0, \dots, t-2\}$ справедливо равенство

$$\begin{aligned}\varepsilon_{r,2^t} \pi_n^{(t)}(c_{j,n}) &= \varepsilon_{r \oplus 2^j, 2^t} = \\ &= \begin{cases} \left(\varepsilon_{r \oplus 2^j, 2^{t-1}}, \vec{0}_{2^{t-1}} \right) = \left(\varepsilon_{r, 2^{t-1}} \pi_n^{(t-1)}(c_{j,n}), \vec{0}_{2^{t-1}} \mathbf{0}_{2^{t-1}, 2^{t-1}} \right), & r \in \{0, \dots, 2^{t-1}-1\}, \\ \left(\vec{0}_{2^{t-1}}, \varepsilon_{r \oplus 2^j, 2^{t-1}} \right) = \left(\vec{0}_{2^{t-1}} \mathbf{0}_{2^{t-1}, 2^{t-1}}, \varepsilon_{r, 2^{t-1}} \pi_n^{(t-1)}(c_{j,n}) \right), & r \in \{2^{t-1}, \dots, 2^t-1\}, \end{cases}\end{aligned}$$

то

$$\pi_n^{(t)}(c_{j,n}) = \begin{pmatrix} \mathbf{0}_{2^{t-1}, 2^{t-1}} & \pi_n^{(t-1)}(c_{j,n}) \\ \pi_n^{(t-1)}(c_{j,n}) & \mathbf{0}_{2^{t-1}, 2^{t-1}} \end{pmatrix} = \tilde{\mathbf{e}}_2 \otimes \pi_n^{(t-1)}(c_{j,n}). \quad (5.2)$$

Если же $j = t-1$, то

$$\begin{aligned}\varepsilon_{r,2^t} \pi_n^{(t)}(c_{t-1,n}) &= \varepsilon_{r \oplus 2^j, 2^t} = \\ &= \begin{cases} \left(\vec{0}_{2^{t-1}}, \varepsilon_{r \oplus 2^{t-1}, 2^{t-1}} \right) = \left(\vec{0}_{2^{t-1}} \mathbf{0}_{2^{t-1}, 2^{t-1}}, \varepsilon_{r, 2^{t-1}} \mathbf{e}_{2^{t-1}} \right), & r \in \{0, \dots, 2^{t-1}-1\}, \\ \left(\varepsilon_{r \oplus 2^{t-1}, 2^{t-1}}, \vec{0}_{2^{t-1}} \right) = \left(\varepsilon_{r, 2^{t-1}} \mathbf{e}_{2^{t-1}}, \vec{0}_{2^{t-1}} \mathbf{0}_{2^{t-1}, 2^{t-1}} \right), & r \in \{2^{t-1}, \dots, 2^t-1\}, \end{cases}\end{aligned}$$

и

$$\pi_n^{(t)}(c_{t-1,n}) = \begin{pmatrix} \mathbf{0}_{2^{t-1}, 2^{t-1}} & \mathbf{e}_{2^{t-1}} \\ \mathbf{e}_{2^{t-1}} & \mathbf{0}_{2^{t-1}, 2^{t-1}} \end{pmatrix} = \tilde{\mathbf{e}}_2 \otimes \mathbf{e}_{2^{t-1}}. \quad (5.3)$$

При этом

$$\pi_n^{(t)}(h_n) = \begin{pmatrix} 0 & 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & 0 & 0 & \dots & 0 & 0 \end{pmatrix}.$$

Из равенств (5.2), (5.3) следует, что

$$\pi_n^{(t)}(c_{j,n}) = \mathbf{e}_{2^{t-j-1}} \otimes \tilde{\mathbf{e}}_2 \otimes \mathbf{e}_{2^j}, \quad j \in \{0, \dots, t-2\}.$$

Например, для $t = 4$ получаем

$$\pi_n^{(4)}(c_{0,n}) = \begin{pmatrix} \pi_n^{(3)}(c_{0,n}) & \mathbf{0}_{8,8} \\ \mathbf{0}_{8,8} & \pi_n^{(3)}(c_{0,n}) \end{pmatrix} = \begin{pmatrix} \pi_n^{(2)}(c_{0,n}) & \mathbf{0}_{4,4} & \mathbf{0}_{4,4} & \mathbf{0}_{4,4} \\ \mathbf{0}_{4,4} & \pi_n^{(2)}(c_{0,n}) & \mathbf{0}_{4,4} & \mathbf{0}_{4,4} \\ \mathbf{0}_{4,4} & \mathbf{0}_{4,4} & \pi_n^{(2)}(c_{0,n}) & \mathbf{0}_{4,4} \\ \mathbf{0}_{4,4} & \mathbf{0}_{4,4} & \mathbf{0}_{4,4} & \pi_n^{(2)}(c_{0,n}) \end{pmatrix},$$

$$\pi_n^{(4)}(c_{1,n}) = \begin{pmatrix} \pi_n^{(3)}(c_{1,n}) & \mathbf{0}_{8,8} \\ \mathbf{0}_{8,8} & \pi_n^{(3)}(c_{1,n}) \end{pmatrix} = \begin{pmatrix} \pi_n^{(2)}(c_{1,n}) & \mathbf{0}_{4,4} & \mathbf{0}_{4,4} & \mathbf{0}_{4,4} \\ \mathbf{0}_{4,4} & \pi_n^{(2)}(c_{1,n}) & \mathbf{0}_{4,4} & \mathbf{0}_{4,4} \\ \mathbf{0}_{4,4} & \mathbf{0}_{4,4} & \pi_n^{(2)}(c_{1,n}) & \mathbf{0}_{4,4} \\ \mathbf{0}_{4,4} & \mathbf{0}_{4,4} & \mathbf{0}_{4,4} & \pi_n^{(2)}(c_{1,n}) \end{pmatrix},$$

$$\pi_n^{(4)}(c_{2,n}) = \begin{pmatrix} \pi_n^{(3)}(c_{2,n}) & \mathbf{0}_{8,8} \\ \mathbf{0}_{8,8} & \pi_n^{(3)}(c_{2,n}) \end{pmatrix} = \begin{pmatrix} \mathbf{0}_{4,4} & \pi_n^{(2)}(c_{0,n}) & \mathbf{0}_{4,4} & \mathbf{0}_{4,4} \\ \pi_n^{(2)}(c_{0,n}) & \mathbf{0}_{4,4} & \mathbf{0}_{4,4} & \mathbf{0}_{4,4} \\ \mathbf{0}_{4,4} & \mathbf{0}_{4,4} & \mathbf{0}_{4,4} & \pi_n^{(2)}(c_{0,n}) \\ \mathbf{0}_{4,4} & \mathbf{0}_{4,4} & \pi_n^{(2)}(c_{0,n}) & \mathbf{0}_{4,4} \end{pmatrix},$$

$$\pi_n^{(4)}(c_{3,n}) = \begin{pmatrix} \mathbf{0}_{8,8} & \pi_n^{(3)}(c_{3,n}) \\ \pi_n^{(3)}(c_{3,n}) & \mathbf{0}_{8,8} \end{pmatrix} = \begin{pmatrix} \mathbf{0}_{4,4} & \mathbf{0}_{4,4} & \mathbf{0}_{4,4} & \pi_n^{(2)}(c_{0,n}) \\ \mathbf{0}_{4,4} & \mathbf{0}_{4,4} & \pi_n^{(2)}(c_{0,n}) & \mathbf{0}_{4,4} \\ \mathbf{0}_{4,4} & \pi_n^{(2)}(c_{0,n}) & \mathbf{0}_{4,4} & \mathbf{0}_{4,4} \\ \pi_n^{(2)}(c_{0,n}) & \mathbf{0}_{4,4} & \mathbf{0}_{4,4} & \mathbf{0}_{4,4} \end{pmatrix}.$$

Список литературы

1. Cusick T. W., Stănică P., *Cryptographic Boolean Functions and Applications*, Elsevier, 2009, 232 pp.
2. Погорелов Б.А., Пудовкина М.А., “Орбитальные производные над кольцом вычетов. Часть I. Общие свойства”, *Математические вопросы криптографии*, **5:4** (2014), 99 – 127.
3. Погорелов Б.А., Пудовкина М.А., “Орбитальные производные над кольцом вычетов. Часть II. Вероятностно-комбинаторные свойства”, *Математические вопросы криптографии*, **6:1** (2015), 117–133.

4. Сачков В.Н., *Введение в комбинаторные методы дискретной математики*, М.: МЦ-НМО, 2004.
5. Grossman E., "Group theoretic remark on cryptographic system based on two types of additions", Tech. Rept. 4742, Math. Sci. Dept., 1974.

Статья поступила 26.12.2014.