УДК 519.688

АЛГОРИТМ РАЗВЕРТКИ В ПОДСЧЕТЕ КОЛИЧЕСТВА S_n^2-ОРБИТ КЭМЕРОНОВСКИХ МАТРИЦ

В. А. Липницкий,
доктор технических наук, профессор,
Военная академия Республики Беларусь
А. И. Сергей
аспирант,
Гродненский государственный университет имени Я. Купалы
Н. В. Спичекова
кандидат физико-математических наук, доцент,
Белорусский государственный университет информатики и радиоэлектроники

В рамках решения третьей проблемы Кэмерона предложен алгоритм подсчета количества орбит на множестве бинарных квадратных матриц порядка n, $n \geq 2$, содержащих в точности n единиц, которые образуются под действием квадрата S_n^2 симметрической группы S_n. Количество орбит вычисляется на основе леммы Бёрнсайда. Для нахождения числа матриц, инвариантных относительно действия фиксированной подстановки, используется линейная развертка бинарной матрицы.

Ключевые слова: (0; 1)-матрицы, симметрическая группа, действие группы на множестве, орбита, мощность орбиты, третья проблема Питера Кэмерона, лемма Бёрнсайда, цикленный тип подстановки.

1. Введение. Матрицы как двумерные массивы информации относятся к базовым объектам высшей математики [1; 2]. Бинарные матрицы, то есть матрицы с элементами 0 и 1, приобрели важное значение в дискретной математике, теории графов и теории групп, теории информации и помехоустойчивом кодировании [3–6]. Английский математик Питер Кэмерон в начале XXI в. обратил внимание на существенную роль в математике класса P_n квадратных (0, 1)-матриц порядка *n*, $n \geq 2$, содержащих в точности *n* единиц, занялся с коллегами систематическим их исследованием [7–9]. Параллельно на исследование этого же класса матриц вышла белорусская школа помехоустойчивого кодирования [10–12]. Определенные общие итоги проведенных исследований подведены в монографии [13].

Мощность класса P_n стремительно растет с ростом *n*. Для эффективной работы с этим классом его следует делить на подклассы каким-то достаточно естественным образом. Одним из общеизвестных систематизаторов здесь является ранг матрицы – классическая матричная характеристика. Однако на классе P_n она оказалась достаточно грубой и весьма неравномерной характеристикой, как показали исследования.

С середины XIX в. в математике приобрела массовое применение идея разбиения множеств на орбиты – классы эквивалентности под действием на этих множествах тех или иных групп. Математические и технические приложения класса P_n показывают, что наиболее естественными преобразованиями матриц этого класса являются перестановки строк между собой или же перестановки столбцов между собой. Иными словами, наибольший интерес для пользователей представляют орбиты на множестве P_n, которые образуются под действием группы $G = S_n^2 = S_n \times S_n$ – квадрата симметрической группы S_n.

Группа S_n подстановок на n элементах – старейший объект в теории групп, исследуется с XVIII в. [14]. Питер Кэмерон уже в XXI вдохнул в эту классическую область новый мощный исследовательский импульс, сформулировав свои 27 проблем в теории подстановок [15]. Третья из них выглядит следующим образом:

Найти общую формулу или алгоритм вычисления количества α_n орбит, на которые разбивается множество P_n под действием группы $G = S_n^2$.

В [16] представлена краткая, но интенсивная история исследования сформулированной проблемы. Решающий рывок здесь принадлежит А.И. Сергею, вычислившему α_n для значений n от 29 до 102. Данная работа посвящена изложению идей, методов и алгоритмов, позволивших получить данный результат, имеющих важное теоретическое и практическое значение. Да и вычислительный их эффект еще далеко не исчерпан. В знак уважения многогранного вклада Питера Кэмерона в рассматриваемую область в дальнейшем матрицы множества P_n будем называть кэмероновскими.

2. Действие группы на множестве. Необходимые сведения. Пусть M – произвольное непустое множество. Через $Simm(M)$ обозначаем симметрическую группу на M, то есть множество всевозможных биекций, взаимно однозначных отображений из множества M в себя, образующих группу относительно операции композиции отображений. Когда M – конечное множество из n элементов, $Simm(M)$ является классической симметрической группой S_n на n элементах, имеющей порядок $n!$, не коммутативной при условии $n > 2$.

Пусть G –произвольная группа. Действием группы G на множестве M называется всякий гомоморфизм $\varphi : G \to Simm(M)$. Другими словами, каждый элемент $g \in G$ определяет взаимно однозначное отображение $\varphi(g) : M \to M$. В частности, в силу свойств гомоморфизмов, образ $\varphi(e_G)$ нейтрального элемента e_G группы G действует тождественно на множестве M для каждого $x \in M$ $(\varphi(e_G))(x) = x$. Конечно, существует определенная вариативность в выборе гомоморфизма φ, то есть в выборе определения действия группы G на множестве M, широта этого выбора определяется спектром нормальных делителей группы G [1, 14].

Мы, однако, за рамки заданного конкретного гомоморфизма φ выходить не будем, будем им пользоваться как незыблемой данностью, и вовсе будем забывать о стоящем где-то у истоков некоем гомоморфизме φ. Поэтому образ точки $x \in M$ при действии $g \in G$ в дальнейшем будем просто обозначать символом $g(x)$.

Для каждой точки $x \in M$ через $St(x)$ обозначаем множество всех тех $g \in G$, для которых $g(x) = x$ и называем его стабилизатором точки x. Легкая проверка критерия подгруппы показывает, что $St(x)$ подгруппа группы G.

Действие G на множестве M определяет естественное бинарное отношение R_G на M: пара элементов $(x, y) \in M \times M$ находится в бинарном отношении R_G, если найдется такое $g \in G$, что $g(x) = y$. Отношение R_G рефлексивно: $e(x) = x$ симметрично в силу наличия взаимно обратных элементов в группе G, транзитивно, благодаря наличию алгебраической операции в группе G. Следовательно, бинарное отношение R_G есть отношение эквивалентности на множестве M.

Всякое отношение эквивалентности на множестве определяет разбиение этого множества на попарно непересекающиеся классы эквивалентности. Классы эквивалентности, определяемые отношением R_G, в теории групп называются орбитами или, если требуется уточнение, G-орбитами. Каждая G-орбита M_i однозначно определяется любым своим фиксированным представителем $x_i \in M_i$: $M_i = \{g(x_i) | g \in G\}$, то есть M_i состоит из всех элементов $g(x_i)$ множества M, которые получаются действием на x_i всех элементов $g \in G$. Тем самым оправдано и другое обозначение G-орбиты M_i – символом $< x_i >$.

Итак, под действием группы G на множестве M каждая точка $x \in M$ образует два объекта: подгруппу $S_t(x)$ в группе G и G-орбиту $< x >$. При этом, как легко видеть, мощности этих двух объектов оказываются тесно взаимосвязанными – мощность орбиты $< x >$ совпадает с индексом стабилизатора $S_t(x_i)$ в группе G

$$|< x >| = [G : St(x)]. \tag{1}$$

Может оказаться, что $S_t(x_i) = \{e\}$ для нейтрального элемента e группы G. Тогда $|M_i| = |G|$ – имеет максимально возможное значение, такая орбита, обычно, называется полной.

Из формулы (1) и из теоремы Лагранжа о конечных группах вытекает следующий факт: для всякой конечной группы G мощность любой ее G-орбиты либо совпадает с $|G|$, либо является делителем порядка $|G|$. Отметим также, что стабилизаторы элементов, принадлежащих одной G-орбите, сопряжены друг с другом: если $y = g(x_i) \in M_i$ для некоторого $g \in G$, то $St(y) = gSt(x_i)g^{-1}$. Отсюда, в частности, следует, что стабилизаторы точек одной G-орбиты равномощны.

Множество M совпадает с объединением своих орбит: $M = \bigcup M_i$. Следовательно, в случае конечного множества M имеет место равенство для мощностей: $|M| = \sum |M_i|$. Получаем выражение мощности множества M полностью через параметры группы G

$$|M| = \sum [G : St(x_i)]. \tag{2}$$

В отдельных ситуациях орбита может совпасть со всем множеством M. Тогда говорят, что группа G действует транзитивно на множестве M. В нашем же случае подобное невозможно, поскольку $|P_n| = C_{n^2}^n = \dfrac{n^2!}{n!\cdot(n^2-n)!} > |S_n^2| = (n!)^2$ для всех $n \geq 2$.

3. Общие формулы для числа орбит при действии конечной группы на конечном множестве. Индекс подгруппы H в конечной группе G вычисляется в силу теоремы Лагранжа весьма просто: $[G:H] = |G|:|H|$. Подставим эту формулу в (1). Получим соотношение

$$|< x_i >||St(x_i)| = |G|. \qquad (3)$$

Просуммируем равенство (3) по всем орбитам, полагая их количество равным числу m. Получим равенство

$$\sum_{i=1}^{m} |< x_i >| \cdot |St(x_i)| = m|G|. \qquad (4)$$

Пусть $m(i)$мощность G-орбиты $< x_i >$, пусть сама орбита $< x_i >$ состоит из точек $x_i = x_{i1}, x_{i2}, \dots, x_{im(i)}$. Как уже отмечалась, $|St(x_i)| = |St(x_{ij})|$ для каждого целого j, $1 \leq j \leq m(i)$. Поэтому равенство (3) превращается в следующую сумму

$$|< x_i >||St(x_i)| = \sum_{j=1}^{m(i)} |St(x_{ij})| = |G|. \qquad (5)$$

Подставим (5) в (4). Получим двойную сумму

$$\sum_{i=1}^{m} \sum_{j=1}^{m(i)} |St(x_{ij})| = m|G|. \qquad (6)$$

Левая часть формулы (6) представляет собой сумму мощностей стабилизаторов всех точек множества M. Изменим нумерацию слагаемых в этой части формулы. Тогда формула (6) приобретет более прозрачную форму:

$$\sum_{k=1}^{|M|} |St(x_k)| = m|G|. \qquad (7)$$

Из равенства (7) непосредственно следует первая формула для числа G-орбит – количество орбит равно средневзвешенной мощности стабилизаторов точек множество M:

$$m = \frac{1}{|G|} \sum_{k=1}^{|M|} |St(x_k)|. \qquad (8)$$

Левая часть формулы (7) по-прежнему остается двойной суммой (из формулы (6)). Перемена порядка суммирования в ней приводит к новому объекту в действии группы на множестве – множеству неподвижных точек: для каждого $g \in G$ через $Inv(g)$ обозначаем множество всех точек $x \in M$, которые g оставляет на месте: $g(x) = x$.

Тогда формулу (7) можно переписать в виде

$$\sum_{l=1}^{|G|}|Inv(g_l)| = m|G|. \tag{9}$$

Из равенства (9) непосредственно следует вторая формула для числа G-орбит – количество орбит равно средневзвешенной мощности множеств неподвижных точек элементов группы G:

$$m = \frac{1}{|G|}\sum_{l=1}^{|G|}|Inv(g_l)|. \tag{10}$$

Формула (10) носит в литературе название леммы Бёрнсайда.

Уильям Бёрнсайд (2.07.1852 – 21.08.1927) – знаменитый английский математик-алгебраист, шотландского происхождения, один из создателей теории представлений и характеров в теории групп, теории конечных групп [17]. Второе издание этой книги, значительно расширенное, дополненное главой о характерах групп, стало эталоном на многие десятилетия в теории конечных групп. Две сформулированные У. Бернсайдом проблемы о конечных группах будоражили математические умы весь двадцатый век [18].

Лемма о числе орбит, о которой шла выше речь, опубликована уже в первом издании книги [17]. Однако она была давно известна в математических кругах, так как существовали ее доказательства, принадлежавшие перу немецкого математика Фердинанда Георга Фробениуса (26.10.1849 – 3.08.1917) – доказательство 1887 г., а также перу великого французского математика и механика Огюстена Луи Коши (21.08.1789 – 23.05.1857) – доказательство 1845 г. Собственно, У. Бернсайд и не претендовал на ее авторство. Однако же первая публикация, оттенившая роль данного утверждения, имеет, как правило, свою магию и свои законы. Поэтому не удивительно, что некоторые щепетильные математики в своих монографиях и учебниках иногда именуют обсуждаемое утверждение вполне справедливо "леммой не Бернсайда".

Именно формулу (10) мы берем в качестве основной для вычисления количества $m = \alpha_n$ орбит множества $M = P_n$

$$\alpha_n = \frac{1}{(n!)^2}\sum_{l=1}^{(n!)^2}|Inv(g_l)|. \tag{11}$$

Главное достоинство формулы (11) в унификации и стандартизации вычисляемого параметра – для каждого элемента $g \in G = S_n \times S_n$ мы должны вычислить $Inv(g)$ – количество кэмероновских матриц, инвариантных относительно действия g. Ниже мы убедимся, что количество реально вычисляемых слагаемых формулы (11) существенно ниже заявленного числа $(n!)^2$. Но сначала мы проведем еще одну унификацию – ликвидируем различие между строками и столбцами, вложив группу $G = S_n \times S_n$ и в стандартную симметрическую группу S_{n^2}.

4. Линейная развертка кэмероновских матриц и квадрата симметрической группы. Откажемся от традиционной двойной индексации элементов кэмероновских матриц.

Пусть

$$A=\begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_{n+1} & a_{n+2} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n(n-1)+1} & a_{n(n-1)+2} & \dots & a_{n^2} \end{pmatrix} \in P_n. \qquad (12)$$

Имея на руках такую запись матрицы, несложно осуществить ее линейную развертку – представить матрицу A в виде одной вектор-строки $\overline{x}_A = (a_1, a_2, \dots, a_{n^2})$ из векторного пространства размерностью n^2

Возьмем произвольный элемент $g \in G = S_n \times S_n$. Тогда

$$g(A)=\begin{pmatrix} a_{m_1} & a_{m_2} & \dots & a_{m_n} \\ a_{m_{n+1}} & a_{m_{m+2}} & \dots & a_{m_{2n}} \\ \dots & \dots & \dots & \dots \\ a_{m_{n(n-1)+1}} & a_{m_{n(n-1)+2}} & \dots & a_{m_{n^2}} \end{pmatrix} \in P_n$$ и элементу g можно поставить в соответствие подстановку

$$h(g)=\begin{pmatrix} \dots & m_1 & \dots & m_2 \dots m_{n^2} & \dots \\ \dots & 1 & \dots & 2 \ \dots n^2 & \dots \end{pmatrix} \in S_{n^2}. \qquad (13)$$

Подстановку $h(g)$ задаваемую формулой (13), будем называть матричной подстановкой, построенной по элементу g. Множество всех матричных подстановок образует подгруппу $h(G)$ в группе S_{n^2}, разумеется, изоморфную группе G. В силу классических результатов теории подстановок [1, 14, 19] имеет место

Предложение 1. *Для всякой подстановки* $g = g_1 \cdot g_2 \in G = S_n \times S_n$ *и разложения сомножителей в произведения независимых циклов:*

$$g_1 = C_1^1 C_2^1 \dots C_k^1;\ g_2 = C_1^2 C_2^2 \dots C_\mu^2 \qquad (14)$$

подстановка $h(g)$ *имеет точно такое же разложение в* $n(k+\mu)$ *зависимых циклов; каждая n-ка этих циклов имеет длину, совпадающую с длиной одного из циклов разложения* (14). Верно и обратное.

Пример 1. Пусть $n=4$, $g=(g_1,g_2)\in S_n\times S_n$, где $g_1=\begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix}$,

$g_2=\begin{pmatrix}1&2&3&4\\1&4&2&3\end{pmatrix}$. Здесь $A=\begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_5 & a_6 & a_7 & a_8 \\ a_9 & a_{10} & a_{11} & a_{12} \\ a_{13} & a_{14} & a_{15} & a_{16} \end{pmatrix} \in P_n$ и $g(A)=\begin{pmatrix} a_1 & a_3 & a_4 & a_2 \\ a_5 & a_7 & a_8 & a_6 \\ a_{13} & a_{15} & a_{16} & a_{14} \\ a_9 & a_{11} & a_{12} & a_{10} \end{pmatrix}$;

Равенства (14) в данном случае имеют вид: $g_1 = (3\ 4)$; $g_2 = (2\ 4\ 3)$. Тогда в соответствии с предложением 1 имеем: Перемножим эти циклы между собой. Получим типичную подстановку из группы S_{16}

$$h(g)=\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 1 & 4 & 2 & 3 & 5 & 8 & 6 & 7 & 13 & 16 & 14 & 15 & 9 & 12 & 10 & 11 \end{pmatrix}.$$

Как элемент S_{16} разложим эту подстановку в произведение независимых циклов. Получим $h(g) = (1)(5)(2\ 4\ 3)(6\ 8\ 7)(9\ 13)(10\ 16\ 11\ 14\ 12\ 15)$.

Аналогично примеру 1 строится разложение в произведение независимых циклов любой матричной подстановки

$$h(g) = C_1 C_2 \cdot \ldots \cdot C_k. \qquad (15)$$

Если матрица $A \in P_n$, то вектор $\bar{x}_A = (a_1, a_2, \ldots, a_{n^2})$ содержит в точности n единиц. Любая матричная подстановка, как и любая подстановка из S_{n^2} только переставит их местами, не меняя их количества. Более того, имеет место

Предложение 2. *Пусть в разложении (15) присутствуют все циклы, в частности, и циклы длиной 1. Тогда:*

1) если l_i длина цикла C_i, $1 \le i \le k$, то $l_1 + l_2 + \ldots + l_k = n^2$;

2) следовательно, для всякой матрицы $A \in P_n$, каждая координата вектора $\bar{x}_A = (a_1, a_2, \ldots, a_{n^2})$ принадлежит в точности своему одному единственному циклу C_i, $1 \le i \le k$;

3) матрица $A \in P_n$, принадлежит $Inv(g)$ в том и только том случае, когда все элементы матрицы A, соответствующие отдельно взятому циклу C_j, $1 \le j \le k$, равны между собой, то есть либо все равны 0, *либо все они равны* 1.

4) если матрица $A \in P_n$, принадлежит $Inv(g)$, а элементы 1 этой матрицы принадлежат только циклам с номерами $i_1, i_2, \ldots, i_s$, то в таком случае

$$l_{i_1} + l_{i_2} + \ldots + l_{i_s} = n. \qquad (16)$$

Соотношение (16) является довольно жестким и не всегда может выполняться. Свидетельством сказанному является

Пример 2. Пусть $n = 5$, $g = (g_1, g_2) \in S_n \times S_n$, где $g_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$,

$g_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$. Вычисления показывают, что здесь

$h(g) = (1\ 7\ 13\ 16\ 22\ 3\ 6\ 12\ 18\ 21\ 2\ 8\ 11\ 17\ 23)(4\ 10\ 14\ 20\ 24\ 5\ 9\ 15\ 19\ 25)$ – произведение двух независимых циклов длиной 10 и 15. Следовательно, $Inv(g)$ пусто для данной подстановки g.

Из предложения 2 непосредственно вытекает следующий способ вычисления мощности $|Inv(g)|$: имеем полный список всех длин циклов

$$\{l_1,\ \ l_2,\ \ \ldots\ \ l_k\} \tag{17}$$

из равенства (15) (включая и все циклы длиной 1, в этом списке может быть много одинаковых чисел), из чисел этого списка длин следует составить всевозможные, отличающиеся друг от друга хотя бы одним индексом, суммы (16). Количество таких сумм будет совпадать с величиной $|Inv(g)|$.

Рассмотрим более подробно методику вычисления мощности $|Inv(g)|$ множества $Inv(g)$, базирующуюся на разложении подстановки $h(g)$ в произведение независимых циклов.

5. Алгоритм вычисления мощности матричных подстановок на основе их цикленного разложения. Зафиксируем величину n и подстановку $g \in G$. Подобно тому, как в вычислениях с целыми числами используется не просто разложение натурального числа в произведение простых множителей, а более точное каноническое разложение этого числа, так и здесь, вместо разложений (14) и (15) мы будем опираться на их более точные варианты.

Пусть в равенстве (15) присутствуют все циклы, в том числе и длиной 1, пусть эти циклы упорядочены по возрастанию их длин так, что $l_1 \geq 1$; $l_i \leq l_j$ при $i < j$. Как показывает пример 1, в разложении (15) может встречаться достаточно много циклов одинаковой длины. Пусть в (15) присутствуют циклы t различных длин, $1 \leq t \leq k$. Пусть циклы $C_1, C_2, \ldots, C_{i_1}$ имеют длину $l_1 = l_2 = \ldots = l_{i_1} \geq 1$, циклы $C_{i_1+1}, C_{i_1+2}, \ldots, C_{i_2}$ имеют длину $l_{i_1+1} = l_{i_1+2} = \ldots = l_{i_2} > l_1$, и так далее, циклы $C_{i_{t-1}+1}, C_{i_{t-1}+2}, \ldots, C_{i_t} = C_k$ имеют длину $l_{i_{t-1}+1} = l_{i_{t-1}+2} = \ldots = l_{i_t} = l_k > l_{i_{t-1}}$.

Также детализируем обозначение элементов последовательности (17) символами $l_{11}, l_{12}, \ldots, l_{1c_1}, \ldots, l_{i1}, l_{i2}, \ldots, l_{ic_i}, \ldots, l_{s1}, l_{s2}, \ldots, l_{sc_s}$, где $l_{i1} = l_{i2} = \ldots = l_{ic_i}$; $1 \leq i \leq s \leq k$. Через L_i, $1 \leq i \leq k$, условимся в дальнейшем обозначать множество $L_i = \{l_{11}, l_{12}, \ldots, l_{1c_1}, \ldots, l_{i1}, l_{i2}, \ldots, l_{ic_i}\}$ – часть циклов последовательности (17), длины которых находятся в пределах от 1 до i включительно.

Через $f_{i,j}$ обозначим количество способов представить число j в виде суммы, используя в качестве слагаемых только числа множества L_i, причем каждый элемент множества L_i может входить в упомянутую сумму не более одного раза. Будем полагать, что $f_{0,0} = 1$, $f_{i,0} = 1$, $i > 1$, $f_{0,j} = 0, j \neq 0$. Для вычисления $f_{i,j}$ все способы представления числа j можно разбить на непересекающиеся классы в зависимости от того, сколько слагаемых, равных l_{i1}, будет содержать результирующая сумма. Если при этом результирующая сумма содержит q слагаемых, равных l_{i1}, то количество способов представить j в требуемом виде будет равно $C_{c_i}^q f_{i-1,j-ql_{i1}}$, поскольку число ql_{i1} уже выбрано, а из чисел множества L_{i-1} нужно набрать сумму, равную $j - ql_{i1}$. Множитель $C_{c_i}^q$ равен числу способов выбрать q из c_i циклов длиной l_i для размещения в них единиц. Так как рассматриваемые классы не пересекаются, то получаем следующую рекуррентную формулу

$$f_{i,j} = \sum_{q,\, j-ql_{i1} \geq 0} C_{c_i}^q f_{i-1,j-ql_{i1}}. \tag{18}$$

Из вышесказанного следует

Предложение 3. $|Inv(g)| = f_{s,n}$, *где s – это количество различных длин циклов в разложении (15), не превосходящих n.*

В силу формулы (18) на практике вычисление осуществляется последовательно, составлением таблицы значений $f_{i,j}$, начиная с $f_{0,0}$, постепенно наращивая значения *i* и *j* до достижения значения $f_{s,n}$ из предложения 3. Для надежности, можно вычисления проводить без возможных пропусков значений *i* и *j* до величины $f_{n,n}$.

Пример 3. Найдем $|Inv(g)|$ для подстановки *g* из примера 1. Из найденного там разложения $h(g) = (1)(5)(9,13)(2,4,3)(6,8,7)(10,16,11,14,12,15)$. Следовательно, список (17) в данном случае имеет вид: 1,1,2,3,3,6 и $s = 3$ Легко видеть, что искомая мощность равна 5. Действие же по алгоритму сводится к последовательному заполнению строк табл. 1 в соответствии с легкими вариантами формулы (18).

Таблица 1 – Значения f_{ij}, $0 \le i \le s = 3$; $0 \le j \le n = 4$; **для примера 2**

$i \backslash j$	0	1	2	3	4
0	1	0	0	0	0
1	1	2	1	0	0
2	1	2	2	2	1
3	1	2	2	4	5

Так как $f_{3,4} = 5$, то для данной подстановки *g* существует в точности 5 неподвижных точек. Каждая неподвижная точка представляет собой матрицу из множества $P_n = P_4$, все единицы в которой заполняют циклы длиной 1,1,2 или 1, 3 из разложения подстановки *h*(*g*). Выпишем неподвижные точки элемента *g*: существует единственная матрица, единицы которой заполняют циклы $(1), (5), (9,13)$ длиной 1, 1, 2 в разложении *h*: $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$; существует четыре матрицы, единицы в которых заполняют пары циклов $(1), (2,4,3)$; $(1), (6,8,7)$; $(5), (2,4,3)$; $(5), (6,8,7)$ длиной 1, 3 из разложения подстановки матрицы *h*:

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Для вычисления точного значения α_4 по приведенному алгоритму следует подобные вычисления таблиц типа табл. 1 провести, вообще говоря, еще для $(4!)^2 - 1 = 575$ подстановок. Правда, выписывать явно инвариантные матрицы при этом вовсе не обязательно.

Для тождественной подстановки $e \in S_n$ подставка $e = (e, e)$ является тождественной в $G = S_n^2$, а подстановка $h(e)$ будет нейтральным элементом в группе $h(G) \subset S_{n^2}$. Отсюда легко видеть, что $|Inv(e)| = |P_n| = C_{n^2}^n$ – общая формула для всех значений *n*. Наверняка найдутся и другие виды подстановок *g* с подобными формулами для $|Inv(g)|$. Мы, однако, оставим этот вопрос для отдельных исследований и перейдем к рассмотрению другого общего подхода сокращения вычислений α_n, который предоставляет общая теория подстановок.

6. Цикленный тип подстановки. Пусть $A = (a_i) \in P_n$, $g = (g_1, g_2) \in S_n \times S_n$ и $g_i = C_1^{g_i} ... C_{k_i}^{g_i}$, $i = 1,2,$– разложение g_i в произведение независимых циклов, содержащее, в том числе, и циклы длиной 1. Через $|C_i^{g_i}|$ будем обозначать длину цикла $C_i^{g_i}$.

Предложение 4. *Пусть в разложении (15) матричной подстановки h(g) в произведение независимых циклов присутствуют все циклы, в том числе и циклы длиной 1. Тогда:*

1) индексы элементов матрицы A, которые расположены на пересечении строк и столбцов, входящих в циклы $C_i^{g_1}$ *и* $C_j^{g_2}$, *будут образовывать*

$$\frac{|C_i^{g_1}||C_j^{g_2}|}{НОК(|C_i^{g_1}|,|C_j^{g_2}|)} \tag{19}$$

циклов в разложении (15);

2) длина каждого цикла равна $НОК(|C_i^{g_1}|,|C_j^{g_2}|)$.

Доказательство. Возьмем элемент a_i матрицы *A*. Пусть строка и столбец, на пересечении которых расположен a_i, входят в циклы $C_i^{g_1}$ *и* $C_j^{g_2}$. Пусть в результате действия *g* элемент a_i будет располагаться на месте элемента a_{i_1} матрицы *A*, a_{i_1} – на месте a_{i_2}, …, a_{i_u} – на месте a_i. Тогда индексы элементов a_i, a_{i_1}, a_{i_2}, …, a_{i_u} будут образовывать один цикл в разложении (15). Чтобы получить матрицу *g*(*A*) можно действовать так: вначале переставить строки матрицы *A* в соответствии с подстановкой g_1, а затем в результирующей матрице переставить столбцы в соответствии с подстановкой g_2. Поэтому в цикл $C_i^{g_1}$ ($C_j^{g_2}$) будут входить те и только те строки (столбцы) матрицы *A*, в которых располагаются элементы a_i, a_{i_1}, a_{i_2}, …, a_{i_u}.

Представим, что элемент a_i "перемещается" по матрице *A* в соответствии с циклами $C_i^{g_1}$ и $C_j^{g_2}$, а именно: пусть вначале a_i перейдет на место элемента a_{i_1} затем – на место элемента a_{i_2}, …, на место элемента a_{i_u} и, наконец, вернется на свое место. За время такого "путешествия" a_i "опишет" цикл, образованный индексами элементов a_i, a_{i_1}, a_{i_2}, …, a_{i_u} в разложении (15). При этом a_i посетит все строки и столбцы матрицы *A*, входящие в циклы $C_i^{g_1}$ и $C_j^{g_2}$, и вернется на свое первоначальное место. За один "шаг" a_i "посещает" только одну строку и столбец. Поэтому, чтобы вернуться на свое первоначальное место, a_i нужно выполнить $НОК(|C_i^{g_1}|,|C_j^{g_2}|)$ шагов, т. е. длина соответствующего цикла в разложении (15) будет равна $НОК(|C_i^{g_1}|,|C_j^{g_2}|)$. В матрице *A* на пересечении строк и столбцов, входящих в циклы $C_i^{g_1}$ и $C_j^{g_2}$ располагается $|C_i^{g_1}||C_j^{g_2}|$ элементов. Поэтому число циклов разложения (15), которые образованы элементами матрицы A, стоящими на пересечении строк и столбцов, входящих в циклы $C_i^{g_1}$ и $C_j^{g_2}$ находится по формуле (19). Доказательство завершено.

Согласно [14], стр. 17, последовательность $\mu_1, \mu_2, \ldots, \mu_n$ мощностей множеств циклов длиной $i, 1 \le i \le n$, в разложении подстановки $g \in S_n$ называется цикленным типом данной подстановки. Будем говорить, что две подстановки относятся к одному цикленному типу, если они имеют одинаковое количество циклов одинаковой длины. Сопряженные подстановки, очевидно, относятся к одному цикленному типу. Согласно теореме 2 из главы 1 [14], верно и обратное утверждение. Подобное утверждение для $G = (S_{n^2})$ и $h(G)$ требует уточнений.

Предложение 5. *Пусть* $g = (g_1, g_2)$, $f = (f_1, f_2) \in G = S_n^2$ *– две подстановки, у которых пара* g_1, f_1 *одного цикленного типа и пара* g_2, f_2 *также одного (но своего) цикленного типа. Тогда* $h(g)$ *и* $h(f)$ *– также подстановки одного цикленного типа в группе* S_{n^2}.

Доказательство. Зафиксируем разложения $g_i = C_1^{g_i} \ldots C_{k_{g_i}}^{g_i}$ и $f_i = C_1^{f_i} \ldots C_{k_{f_i}}^{f_i}, i = 1,2,$ в произведения независимых циклов, включающие, в том числе, и циклы длиной 1. Так как g_i и $f_i, i = 1,2,$ – подстановки одного цикленного типа, то для каждой пары циклов $C_p^{g_1}$ и $C_q^{g_2}$ найдется пара циклов $C_u^{f_1}$ и $C_v^{f_2}$ таких, что $|C_p^{g_1}| = |C_u^{f_1}|, |C_q^{g_2}| = |C_v^{f_2}|$. Обратное также верно.

В соответствии с предложением 4, индексы элементов матрицы $A \in P_n$, которые располагаются на пересечении строк и столбцов, входящих в циклы $C_p^{g_1}$, $C_q^{g_2}$ или $C_u^{f_1}$, $C_v^{f_2}$, образуют одно и то же число циклов одинаковой длины в разложениях $h(g)$ и $h(f)$. Значит, $h(g)$ и $h(f)$ являются подстановками одного цикленного типа в группе S_{n^2}. Доказательство завершено.

Предложение 6. Если g_1 *и* g_2, $g_1, g_2 \in G = S_n^2$, *– подстановки одного цикленного типа, то* $|Inv(g_1)| = |Inv(g_2)|$.

Доказательство следует из предложений 3, 5 и формулы (18) для $f_{s,n}$.

Предложение 7. *Пусть в подстановке из n элементов имеется* c_i *циклов длины* $l_i, i = \overline{1,k}$. *Тогда количество подстановок такого же цикленного типа равно* $n!\prod_{i=1}^{k}\left(c_i! l_i^{c_i}\right)^{-1}$.

Доказательство. Пусть подстановка $g \in S_n$ содержит c_i циклов длины $l_i, i = 1, \ldots, k$. Можно полагать, что в представлении g в виде произведения циклов вначале располагаются все циклы длиной l_1, затем – все циклы длиной l_2 и т. д. Всего существует $n!$ способов расставить n чисел по имеющимся циклам. Однако в некоторых случаях получающиеся подстановки будут различными записями одной и той же подстановки, а именно:

цикл длины $l_i, i = 1,...,k$ может быть представлен l_i различными способами, в зависимости от того, с чего начинать перечислять элементы цикла. Для того, чтобы учесть все такие представления только один раз, необходимо $n!$ разделить на каждое из возможных значений l_i. В результате будет получена величина $n!\prod_{i=1}^{k}\left(l_i^{c_i}\right)^{-1}$;

при замене местами циклов одной длины получаются различные записи одной и той же подстановки, т. е. для циклов длины l_i существует $c_i!$ вариантов их расстановки, которые нужно учесть только один раз. Для этого $n!\prod_{i=1}^{k}\left(l_i^{c_i}\right)^{-1}$ нужно разделить на $c_i!$ для каждого i. Доказательство предложения 7 завершено.

Следующий классический результат теории подстановок имеет важнейшее для нас значение, а потому приводится его практически дословная формулировка.

Предложение 8 ([14], Глава 1, следствие 1 из теоремы 2). *Количество различных цикленных типов подстановок на множестве длиной n совпадает с $p(n)$ – числом неупорядоченных разбиений числа n, т. е. количеством способов представить n в виде суммы положительных целых чисел.*

Явный рекуррентный вид и свойства функции представлены в монографиях [20, глава 1], [21, глава 4].

Следствие. *В группе $G = S_n^2$ имеется не более $p^2(n)$ различных цикленных типов подстановок.*

К примеру, $p(4) = 5$ следовательно, $p^2(4) = 25$ и для нахождения α_4 понадобится реально составление не более 25 таблиц вида табл. 1. Рассмотренный метод развертки показал свою эффективность на практике, позволив существенно увеличить таблицу значений величины α_n.

7. Оценка сложности алгоритма развертки.

Предложение 9. *Вычисление $f_{s,n}$ по формуле (18) требует выполнения $O(n^2 \log(n))$ операций.*

Доказательство. Оценим количество операций сложения, которые необходимо выполнить для вычисления $f_{s,n}$ по формуле (18). Для фиксированной величины j, $1 \le j \le n$, q может принимать одно из $\left[\frac{j}{l_{i1}}\right]+1$ значений. Просуммировав эту величину по i, получим $\sum_{i=1}^{s}\left(\left[\frac{j}{l_{i1}}\right]+1\right)$. Так как при любом i выполняется $l_{i1} \ge i$,

то $\sum_{i=1}^{s}\left(\left[\frac{j}{l_{i1}}\right]+1\right) \le \sum_{i=1}^{s}\left(\frac{j}{l_{i1}}+1\right) \le \sum_{i=1}^{s}\left(\frac{j}{i}+1\right) \le \sum_{i=1}^{n}\left(\frac{j}{i}+1\right) = \sum_{i=1}^{n}\frac{j}{i}+n \le \sum_{i=1}^{n}\frac{n}{i}+n = O(n\log n).$

Последнее равенство вытекает из того, что сумма гармонического ряда имеет логарифмическую асимптотику [22, с. 270]. Так как $1 \le j \le n$, то количество операций, которые необходимо выполнить при вычислении $f_{s,n}$ по формуле (18) не превосходит $O(n^2 \log(n))$. Доказательство завершено.

Следствие. *Количество орбит множества P_n может быть найдено за $O(p^2(n)n^2 \log(n))$ операций.*

Доказательство. Рассмотрим пару p_i и p_j разбиений (возможно, совпадающих между собой) числа n. p_i и p_j задают цикленный тип подстановок $g_i, g_j \in S_n$. Используя формулу (19), несложно определить цикленный тип подстановки $g_{ij} = (g_i, g_j) \in G = S_n \times S_n$. В соответствии с предложением 3, количество $|Inv(g_{ij})|$ неподвижных точек подстановки g_{ij} совпадает с $f_{s,n}^{g_i,g_j}$ и вычисляется по формуле (18). Количество $k_{p_t}, t = i, j$, подстановок множества S_n, имеющих такой же цикленный тип, как и подстановка g_t может быть вычислена в соответствии с предложением 7. Тогда формулу (11) для вычисления числа α_n орбит множества P_n, можно переписать так:

$$\alpha_n = \frac{1}{(n!)^2} \sum_{i,j=1}^{p(n)} f_{s,n}^{g_i,g_j} k_{p_i} k_{p_j}. \qquad (20)$$

Так как вычисление $f_{s,n}^{g_i,g_j}$, в соответствии с предложением 9, требует $O(n^2 \log(n))$ операций и сумма в правой части формулы (20) содержит $p^2(n)$ слагаемых, то вычисление α_n требует $O(p^2(n)n^2 \log(n))$ операций, что и требовалось доказать.

Пример 4. Вычислим α_n при $n = 4$. Для числа 4 существует пять разбиений: $p_1 = \{1,1,1,1\}$, $p_2 = \{2,1,1\}$, $p_3 = \{2,2\}$, $p_4 = \{3,1\}$, $p_5 = \{4\}$. Пусть цикленный тип подстановки $g_i \in S_4, i = 1,2,3,4,5$ задается множеством p_i. Для определенности будем считать, что $g_1 = (1)(2)(3)(4)$, $g_2 = (1\,2)(3)(4)$, $g_3 = (1\,2)(3\,4)$, $g_4 = (1\,2\,3)(4)$, $g_5 = (1\,2\,3\,4)$. В соответствии с предложением 7, количество $k_{p_i}, i = 1,2,3,4,5$, подстановок множества S_4, имеющих такой же цикленный тип, как подстановка g_i будет равно: $k_{p_1} = \frac{4!}{4!\cdot 1^4} = 1$, $k_{p_2} = \frac{4!}{2!\cdot 1^2 \cdot 1!\cdot 2^1} = 6$, $k_{p_3} = \frac{4!}{2!\cdot 2^2} = 3$, $k_{p_4} = \frac{4!}{1!\cdot 1^2 \cdot 1!\cdot 3^1} = 8$, $k_{p_5} = \frac{4!}{1!\cdot 4^1} = 6$. Для каждой пары g_i, g_j определим цикленный тип подстановки $g_{ij} = (g_i, g_j) \in G = S_4 \times S_4$, используя формулу (19), и вычислим $|Inv(g_{ij})|$. Результаты вычислений представлены в таблице 2.

Таблица 2 – Мощность множеств $Inv(g_{ij})$

g_{ij}	Цикленный тип подстановки $h(g_{ij})$	$\lvert Inv(g_{ij})\rvert$
(g_1,g_1)	1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1	1820
(g_1,g_2), (g_2,g_1)	1, 1, 1, 1, 1, 1, 1, 1, 2, 2, 2, 2	188
(g_1,g_3), (g_2,g_3), (g_3,g_1), (g_3,g_2), (g_3,g_3)	2, 2, 2, 2, 2, 2, 2, 2	28
(g_1,g_4), (g_4,g_1)	1, 1, 1, 1, 3, 3, 3, 3	17

Окончание таблицы 2

g_{ij}	Цикленный тип подстановки $h(g_{ij})$	$\lvert Inv(g_{ij})\rvert$
(g_1,g_5), (g_2,g_5), (g_3,g_5), (g_5,g_1), (g_5,g_2), (g_5,g_3), (g_5,g_5)	4, 4, 4, 4	4
(g_2,g_2)	1, 1, 1, 1, 2, 2, 2, 2, 2, 2	52
(g_2,g_4),(g_4,g_2)	1, 1, 2, 3, 3, 6	5
(g_3,g_4), (g_4,g_3)	2, 2, 6, 6	1
(g_4,g_4)	1, 3, 3, 3, 3, 3	5
(g_4,g_5), (g_5,g_4)	4, 12	1

Применим формулу (20) для вычисления α_4:

$$\alpha_4=\frac{1}{(4!)^2}(1820\cdot1\cdot1+188\cdot1\cdot6+28\cdot1\cdot3+17\cdot1\cdot8+4\cdot1\cdot6+188\cdot6\cdot1+52\cdot6\cdot6+28\cdot6\cdot3+$$
$$+5\cdot6\cdot8+4\cdot6\cdot6+28\cdot3\cdot1+28\cdot3\cdot6+28\cdot3\cdot3+1\cdot3\cdot8+4\cdot3\cdot6+17\cdot8\cdot1+5\cdot8\cdot6+1\cdot8\cdot3+$$
$$+5\cdot8\cdot8+1\cdot8\cdot6+4\cdot6\cdot1+4\cdot6\cdot6+4\cdot6\cdot3+1\cdot6\cdot8+4\cdot6\cdot6)=16.$$

Полученное значение α_4 совпадает с четвертым членом последовательности A049311 [16].

8. Заключение. В работе предложен алгоритм подсчета количества орбит α_n, на которые разбивается множество P_n квадратных (0, 1) матриц под действием квадрата S_n^2 симметрической группы S_n. Алгоритм основан на лемме Бёрнсайда, применение которой требует вычисления количества $|Inv(g)|$ матриц множества P_n, инвариантных относительно действия подстановки g для каждого $g=(g_1,g_2)\in S_n^2$. Показано, что если известен цикленный тип подстановки g, то $|Inv(g)|$ может быть вычислено по реккурентной формуле. Цикленный тип подстановки g определяется по цикленным типам подстановок $g_1,g_2\in S_n$.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. ***Кострики, А. И.*** Введение в алгебру / А. И. Кострикин. – Москва : Наука, 1977. – 496 с.
2. ***Липницкий, В. А.*** Высшая математика. Основы линейной алгебры и аналитической геометрии / В. А. Липницкий. – Минск : ВА РБ, 2015. – 229 с.
3. ***Яблонский, С. В.*** Введение в дискретную математику / С. В. Яблонский. – Москва : Наука, 1986. – 384 с.
4. ***Оре, О.*** Теория графов / О. Оре. – Москва : Наука, 1980. – 336 с.
5. ***Самсонов, Б.Б.*** Теория информации и кодирование / Б. Б. Самсонов, Е. М. Плохов, А. И. Филоненков, Т. В. Кречет. – Ростов-на-Дону : Феникс, 2002. – 288 с.
6. ***Мак-Вильямс, Ф. Дж.*** Теория кодов, исправляющих ошибки / Ф. Дж. Мак-Вильямс, Н. Дж. А. Слоэн. – Москва : Связь, 1979. – 744 с.
7. ***Cameron, P. J.*** Sequences realized by oligomorphic permutation groups / P. J. Cameron // Integer Sequences, 2000. – Vol. 3(1). – Article 00.1.5. – [Электронный ресурс] – Режим доступа: https://cs.uwaterloo.ca/journals/JIS/VOL3/groups.html. – Дата доступа: 07.02.2017.

8. ***Cameron, P. J.*** Asymptotics for incidence matrix classes / P. J. Cameron, T. Prellberg, D. Stark // The Electronic Journal of Combinatorics, 2006. – Vol. 13.1. – [Электронный ресурс] – Режим доступа: http://www.combinatorics.org/ojs/index.php/eljc/article/view/v13i1r85/pdf. – Дата доступа: 07.02.2017.
9. ***Cameron, P. J.*** Product action / P. J. Cameron, D. A. Gewurz, F. Merola // Discrete Math., 2008. – No. 308. – Pp. 386–394.
10. ***Конопелько, В. К.*** Классификация векторов-ошибок при двумерном кодировании информации / В. К. Конопелько, О. Г. Смолякова // Доклады БГУИР. – 2008. – № 7(37). – С. 19–28.
11. ***Конопелько, В. К.*** Действие квадрата симметрической группы на специальном классе (0; 1)-матриц. Отсутствие полных орбит / В. К. Конопелько, В. А. Липницкий, Н. В. Спичекова // Доклады БГУИР. – 2010. – № 5(54). – С. 40–46.
12. ***Конопелько, В. К.*** Классификация точечных образов и классическая проблема разбиения чисел / В. К. Конопелько, В. А. Липницкий, Н. В. Спичекова // Доклады БГУИР. – 2010. – № 8(57). – С. 127–154.
13. ***Цветков, В. Ю.*** Предсказание, распознавание и формирование образов многоракурсных изображений с подвижных объектов / В. Ю. Цветков, В. К. Конопелько, В. А. Липницкий. – Минск : Издательский центр БГУ, 2014. – 224 с.
14. ***Супруненко, Д. А.*** Группы подстановок / Д. А. Супруненко. – Минск : Навука і тэхніка, 1996. – 368 с.
15. ***Cameron, P. J.*** Problems on permutation groups // P. J. Cameron – [Электронный ресурс] – Режим доступа: http://www.maths.qmul.ac.uk/~pjc/pgprob.html. – Дата доступа: 07.02.2017.
16. The On-Line Encyclopedia of Integer Sequences. – [Электронный ресурс] – Режим доступа: http://oeis.org/. – Дата доступа: 07.02.2017.
17. ***Burnside, William.*** Theory of groups of finite orders. – Cambridge : At The University Press, 1897. – 430 P.; 2 ed. – Cambridge, 1911; Repr. – N.Y. : Dover, 1955.
18. ***Кострикин, А.И.*** Вокруг Бернсайда / А. И. Кострикин. – Москва : Наука, 1986. – 232 с.
19. ***Липницкий, В. А.*** Современная прикладная алгебра. Математические основы защиты информации от помех и несанкционированного доступа / В. А. Липницкий. – Минск : БГУИР, 2006. – 88 с.
20. ***Эндрюс, Г.*** Теория разбиений / Г. Эндрюс. – Москва : Наука, 1982. – 256 с.
21. ***Холл, М.*** Комбинаторика / М. Холл. – Москва : Мир, 1970. – 424 с.
22. ***Фихтенгольц, Г. М.*** Курс дифференциального и интегрального исчисления. Том 2 / Г. М. Фихтенгольц. – Москва : Физматлит, 2001. – 810 с.

Поступила в редакцию 30.03.2017 г.
Контакты: valipnitski@yandex.ru (Липницкий Валерий Антонович)

Lipnitski V., Sergey A., Spichekova N. UNWINDING ALGORITHM TO CALCULATE NUMBER OF S_n^2-ORBITS FOR CAMERON MATRICES.

In addressing the third Cameron's problem, the authors offer an algorithm to calculate the number of orbits in the set of binary square matrices of order n, $n \geq 2$ with n ones that are formed under the action of square S_n^2 of the symmetric group S_n. The number of orbits is calculated on the basis of Burnside's lemma. A linear unwinding of a binary matrix is used to determine the number of matrices that are invariant with respect to a fixed substitution.

Keywords: binary matrix, symmetric group, orbit, orbit cardinality, the third Peter Cameron's problem, Burnside's lemma, orbital type of a substitution.