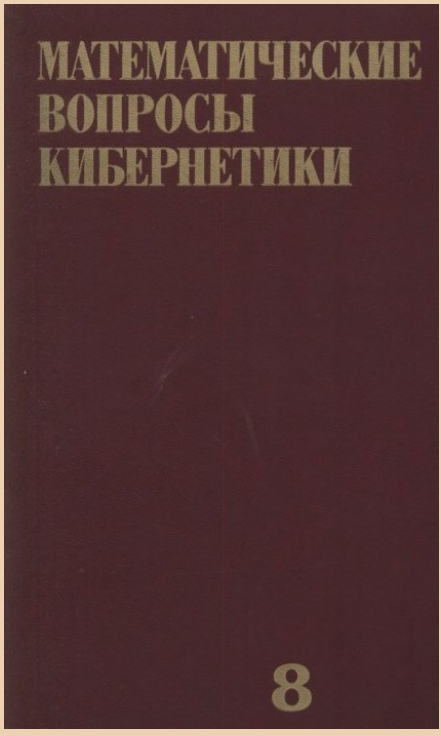
ИПМ им. М.В. Келдыша РАН • Электронная библиотека
Математические вопросы кибернетики • Выпуск 8



**М. М. Глухов,
А. Ю. Зубов**

О длинах симметрических и знакопеременных групп подстановок в различных системах образующих (обзор)

Рекомендуемая форма библиографической ссылки: Глухов М. М., Зубов А. Ю. О длинах симметрических и знакопеременных групп подстановок в различных системах образующих (обзор) // Математические вопросы кибернетики. Вып. 8. — М.: Наука, 1999. — С. 5–32. URL: http://library.keldysh.ru/mvk.asp?id=1999-5

О ДЛИНАХ СИММЕТРИЧЕСКИХ И ЗНАКОПЕРЕМЕННЫХ ГРУПП ПОДСТАНОВОК В РАЗЛИЧНЫХ СИСТЕМАХ ОБРАЗУЮЩИХ (ОБЗОР)

М. М. ГЛУХОВ, А. Ю. ЗУБОВ

(МОСКВА)

Введение

Роль порождающих элементов любой алгебры при ее изучении и при использовании в приложениях хорошо известна и определяется самой природой алгебры как множества с операциями. При конструктивном определении основных операций алгебры перечисление порождающих ее элементов по существу является одним из способов ее задания. Именно на этом пути зачастую удается всю информацию о «большой» и даже бесконечной алгебре записать в небольшом объеме памяти. При этом сложность извлечения нужной информации существенно зависит от системы образующих. Наиболее ценными с этой точки зрения являются такие системы образующих, в которых каждый элемент алгебры однозначно представляется некоторым каноническим словом. Ярким примером тому служат канонические представления натуральных чисел в виде произведения простых чисел (порождающих полугруппу $(\mathbb{N}; \cdot)$).

Наличие хороших представлений элементов алгебры через ее образующие используется при нахождении определяющих соотношений алгебры (см. [39]), облегчает решение различных алгоритмических вопросов (см., например, [42, 57]) и изучение строения самой алгебры. Так, например, Э. Картан и Ж. Дьёдонне (см. [1, 28]) широко использовали образующие симметрии при исследовании симплектических и ортогональных групп; Дж. Диксон, А. А. Марков [43, 84] и другие авторы существенно использовали так называемые нормальные формы слов в канонической системе образующих при изучении групп кос и т. д. С помощью образующих элементов и определяющих соотношений были определены многие интересные классы алгебр, например, свободные группы, группы Коксетера [13] и др.

Системы образующих используются для технической реализации элементов алгебр в теории автоматов, в криптографии и других областях. В связи с этим для групп подстановок полезно знать различные системы образующих и некоторые их характеристики.

В данной работе дается обзор результатов о системах образующих для симметрических и знакопеременных групп подстановок конечных степеней. Наряду с опубликованными результатами авторы обзора сочли целесообразным привести отдельные результаты по этой теме, известные им из различных научных отчетов. В таких случаях ссылки на первоисточники не приводятся, указываются лишь авторы и годы появления результатов.

Работа состоит из двух параграфов. В § 1 по существу перечисляется ряд известных систем образующих для указанных групп, в § 2 приводятся сведения о длинах групп в различных системах образующих. Заметим, что ряд результатов по этим вопросам изложен в обзорной статье Ю. В. Голункова [26]. Эти результаты здесь, как правило, не приводятся, хотя в библиографию соответствующие работы включены [10–12, 14–24].

Авторы отдают себе отчет в том, что приведенные здесь сведения по рассматриваемому вопросу недостаточно полны, и заранее приносят свои извинения всем авторам, результаты которых оказались не отражены.

В обзоре используются следующие обозначения:

$S(\Omega)$ и $A(\Omega)$ — соответственно симметрическая и знакопеременная группы подстановок множества Ω с операцией умножения подстановок; S_n и A_n — указанные группы при $\Omega = \{1, 2, \ldots, n\}$;

$P(\Omega)$ — симметрическая полугруппа преобразований множества Ω с операцией умножения преобразований;

$GF(q)$ — конечное поле из q элементов;

$V_m(q)$ — линейное пространство строк (векторов) длины m над полем $GF(q)$; пространство $V_m(2)$ будем также сокращенно обозначать V_m;

$\langle M\rangle$ и $\langle g_1, \ldots, g_m\rangle$ — группы, порожденные множествами подстановок M и $\{g_1, \ldots, g_m\}$, соответственно;

M^l — множество всех элементов группы $\langle M\rangle$, представимых словами длины l (множество M^l иногда называют *l-м слоем группы G относительно системы образующих M*);

M^{-1} — множество подстановок, обратных к подстановкам из M;

$L(g; M)$ — *длина элемента g относительно системы образующих M*, т. е. минимальная длина слова в алфавите M, представляющего элемент $g \in \langle M\rangle$;

$L(G; M) = \max\limits_{g \in G} L(g; M)$ — *длина группы G относительно системы образующих M*.

§ 1. Образующие элементы групп S_n и A_n

Для решения вопроса о порождении группы S_n или A_n заданным множеством подстановок чаще всего применяют следующие методы.

1. Метод, основанный на алгоритме представления любой подстановки в виде произведения подстановок из заданного множества. Так, например, из хорошо известного алгоритма представления подстановки в виде произведения независимых циклов следует, что множество всех циклов из S_n порождает S_n.

2. Метод сведе́ния к известным системам образующих. Например, каждый цикл из S_n можно представить в виде произведения транспозиций. Следовательно, множество всех транспозиций также является системой образующих группы S_n. Аналогично, произведение любых двух транспозиций представляется в виде произведения циклов длины 3 (3-циклов), поэтому множество всех 3-циклов из группы S_n порождает группу A_n.

3. Метод, который основан на использовании графа Γ_A, определяемого по системе подстановок A из S_n следующим образом: вершинами графа Γ_A являются числа $1, 2, \ldots, n$, ребро (i, j) содержится в Γ_A в том и только том случае, когда в A существует такая подстановка g, что $g(i) = j$. В общем случае граф Γ_A является ориентированным, однако при $A^{-1} = A$ его можно считать неориентированным. В терминах свойств графа Γ_A очевидным образом выражаются такие свойства группы $\langle A\rangle$, как транзитивность, примитивность, наличие транспозиции и др.

4. Методы, использующие различные характеристические свойства групп A_n и S_n или группы G, содержащей A_n. Примеры таких свойств можно найти в книге [125]. Приведем наиболее популярные из них.

Теорема Жордана (1873). Пусть $n = p + k$, где p — простое число, $k \geqslant 3$. Если подгруппа G группы S_n примитивна и содержит цикл длины p, то $G \supseteq A_n$.

Теорема Маркграфа (1892). Пусть G — подгруппа группы S_n, $\Delta \subset \{1, \ldots, n\}$ и $|\Delta| > n/2$. Если группа G примитивна, а ее поточечный стабилизатор G_Δ транзитивен на множестве $\{1, \ldots, n\} \setminus \Delta$, то $G \supseteq A_n$.

Теорема Миллера (1915). Пусть*) $G < S_n$, $n = qp + k$, p — простое число, $p > q > 1$, $k > q$. Если группа G является $(k+1)$-транзитивной, то $G \supseteq A_n$.

Теорема Бохерта. Если $G < S_n$, группа G примитивна и $|G| > n!/((n+1)/2)!$, то $G \supseteq A_n$.

Из работ Жордана (1873, 1875), Маннинга (1909, 1911, 1918, 1919) и Вайса (1928) можно извлечь следующее утверждение.

Пусть $G < S_n$, группа G примитивна, $n = qp + k$, где p — простое число и параметры q, p, k удовлетворяют одному из наборов условий из табл. 1. Тогда если G содержит подстановку порядка p и степени qp, то $G \supseteq A_n$. (Напомним, что степень подстановки — это число ее мобильных элементов.)

Таблица 1

q	1	2	3	4	4	5	6	7	$\geqslant 8$
p	$\geqslant 2$	$\geqslant 5$	$\geqslant 5$	$\geqslant 7$	$\geqslant 5$	$\geqslant 7$	$\geqslant 11$	$\geqslant 11$	$\geqslant 2q-1$
k	> 2	> 2	> 3	> 4	> 5	> 6	> 6	> 8	$> 4q-4$

Из результатов Маннинга и Бохерта вытекают определенные ограничения на минимальную степень k-транзитивных подгрупп из S_n, не содержащих A_n.

Пусть $G < S_n$, группа G является k-транзитивной, m — минимальная степень G (т. е. наименьшая из степеней нетождественных подстановок из G) и параметры k и m удовлетворяют одной из пар условий, указанных в табл. 2. Тогда $G \supseteq A_n$.

Таблица 2

k	$\geqslant 2$	$\geqslant 3$	$\geqslant 4$	$\geqslant 5$	$\geqslant 6$	$\geqslant 8$	$\geqslant 25$
m	$< \frac{n-2\sqrt{n}}{3}$	$< \frac{n-3}{3}$	$< \frac{n-1}{2}$	$< \frac{n}{2}$	$< \frac{3n}{5}$	$< \frac{2n}{3}$	$< \frac{25n}{31}$

Весьма полезными при решении вопроса о совпадении подгруппы G группы S_n со всей группой S_n являются результаты классификации примитивных групп подстановок степени n, содержащих цикл длины 2^m. При $2^m \leqslant n-2$ такая классификация проведена в работах [116, 117]. Оказалось, что при $2^m < n-2$ группа G совпадает с S_n. При $2^m = n-2$ имеются исключения: если $m = 3$, то G может с точностью до изоморфизма совпадать с $PGL(2, 9)$ или с $P\Gamma L(2, 9)$; если $2^m + 1$ — простое число, то G может оказаться изоморфной группе $PGL(2, p)$. В случае $2^m = n-1$ и в наиболее трудном случае $2^m = n$ классификацию указанных групп осуществил Б. А. Погорелов [49], используя достаточно разнообразные и глубокие результаты, полученные в ходе описания кратно-транзитивных групп подстановок и конечных простых групп.

При $2^m = n-1$ здесь, как и выше, исключения получаются лишь для $m = 3$ и для случая, когда $2^m + 1$ — простое число. При $2^m = n$ примитивная подгруппа G группы S_n, содержащая цикл длины 2^m, совпадает

*) Здесь и далее запись $A < B$, где B — группа, обозначает, что A — подгруппа группы B. — *Ред.*

с S_n или может оказаться подстановочно изоморфной естественному подстановочному представлению степени $p+1$ проективной линейной группы $PGL(2, p)$, если $p=2^n-1$ — простое число.

К последнему утверждению примыкает следующий известный авторам обзора результат А. А. Нечаева (1978): если $n=2^m$ и примитивная подгруппа H группы S_n содержит подстановку, разлагающуюся в произведение двух независимых циклов длины 2^{m-2}, то $H \supseteq A_n$.

Следует отметить, что в большинстве работ о системах образующих групп S_n и A_n используется метод сведе́ния к другим системам образующих. В связи с этим исследователю по рассматриваемой тематике полезно иметь достаточно широкий набор систем образующих групп S_n и A_n. Много таких систем приведено в монографии С. Пикар [113], посвященной специально базисам этих групп (под базисом понимается неприводимая система образующих). В частности, в этой работе методом сведе́ния устанавливаются следующие факты.

При любых натуральных m, n и k, удовлетворяющих условиям $n \geqslant 3$, $1 < k < n$, $1 \leqslant m \leqslant n$, группа $\langle (1, 2, \ldots, n), (m, m+1, \ldots, m+k-1)\rangle$ совпадает с A_n, если n и k нечетны, и с S_n в противном случае (здесь и ниже при записи циклов из группы S_n сложение и вычитание производится по модулю n).

При $n \geqslant 4$ и любых a, b, c из $\{1, \ldots, n\}$ группа $\langle (1, 2, \ldots, n), (a, b, c)\rangle$ совпадает с S_n (при четном n) или с A_n (при нечетном n) в том и только том случае, когда выполнено условие НОД$(b-a, c-b, n)=1$.

При $n \geqslant 2$ и $a, b \in \{1, \ldots, n\}$ группа $\langle (1, 2, \ldots, n), (a, b)\rangle$ совпадает с S_n в том и только том случае, когда НОД$(a-b, n)=1$.

В [113] содержатся также общие критерии порождения группы S_n системой транспозиций и группы A_n системой тройных циклов. В обоих случаях необходимым и достаточным условием порождения является условие связности заданной системы циклов. Заметим, что в [37] эти критерии обобщены на произвольную систему циклов простых длин, содержащую хотя бы один цикл длины p, $p \leqslant n-3$, где $n \geqslant 5$.

Наиболее интересным общим результатом монографии [113] является следующее утверждение, называемое теперь теоремой С. Пикар.

При $n \geqslant 3$ ($n \geqslant 4$) для любой подстановки g из S_n (из A_n), отличной при $n=4$ от подстановок группы Клейна

$$K_4 = \{e,\ (1,2)(3,4),\ (1,3)(2,4),\ (1,4)(2,3)\},$$

существует такая подстановка h из S_n (из A_n), что $\langle g, h\rangle = S_n$ ($\langle g, h\rangle = A_n$). Подстановки из группы Клейна не входят ни в один базис группы S_4.

Монография [113] является библиографической редкостью, поэтому последняя теорема С. Пикар опубликована на русском языке в «Кибернетическом сборнике» [47] в 1965 г. В том же году она была передоказана Г. Я. Биндером [5]. Позднее он неоднократно обобщал эту теорему, [6–8].

Для формулировки его результатов введем обозначение Γ_m для следующего свойства любой группы G. Будем писать $G \in \Gamma_m$, если

$$(\forall a_1, \ldots, a_m \in G \setminus \{e\})(\exists b)\ (\langle a_i, b\rangle = G,\ i \in \{1, \ldots, m\}).$$

Теорема С. Пикар утверждает, что $S_n \in \Gamma_1$ при $n \neq 4$. В работе [7] доказано, что $S_n \in \Gamma_2$ при $n > 4$. В [8] установлено, что $S_n \notin \Gamma_4$, если n нечетно и $n > 4$. Если n четно и $n > 4$, то $S_n \notin \Gamma_3$.

Аналогичные исследования проводили Дж. Бреннер и Дж. Вигольд [71, 72]. В работе [71] они независимо от Г. Я. Биндера доказали, что $A_n \in \Gamma_4 \setminus \Gamma_5$ для четных n, $n \geqslant 8$. В [72] они рассмотрели случай нечетного n. Здесь ситуация более сложная. Так, например, $A_{19} \in \Gamma_t$ при некотором t, $t > 6 \cdot 10^9$. Дж. Бреннер и Дж. Вигольд доказали, что $A_n \in \Gamma_3$

при любом нечетном n, $n \geqslant 11$, и $A_n \notin \Gamma_t$ при $t = C_{n-1}^{d-1}$ для нечетного составного n с наименьшим простым делителем d. Особое внимание уделено группам A_p, S_p для «хороших» простых p (простое p они называют хорошим, если A_p и S_p — единственные неразрешимые транзитивные группы подстановок степени p). В этом случае значение параметра m найдено с точностью до слагаемого s, $s \leqslant 3$.

В [8] рассмотрен вопрос о дополнении любого элемента a из $S_n \setminus \{e\}$ до базиса $\{a, b\}$ группы S_n элементом b из некоторого фиксированного подмножества R группы S_n. В частности, этот вопрос положительно решен для класса R всех элементов, сопряженных при нечетном n, $n > 4$, с подстановкой $(a_1, \ldots, a_m)(a_{m+1}, \ldots, a_n)$, где $1 < m < n$, НОД$(m, n) = 1$, и с подстановкой $(a_1, \ldots, a_n)$ при четном n, $n > 6$.

Заметим, что в работах Г. Я. Биндера имеются вспомогательные результаты, позволяющие строить новые серии систем образующих для групп S_n или A_n. Приведем в качестве примера один результат из [8]: транзитивная группа подстановок степени n, содержащая подстановку, равную произведению двух независимых циклов длин k и $n-k$, совпадает с A_n или S_n, если $1 < k < n$ и НОД$(k, n-k) = 1$.

Теорема С. Пикар и ее обобщения свидетельствуют о том, что группа S_n имеет большое число 2-элементных базисов. Этот факт еще более усиливается следующим асимптотическим результатом Дж. Диксона 1969 г. [83]: при случайном выборе двух подстановок из S_n вероятность получить базис стремится к 3/4 при $n \to \infty$. Таким образом, при достаточно больших n вероятность получить базис при случайном выборе двух подстановок близка к вероятности выбора хотя бы одной из двух подстановок не из A_n. При доказательстве этого факта использовалась приведенная выше теорема Жордана, и главная трудность состояла в нахождении оценок вероятностей примитивности группы $\langle a, b\rangle$ и наличия в ней цикла нужной длины.

На этом же пути В. Н. Сачков в 1971 г. оценил вероятность $p_n(m)$ порождения группы A_n или S_n системой из m случайно выбранных подстановок, $m \geqslant 2$. Им доказано асимптотическое равенство $p_n(m) = 1 - O(1/(\ln \ln n)^m)$ при $n \to \infty$ и фиксированном m.

Позднее (1980) Дж. Бовей [63], оценивая минимальную степень группы, порожденной случайной подстановкой, улучшает оценку вероятности $p_n(2)$. Он доказывает, что для любого фиксированного положительного ε при достаточно больших n выполнено неравенство $p_n(2) > 1 - n^{-1+\varepsilon}$.

Рядом авторов (см. [4, 78, 91]) исследовалась система образующих D_n группы S_n,

$$D_n = \{d_0 = (0, 1),\ d_1 = (0, 1, 2),\ \ldots,\ d_{n-2} = (0, 1, \ldots, n-1)\}.$$

По-видимому, первые результаты по получению кратчайших представлений подстановок в данной системе образующих получил В. П. Зязин (1971), который, кроме того, обратил внимание на ее оптимальность (см. § 2).

В [90] показано, что каждая подстановка однозначно представима несократимым словом $d_{i_1} d_{i_2} \ldots d_{i_m}$, в котором $i_1 \leqslant i_2 \leqslant \ldots \leqslant i_m$. В [90] также найдены определяющие соотношения для системы $D_n \cup \{e\}$.

Алгоритм нахождения кратчайшего представления для элемента g группы S_n приведен также в [4]. Он состоит в следующем:

1) находится число k, $k = \max\{x: x < n-1,\ g^{-1}(x) > g^{-1}(x+1)\}$;

2) для каждого x, $0 \leqslant x \leqslant k$, вычисляется величина $m_x = k - x + g^{-1}(x) - |R_x|$, где $R_x = \{y: x < y \leqslant k,\ g^{-1}(y) < g^{-1}(x)\}$;

3) вычисляется кратчайшее представление $g = g_{m_k} g_{m_{k-1}} \ldots g_{m_0}$.

Из теоремы Галуа о простоте знакопеременной группы A_n следует, что при $n \geqslant 5$ для любого класса C сопряженных элементов в S_n выполняет-

ся равенство $\langle C\rangle = A_n$, если C состоит из четных подстановок, и $\langle C\rangle = S_n$ в противном случае. В связи с этим имеется много работ, в которых рассматриваются различные вопросы, связанные с порождением группы S_n или A_n подстановками из одного класса сопряженных элементов.

Сравнительно просто такие вопросы решаются для транспозиций. Классическими примерами систем образующих-транспозиций являются:

T — все транспозиции;

T_1 — все транспозиции вида $(1, i)$, $i \in \{2, \ldots, n\}$;

T_2 — все транспозиции вида $(i, i+1)$, $i \in \{1, \ldots, n-1\}$.

При решении вопроса о порождении группы S_n произвольным множеством транспозиций A часто используется теоретико-графовый подход. При этом граф Γ_A можно считать неориентированным. Если $\langle A\rangle = S_n$, то в силу транзитивности группы S_n граф Γ_A должен быть связным. Методом математической индукции нетрудно доказать, что верно и обратное утверждение (см., например, [45]).

О. Оре в [45] доказывает, что множество транспозиций A является базисом группы S_n в том и только том случае, когда граф Γ_A является деревом. Отсюда видно, что любой базис из транспозиций содержит ровно $n-1$ подстановок. В работе [80] найдено число различных базисов из транспозиций; оно равно n^{n-2}.

Продолжая исследования О. Оре, У. Фрухт [90] находит рекуррентную формулу для числа $F_{m,n}$ систем из m транспозиций, порождающих группу S_n.

Несколько сложнее сходные вопросы решаются для систем образующих из тройных циклов и, тем более, циклов произвольной длины. Вместе с тем, для тройных циклов критерий полноты формулируется точно так же, как и для транспозиций (см., например, [104]). В [104] приводится и минимальная по мощности система тройных циклов, порождающая группу S_n:

$$\langle (1,2,3),\ (1,4,5),\ \ldots,\ (1,2m-2,2m-1),\ (1,2,r)\rangle,$$

где $r = n$ при $n = 2m+1$, или r — любое из чисел $1, \ldots, 2m-1$ при $n = 2m$.

Вопросам порождения групп S_n и A_n циклами длины k посвящена работа В. И. Сущанского и Р. А. Восканяна [52], где также используются графы. В этой работе находятся минимальный и максимальный порядки неприводимых систем образующих группы S_n или A_n из циклов длины k. Для минимального числа $\gamma(k, n)$ циклов длины k, $k \geqslant 5$, порождающих S_n или A_n, имеет место соотношение

$$\gamma(k,n) = \begin{cases} 2, & k > \frac{n}{2}; \\ 3, & k = \frac{n}{2}; \\ \frac{n-1}{k-1}, & k < \frac{n}{2},\ k-1 \text{ делит } n-1; \\ \left\lfloor \frac{n-1}{k-1} \right\rfloor + 1, & k < \frac{n}{2},\ k-1 \text{ не делит } n-1. \end{cases}$$

При этом системы образующих, состоящие из $\gamma(k, n)$ элементов, характеризуются тем, что в соответствующих графах нет ребер, принадлежащих двум различным простым циклам графа.

В то же время максимальная по мощности неприводимая система содержит $n-k+1$ циклов, и для любого числа l, удовлетворяющего условию $\gamma(k, n) \leqslant l \leqslant n-k+1$, существует неприводимая система k-циклов, порождающая S_n или A_n и состоящая из l элементов k-циклов. В терминах графа Γ_A приводится достаточное условие неприводимости системы образующих. Заметим, что значение величины $\gamma(k, n)$ при любых возможных k, n ранее было найдено в [92].

В [76] при $n > 167$ конструируется система образующих x, y, t группы S_n, удовлетворяющая условиям:

$$x^2 = y^2 = (xy)^7 = t^2 = (xt)^2 = (yt)^2 = 1.$$

В ряде работ, посвященных вопросу о порождении групп S_n и A_n подстановками из одного класса сопряженных элементов или из объединения классов, главное внимание обращается нахождению длины группы в рассматриваемых системах образующих. Поэтому обзор результатов этих работ будет сделан в следующем параграфе. Здесь же мы отметим лишь, что в одной из последних работ этой серии [58] показано, что почти в любом из классов сопряженных элементов группы A_n содержится пара подстановок, порождающих A_n. Точнее, отношение числа классов, содержащих такую пару элементов, к числу всех классов стремится к 1 при $n \to \infty$.

Еще один класс систем образующих групп S_n и A_n, состоящий из циклов (вообще говоря, разной длины), каждый из которых содержит фиксированный символ, рассматривается в работах [102, 126]. Упомянутые системы образующих связаны с так называемыми «играми на графах», обобщающими известную «игру в 15» С. Ллойда.

Более специфические системы образующих групп S_n и A_n используются в прикладных областях — в криптографии, в теории автоматов и т. п. Здесь существенное влияние на выбор систем образующих оказывают требования, связанные с технической реализацией. Именно в силу этих требований здесь в качестве множества Ω, на котором действуют подстановки, чаще всего берется пространство V_m векторов-строк длины m над полем $GF(2)$ с операцией покомпонентного сложения в этом поле. Отождествляя группу $(V_m; \oplus)$ с аддитивной группой некоторого поля $GF(2^m)$, можно ввести на V_m операцию умножения как умножение в поле $GF(2^m)$. Кроме того, вектор $(x_1, \ldots, x_m)$ из V_m зачастую отождествляют с числом $x_1 2^{m-1} + \ldots + x_{m-1} 2 + x_m$; тогда появляется возможность ввести на V_m операции сложения и умножения по модулю 2^m. Все эти операции, а также логические операции на множестве $\{0, 1\}$, широко используются при построении систем образующих групп $S(V_m)$ и $A(V_m)$. При этом сами подстановки множества V_m записывают в координатной форме:

$$g\colon (x_1, x_2, \ldots, x_m) \to (f_1(x_1, \ldots, x_m),\ f_2(x_1, \ldots, x_m),\ \ldots,\ f_m(x_1, \ldots, x_m)),$$

где $f_1, f_2, \ldots, f_m$ — система булевых функций, называемая системой координатных функций преобразования g.

Приведем примеры. Так, в работе [77], нацеленной на приложения в криптографии, в качестве образующих элементов рассматриваются отображения $\sigma\colon V_m \to V_m$ вида $\sigma(a_1, \ldots a_m) = (b_1, \ldots, b_m)$, где

$$b_i = \begin{cases} a_i, & i \neq j, \\ a_i \oplus f(a_{i_1}, \ldots, a_{i_k}), & i = j, \end{cases} \qquad i_1, \ldots, i_k, j \in \{1, \ldots, m\}. \qquad (1)$$

Используя сведéние к состоящей из тройных циклов системе образующих группы A_m, автор доказывает, что при фиксированном k и всевозможных булевых функциях $f(x_1, \ldots, x_k)$ указанная система образующих порождает группу $S(V_m)$ при $m > 1$, $k = m - 1$ и группу $A(V_m)$ при $m \geqslant 4$, $k \in \{2, \ldots, m-2\}$.

В работе [25] Ю. В. Голунков рассматривает вопрос о порождении симметрической полугруппы $P(V_m)$ и группы $S(V_m)$ преобразованиями вида (1) при ограничениях на используемые функции f. В частности, рассмотрена задача порождения $P(V_m)$ с использованием лишь функций f_1, f_2, f_3 и $f_3 \oplus 1$,

но с возможностью любых замен переменных на переменные из множества $\{x_1, \ldots, x_n\}$. Сформулирован критерий порождения $P(V_m)$, заключающийся в том, что

$$f_1 = x_1^{\alpha_1} \ldots x_{k-1}^{\alpha_{k-1}} x_k x_{k+1}^{\alpha_{k+1}} \ldots x_m^{\alpha_m} \oplus \varphi(x_1, \ldots, x_{k-1}, x_{k+1}, \ldots, x_m),$$
$$f_2 = x_1 \oplus x_2 \oplus \ldots \oplus x_m \oplus \alpha,$$
$$f_3 = x_i \oplus \psi(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_m),$$

где $\alpha, \alpha_1, \ldots, \alpha_m \in \{0, 1\}$, φ — любая булева функция, а ψ — булева функция нечетного веса $\|\psi\|$.

Приводится конкретный пример такой системы функций:

$$f_1 = x_1 \vee \bar{x}_2 \bar{x}_3 \ldots \bar{x}_m, \quad f_2 = x_1 \oplus \ldots \oplus x_m, \quad f_3 = x_1 \oplus \bar{x}_2 \bar{x}_3 \ldots \bar{x}_m.$$

Заметим, что преобразования, использующие функцию f_1, не биективны. Поэтому, исключив из системы $f_1, f_2, f_3, \bar{f}_3$ функцию f_1, получим критерий порождения группы $S(V_m)$.

В работе Ю. В. Голункова [23] рассматривается вопрос о порождении полугруппы $P(V_m)$ и группы $S(V_m)$ так называемыми регистрами сдвига, т. е. преобразованиями вида

$$\rho_f\colon (x_1, x_2, \ldots, x_m) \to (x_2, \ldots, x_m, f(x_1, \ldots, x_m)),$$

где f — любая булева функция. Нетрудно видеть, что ρ_f — подстановка в том и только том случае, когда функция f зависит от x_1 линейно; такие регистры сдвига называют регулярными.

В [23] доказывается, что необходимым условием совпадения группы $S(V_m)$ с группой $\langle \rho_f, \rho_f \rangle$ является нечетность веса функции $x_1 \oplus f(x_1, \ldots, x_m)$ как функции от переменных $x_2, \ldots, x_m$. Высказывается гипотеза о том, что это условие является и достаточным. Гипотеза проверена для $m \leqslant 5$ и для функции $f = x_1 \oplus x_2 x_3 \ldots x_m$ при любом m.

В начале 80-х годов в связи с анализом стандарта шифрования США (DES, см. [53]) многие специалисты рассматривали группы подстановок множества $V_n \times V_n$, порожденные подстановками вида g_F: $(a, b) \to (b, F(a, b))$ при различных отображениях F: $V_n \times V_n \to V_n$. Такие подстановки g_F обобщают так называемые раундовые функции DES-алгоритма.

С. Ивен и О. Голдридж [88] доказали в 1983 г., что множество

$$A = \{g_F\colon F(a, b) = a \oplus \varphi(b), \ \varphi \in P(V_n)\}$$

порождает знакопеременную группу $A(V_n \times V_n)$. В работе Р. Вернсдорфа [124] изучается возможность порождения знакопеременной группы подстановками, реализуемыми конкретными раундовыми функциями DES-алгоритма. Показано, что все 2^{48} таких подстановок порождают группу $A(V_{64})$. Основная идея состоит в доказательстве 3-транзитивности рассматриваемой группы, после чего используется один результат Камерона, основанный на классификации конечных простых групп.

Теоретико-групповые свойства преобразований, реализуемых полной схемой DES, исследовались в работах [73, 100, 114].

Изучались группы подстановок, связанные и с другими блочными шифрами. Так, в работе Р. Диттмара, Г. Хёрнауэра, и Р. Вернсдорфа [82] доказано, что раундовые функции шифра SAFER порождают знакопеременную группу, а также представлено новое доказательство аналогичного утверждения для DES. Кроме того, показано, что если раундовые функции шифра

FEAL порождают примитивную группу, то она совпадает со знакопеременной группой.

Несколько классов систем образующих групп подстановок, связанных с реализацией криптографических преобразований блочных шифров, изучен Т. Цишангом в [128]. В этой работе рассматриваются преобразования пространства V_m:

$$\text{ADD\_c}, \quad \text{XOR\_c}, \quad \text{SHIFT\_}k, \quad \text{MUL\_c}, \quad \text{MULT\_c},$$

определяемые для любого вектора $\mathbf{x}$ из V_m следующим образом ($\mathbf{c}$ — фиксированный вектор из V_m, k — фиксированное число):

1) $\text{ADD\_c}(\mathbf{x}) = \mathbf{x} + \mathbf{c} \pmod{2^m}$;

2) $\text{XOR\_c}(\mathbf{x}) = \mathbf{x} \oplus \mathbf{c}$, где $\oplus$ — покоординатное сложение по модулю 2;

3) $\text{MUL\_c}(\mathbf{x}) = \mathbf{x} \cdot \mathbf{c} \pmod{2^m}$;

4) $\text{MULT\_c}(\mathbf{x}) = \mathbf{x} \cdot \mathbf{c} \pmod{2^m+1}$, здесь $\text{НОД}(\mathbf{c}, 2^m+1) = 1$;

5) $\text{SHIFT\_}k(x_1, \ldots, x_m) = (x_{k+1}, \ldots, x_m, x_1, \ldots, x_k)$.

В 1), 3) и 4) вектор $\mathbf{y} = (y_1, \ldots, y_m)$ из V_m отождествляется с числом $y_m + 2y_{m-1} + \ldots + 2^{m-1}y_1$, а „+“ и „·“ — операции сложения и умножения, производимые над числами.

Обращается внимание на то, что $\text{MUL\_c} \in A(V_m) \iff \mathbf{c} \equiv 1 \pmod 4$ и $\text{MULT\_c} \in A(V_m) \iff$ ($\mathbf{c}$ — квадратичный вычет по модулю 2^m+1).

Получены следующие результаты.

1. Группа $G = \langle \{\text{SHIFT\_}k, \text{XOR\_c}: 0 \leqslant k < m, \mathbf{c} \in V_m\} \rangle$ изоморфна полупрямому произведению $N \times U$ элементарной абелевой 2-группы N порядка 2^m и циклической группы U порядка m;

имеет место соотношение $|G| = m2^m$;

группа G может быть порождена $m+1$ элементами;

если $m = 2^k$, то G — неабелева 2-группа порядка 2^{k+m};

длина группы G равна 2.

2. Группа $G = \langle \{\text{ADD\_c}, \text{SHIFT\_}d: 0 \leqslant \mathbf{c} < 2^m, 0 \leqslant d < m\} \rangle$ изоморфна S_{2^m}.

3. Для нечетного $\mathbf{c}$ группа $G = \langle \{\text{MUL\_c}, \text{SHIFT\_}d: 0 < \mathbf{c} < 2^m, 0 \leqslant d < m\} \rangle$ изоморфна S_{2^m-1}. Здесь G рассматривается как группа подстановок на всех ненулевых векторах из V_m.

4. Рассматриваются также некоторые «смеси» преобразований 1)–5). Например, приведен алгоритм MIX-2. По сути, это — криптографический алгоритм, реализующий блочное шифрование. Здесь $\mathbf{M}$ — исходный вектор из V_m, а $b_1, \ldots, b_r$ — первые r бит ключа $\mathbf{K}$, который является k-битовым вектором $(b_1, \ldots, b_r, b_{r+1}, \ldots, b_k)$; указывается, что обычно k — степень двойки. Параметр r — это число итераций, в каждой из которых применяется либо ADD_b, либо SHIFT_a. Предлагается выбрать $r = k - (m + \log_2 m - 2)$. Доказывается, что группа G, порожденная преобразованиями MIX-2, реализуемыми при всевозможных ключах $\mathbf{K}$, изоморфна S_{2^m}.

```
FOR (i=0; i<r; ++i)
  IF b_i
    ADD_b(M);
  ELSE
    SHIFT_a(M);
```

Алгоритм MIX-2

В заключении работы сказано, что комбинации базисных операций порождают разные группы подстановок: полупрямые произведения, аффинные линейные группы, сплетения, симметрические и знакопеременные группы.

Из приведенных выше классических теорем и других результатов видно, что при решении вопросов о порождении группы S_n или A_n заданным множеством подстановок M важную роль играет условие примитивности группы $\langle M \rangle$. Это условие проверяется особенно просто, если подстановки действуют на V_m и множество M содержит подстановку g: $x \to x + 1 \pmod{2^m}$. В этом случае любая полная система блоков (областей импримитивности) группы $\langle M \rangle$ должна быть полной системой блоков группы

$G = \langle g \rangle$, т. е. системой смежных классов группы $(V_m, +)$ по некоторой ее подгруппе. Отсюда следует, что группа $\langle M \rangle$ импримитивна в том и только том случае, когда в координатном задании любого преобразования из M последние k функций не зависят существенно от первых $m-k$ переменных $x_1, \ldots, x_{m-k}$ при некотором $k \geqslant 1$. Отрицание последнего условия и дает критерий примитивности группы $\langle M \rangle$.

Аналогичный критерий имеет место и для преобразований пространства $V_m(p)$ над полем $GF(p)$ при любом простом p.

Заметим, что указанные условия примитивности группы $\langle M \rangle$ при $g \in M$ ранее (1977) в терминах графов были сформулированы А. А. Нечаевым. Интересно отметить, что они совпали с условиями полноты системы координатных функций преобразований из M, см. [44].

Определенная связь между условием примитивности подгрупп группы S_n и условием полноты систем функций n-значной логики проявлялась также в работах Р. А. Байрамова [2, 3].

Пользуясь указанным критерием примитивности и приведенными выше результатами Б. А. Погорелова и А. А. Нечаева о группах, содержащих 2^m-цикл или произведение двух 2^{m-2}-циклов, М. М. Глухов доказал (1978) совпадение группы $\langle g, h \rangle$ с группой $S(V_m)$ для достаточно широкого класса подстановок h. Оказалось, что равенство $\langle g, h \rangle = S(V_m)$ выполняется, если выбрать в качестве h:

а) любой регулярный регистр сдвига ρ_f;

б) любое функциональное преобразование h: $x \to xA \oplus \alpha$ пространства V_m, где невырожденная матрица A ни при каком k, $1 \leqslant k < m$, не имеет нулевой правой верхней $(k \times (m-k))$-подматрицы;

в) любое преобразование вида h: $x \to x \oplus \alpha_{f(x)}$, где

$$\alpha_0, \alpha_1 \in V_m, \qquad \alpha_0 \oplus \alpha_1 = (a_1, \ldots, a_{m-1}, 1), \qquad a_1, \ldots, a_{m-1} \in GF(2),$$

и функция $f(x) = f(x_1, \ldots, x_m)$ существенно зависит от x_1 (см. [16]).

В работах [21, 22] приводятся системы образующих полугруппы $P(V_m)$ и группы $S(V_m)$, реализуемые на так называемых однородных ленточных структурах (см. также [10, 11]). Построением систем образующих группы $S(GF(q))$ с использованием аффинных преобразований поля $GF(q)$ занимался Л. Карлиц [74].

В приложениях зачастую системы образующих группы S_n (да и других групп) используются для перечисления всех элементов группы (без повторений). В связи с этим возникает задача построения таких систем образующих конечной группы G, при которых все элементы группы можно расположить в ряд длины $|G|$ так, чтобы каждый элемент ряда получался умножением предыдущего на некоторый образующий элемент [113]. В [45] этот вопрос сформулирован на языке графа Кэли группы $G = \langle M \rangle$.

Напомним (см. [45, 57]), что графом Кэли группы $G = \langle M \rangle$ называется ориентированный граф $\Gamma(G; M)$ с $|G|$ вершинами, индексированными элементами группы G, в котором вершины g_i и g_j соединены ребром, направленным от g_i к g_j, в том и только том случае, когда $g_j = g_i m_s$ для некоторого m_s из M. Указанное ребро обычно помечается знаком m_s. Из этого определения легко усмотреть, что возможность указанного выше расположения элементов группы G равносильна наличию в графе $\Gamma(G; M)$ гамильтоновых путей.

В [115] указаны алгоритмы построения гамильтоновых путей для группы S_n, заданной системами образующих M_1 и M_2, $|M_1| = n-1$, $|M_2| = 3$:

$M_1 = \{(1,2), (1,2)(3,4), (1,2)(3,4)(5,6), \ldots, (2,3), (2,3)(4,5), (2,3)(4,5)(6,7), \ldots\}$,
$M_2 = \{(1,2), (1,2)(3,4)(5,6)\ldots, (2,3)(4,5)(6,7)\ldots\}$.

В [99] аналогичная задача решена для группы S_n с системой образующих T_2. В работе [33] доказано существование и указан алгоритм построения гамильтоновой последовательности в графе $\Gamma(G; M)$ для любого базиса из транспозиций M. При этом существенно использовался критерий О. Оре о представлении базиса из транспозиций деревом.

В заключение § 1 сделаем одно замечание о числе образующих элементов группы подстановок: если группу S_n или A_n можно породить двумя образующими, то для произвольной группы подстановок вопрос о минимальном числе образующих не очевиден.

В работах [29, 96] показано, что любую подгруппу G группы S_n можно породить системой с не более, чем $n-1$ элементами. Предлагаются несложные алгоритмы построения таких систем образующих.

§ 2. Представления элементов групп S_n и A_n через образующие. Длина группы в заданной системе образующих

Представлениями элементов группы через образующие занимались многие математики по разным причинам. В частности, на представлении элементов группы основан один из методов доказательства порождения группы заданным множеством ее элементов. На этом же основан и один из методов получения оценок длины группы и мощностей ее слоев в заданной системе образующих. Наличие канонических представлений помогает находить определяющие соотношения группы и решать многие другие задачи.

В общем случае, когда группа подстановок G задана произвольной системой образующих, существуют различные алгоритмы перечисления всех элементов группы как произведений образующих. Одним из самых простых является алгоритм, предложенный Ч. Симсом [51, 118], который использует переход от образующих группы к образующим ее стабилизаторов (см. ниже о сильных системах образующих). Однако и этот алгоритм, и его модификации (см., например, [97, 101]) в общем случае являются достаточно сложными. Ясно, что не проще будет и задача нахождения кратчайших представлений подстановок через образующие. В связи с этим возникает вопрос о сложностной характеристике указанной проблемы, а также проблем нахождения длин элементов группы подстановок и длины самой группы. Последние были рассмотрены в работе [87] С. Ивена и О. Голдрича (см. также [98]). Приведем формулировки проблем.

1. Проблема минимальной длины последовательности образующих (MGS-problem). Исходные данные: система подстановок $A = \{g_1, \ldots, g_r\}$, подстановка g, принадлежащая группе $G = \langle g_1, \ldots, g_r \rangle$, и натуральное число k. Требуется выяснить, существует ли слово длины k в алфавите A, представляющее элемент g.

2. Проблема минимальной верхней грани последовательности образующих (MBGS-problem). Исходные данные: система подстановок $A = \{g_1, \ldots, g_r\}$ и натуральное число k. Требуется выяснить, все ли элементы группы $G = \langle g_1, \ldots, g_r \rangle$ представляются в алфавите A словами длины менее k.

Ясно, что эти проблемы равносильны соответственно проблемам нахождения длин элементов и длины группы. В [87] доказано, что обе эти проблемы NP-трудны, причем MGS-проблема NP-полна.

Вместе с тем, существуют такие системы образующих групп подстановок (в частности, групп S_n и A_n), для которых соответствующие проблемы решаются легко. Ниже в основном о таких системах образующих групп S_n и A_n и будет идти речь.

Классическим примером представления подстановок является их разложение в произведение независимых циклов. Роль такого представления в теории групп подстановок хорошо известна. Оно очевидным образом дает и точное значение длины группы S_n в системе всех (неединичных) циклов — оно равно $\lfloor n/2 \rfloor$ и достигается на подстановках $h_1 = (1,2)(3,4)\ldots(n-1,n)$ при четном n и $h_2 = (1)(2,3)\ldots(n-1,n)$ при нечетном n.

Ниже мы не указываем в таких разложениях единичные циклы, подразумевая их с учетом того, что подстановки действуют на множестве $\{1,\ldots,n\}$.

Пользуясь разложением подстановок в произведение независимых циклов, можно получать их представления в системе T всех транспозиций, заменяя каждый цикл по формуле

$$(a_1, a_2, \ldots, a_k) = (a_1, a_2)(a_1, a_3)\ldots(a_1, a_k).$$

В системе T_1 всех транспозиций вида $(1, i)$, $i \in \{2,\ldots,n\}$, при $a_1 = 1$ можно воспользоваться этим же разложением, а при $1 \notin \{a_1,\ldots,a_k\}$ — произведением

$$(1, a_1)(1, a_2)\ldots(1, a_k)(1, a_1).$$

Указанные представления приводят к оценкам длин и подстановок, и группы S_n в этих системах образующих. В частности,

$$L(S_n; T) \leqslant n-1, \qquad L(S_n; T_1) \leqslant \lfloor 3(n-1)/2 \rfloor.$$

С другой стороны, нетрудно видеть, что эти оценки достигаются: первая — на подстановке $h = (1, 2, \ldots, n)$, вторая — на указанных выше подстановках h_1 и h_2. Доказательство достижимости первой оценки можно найти, например, в работах [80, 98]; в каждой из них доказано, что $L(g; T) = n-k$, где k — число всех циклов подстановки g (вместе с циклами длины 1). В [80] найдены рекуррентные формулы для числа представлений любой подстановки g в виде произведения минимального числа транспозиций. В частности, если g есть t-цикл, то это число равно t^{t-2}.

А. А. Марков в работе [43] получает, факторизуя группу кос, канонические представления элементов группы S_n через систему транспозиций $T_2 = \{(i, i+1)\colon i \in \{1,\ldots,n-1\}\}$. Для любого элемента группы S_n такое представление имеет вид

$$a_{k_1} a_{k_1-1} \ldots a_{k_1-s_1} a_{k_2} a_{k_2-1} \ldots a_{k_2-s_2} \ \ldots \ a_{k_t} a_{k_t-1} \ldots a_{k_t-s_t}, \tag{2}$$

где $1 \leqslant k_1 < k_2 < \ldots < k_t \leqslant n$, $0 \leqslant s_i < k_i$, $i \in \{1,\ldots,t\}$. Сам же алгоритм приведения к такому виду основан на использовании определяющих соотношений

$$\begin{aligned} &a_i^2 = e, && i \in \{1,\ldots,n-1\},\\ &a_i a_{i+1} a_i = a_{i+1} a_i a_{i+1}, && i \in \{1,\ldots,n-2\},\\ &a_i a_j = a_j a_i, && i, j \in \{1,\ldots,n-1\}, \quad |i-j| \geqslant 2. \end{aligned}$$

Из описания алгоритма видно, что любое произведение элементов множества T_2 приводится к виду (2) без увеличения числа сомножителей. Отсюда следует, что канонические слова являются кратчайшими и что значение $L(S_n; T_2)$ равно максимальной длине слова вида (2), т. е. $L(S_n; T_2) = n(n-1)/2$.

Известно, что длина подстановки $g = \begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix}$ в системе образующих T_2 равна числу инверсий в перестановке $(i_1,\ldots,i_n)$. Этот факт можно

найти, например, в работе [98]. Кстати, там же указан простой алгоритм вычисления длины произвольного элемента группы S_n в системе образующих T_2', полученной из T_2 добавлением транспозиции $(1, n)$.

В [120] рассмотрен вопрос о числе различных представлений любого элемента группы S_n через систему T_2. Пользуясь связью этих представлений с симметрическими функциями, автор находит число различных представлений элемента с максимальной длиной $n(n-1)/2$ в виде редуцированных произведений. Оно равно $\binom{n}{2}! \, 1^{n-1}3^{n-2}\ldots(2n-3)^1$. Указывается, что это число можно найти и для других элементов группы S_n.

М. М. Глухов (1965) указал рекуррентную формулу для числа $a_{n,k}$ элементов длины k группы S_n в системе образующих T_2:

$$a_{n+1,k} = a_{n,k} + a_{n,k-1} + \ldots + a_{n,k-n}, \tag{3}$$

где $a_{1,0} = 1$ и $a_{n,k-i} = 0$ при $i > k$. Г. И. Ивченко и В. Н. Сачков рассмотрели на группе S_n случайную величину ξ_n, равную длине случайно выбранного элемента. Пользуясь формулой (3), они доказали асимптотическую нормальность величины ξ_n при $n \to \infty$ и вычислили параметры

$$\mu_n = \mathsf{E}\xi_n = \frac{n(n-1)}{4}, \qquad \sigma_n = \mathsf{D}\xi_n = \frac{n(n-1)(2n-5)}{72}.$$

В. Н. Сачков также нашел все кумулянты величины ξ_n.

Прежде чем перейти к другим системам образующих, полезно обратить внимание на сравнение длин группы S_n в системах образующих T_1 и T_2. Обе эти системы являются неприводимыми и состоят из одного и того же числа элементов: $|T_1| = |T_2| = n-1$, но порождают группу S_n на различных по порядку длинах: $\lfloor 3(n-1)/2 \rfloor$ и $n(n-1)/2$.

В общем случае для параметра $L(G; M)$ нетрудно получить тривиальную нижнюю оценку:

$$L(G; M) \geqslant \lceil \log_{|M|} |G| \rceil. \tag{4}$$

При $G = S_n$ или $G = A_n$ систему образующих обычно рассматривают для произвольного (а не какого-то фиксированного) n. Иначе говоря, рассматривается последовательность систем образующих $M_1, M_2, \ldots$ В таком случае можно говорить об асимптотическом поведении величины $L(S_n; M_n)$. Из (4) следует, что имеет место неравенство $L(S_n; M_n) \geqslant \frac{\log_2 n!}{\log_2 |M_n|}$, или, как это следует из формулы Стирлинга,

$$L(S_n; M_n) \gtrsim \frac{n \log_2 n}{\log_2 |M_n|}, \qquad n \to \infty.$$

В случае $L(S_n; M_n) \sim \frac{cn \log_2 n}{\log_2 |M_n|}$, где c — константа, систему образующих M_n будем называть оптимальной по порядку (и просто оптимальной при $c = 1$).

Сравнивая системы T_1 и T_2, можно сказать, что первая оптимальна по порядку (с константой $c = 3/2$), а вторая — нет.

Вернемся к вопросу о других представлениях подстановок из S_n и A_n.

Из разложений подстановок в произведения независимых циклов нетрудно получить также разложения четных подстановок в произведение 3-циклов (т. е. циклов длины 3). Для этого достаточно воспользоваться равенствами

$$(a_1, \ldots, a_k) = \begin{cases} (a_1, \ldots, a_{k-1})(a_1, a_k), & k \text{ четное}, \\ (a_1, a_2, a_3)(a_1, a_4, a_5)\ldots(a_1, a_{k-1}, a_k), & k \text{ нечетное} \end{cases}$$

и заметить, что при различных a, b, c, d имеет место соотношение $(a, b)(c, d) = (a, c, b)(b, d, c)$.

Отсюда получается оценка $L(A_n; B_3) \leqslant \lfloor n/2 \rfloor$, где B_3 — множество всех 3-циклов. Эта оценка, кстати, также достигается на указанных выше подстановках h_1 и h_2 при четном $n/2$ (соответственно, при четном $(n-1)/2$). В других случаях она достигается на подстановках

$$(1, 2, 3)(4, 5)\dots(n-1, n), \qquad (1, 2, 3, 4)(5, 6)\dots(n-1, n).$$

Таким образом, $L(A_n; B_3) = \lfloor n/2 \rfloor$, см. [69]. Отсюда видно, что система B_3 является оптимальной по порядку с константой $3/2$.

Группа A_n порождается и собственным подмножеством из B_3, а именно, 3-циклами вида $(1, 2, i)$, $i \in \{3, \dots, n\}$. Однако здесь вопрос о длине группы A_n решается сложнее. Авторам настоящего обзора известно, что Б. А. Погорелов, используя указанные в [75] определяющие соотношения группы A_n в системе образующих $B_3' = \{(1, 2, i),\ i \in \{3, \dots, n\}\}$, в 1971 г. показал, что

$$\tfrac{3}{2}n - \tfrac{7}{2} \leqslant L(A_n; B_3') \leqslant \tfrac{3}{2}n - 1.$$

Заметим, что множества T и B_3 являются в группах S_n и A_n классами сопряженных элементов (говоря короче, классами). Вопрос о представлении подстановок из S_n и A_n через классы и о длинах таких представлений привлекал внимание многих известных специалистов по теории групп. Соответствующие исследования были инициированы в 1951–52 гг. работами О. Оре и Н. Ито [95]. О. Оре установил, что каждая подстановка из A_n является коммутатором подходящих подстановок из S_n. Н. Ито доказал, что эти подстановки можно выбрать из A_n (при $n \geqslant 5$). Дж. Бреннер [64] в 1960 г. показал, что для $n \in \{5, \dots, 9\}$ каждый элемент группы A_n представляется в виде $u^{-1}a_n y a_n^{-1} y^{-1} u$ при фиксированном a_n и подходящих u и y из A_n, и поставил вопрос об описании всех знакопеременных групп с этим свойством. Иначе говоря, требовалось описать группы A_n, в которых имеется такой класс сопряженных элементов C_n, что

$$A_n = C_n \cdot C_n^{-1}, \tag{5}$$

где $(\,)^{-1}$ и $\cdot$ понимаются как операции над комплексами.

Интерес к этой проблеме подогрела и высказанная Д. Томпсоном гипотеза о том, что в любой неабелевой простой группе G имеются классы C и $\overline{C}$, удовлетворяющие условию $A_n = C\overline{C}$. А. Глиссон в 1962 г. показал, что условию (5) удовлетворяет класс C_n группы S_n, содержащий полный цикл $g = (1, 2, \dots, n)$. В том же году этот результат был повторен Д. Хьюзмюллером и Г. Рамифильдом [94], которые, кроме того, доказали, что каждая четная подстановка есть коммутатор вида $t_1 t_2 t_1^{-1} t_2^{-1}$, где $t_1 \in C_n$.

Результат А. Глиссона не был решением проблемы Дж. Бреннера, поскольку $C_n \subset A_n$ при четном n, однако он имел продолжение. А именно, И. Бертрам рассмотрел [59] более общий вопрос: при каких l, $l \leqslant n$, выполняется равенство $A_n = C_l \cdot C_l$, а также — при каких l, $l \leqslant n$, выполняется равенство $S_n \setminus A_n = C_l \cdot C_{l+1}$, где C_l — класс всех l-циклов. На эти вопросы он дал исчерпывающие ответы:

1) $A_n = C_l^2 \iff l \geqslant \lfloor 3n/4 \rfloor$ при $n \neq 4$; точнее, если $g \in A_n$, $m(g)$ — число мобильных элементов и $\overline{C}(g)$ — число неединичных циклов в g, то $g \in C_l^2$ при любом l, удовлетворяющем условию

$$(m(g) + \overline{C}(g))/2 \leqslant l \leqslant n;$$

2) $S_n \setminus A_n = C_l \cdot C_{l+1} \Longleftrightarrow \lfloor 3n/4 \rfloor \leqslant l \leqslant n-1$ при $n \neq 5$, $n \equiv 1, 2 \pmod 4$, и $S_n \setminus A_n = C_l \cdot C_{l+1} \Longleftrightarrow \lfloor 3n/4 \rfloor - 1 \leqslant l \leqslant n-1$ при $n \equiv 0, 3 \pmod 4$. Точнее, если $n \in S_n \setminus A_n$, то $g \in C_l \cdot C_{l+1}$ при любом l, удовлетворяющем условию

$$(m(g) + \overline{C}(g) - 1)/2 \leqslant l \leqslant n-1.$$

Заметим, что некоторая детализация метода разложения подстановок в произведение двух циклов дана в работе [123] (на китайском языке).

Проблему Дж. Бреннера решил Ху Чен-Хао в 1965 г. [127]; он доказал, что при $n \geqslant 5$ условию (5) удовлетворяет класс D_n, содержащий подстановку $(1, 2)(3, 4, \ldots, n)$ при четном n. Легко видеть, что класс D_n обладает тем свойством, что $D_n^{-1} = D_n$, и, значит, выполняется соотношение $A_n = D_n^2$.

В 1974 г. в работе [69] Дж. Бреннер, М. Рэнделл и Д. Риддэл заметили, что в любой конечной неабелевой группе G для любого класса сопряженных элементов C существует такое k, что $C^k = G$. Минимальное из таких k они назвали экспонентой класса C и сформулировали два вопроса.

1. Каким может быть период класса C (т. е. порядок элементов из C), если $C \cdot C = A_n$?

2. Какие классы из A_n имеют максимальную экспоненту?

Заметим, что экспонента класса C из A_n не меньше длины группы A_n в системе образующих C.

В работе [69] показано, что при $n > 6$ в A_n нет классов периода 2 и экспоненты 2, а при $n = 6$ и $n = 12l + 10$ ($l \geqslant 0$) в S_n нет классов периода 3 и экспоненты 2. Если же $n \in \{5, 7, 8, 9, 11, 12\}$, то экспоненту 2 имеют соответственно цикловые классы типа $[1^2 3]$, $[1^1 3^2]$, $[1^2 3^2]$, $[1^3 3^2]$, $[1^2 3^3]$, $[1^3 3^3]$. И, наконец, класс 3-циклов в A_n имеет экспоненту $\lfloor n/2 \rfloor$.

В дальнейшем указанные и близкие к ним вопросы рассматривались в ряде статей Дж. Бреннера, Г. Морана и других авторов [65, 68, 70, 72, 110–112].

В [65, 68] указаны значения параметра l, $l \in \{1, \ldots, n\}$, при которых A_n совпадает с квадратом класса l-циклов. В [68], в частности, доказано, что $C \cdot C \neq A_n$ для любого класса инволюций из A_n при $n > 6$, и $C \cdot C = A_n$ для классов C типа $[n^1]$ и $[(4k)^4]$; в [86] найдено условие на класс C в A_n, при котором $C^3 = A_n$; в [66] доказано, что экспоненты почти всех классов в A_n не превосходят 4, т. е. отношение их числа к числу всех классов стремится к 1 с ростом n.

Особое внимание было уделено представлению подстановок в виде произведения инволюций или циклов. Так, А. Фестракс [89] доказывает простое утверждение о том, что любой элемент группы S_n представляется в виде произведения двух инволюций и уточняет вид сомножителей в зависимости от четности или нечетности произведения.

Н. Т. Петров [46] формулирует гипотезу А. И. Кострикина о том, что длины всех простых групп четного порядка в системах образующих, состоящих из инволюций, ограничены некоторой константой, которая, возможно, равна 4, и доказывает, что для всех известных к тому времени простых групп четного порядка такая константа существует и не превосходит 20. В частности, для группы A_n указанная длина равна двум при $n = 10$ и $n = 14$ и трем при $n > 6$, $n \neq 10$, $n \neq 14$.

Г. Моран [110] рассмотрел вопрос о представлении подстановок в виде произведения t-инволюций, т. е. инволюций из класса $R_t = [1^{n-2t} 2^t]$. Для любой подстановки g из S_n доказано, что при $k > 2$ и $n > 2t$ и подходящем неотрицательном r имеет место соотношение

$$g \in R_t^k \Longleftrightarrow kt = n - c(g) + 2r.$$

Находятся также и минимальные значения k, при которых $A_n \subset R_t^k$ и $S_n \setminus A_n \subset R_t^k$, т. е. по существу находится длина группы S_n в системе

образующих R_t. Например, минимальное k, при котором $A_n \subset R_t^k$, является наименьшим натуральным числом, удовлетворяющим таким условиям: kt четно и $kt \geqslant n-2$ при четном n, и $kt \geqslant n-1$ при нечетном n.

В [112] находится критерий принадлежности любой подстановки из S_n произведению $R_i \cdot R_j$ двух сопряженных классов инволюций.

Работа Г. Морана [111] посвящена вычислению числа возможных представлений любой заданной подстановки в виде произведения двух инволюций из S_n (в терминологии автора — числа $BR(g)$ бирефлексий подстановки g, $g \in S_n$). Это число Г. Моран выражает в терминах слоев решетки подразбиения множества $\{1, \ldots, n\}$ на орбиты группы $\langle g \rangle$.

Заметим, что в большинстве указанных выше работ используются в основном комбинаторные методы сведе́ния к известным системам образующих. В то же время при работе с классами сопряженных элементов естественно использовать групповую алгебру CS_n и теорию характеров. Именно эта техника использовалась в работе [122] при нахождении производящей функции для числа e_k^W подстановок, имеющих ровно k циклов и представимых в виде произведения одной (фиксированной) полноцикловой подстановки и любой подстановки из класса C_W. Выделяется частный случай, когда C_W имеет цикловой тип $[p^m]$. В этом случае для e_k^W используется обозначение $e_k^p(n)$; для вычисления $e_k^p(n)$ находится рекуррентное соотношение. Указывается, что рекуррентная формула для $e_k^2(n)$ ранее другим методом была найдена в [96] (мотивировка постановки задачи — топологическая).

Техника характеров использовалась также в работах Е. Бертрама, Ф. Вея [60] и П. Стенли [119] для нахождения числа $g_k(\pi)$ различных представлений подстановки π в виде произведения k штук n-циклов, т. е. словами в алфавите C_n.

Ясно, что значение функции $g_k(\pi)$ зависит только от цикловой структуры $\rho(\pi)$ подстановки π. В частности, в [60] найдены формулы в случаях $\rho(\pi) = [1, n-1]$ и $\rho(\pi) = [1^n]$, а также для любого ρ, $\rho = [1^a, \ldots, n^a]$, при $k = 2$.

В [119] значение $g_k(\pi)$ выражено через неприводимые характеры группы S_n (при их записи получена достаточно громоздкая формула). При некоторых условиях найдена асимптотика. Доказана гипотеза Д. Уокапа [122]:

$$\lim_{n \to \infty} g_2(\pi_n)/(n-2)! = 2$$

для любой последовательности подстановок без неподвижных точек из A_n. Заметим, что формула для вычисления $g_2(\pi)$ комбинаторным методом найдена и в [62].

В ряде работ рассматривались представления элементов групп S_n и A_n и длины этих групп в системах образующих, состоящих из элементов заданных порядков. Так, В. Багинский показал [56], что при $n > 4$ имеет место соотношение

$$A_n = K_2 \cdot K_2 \iff n \in \{5, 6, 10, 14\}$$

(здесь и далее K_m — множество всех элементов порядка m группы A_n). Если же $n > 2$, то $A_n = K_3 \cdot K_3$.

В статье [67] показано, что при $n \geqslant 15$ выполнятся равенство $A_n = K_5 \cdot K_5$, а при $n \leqslant 14$ четная подстановка g принадлежит $K_5 \cdot K_5$ в том и только том случае, когда ее цикловой тип отличен от

$$[3^1], [2^2], [2^4], [3^3], [2^1 3^1 4^1], [2^5 5^1], [2^5], [4^1], [1^1], [1^3], [1^4], [3^1 1^1], [2^4 1^1].$$

Упомянем еще известный авторам обзора результат А. Б. Пичкура (1990): $S_n = C_l \cdot M_l$, где M_l — множество всех подстановок из S_n с l мобильными элементами, $n \geqslant 5$ и $\lfloor 3n/4 \rfloor \leqslant l \leqslant n$.

Приведенные выше результаты по длинам групп относятся к мощным системам образующих групп S_n и A_n, а поэтому длина оказывается, как правило, небольшой. Ниже мы остановимся на системах образующих с небольшим числом элементов — в частности, с двумя.

Большой цикл работ по таким системам связан с решением проблемы оценки меры информационной избыточности систем образующих симметрической полугруппы P_n — эта проблема была поставлена В. М. Глушковым в 1968 г. [17] в связи с абстрактно-автоматным подходом к понятию полноты системы операций в ЭВМ.

В применении к системе образующих A полугруппы или группы подстановок G мера информационной избыточности $\mu(G; A)$ есть не что иное, как длина полугруппы или группы в данной системе, умноженная на число элементов системы: $\mu(G; A) = L(G; A)\,|A|$.

В связи с этим из результатов по оценкам величины $\mu(P_n; A)$ легко извлекаются и оценки длины группы S_n в системе A' всех биективных отображений из A. Один из результатов В. М. Глушкова состоял в нахождении верхней оценки $L(S_n; B) \leqslant 2n^2$ для системы образующих $B = \{a, b\}$, где $a = (1, 2)$, $b = (1, 2, \ldots, n)$.

Позднее мера информационной избыточности различных систем образующих симметрической полугруппы P_n рассматривалась в работах [4, 9, 12, 14, 15, 18–21, 23–26, 34, 36, 41, 48, 50] Здесь мы не будем излагать представленные в них результаты, поскольку их можно найти в большой обзорной статье Ю. В. Голункова [26] по вопросам полноты и сложности микропрограмм.

После работы В. М. Глушкова большое внимание было уделено рассмотренной им системе образующих B. Заметим, что через нее легко выражаются подстановки из T_2: $(i, i+1) = b^{-(i-1)}ab^{i-1}$, $i \in \{1, \ldots, n-1\}$. Проделав соответствующие замены в каноническом слове относительно системы T_2 и произведя очевидные сокращения слов по определяющим соотношениям группы S_n в системе B, получим оценку

$$L(S_n; B) \leqslant 3n(n-1)/2.$$

Эта оценка, улучшающая результат В. М. Глушкова, была получена в 1971 г., см. [93]. Вопрос о возможности снижения верхней оценки (хотя бы по порядку) оставался открытым, поскольку тривиальная нижняя оценка для любой 2-элементной системы образующих группы S_n имеет порядок $n \log_2 n$.

Б. А. Погорелов дал в 1973 г. отрицательный ответ на этот вопрос [48]. Прослеживая изменение суммарного числа инверсий при переходе от одного смежного класса по подгруппе $\langle b \rangle$ к другому, он нашел нетривиальную нижнюю оценку величины $L(S_n; B)$. Кроме того, используя ту же идею, он модифицировал предложенный ранее В. Г. Бондаревым [12] алгоритм представления подстановок через базис B и улучшил также верхнюю оценку величины $L(S_n; B)$. В итоге было установлено, что

$$\frac{n^2}{3} - \frac{n}{3} - 1 \leqslant L(S_n; B) \leqslant \frac{4n^2}{3} - \frac{n}{2} - \frac{5}{6},$$

т. е. система образующих B не является оптимальной даже по порядку.

А. Ю. Зубов в 1979 г. нашел совпадающие по порядку верхнюю и нижнюю оценки величины $L(S_n; B)$, дающие асимптотическое равенство $L(S_n B) \sim 3n^2/4$.

Позднее [31] он получил оценки длины группы S_n в системе образующих, состоящей из произвольного полного цикла и транспозиции (естественно, порождающих S_n). Кроме указанной выше оценки, в [31] получены также следующие результаты.

Если $a' = (1, r)$ и НОД$(r-1, n) = 1$, то при $1 < r \leqslant n/2$ имеет место неравенство

$$L(S_n; \{a', b\}) \leqslant \begin{cases} \frac{3n^2}{4} - \frac{(n+2)(r-1)}{2}, & n \text{ четно}, \\ \frac{3n^2}{4} - \frac{(n+3)(r-2)}{2}, & n \text{ нечетно}. \end{cases}$$

В частном случае, когда n четно, $a' = (1, n/2)$ и НОД$(n, n/2-1) = 1$, или когда n нечетно и $a' = (1, (n-1)/2+1)$, имеет место оценка

$$L(S_n; \{a', b\}) \leqslant \frac{n(n+1)}{2} + 2.$$

В случае, если $n = 2^k$ и $a' = (1, 2^{k-1})$, справедливы оценки

$$\frac{n(n-1)}{2} - 2 \leqslant L(S_n\{a', b\}) \leqslant \frac{n(n+1)}{2} + 2,$$

показывающие, что в классе систем образующих группы S_n, состоящих из транспозиции и полного цикла, достигается асимптотическое равенство

$$L(S_n; \{a', b\}) \sim n^2/2.$$

Такой же по порядку является верхняя оценка длины группы S_n в системе образующих $\{(1, \ldots, n-1), (n, n-1)\}$ [35]. Точнее, в [35] доказано, что для системы образующих $P_{k,n} = \{(1, \ldots, n-1)^k, (n, n-k), \ldots, (n, n-1)\}$, где $k \mid n$, выполняется неравенство

$$L(S_n; P_{k,n} \leqslant n - 1\left(\frac{n-1}{k} + 1\right) + \left\lfloor \frac{n}{2} \right\rfloor.$$

Заметим, что пар образующих, порождающих группу S_n с длиной, превосходящей n^2, неизвестно. В связи с этим в работе [50] высказана гипотеза о том, что таких пар не существует. Эта гипотеза с помощью ЭВМ подтверждена в [50] для $n \leqslant 7$.

Выше уже упоминалось об оптимальных системах образующих группы S_n. Впервые примеры оптимальных по порядку пар образующих группы S_n были в 1971 г. построены Ю. В. Голунковым [19]. Точнее, он доказал, что для любых n и k, $2 \leqslant k < n$, существует оптимальная по порядку (с константой, не превосходящей 100) система из k образующих группы S_n. Такие системы находятся конструктивно, но соответствующие построения весьма искусственны и громоздки. В связи с этим представляет интерес другой результат Ю. В. Голункова [23] о длине группы $S(V_m)$ (здесь, как и выше, V_m — пространство строк длины m над $GF(2)$ в системе образующих из двух регистров сдвига, ρ_{f_1} и ρ_{f_1}, где $f_1 = x_1 \oplus x_2 \ldots x_m$):

$$L(S(V_m); \rho_{f_1}, \rho_{f_1}) \leqslant 17m^3 2^m,$$

тогда как нижняя энтропийная оценка в этом случае равна $m2^m$.

Одним из первых примеров оптимальной системы образующих группы S_n является также множество подстановок

$$D_n = \{d_0 = (0, 1),\ d_1 = (0, 1, 2),\ \ldots,\ d_{n-2} = (0, 1, \ldots, n-1)\}.$$

В. П. Зязин в 1971 г. показал, что $L(S_n; D_n) = n - 1$. Кроме того, он нашел число $N_l(D_n)$ различных элементов группы S_n, содержащихся в множестве D_n^l:

$$N_l(D_n) = \begin{cases} n-1, & l = 1, \\ (n-1)^2, & l = 2, \\ n(n-1)\ldots(n-l+1), & 3 \leqslant l \leqslant n-2, \\ n!, & l \geqslant n-1. \end{cases}$$

Приведем еще ряд известных результатов о системах образующих группы S_n, в которых используется группа $G=\langle g\rangle$, где $g=(0, 1, 2, \ldots, n-1)$.

В [31] найдено точное значение величины $L(S_n; GhG)$ в случае $h=(i, j)$, где НОД$(|i-j|, n)=1$:

$$L(S_n; GhG)=\lfloor n/2\rfloor\lfloor (n-1)/2\rfloor.$$

Этот результат показывает, что рассматриваемая система образующих не является оптимальной по порядку.

В [16] М. М. Глухов приводит оптимальные по порядку (с константой 7) и достаточно просто реализуемые системы образующих типа Gh группы $S(V_m)$, где h: $x\to x\oplus\alpha_{f(x)}$.

К оптимальным системам образующих группы $S(V_{2m})$ относится система R_{2m} всех подстановок вида $(x, y)\to(y, x\oplus f(y))$, где $x, y\in V_m$, реализующих преобразования типа DES [53] при случайном выборе булевых функций f. В работе [105], посвященной построению псевдослучайного генератора подстановок, показано, что $S(V_{2m})=R_{2m}^3$, и, значит, $L(S(V_{2m}); R_{2m})\leqslant 3$.

Приведем также серию результатов о длинах групп подстановок, не обязательно совпадающих с A_n или S_n. В тех случаях, когда результаты носят асимптотический характер, мы, говоря о группе G, всегда будем иметь в виду последовательность групп подстановок возрастающих степеней с общими ограничениями на системы образующих.

Рассмотрим класс систем образующих, широко используемых при компактных представлениях групп подстановок (в частности, S_n и A_n), для которых имеется простой алгоритм нахождения кратчайшего представления любой подстановки. Речь пойдет о так называемых «сильных системах» образующих, введенных Ч. Симсом в работе [118]. Эти системы образующих были использованы и в ряде работ по проблеме изоморфизма графов (см., например, обзор [30]). В более общей форме, чем у Ч. Симса, сильные системы образующих изучались в [101, 103].

В общем случае такие системы образующих определяются следующим образом. Пусть $G<S_n$; рассмотрим ряд стабилизаторов

$$G=G_0\supseteq G_1\supseteq\ldots\supseteq G_{n-1}\supseteq G_n=\{e\},$$

построенный по некоторой перестановке J, $J=(i_1, i_2, \ldots, i_n)$. Здесь

$$G_k=\{g\in G:\ g(i_r)=i_r,\ r\in\{1, \ldots, k\}\},\qquad k\in\{1, \ldots, n-1\}.$$

Пусть $G_{k-1}=G_k\cup G_k\cdot g_{k+1}^{(k)}\cup\ldots\cup G_k\cdot g_n^{(k)}$ — разложение группы G_{k+1} в смежные классы по G_k, где $g_p^{(k)}(i_r)=i_r$, $1\leqslant r<k<n$, и

$$g_p^{(k)}(i_k)=i_p,\qquad p\in\{k+1, \ldots, n\}. \tag{6}$$

Сильной системой образующих группы G, отвечающей перестановке J, называется множество подстановок — представителей смежных классов $\overline{G}_J=\{g_p^{(k)}:\ k\in\{1, \ldots, n-1\},\ p\in\{k+1, \ldots, n\}\}$.

Для любой перестановки J и любых представителей смежных классов $\{g_p^{(k)}\}$, удовлетворяющих (6), имеют место следующие утверждения:

1) $G=\langle\overline{G}_J\rangle$;

2) любой элемент g группы G однозначно представляется в виде

$$g=g_{t_{n-1}}^{(n-1)}\cdot g_{t_{n-2}}^{(n-2)}\cdot\ldots\cdot g_{t_1}^{(1)}, \tag{7}$$

где $g_{t_r}^{(r)}\in\overline{G}_J$, $1\leqslant r<t_r\leqslant n$, причем некоторые сомножители в (7) могут быть пропущены (т. е. заменены на e).

Сильные системы образующих можно строить с помощью произвольной системы образующих M данной группы. Для этого используется индуктивная процедура заполнения таблицы, называемой каскадом. Эта процедура заключается в следующем.

Пусть задана перестановка J, $J=(i_1, i_2, \ldots, i_n)$. С ее помощью заполняется треугольная таблица (каскад):

$$\begin{array}{llll} i_1 \to i_2 & i_1 \to i_3 & \ldots & i_1 \to i_{n-1} \quad i_1 \to i_n \\ & i_2 \to i_3 & & i_2 \to i_{n-1} \quad i_2 \to i_n \\ & & \ddots & \vdots \\ & & & i_{n-2} \to i_{n-1} \quad i_{n-2} \to i_n \\ & & & i_{n-1} \to i_n \end{array}$$

В каскаде указаны переходы подстановок, определяющих представители соответствующих смежных классов группы G_i по подгруппе G_{i+1}.

На первом этапе процедуры в пустой каскад записываются образующие из M. Если при этом $m \in M$ и $m(i_\alpha)=i_\alpha$, $1 \leqslant \alpha \leqslant r$, а $m(i_{r+1})=i_p$, $p>r+1$, то m записывается в каскад на место образующей $g_p^{(r+1)}$, т. е. на место, указанное переходом $i_{r+1} \to i_p$. Если соответствующее место в каскаде уже занято некоторым элементом a, то строится произведение $b=m \cdot a^{-1}$, подлежащее записи в более низкую строку каскада с помощью аналогичной процедуры. Некоторые образующие могут оказаться выражаемыми через предыдущие, и определяемые ими элементы не попадут в каскад.

На втором этапе строятся всевозможные произведения элементов g и h, уже попавших в каскад. Эти произведения «пропускаются» через частично заполненный каскад и подлежат записи в него согласно процедуре, описанной на первом этапе. Второй этап проводится до тех пор, пока в каскаде перестанут появляться новые элементы.

В результате в каскаде будет записана сильная система образующих $\overline{G}_J$ (каждый элемент которой выражен через элементы из M), причем для этого через каскад будет «пропущено» не более $O(\max(M, n^4))$ подстановок. Все ячейки каскада будут заполнены лишь в случае $G=S_n$.

В силу своего большого многообразия и простоты построения сильные системы образующих могут быть использованы для построения алгоритмов решения некоторых уравнений в группах подстановок, что необходимо учитывать в криптографических приложениях.

Следующая серия результатов связана с получением оценок длин групп подстановок (в частности, S_n и A_n) относительно систем образующих, состоящих из некоторых множеств циклов.

В работе [85] Д. Дрисколл и М. Фёрст получили сильный результат о том, что длина любой группы подстановок степени n, порожденной множеством циклов ограниченной степени, не превосходит $O(n^2)$. Здесь имеется в виду, что с ростом n число мобильных элементов в каждой из образующих ограничено константой. Вместе с этим основным результатом приведем некоторые вспомогательные утверждения из [85], которые могут оказаться полезными при получении оценок длин групп подстановок.

1. Если $G=\langle g_1, g_2, \ldots, g_m\rangle$ — примитивная подгруппа группы S_n, содержащая полиномиально выражаемый 3-цикл, причем либо $\max\limits_i \operatorname{ord} g_i = O(1)$, либо $\{g_1, \ldots, g_m\}^{-1}=\{g_1, \ldots, g_m\}$, то длина $L(G; M)$ подгруппы G полиномиально ограничена (ограничена сверху значениями $f(n)$ некоторого полинома).

2. Пусть подгруппа G группы S_n порождена множеством циклов, попарно пересекающихся не более чем по одному символу. Тогда $L(G; M)=O(n^4)$.

3. Пусть $H < G = \langle g_1, \ldots, g_m \rangle < S_n$. Длиной $L(G/H; M)$ фактормножества G/H называется минимальное натуральное k, при котором каждый смежный класс G по H содержит k-представимый (т. е. имеющий длину не более k) элемент. Тогда $L(G; M) \leqslant L(H; M) + L(G/H; M)$.

4. Пусть $G = \langle g_1, \ldots, g_m \rangle$ — группа подстановок степени n, и $H < G$, причем $|H| \leqslant k$ для некоторого числа k (не зависящего от n). Если длина группы G/H есть $f(n)$, то длина группы G есть $O(f(n))$.

Подчеркнем, что задача получения полиномиальных оценок длин подгрупп группы S_n является актуальной, поскольку существуют последовательности групп подстановок, длины которых в заданных системах образующих не ограничены сверху никакими полиномами. Приведем два примера.

Пусть $g = (1, 2)(3, 4, 5)(6, 7, 8, 9, 10) \ldots \in S_n$, причем длина i-го цикла в указанном разложении элемента g на независимые циклы равна i-му простому числу p_i. Группа $G = \langle g \rangle$ имеет порядок $p_1 p_2 \ldots p_k$. Из теории чисел известно, что асимптотически (при $n \to \infty$) эта величина является субэкспоненциальной функцией от n. Но $|G| = \operatorname{ord} g$, а потому длина группы G не ограничена никаким полиномом.

Имеются также и нециклические группы с указанным свойством.

Пусть G_i — группа симметрий правильного p_i-угольника, представленная как группа подстановок множества вершин, где p_i снова есть i-е простое число. Рассмотрим группу $G = G_1 \times G_2 \times \ldots \times G_k$. Известно, что G_i порождается двумя симметриями, a_i и b_i, где $\operatorname{ord}(a_i \cdot b_i) = p_i$. Итак, $G_i = \langle a_i, b_i \rangle < S_n$, где $n = p_1 + \ldots + p_k$. Ясно, что $G = \langle a, b \rangle$, где $a = (a_1, \ldots, a_k)$, $b = (b_1, \ldots, b_k)$, $\operatorname{ord} a = \operatorname{ord} b = 2$ (поскольку a_i и b_i — симметрии), $|G| = p_1 \ldots p_k$.

Любой элемент группы G представим в виде $\alpha(ab)^i\beta$, где $\alpha, \beta \in \{e, a, b\}$, и поэтому число элементов в G не выражается полиномом от n. Одна из полиномиальных оценок длины группы подстановок получена Маккензи в работе [108]. Оказывается, что длина группы подстановок полиномиально ограничена сверху относительно любой системы образующих, каждая из которых перемещает ограниченное число символов. Точнее, если $G = \langle g_1, \ldots, g_m \rangle < S_n$, причем $\deg(g_i) \leqslant k$, где k — константа, не зависящая от n, $1 \leqslant i \leqslant m$, то $L(G; M) = O(n^{2k})$.

Следует отметить результат Л. Бабаи и А. Сереша [55], получивших общую верхнюю оценку длины групп S_n и A_n относительно произвольной системы образующих M, обладающей свойством $M^{-1} = M$. Пусть $G < S_n$ и $L(G) = \max\limits_M L(G; M)$. Тогда имеет место оценка

$$L(G) \leqslant \exp \sqrt{n \log n}\,(1 + o(1))$$

в случае, когда G содержит A_n.

В [55] выдвинута гипотеза относительно величины $L(G)$ в том случае, когда G — неабелева конечная простая группа: $L(G) \leqslant \log^c |G|$, где c — некоторая константа. Упоминается также следующий любопытный результат: каждая неабелева конечная простая группа G имеет такую систему образующих M, что $|M| \leqslant 7$ и $L(G; M) = O(\log |G|)$.

Полиномиальная верхняя оценка длины группы S_n или A_n может быть получена относительно множества порождающих ее циклов, которое является системой образующих игры на некотором двусвязном графе (см. § 1 данного обзора). Так, в упоминаемой выше статье [102] анонсируется верхняя оценка $O(n^3)$. В этой статье приводятся (без доказательства) некоторые утверждения, которые могут оказаться полезными при получении оценок длин групп подстановок.

1. Если подгруппа $G = \langle M \rangle$ группы S_n является k-транзитивной на словах длины l, причем $M^{-1} = M$ и $k > n/3 - 1$, то G содержит A_n и $L(G; M) < 4n^2 l$.

2. Пусть $G = \langle M \rangle$ — примитивная подгруппа группы S_n, причем $M^{-1} = M$, и H — ее подгруппа, порожденная циклической подстановкой простой длины p, где $p < n$. Тогда G является $(n-p+1)$-транзитивной на словах длин, меньших $2^{\sqrt[3]{p}+1} n^3 (n^2 + L(H; M))$.

3. Пусть $G = \langle M \rangle$ — примитивная подгруппа группы S_n, причем $M^{-1} = M$, и пусть H — перемещающая m букв, $2 \leqslant m < n$, 2-транзитивная на множестве всех мобильных элементов подгруппа группы G. Тогда группа G является $(n-m+1)$-транзитивной на словах длин, меньших $2^{\sqrt[3]{m}+1} n^3 (n^2 + L(H; M))$.

4. Если $G = \langle M \rangle$ — примитивная подгруппа группы S_n, порожденная циклами, один из которых имеет простую длину p, где $p < 2n/3$, то $G \supseteq A_n$ и $L(G; M) < 2^{\sqrt[3]{p}+4} n^8$.

Целый ряд результатов по оценкам длин групп подстановок связан с теоретико-графовым подходом. Дело в том, что длина группы G относительно системы образующих M совпадает с диаметром*) графа Кэли группы $G = \langle M \rangle$. Кстати, в силу этого длину группы G называют также ее диаметром (см. [55, 85] и др.).

Равенство $L(G; M) = D(\Gamma(G; M))$ позволяет использовать для получения оценок длины групп ряд результатов из теории графов. Например, в книге Н. Биггса [61] показано, что диаметр ориентированного связного графа Γ не превосходит ранга его матрицы смежности:

$$D(\Gamma) \leqslant \operatorname{rk} A(\Gamma), \tag{8}$$

где $A(\Gamma) = (a_{ij})$, $a_{ij} = 0$, если в Γ нет ребра (x_i, x_j), и $a_{ij} = 1$ в противном случае.

В работе ван Нуттелена [121] дается критерий достижимости оценки (8) для связных обыкновенных неориентированных графов. А именно, равенство

$$D(\Gamma) = \begin{cases} \operatorname{rk} A(\Gamma), & D(\Gamma) \text{ четно}, \\ \operatorname{rk} A(\Gamma) - 1, & D(\Gamma) \text{ нечетно} \end{cases}$$

имеет место в том и только том случае, когда для всех вершин $x, y, \ldots, z$ графа Γ, которые находятся на одинаковом расстоянии от одной из начальных вершин пути длины $D(\Gamma)$, имеют место равенства $\Gamma(x) = \Gamma(y) = \ldots = \Gamma(z)$. Здесь через $\Gamma(x)$ обозначено множество вершин, смежных с вершиной x в графе Γ.

Следующая оценка [61] связана со степенью минимального многочлена $m_\Gamma(\lambda)$ матрицы смежности графа Γ: для любого графа Γ выполняется неравенство $D(\Gamma) \leqslant \deg m_\Gamma(\lambda) - 1$.

Для неориентированного графа имеет место неравенство

$$D(\Gamma) \leqslant m - 1, \tag{9}$$

где m — число различных комплексных корней многочлена $m_\Gamma(\lambda)$.

Напомним, что в случае $M^{-1} = M$ граф Кэли $\Gamma(G; M)$ может рассматриваться как неориентированный. Для таких систем образующих M можно использовать неравенство (9) для получения верхних оценок длины группы G. В некоторых случаях (например, для групп S_n и A_n при $n \leqslant 5$) такая оценка может быть достаточно точной.

Множество собственных значений матрицы смежности графа называется спектром графа. Л. Бабаи [54] получил связь между элементами спектра графа группы G, порожденной множеством образующих M, где $M^{-1} = M$,

*) Напомним, что диаметром графа (орграфа) Γ называется величина $D(\Gamma)$, равная длине максимального среди кратчайших путей, соединяющих пары его вершин, по (ориентированным) ребрам графа [32].

со значениями неприводимых комплекснозначных характеров этой группы на ее слоях. Он получил следующий результат.

Пусть G — конечная группа, порожденная множеством образующих M, где $M^{-1}=M$, а $\Psi_1,\ldots,\Psi_s$ — характеры ее неприводимых представлений степеней $n_1,\ldots,n_s$ соответственно, где $n_1^2+\ldots+n_s^2=|G|$. Тогда для любого натурального t имеет место формула

$$\lambda_{i,1}^t+\ldots+\lambda_{i,n}^t=\sum_{h_1,\ldots h_t\in M}\Psi_i\left(\prod_{l=1}^{t}h_l\right). \tag{10}$$

Поясним, что здесь для каждого n_i имеются собственные значения $\lambda_{i,1},\lambda_{i,2},\ldots,\lambda_{i,n}$, каждое кратности n_i. Суммирование в (10) ведется по всем $|M|^t$ возможным наборам из l образующих.

Формулу (10) можно использовать при составлении системы уравнений для нахождения спектров графов небольших групп, например, для S_4.

Сформулированное утверждение имеет очевидное следствие: если G — конечная группа, $G=\langle M\rangle$, причем $M^{-1}=M$, то $L(G;M)\leqslant n_1+\ldots+n_s-1$, где n_i — степени неприводимых представлений группы G. Отсюда, в частности, следуют такие утверждения.

1. Если $G=S_n=\langle M\rangle$, причем $M^{-1}=M$, то $L(G;M)$ меньше числа инволюций в G.

2. Если $G=GL(n,q)=\langle M\rangle$, причем $M^{-1}=M$, то $L(G;M)$ меньше числа симметрических матриц из G.

Еще один подход к получению оценок длин групп связан с соотношением между степенью минимального многочлена матрицы $A(\Gamma)$ и некоторыми характеристиками группы автоморфизмов графа Γ группы.

Заметим, что при отождествлении автоморфизма графа Γ с соответствующей ему подстановочной матрицей группа автоморфизмов графа состоит из всех подстановочных матриц P, для которых $P\cdot A(\Gamma)=A(\Gamma)\cdot P$.

В статье [79] для неориентированного графа Γ с транзитивной группой автоморфизмов $\mathrm{Aut}\,\Gamma$ получено неравенство $\deg m_\Gamma(\lambda)\leqslant \mathrm{rk}(\mathrm{Aut}\,\Gamma)_\alpha$, где через $\mathrm{rk}(\mathrm{Aut}\,\Gamma)_\alpha$ обозначено число орбит стабилизатора вершины α графа Γ в группе $\mathrm{Aut}\,\Gamma$.

Заметим, что в случае $M^{-1}=M$ группа $\Xi=(\mathrm{Aut}\,\Gamma(G;M))_e$, обладает следующими полезными свойствами.

1. Любой элемент $\varphi\in\Xi$ является биекцией каждого слоя группы G на себя.

2. Орбиты группы Ξ состоят из элементов группы G одинаковой длины.

3. Длина группы G относительно системы образующих M не превосходит числа орбит группы Ξ. Равенство достигается лишь в том случае, когда группа Ξ транзитивна на слоях группы G.

4. Любой элемент $\varphi\in\Xi$ является биекцией на множестве циклов одинаковой длины графа $\Gamma(G;M)$, проходящих через e. При этом простые циклы переходят в простые циклы.

Перечисленные свойства группы Ξ облегчают вычисление числа ее орбит для групп G сравнительно небольшого порядка. Например, для группы S_n при $n\leqslant 4$ эту работу несложно проделать вручную.

Ряд работ по оценке диаметра графа (и, в частности, графа группы) опирается не только на алгебраические, но и на чисто геометрические свойства графов.

Граф Кэли любой конечной группы $G=\langle M\rangle$ является регулярным сильно связным орграфом валентности $|M|$, содержащим $|G|$ вершин и $|G|\,|M|/2$ ребер. В случае $M^{-1}=M$ этот граф можно рассматривать как неориентированный, причем при указанном условии он имеет обхват 2.

А. Гуя-Ури (см. [40]) доказал, что среди всех сильно связных ориентированных N-вершинных графов с k ребрами (без петель и кратных ребер) максимальное значение диаметра равно $N-1$, если $N \leqslant k \leqslant N(N+1)/2$, и равно $\left\lfloor N+1/2-\sqrt{2k-N^2-N+17/4}\right\rfloor$, если $N(N+1)/2 \leqslant k < N(N-1)$.

Для этого класса графов выполняется неравенство $D(\Gamma) \geqslant \left\lceil \frac{2(N-1)}{k-N+1} \right\rceil$, см. [27]. Более точно, имеет место равенство

$$D(\Gamma) = \begin{cases} \left\lceil \frac{2(N-1)}{k-N+1} \right\rceil + 1 = 2, & 3(N-1) \leqslant k < N(N-1), \\ \left\lceil \frac{2(N-1)}{k-N+1} \right\rceil & \text{в противном случае.} \end{cases}$$

В работах Р. Люса [106] и М. Линна [107] для рассматриваемого класса графов связь между N, k и $D(\Gamma)$ находится в виде неравенства

$$2k \leqslant 2N^2 - 2ND(\Gamma) + D(\Gamma)^2 + 2N - D(\Gamma) - 4,$$

а при дополнительном условии, что наибольший общий делитель длин всех циклов графа Γ равен $2p$, в [107] получено неравенство

$$4k \leqslant 2N^2 - 2ND(\Gamma) + D(\Gamma)^2 + 6N - 2D(\Gamma) - \begin{cases} 8, & D(\Gamma) \text{ четно}, \\ 7, & D(\Gamma) \text{ нечетно}, \ N \text{ четно}, \\ 9, & D(\Gamma) \text{ и } N \text{ нечетны}. \end{cases}$$

Полезное соотношение между числом вершин, валентностью и диаметром неориентированного связного графа Γ (без петель и кратных ребер) получено в работе Д. Муна [109]. Пусть s — наименьшее натуральное число, для которого в N-вершинном неориентированном связном графе Γ диаметра, не превосходящего ν, степень любой вершины не менее s. Тогда для любого ν, $\nu \geqslant 3$, имеет место равенство

$$s = \begin{cases} \lfloor N/t \rfloor, & \nu = 3t-4, \\ \lfloor (N-1)/t \rfloor, & \nu = 3t-3, \\ \lfloor (N-2)/t \rfloor, & \nu = 3t-2. \end{cases}$$

В работе А. В. Князева [38] рассматривается класс сильно связных орграфов с обхватом не менее p, в которых каждая вершина имеет в точности два входящих и два выходящих непараллельных ребра. Для таких графов с N вершинами получена достижимая оценка

$$D(\Gamma) \leqslant \left\lfloor \frac{(N+1)(p+1)}{2p-1} \right\rfloor.$$

Теоретико-графовый подход использован также в работе И. Хамидонне [91] для получения следующих верхних оценок длины представления $l(g; M)$ элемента группы G. Если $G = \langle M \rangle$, $e \notin M$, то для любого элемента g из $G \setminus \{e\}$ имеет место оценка

$$l(g; M) \leqslant \left\lfloor \frac{N+1-2s+3\lfloor s/2 \rfloor}{\lfloor s/2 \rfloor + 1} \right\rfloor.$$

где $s = |M|$. Эта оценка уточняется для случая $M \cap M^{-1} = \varnothing$:

$$l(g; M) \leqslant \left\lfloor \frac{N+1-2s+3\lfloor 2s/3 \rfloor}{\lfloor 2s/3 \rfloor + 1} \right\rfloor.$$

СПИСОК ЛИТЕРАТУРЫ

1. Артин Э. Геометрическая алгебра. — М.: Наука, 1969.
2. Байрамов Р. А. К проблеме полноты в симметрической полугруппе // Дискретный анализ. Вып. 8. — Новосибирск, ИМ СО АН СССР, 1966. — С. 3–26.
3. Байрамов Р. А. Критерии фундаментальности групп подстановок и полугрупп отображений // Докл. АН СССР. — 1969. — Т. 189, № 3. — С. 455–457.
4. Бижев Г. Т., Касабов Н. К. Минимальное представление S_n, близкое к предельно компактному // Кибернетика. — 1980. — № 3. — С. 135–136.
5. Биндер Г. Я. О вложении элементов симметрической группы в систему образующих из двух элементов // Сборник аспирантских работ. — Казань: Изд-во Казанского ун-та, 1965. — С. 3–5.
6. Биндер Г. Я. О базисах симметрической группы // Изв. вузов. Математика. — 1968. — № 11. — С. 19–25.
7. Биндер Г. Я. О двухэлементных базисах симметрических групп // Изв. вузов. Математика. — 1970. — № 1. — С. 9–11.
8. Биндер Г. Я. Некоторые полные множества дополняющих симметрической и знакопеременной группы n-й степени // Математич. заметки. — 1970. — Т. 7, № 2. — С. 173–180.
9. Битюцкий В. П. Итеративные процедуры разложения элементов симметрической полугруппы // Кибернетика. — 1975. — № 5. — С. 49–50.
10. Битюцкий В. П., Чистов В. П. Функциональная полнота в ленточных однородных структурах // Изв. АН СССР. Сер. технич. кибернетика. — 1971. — № 3. — С. 116–121.
11. Битюцкий В. П., Чистов В. П. Простейшие ленточные структуры // Изв. АН СССР. Сер. технич. кибернетика. — 1971. — № 6. — С. 126–130.
12. Бондарев В. Г. Алгоритм разложения в конечных симметрических полугруппах // Кибернетика. — 1970. — № 4. — С. 24–28.
13. Бурбаки Н. Группы и алгебры Ли. — М.: Мир, 1972.
14. Вавилов Е. Н., Вичев В. П., Осинский Л. М. Оценка длины микропрограмм для автоматов // Изв. АН СССР. Сер. технич. кибернетика. — 1972. — № 6. — С. 160–165.
15. Ганов В. А. Верхняя оценка меры информационной избыточности симметрической полугруппы // Кибернетика. — 1970. — № 6. — С. 63–65.
16. Глухов М. М. О числовых параметрах, связанных с заданием конечных групп системами образующих элементов // Труды по дискретной математике/РАН. Академия криптографии РФ. Т. I. — М.: ТВП, 1997. — С. 43–66.
17. Глушков В. М. О полноте систем операций в электронных вычислительных машинах // Кибернетика. — 1968. — № 2. — С. 1–5.
18. Годлевский А. Б., Шевченко В. П. К вопросу оценки меры информационной избыточности микропрограммной алгебры // Теория автоматов. Тр. Ин-та кибернетики АН УССР. — 1969. — № 5. — С. 37–39.
19. Голунков Ю. В. О сложности представления подстановок симметрической полугруппы через элементы систем образующих // Кибернетика. — 1971. — № 1. — С. 43–44.
20. Голунков Ю. В. Программно-автоматная реализация подстановок симметрической полугруппы. I // Кибернетика. — 1971. — № 5. — С. 6–12.
21. Голунков Ю. В. Несколько замечаний об однородных ленточных структурах // Изв. АН СССР. Сер. технич. кибернетика. — 1972. — № 6. — С. 176–180.
22. Голунков Ю. В. Функциональная полнота ленточных структур из простейших однонаправленных каскадов // Изв. АН СССР. Сер. технич. кибернетика. — 1973. — № 2. — С. 96–101.
23. Голунков Ю. В. Реализация микропрограммных базисов на регистрах сдвига // Кибернетика. — 1975. — № 3. — С. 33–39.
24. Голунков Ю. В. Программно-автоматная реализация подстановок симметрической полугруппы. II // Кибернетика. — 1975. — № 5. — С. 35–42.
25. Голунков Ю. В. Полнота систем микроопераций и сложность микропрограмм. I // Изв. АН СССР. Сер. технич. кибернетика. — 1976. — № 3. — С. 117–123.
26. Голунков Ю. В. Алгоритмическая полнота и сложность микропрограмм // Кибернетика. — 1977. — № 3. — С. 1–15.
27. Гольдберг М. К. Управляемые системы. Вып. 2. — Новосибирск, 1969. — С. 92.
28. Дьёдонне Ж. Геометрия классических групп. — М.: Мир, 1974.
29. Зайченко В. А., Клин М. Х., Фараджев И. А. О некоторых вопросах, связанных с представлением групп подстановок в памяти ЭВМ // Вычисления в алгебре, теории чисел и комбинаторике. — Киев: Ин-т матем. АН УССР, 1980. — С. 3–19.
30. Земляченко В. Н., Корнеенко Н. М., Тышкевич Р. И. Проблема изоморфизма графов // Теория сложности вычислений. — Л.: Наука, 1982. — С. 83–158.
31. Зубов А. Ю. О диаметре группы S_n относительно системы образующих, состоящей из полного цикла и транспозиции // Труды по дискретной математике/РАН. Академия криптографии РФ. Т. II. — М.: ТВП, 1998. — С. 112–150.
32. Зыков А. А. Теория конечных графов. — Новосибирск: Наука, 1969.

33. Капельмахер В. Л., Лисовец В. А. Последовательное порождение перестановок с помощью базиса транспозиций // Кибернетика. — 1975. — № 3. — С. 17–21.
34. Капитонова Ю. В. К вопросу оценки длины микропрограмм в одной микропрограммной алгебре // Кибернетика. — 1969. — № 1. — С. 101–102.
35. Касабов Н. К. О порождении симметрической группы // Годишн. виш. учебни завед. Прилож. мат. — 1974. — Т. 10, № 3. — С. 55–59.
36. Клевачев В. И. О критериях полноты систем подстановок, содержащих транспозиции // Кибернетика. — 1972. — № 6.
37. Клевачев В. И. О критериях полноты в симметрической группе конечной степени // Кибернетика. — 1975. — № 3. — С. 22–25.
38. Князев А. В. О диаметрах дихотомических графов // Математич. заметки. — 1987. — Т. 41, № 6. — С. 829–843.
39. Коксетер Г. С. М., Мозер У. О. Дж. Порождающие элементы и определяющие соотношения дискретных групп. — М.: Наука, 1980.
40. Коршунов А. Д. О диаметре графов // Докл. АН СССР. — 1971. — Т. 196, № 5. — С. 1013–1015.
41. Кратко М. И., Плесневич Г. С. Об одной задаче В. М. Глушкова // Кибернетика. — 1969. — № 2. — С. 97.
42. Лазарев А. Г. Практические результаты изучения порождения симметрической группы системами образующих // Кибернетика и системный анализ. — 1992. — № 6. — С. 39–47.
43. Марков А. А. Основы алгебраической теории кос // Тр. МИАН СССР. — 1945. — Т. XVI. — С. 1–53.
44. Нечаев А. А. Критерий полноты систем функций p^n-значной логики, содержащих операции сложения и умножения по модулю p^n // Методы дискретного анализа в решении комбинаторных задач. Вып. 34. — Новосибирск, ИМ СО АН СССР, 1980. — С. 74–87.
45. Оре О. Теория графов. — М.: Наука, 1968.
46. Петров Н. Т. О длине простых групп // Докл. АН СССР. — 1973. — Т. 208, № 3. — С. 537–540.
47. Пикар С. О базисах симметрической группы // Кибернетич. сб. Новая серия. Вып. 1. — М.: Мир, 1965. — С. 7–34.
48. Погорелов Б. А. Об одной задаче В. М. Глушкова // Кибернетика. — 1973. — № 5. — С. 141–144.
49. Погорелов Б. А. Примитивные группы подстановок, содержащие 2^m-цикл // Алгебра и логика. — 1980. — Т. 19, № 2. — С. 236–247.
50. Рубцов В. А. О некоторых оценках меры информационной избыточности систем образующих, порождающих симметрическую группу подстановок // Кибернетика. — 1975. — № 5. — С. 51–55.
51. Симс Ч. Вычислительные методы в изучении групп подстановок // Вычисления в алгебре и теории чисел. — М.: Мир, 1976. — С. 129–148.
52. Сущанский В. И., Восканян Р. А. О системах порождающих симметрических и знакопеременных групп, состоящих из циклов одинаковой длины // Вопросы теории групп и гомологической алгебры. — Ярославль, 1985. — С. 43–49.
53. Хоффман Л. Д. Современные методы защиты информации. — М.: Сов. радио, 1980.
54. Babai L. Spectra of Cayley graphs // J. Comb. Theory. — 1979. — V. B27. — P. 180–189.
55. Babai L., Seress A. On the diameter of Cayley graphs of the symmetric group // J. Comb. Theory. — 1988. — V. A49. — P. 175–179.
56. Baginski C. On sets of elements of the same order in the alternating group A_n // Publ. Math. — 1987. — V. 34, № 3–4. — P. 313–316.
57. Batler G. Fundamental algorithms for permutation groups. — Springer-Verlag, 1991.
58. Beasby L. B., Brenner J. L., Erdös P., Szalay H., Williamson A. G. Generation alternating groups by conjugates // Periodica Mathematica Hungarica. — 1987. — V. 18, № 4. — P. 259–269.
59. Bertram E. Even permutation as a product of two conjugate cycles // J. Comb. Theory. — 1972. — V. A12. — P. 368–380.
60. Bertram E. A., Wei V. K. Decomposing a permutation into two large cycles: A_n enumeration // SIAM J. Algebraic and Discrete Methods. — 1980. — V. 1. — P. 105–134.
61. Biggs N. Algebraic graph theory. — Cambridge Univ. Press, 1974.
62. Boccara G. Nombre de représentation d'une permutation comme produit de deux cycles de longueurs données // Discrete Math. — 1980. — V. 29. — P. 105–134.
63. Bovey J. D. The probability that some power of a permutation has small degree // Bull. Lond. Math. Soc. — 1980. — V. 12, № 1. — P. 47–51.
64. Brenner J. L. Group theory reseach problems // Bull. Amer. Math. Soc. — 1960. — V. 66, № 4. — P. 275.
65. Brenner J. L. Covering theorems for finite non-abelian simple groups. II // J. Comb. Theory. — 1973. — V. A14, № 2. — P. 264–269.
66. Brenner J. L. Covering theorems for non-abelian simple groups. VIII // J. Austral. Math. Soc. — 1978. — V. A25. № 2. — P. 210–214.

67. Brenner J. L., Evans R. J. Even permutations as a product of two elements of order five // J. Comb. Theory. — 1987. — V. A32. — P. 196–206.
68. Brenner J. L., Granwell R. M., Riddell J. Covering theorems for finite non-abelian simple groups // Pacific J. Math. — 1975. — V. 58, № 1. — P. 55–60.
69. Brenner J. L., Randall M., Riddell J. Covering theorems for finite non-abelian simple groups. I // Colloq. Math. — 1974. — V. 32. — P. 39–48.
70. Brenner J. L., Riddell J. Noncanonical factorization a permutation // Amer. Math. Monthly. — 1977. — V. 84, № 1. — P. 39–40.
71. Brenner J. L., Wiegold J. Two-generator groups. I // Michigan Math. J. — 1975. — V. 22. — P. 53–64.
72. Brenner J. L., Wiegold J. Two-generator groups. II // Bull. Austral. Math. Soc. — 1980. — V. 22. — P. 113–124.
73. Campbell K. W., Wiener M. J. DES is not a group // Lecture Notes in Comp. Sci. — 1993. — V. 740. — P. 512–520.
74. Carlitz L. A. Permutations in a finite field // Proc. Amer. Math. Soc. — 1960. — V. 11. — P. 456–459.
75. Carmichael R. D. Abstract definitions of the symmetric and alternating groups and other permutations groups // Quart. J. Pure Appl. Math. — 1923. — V. 49. — P. 226–283.
76. Conder M. D. E. Generators for alternating and symmetric groups // J. London Math. Soc. — 1980. — V. 22, № 1. — P. 75–86.
77. Coppersmith D., Grossman E. Generators for certain alternating groups with applications to cryptography // SIAM J. Appl. Math. — 1975. — V. 29, № 4. — P. 624–627.
78. Craig W. A presentation of the symmetric group based on unique irredundant nondecreasing factorisation // J. Pure Appl. Algebra. — 1978. — V. 13, № 2. — P. 165–168.
79. Criscuolo G., Chung-Mo K. The group and the minimal polinomial of a graph // J. Comb. Theory. — 1980. — V. B29, № 3. — P. 293–302.
80. Denes J. The representation of a permutation as the product of a minimal number of transpositions and its connection with the theory of graphs // Publ. Math. Inst. Hungar. Acad. Sci. — 1959. — V. 4. — P. 63–70.
81. Dey M. S., Wiegold J. Generators for altarnating and symmetric groups // J. Austral. Math. Soc. — 1971. — V. 12. — P. 63–68.
82. Dittmar R., Hoernaner G., Wernsdorf R. SAFER, DES and FEAL: algebraic properties of two round functions // Proc. of Pragocrypt '96, International Conference on the Theory and Applications of Cryptology. — Prague: Czech Techn. Univ. Publ. House, 1996. — P. 55–66.
83. Dixon J. D. The probability of generating the symmetric group // Math. Z. — 1969. — V. 110. — P. 199–205.
84. Dixon J. D. Problems in group theory. — Dover Publication Inc., 1973.
85. Driscoll J. R., Furst M. L. On the diameter of permutations groups // Proc. 15*th* Annual Symp. on Theory of Computing. — 1983. — P. 152–162.
86. Driv Y. Covering properties of permutation groups // Lect. Notes in Math. — 1985. — V. 1112. — P. 197–221.
87. Even S., Goldreich O. The minimum-lenth generator sequence problem is NP-hard // J. Algorithms. — 1981. — № 2. — P. 311–313.
88. Even S., Goldreich O. DES-like functions can generate the alternating group // IEEE Trans. Inform. Theory. — 1983. — V. IT-29, № 6. — P. 863–865.
89. Festracts A. Sur les involutions du groupe alterne d'un ensemble fini // Bull. Acad. Roy. Belg. Cl. Sci. — 1964. — V. 50, № 3.
90. Frucht W. Un problema combinatorique interesa en la teoria ole los grupos ole permutaciones // Scientia (Chil.) — 1962. — V. 29, № 117. — P. 39–49.
91. Hamidonne Y. O. Factorisations courtes dans un groupe fini // Discrete Appl. Math. — 1989. — V. 24. — P. 153–165.
92. Herzog M., Reid K. Permutation groups generated by cycles of fixed length // Isr. J. Math. — 1977. — V. 26, № 3–4. — P. 221–231.
93. Huang J.-C. A universal cellular array // IEEE Trans. on Computers. — 1971. — V. C–20, № 3.
94. Husemuller D. H. Ramified coverings of Riemann surfaces // Disc. Math. J. — 1962. — V. 29. — P. 167–174.
95. Ito N. A theorem on the alternating group A_n, ($n \geqslant 5$) // Math. Japon. — 1951. — V. 2. — P. 59–60.
96. Jackson D. M. Counting cycles in permutations by group characters, with an application to a topological problem // Trans. Amer. Math. Soc. — 1987. — V. 229, № 2. — P. 785–801.
97. Jerrum M. A compact representation for permutation groups // Proc. 23rd Ann. Symp. on Foundations of Comput. Sci. (Chicago, 3–5 Nov.) — Silver Spring, 1982. — P. 126–133.
98. Jerrum M. The complexity of finding minimum length generator sequences // Theoret. Comp. Sci. — 1985. — V. 36. — № 2–3. — P. 265–289.
99. Johnson S. M. Generation of permutations by adjacent transpositions // Math. Comp. — 1963. — V. 17, № 83. — P. 282–285.
100. Kalisky B. S., Rivest R. L., Sherman A. T. Is the DES a group? // J. Cryptology. — 1988. — V. 1, № 1. — P. 3–36.

101. Knuth D. E. Efficient representation of permutation groups // Int. J. Comb. and Theory Comp. — 1991. — V. 11, № 1. — P. 33–43.
102. Kornhauser D., Miller G., Spirakis P. Coordinating pebble motion on graphs, the diameter of permutations groups, and applications // Proc. 25*th* Annual Symp. on Foundations of Comp. Sci. — IEEE, 1984. — P. 241–250.
103. Leon J. S. On an algorithm for finding a base and a strong generating set for a group given by generating permutations // Math. Comp. — 1980. — V. 35, № 151. — P. 941–974.
104. Lewin M. Generating the alternating group by cycles triples // Discrete Math. — 1975. — V. 11. — P. 187–189.
105. Luby M., Rackoff C. How to construct pseudorandom permutations from pseudorandom functions // SIAM J. Comput. — 1988. — V. 17, № 2. — P. 373–386.
106. Luce R. D. Connectivity and generalized cliques in sociometric group structure // Psychometrika. — 1950. — V. 15. — P. 159–190.
107. Lynn M. S. Canad. J. Math. — 1968. — V. 20, № 3. — P. 749.
108. McKenzie P. Permutations of bounded degree generate groups of polinomial diameter (manuscript) // Inform. Proc. Lett. — 1984. — V. 19, № 5. — P. 253–254.
109. Moon J. W. On the diameter of a graph // Michigan Math. J. — 1965. — V. 12, № 3. — P. 349–351.
110. Moran G. Permutations as products of k conjugate involutions // J. Comb. Theory. — 1975. — V. A19. — P. 240–242.
111. Moran G. The bireflections of a permutation // Discrete Math. — 1976. — V. 15. — P. 55–62.
112. Moran G. The product of two reflection classes of the symmetric group // Discrete Math. — 1976. — V. 15. — P. 63–77.
113. Piccard S. Sur les bases des groupes d'ordre fini. — Neuchatel, 1957.
114. Pieprzyk J., Zhang X.-M. Permutations generators of alternating groups // Lecture Notes in Comput. Sci. V. 453. — Berlin: Springer-Verlag, 1990. — P. 237–244.
115. Rapaport E. S. Cayley color groups and Hamilton lines // Scripta Math. — 1959. — V. 24, № 1.
116. Rowlinson P. Primitive permutation groups containing a 2-cycle // J. London Math. Soc. — 1975. — V. 10, № 2. — P. 225–227.
117. Rowlinson P., Williamson A. On primitive permutation groups which contain a cycle // Bull. Austral. Math. Soc. — 1976. — V. 15, № 1. — P. 125–128.
118. Sims C. C. Computation with permutation groups // Proc. 2*nd* Symp. on symbolic and algebraic manipulation. — Assoc. comp. math. V. 4. — New York, 1971.
119. Stanley R. Factorization of permutations into n-cycles // Discrete Math. — 1981. — V. 37. — P. 255–262.
120. Stanley R. On the number of reduced decompositions of elements of Coxeter groups // Eur. J. Comb. — 1985. — V. 5, № 4. — P. 359–372.
121. Van Nuttelen C. Rank and diameter of a graph // Bull. Soc. Math. Belgium. — 1982. — V. B34, № 1. — P. 105–111.
122. Walkup D. W. How many ways can a permutation be factored into two n-cycles // Discrete Math. — 1979. — V. 28. — P. 315–319.
123. Wang Efang. The conditions and methods about expressing permutations as a product of two cycles // Бэйцзин дасьюэ сюэбао. — 1986. — № 5. — P. 26–36.
124. Wernsdorf R. The one-round functions of the DES generate the alternating group // Proc. Eurocrypt-92. — Lect. Notes Comp. Sci. — 1993. — V. 658. — P. 99–112.
125. Wilandt H. Finite permutation groups. — New York: Acad. Press, 1964.
126. Wilson R. M. Graph puzzles, homotopy, and the alternating group // J. Comb. Theory. — 1974. — V. B16. — P. 86–96.
127. Xu Cheng-Hao. The commutators of the alternating group // Scientia Sinica. — 1965. — V. 14, № 3. — P. 339–342.
128. Zieschang T. Combinatorial properties of basic encryption operations // Lect. Notes in Comput. Sci. V. 1233. — Berlin: Springer-Verlag, 1997. — P. 14–26.

Поступило в редакцию 25 IX 1998