УДК 519.688

ДИНАМИЧЕСКОЕ ПРОГРАММИРОВАНИЕ В МЕТОДЕ РАЗВЕРТКИ РЕШЕНИЯ ТРЕТЬЕЙ ПРОБЛЕМЫ КЭМЕРОНА

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

Рассматривается модификация предложенного ранее авторами алгоритма развертки для вычисления 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. Предлагаемая модификация алгоритма требует выполнения $O(p(n)n^4)$ арифметических операций, где p(n) – количество неупорядоченных разбиений числа n.

Ключевые слова: бинарная матрица, симметрическая группа, орбита, мощность орбиты, третья проблема Питера Кэмерона, лемма Бёрнсайда, цикленный тип подстановки.

Введение

Матрицы относятся к важнейшим объектам математики [1, 2]. Бинарные (0, 1)-матрицы, то есть матрицы с элементами 0 и 1, нашли широкое применение в дискретной математике, теории графов и теории групп, теории информации и помехоустойчивом кодировании [3–6]. В начале XXI в. английский математик Питер Кэмерон обратил внимание на важность в математике класса P_n квадратных (0, 1)-матриц порядка n, $n \geq 2$, содержащих в точности n единиц, и приступил к их систематическим исследованиям [7–9]. Практически одновременно исследованием этого же класса матриц занялась белорусская школа помехоустойчивого кодирования [10–12]. Результаты проведенных исследований изложены в монографии [13].

Мощность класса P_n стремительно растет с ростом n. Для эффективной работы с этим классом следует выделять в P_n подклассы некоторым достаточно естественным образом. Приложения класса P_n показывают, что наиболее естественными преобразованиями матриц этого класса являются перестановки строк между собой или же перестановки столбцов между собой. Другими 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, являясь старейшим объектом в теории групп, интенсивно исследуется с XVIII в. [14]. Уже в XXI в. Питер Кэмерон привлек внимание исследователей к этой классической области исследования, сформулировав свои 27 проблем в теории подстановок [15]. Третья из них выглядит следующим образом: найти общую формулу или алгоритм вычисления количества орбит α_n, на которые разбивается множество P_n под действием группы $G = S_n^2$.

В знак уважения многогранного вклада Питера Кэмерона в рассматриваемую область в дальнейшем матрицы множества P_n будем называть кэмероновскими.

Одним из возможных подходов к вычислению количества α_n, орбит множества P_n является использование формулы Бёрнсайда, которая применительно к рассматриваемой задаче может быть переписана [16] в виде

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

Здесь $\left| Inv(g) \right|$ – это количество матриц из множества P_n, инвариантных относительно действия элемента $g \in G = S_n \times S_n$.

Непосредственное применение формулы (1) связано с перебором всех элементов группы $G = S_n^2$ и влечет за собой значительные вычислительные трудности. В [16] для вычисления α_n, предложен алгоритм развертки, который реализует идеи метода динамического программирования [17].

Динамическое программирование – это способ решения сложных задач путем разбиения их на вспомогательные, более простые задачи и последующего объединения решений подзадач в единое общее решение. Оно находит свое применение тогда, когда разные подзадачи используют решения одних и тех же подзадач. В алгоритме динамического программирования каждая подзадача решается только один раз, после чего ответ сохраняется. Это позволяет избежать повторных вычислений каждый раз, когда встречается данная, уже решенная подзадача.

В рамках предлагаемого в [16] алгоритма развертки количество реально вычисляемых слагаемых формулы (1) значительно ниже заявленного числа $(n!)^2$. Сокращение числа перебираемых слагаемых происходит за счет того, что $\left| Inv(g) \right|$ оказывается одинаковым для всех подстановок $g = (g_1, g_2) \in S_n^2$, имеющих один и тот же цикленный тип. В случае если известен цикленный тип подстановки g (т. е. последовательность $\mu_1, \mu_2, ..., \mu_n$ мощностей множеств циклов длиной $i, 1 \le i \le n$, в разложении подстановки g), то $\left| Inv(g) \right|$ может быть найдено по реккурентной формуле. Цикленный тип подстановки g определяется по цикленным типам подстановок $g_1, g_2 \in S_n$. Сложность предложенного в [16] алгоритма составляет $O(p^2(n)n^2\log(n))$, здесь $p(n)$ – это число неупорядоченных разбиений числа n, т. е. количество способов представить n в виде суммы положительных целых чисел.

Данная работа является развитием идей и методов, изложенных в [16]. Ее целью является построение алгоритма вычисления количества α_n орбит множества P_n, имеющего меньшую вычислительную сложность, чем алгоритм, предложенный в [16].

Линейная развертка бинарных матриц и матричные подстановки. Пусть $P_{i,j,k}$ – это множество бинарных матриц размера $i \times j$, которые содержат в точности k единиц. Очевидно, что $P_{n,n,n} = P_n$. На $P_{i,j,k}$ действует группа $G_{i,j} = S_i \times S_j$, где S_t – это симметрическая группа из t элементов.

Аналогично [16] для матрицы

$$A = \begin{pmatrix} a_1 & a_2 & \dots & a_j \\ a_{j+1} & a_{j+2} & \dots & a_{2j} \\ \dots & \dots & \dots & \dots \\ a_{j(i-1)+1} & a_{j(i-1)+2} & \dots & a_j \end{pmatrix} \in P_{i,j,k}$$

легко построить ее линейную развертку – представить матрицу A в виде одной вектор-строки $\overline{x}_A = (a_1, a_2, \dots, a_j)$ из векторного пространства размерностью ij.

Возьмем произвольный элемент $g \in G_{i,j} = S_i \times S_j$. Тогда

$$g(A) = \begin{pmatrix} a_{m_1} & a_{m_2} & \dots & a_{m_j} \\ a_{m_j+1} & a_{m_j+2} & \dots & a_{m_{2j}} \\ \dots & \dots & \dots & \dots \\ a_{m_{j(i-1)+1}} & a_{m_{j(i-1)+2}} & \dots & a_{m_j} \end{pmatrix} \in P_{i,j,k}$$

и элементу g можно поставить в соответствие подстановку

$$h(g) = \begin{pmatrix} \dots & m_1 & \dots & m_2 \dots m_{ij} & \dots \\ \dots & 1 & \dots & 2 \ \dots ij & \dots \end{pmatrix} \in S_i \times S_j. \qquad (2)$$

Как и в [16], подстановку $h(g)$, задаваемую формулой (2), будем называть матричной подстановкой, построенной по элементу g. Любая матричная подстановка может быть представлена в виде произведения независимых циклов:

$$h(g) = C_1 C_2 \dots C_\alpha. \qquad (3)$$

Свойства матричных подстановок для элементов из $G_{i,j}$ аналогичны подробно обсуждаемым в [16] свойствам матричных подстановок для элементов из множества $G = S_n \times S_n$. Сформулируем здесь только два предложения, которые понадобятся в дальнейшем.

Предложение 1. *Пусть в разложении (3) присутствуют все циклы, то есть и циклы длиной* 1. *Тогда:*

1) если l_i *– длина цикла* $C_i, 1 \le i \le \alpha$, *то* $l_1 + l_2 + \ldots + l_k = j$;

2) следовательно, для всякой матрицы $A \in P_{i,j,k}$ *каждая координата вектора* $\overline{x}_A = (a_1, a_2, \ldots, a_{ij})$ *принадлежит своему циклу* $C_i, 1 \le i \le \alpha$;

3) матрица $A \in P_{i,j,k}$ *принадлежит* $Inv(g)$ *в том и только том случае, когда элементы матрицы A, соответствующие отдельному циклу* C_j, $1 \le i \le \alpha$, *равны между собой, т. е. либо все равны* 0, *либо все равны* 1.

4) пусть матрица $A \in P_{i,j,k}$ *принадлежит* $Inv(g)$ *а единицы этой матрицы принадлежат только циклам с номерами* $i_1, i_2, \ldots, i_s$; *в таком случае* $l_{i_1} + l_{i_2 2} + \ldots + l_{i_s} = k$.

Пусть $A \in P_{i,j,k}$, $g = (g_1, g_2) \in S_i \times S_j$ и $g_i = C_1^{g_i} \ldots C_{k_i}^{g_i}$, $i = 1,2,-$ разложение g_i в произведение независимых циклов, содержащее в том числе и циклы длиной 1. Через $\left|C_i^{g_i}\right|$ будем обозначать длину цикла $C_i^{g_i}$.

Предложение 2. *Пусть в разложении (3) матричной подстановки h(g) в произведение независимых циклов присутствуют все циклы, то есть 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* $НОД(\left|C_i^{g_1}\right|, \left|C_j^{g_2}\right|)$ *циклов в разложении (3);*

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

Формулировка и доказательства предложений 1 и 2 аналогичны формулировкам и доказательствам предложений 2 и 4 из [16].

Вычислим количество неподвижных точек для подстановок специального вида.

Пусть $g = (g_1, g_2) \in S_i \times S_j$, $g_1 = C_1^1 C_2^1 \ldots C_s^1$, $g_2 = C_1^2$ – разложения g_1 и g_2 в произведение независимых циклов, содержащие в том числе и циклы длиной 1. Зафиксируем порядок следования циклов в разложении подстановки g_1. Через $t_{g,i,j,k}$ условимся обозначать количество матриц из множества $P_{i,j,k}$, являющихся неподвижными точками для подстановки *g*, т. е. $t_{g,i,j,k} = |Inv(g)|$. Условимся считать, что $t_{g,0,j,0} = 1$. Из предложения 1 следует, что $t_{g,i,j,k}$ – это число способов, которыми можно выбрать циклы $C_{i_1}, C_{i_2}, \ldots, C_{i_s}$ из разложения (3) так, чтобы суммарная длина этих циклов равнялась *k*.

Предложение 3. Справедлива *следующая реккурентная формула*:

$$t_{g,i,j,k} = \sum_{\substack{l, \\ k \geqslant l \cdot НОК(|C_s^1|, |C_1^2|)}} C^l_{НОД(|C_s^1|, |C_1^2|)} t_{\tilde{g}, i-|C_s^1|, j, k-l \cdot НОК(|C_s^1|, |C_1^2|)}, \quad (4)$$

где $\left|C_u^v\right|$ – *длина цикла* C_u^v, $\widetilde{g} = (\widetilde{g}_1, g_2) \in S_{i-|C_s^1|} \times S_j$, $\widetilde{g}_1 = C_1^1 C_2^1 \ldots C_{s-1}^1$.

Доказательство. Пусть в разложении (3) матричной подстановки $h(g)$ в произведение независимых циклов присутствуют все циклы, в том числе и циклы длиной 1. Пусть матрица $A \in Inv(g)$ Из предложения 1 следует, что элементы матрицы A, соответствующие любому из циклов разложения (3), равны 0 или 1. Индексы элементов матрицы A, которые стоят на пересечении строк и столбцов, входящих в циклы C_s^1 и C_1^2, в соответствии с предложением 2 образуют $НОД(\left|C_s^1\right|, \left|C_1^2\right|)$ циклов разложения (3), каждый цикл имеет длину $НОК(\left|C_s^1\right|, \left|C_1^2\right|)$. Пусть элементы матрицы A, соответствующие l из этих циклов, равны 1. Существует $C^l_{НОД(\left|C_s^1\right|, \left|C_1^2\right|)}$ способов выбрать эти циклы.

Из циклов разложения (3) удалим циклы, которые соответствуют элементам матрицы A, расположенным на пересечение строк и столбцов из C_s^1 и C_1^2. Оставшиеся циклы $C_{\alpha_1}, C_{\alpha_2}, \ldots, C_{\alpha_k}$ образуют подстановку $\widetilde{g} = (\widetilde{g}_1, g_2) \in S_{i-\left|C_s^1\right|} \times S_j$, $\widetilde{g}_1 = C_1^1 C_2^1 \ldots C_{s-1}^1$. Среди элементов матрицы A, соответствующих этим циклам, имеется $k - l \cdot НОК(\left|C_s^1\right|, \left|C_1^2\right|)$ единиц. Существует $t_{\widetilde{g}, i-|C_s^1|, j, k-l \cdot НОК(|C_s^1|, |C_1^2|)}$ способов выбрать из $C_{\alpha_1}, C_{\alpha_2}, \ldots, C_{\alpha_k}$ циклы $C_{\beta_1}, C_{\beta_2}, \ldots, C_{\beta_k}$ так, чтобы их суммарная длина была равна $k - l \cdot НОК(\left|C_s^1\right|, \left|C_1^2\right|)$.

Так как выбор l циклов, соответствующих элементам матрицы A, стоящим на пересечении строк и столбцов, входящих в C_s^1 и C_1^2, и циклов $C_{\beta_1}, C_{\beta_2}, \ldots, C_{\beta_k}$ не зависит друг от друга, то существует $A_l = C^l_{НОД(|C_s^1|, |C_1^2|)} t_{\widetilde{g}, i-|C_s^1|, j, k-l \cdot НОК(|C_s^1|, |C_1^2|)}$ вариантов такого выбора. Для нахождения $t_{g,i,j,k}$ необходимо просуммировать A_l по всем допустимым l. Понятно, что имеет смысл рассматривать только те l, для которых $k - l \cdot НОК(\left|C_s^1\right|, \left|C_1^2\right|) \geq 0$. Доказательство завершено.

Алгоритм вычисления мощности $|Inv(g)|$ для матричных подстановок

Обозначим через $P_n(i, j)$ множество бинарных матриц размера $n \times i$, которые содержат в точности j единиц. Очевидно, что $P_n(i, j) = P_{n,i,j}$ и $P_n(n, n) = P_n$. На $P_n(i, j)$ действует группа $G_i = S_n \times S_i$.

Зафиксируем натуральное число $k \leq i$, подстановку $g \in S_n$ и порядок следования множителей в ее разложении $g = C_1^g C_2^g \ldots C_\nu^g$ в произведение независимых циклов.

Рассмотрим множество $H_{g,i,k} = \{(g, h_k) | h_k \in S_i\} \subset G_i = S_n \times S_i$, где h_k из S_i удовлетворяет следующему условию: в разложении h_k в произведение независимых циклов число i входит в цикл длины k.

Пусть $h_{g,i,k} = (g, h_k) \in H_{g,i,k}$ и

$$h_k = C_1^{h_k} C_2^{h_k} \ldots C_{\mu_{h_k}}^{h_k} - \quad (5)$$

это разложения подстановки $h_k \in S_i$ в произведение независимых циклов, содержащее в том числе и все циклы длины 1. Далее будем считать, что в разложении (5) подстановки h_k множители упорядочены так, что число i входит в цикл $C_1^{h_k}$ длины k, т. е. $C_1^{h_k} = (h_1^{h_k}, h_2^{h_k}, ..., h_{k-1}^{h_k}, i)$, где $h_1^{h_k}, h_2^{h_k}, ..., h_{k-1}^{h_k}, i$ – некоторые натуральные числа, не превосходящие i. В дальнейшем элемент $h_{g,i,k}$ также будем записывать в виде $\left(C_1^g C_2^g ... C_\nu^g, C_1^{h_k} C_2^{h_k} ... C_{\mu_{h_k}}^{h_k}\right)$.

Пусть

$$f_{g,i,j} = \sum_{h_{g,i,k} \in \bigcup_{k=1}^{i} H_{g,i,k}} \left| Inv(h_{g,i,k}) \right|. \qquad (6)$$

Будем считать, что $f_{g,0,0} = 1$. $f_{g,i,j}$ равно числу матриц из множества $P_n(i, j)$ которые являются неподвижными точками для подстановок из множества $H_{g,i} = \bigcup_{k=1}^{i} H_{g,i,k}$.

Предложение 4. *Справедлива следующая реккурентная формула:*

$$f_{g,i,j} = \sum_{k=1}^{i} \sum_{l=0}^{j} A_{i-1}^{k-1} f_{g,i-k,j-l} t_{\tilde{g},n,k,l}, \qquad (7)$$

где $t_{\tilde{g},n,k,l}$ *равно количеству матриц из множества* $P_{n,k,l}$, *являющихся неподвижными точками для подстановки* $\tilde{g} = (g, C^{h_k}) = \left(C_1^g C_2^g ... C_\nu^g, C^{h_k}\right) \in S_n \times S_k$, *где* $C^{h_k} = (1, 2, ..., k-1, k)$ *– цикл длины k, и может быть найдено по формуле* (4).

Доказательство. Из формулы (6) легко следует, что $f_{g,i,j} = \sum_{k=1}^{i} \sum_{h_{g,i,k} \in H_{g,i,k}} \left| Inv(h_{g,i,k}) \right|$.

Пусть $h_{g,i,k} = (g, h_k) \in H_{g,i,k}$, $A_{g,i,k} \in Inv(h_{g,i,k})$ и (5) – это разложение h_k в произведение независимых циклов. В столбцах матрицы $A_{g,i,k}$ с номерами $h_1^{h_k}, h_2^{h_k}, ..., h_{k-1}^{h_k}, i$, которые образуют цикл $C_1^{h_k}$, может содержаться от 0 до j единиц. Тогда множество $\bigcup_{h_{g,i,k} \in H_{g,i,k}} Inv(h_{g,i,k})$ может быть представлено в виде прямого объединения $j+1$ непересекающихся множеств $\bigcup_{h_{g,i,k} \in H_{g,i,k}} Inv(h_{g,i,k}) = \bigcup_{l=0}^{j} A_{h_{g,i,k}}^l$. При этом множество $A_{h_{g,i,k}}^l$ состоит из матриц $\tilde{A}_{h_{g,i,k}}^l$, удовлетворяющих следующим двум условиям: 1) $\tilde{A}_{h_{g,i,k}}^l$ является неподвижной точкой для некоторого элемента $\left(C_1^g C_2^g ... C_\nu^g, C_1^{h_k} C_2^{h_k} ... C_\mu^{h_k}\right) \in H_{g,i,k}$, где $C_1^{h_k} = (h_1^{h_k}, h_2^{h_k}, ..., h_{k-1}^{h_k}, i)$ – цикл длины k; 2) столбцы матрицы $\tilde{A}_{h_{g,i,k}}^l$, номера которых образуют цикл $C_1^{h_k}$, содержат в точности l единиц. Поэтому $f_{g,i,j} = \sum_{k=1}^{i} \sum_{l=0}^{j} \left| A_{h_{g,i,k}}^l \right|$.

Зафиксируем k и l. Вычислим $\left|A^l_{h_{g,i,k}}\right|$. Для этого найдем количество способов, которыми можно сформировать матрицу $A^l_{h_{g,i,k}}$, удовлетворяющую условиям 1) и 2).

Рассмотрим цикл $C_1^{h_k} = (h_1^{h_k}, h_2^{h_k}, ..., h_{k-1}^{h_k}, i)$ $C_1^{h_k}$ содержит число i. Остальные k–1 элемент этого цикла можно выбрать A_{i-1}^{k-1} способом, где A_n^k – это число размещений из n элементов по k. Зафиксируем цикл $C_1^{h_k} = \widetilde{C}_1^{h_k}$ и рассмотрим множество подстановок

$$h_{g,i,k} = (g, h_k) = \left(C_1^g C_2^g ... C_\nu^g, \widetilde{C}_1^{h_k} C_2^{h_k} ... C_{\mu_{h_k}}^{h_k}\right) \in H_{g,i,k}. \quad (8)$$

Пусть матрица $\widetilde{A}^l_{h_{g,i,k}}$ является неподвижной точкой для подстановки $\widetilde{h}_{g,i,k}$ вида (8). В столбцах этой матрицы, отличных от столбцов, номера которых образуют цикл $\widetilde{C}_1^{h_k}$, размещается $j-l$ единиц. Количество таких столбцов равно $i-k$.

При вычислении $\widetilde{h}_{g,i,k}(\widetilde{A}^l_{h^k_{g,i}})$ столбцы, входящие в циклы $\widetilde{C}_1^{h_k}, C_2^{h_k}, ..., C_{\mu_{h_k}}^{h_k}$, переставляются независимо друг от друга. Поэтому матрицу $\widetilde{A}^l_{h^k_{g,i}}$ можно строить так: разместить вначале l единиц в столбцах, номера которых входят в цикл $\widetilde{C}_1^{h_k}$ так, чтобы при перестановке столбцов в соответствии с циклом $\widetilde{C}_1^{h_k}$ и строк в соответствии с подстановкой g результирующая матрица не изменялась. Количество таких возможных размещений равно количеству $t_{\widetilde{g},n,k,l}$ матриц из множества $P_{n,k,l}$, являющихся неподвижными точками для подстановки $\widetilde{g} = (g, C^{h_k}) = \left(C_1^g C_2^g ... C_\nu^g, C^{h_k}\right) \in S_n \times S_k$, где $C^{h_k} = (1,2,...,k-1,k)$ – цикл длины k. После расстановки l единиц в столбцах, которые образуют цикл $\widetilde{C}_1^{h_k}$, нужно разместить $j-l$ единиц в $i-k$ столбцах, номера которых входят в циклы $C_2^{h_k}, ..., C_{\mu_{h_k}}^{h_k}$, так, чтобы результирующая матрица не изменялась при перестановке столбцов в соответствии с циклами $C_2^{h_k}, ..., C_{\mu_{h_k}}^{h_k}$, и строк в соответствии с подстановкой g. Количество таких размещений равно $f_{g,i-k,j-l}$. Поэтому для подстановок вида (8) имеется $f_{g,i-k,j-l} t_{\widetilde{g},n,k,l}$ неподвижных точек. Следовательно, $\left|A^l_{h^k_{g,i}}\right| = A_{i-1}^{k-1} f_{g,i-k,j-l} t_{\widetilde{g},n,k,l}$ и $f_{g,i,j} = \sum_{k=1}^{i} \sum_{l=0}^{j} A_{i-1}^{k-1} f_{g,i-k,j-l} t_{\widetilde{g},n,k,l}$. Доказательство завершено.

Предложение 5. *Вычисление* $f_{g,n,n}$ *по формуле* (7) *требует выполнения* $O(n^4)$ *операций.*

Доказательство. Вычисление $f_{g,n,n}$ по формуле (7) требует нахождения величин $f_{g,i,j}$ и $t_{\widetilde{g},i,j,k}$, каждой величины – по $O(n^2)$ значений. Использование формулы (7) требует выполнения $O(n^2)$ операций сложения и умножения для нахождения каждого $f_{g,i,j}$. Использование формулы (4) для нахождения $t_{\widetilde{g},i,j,k}$ предполагает вычисление $O(n^3)$ величин $t_{\widetilde{g},\alpha,\beta,\gamma}$ и требует $O(n)$ операций сложения. Следовательно, вычисление $f_{g,n,n}$ по формуле (7) требует выполнения $O(n^4)$ операций. Доказательство завершено.

Следствие. Количество орбит множества P_n может быть найдено за $O(p(n)n^4)$ операций.

Доказательство. Пусть p_i – это разбиение числа *n*. p_i задает цикленный тип подстановки $g_i \in S_n$. Зная цикленный тип подстановки g_i, по формуле (7) можно вычислить $f_{g_i,n,n}$ – количество матриц из множества $P_n(n,n) = P_n$, являющихся неподвижными точками для подстановок из множества $H_{g_i,n} = \bigcup_{k=1}^{n} H_{g_i,n,k} = \{(g_i, h_k) | h_k \in S_n\} \subset G = S_n \times S_n$. Тогда формулу (1) для вычисления числа α_n орбит множества P_n можно переписать так:

$$\alpha_n = \frac{1}{(n!)^2} \sum_{g \in S_n} f_{g,n,n}. \tag{9}$$

Если $g_i \in S_n$ и $g_j \in S_n$ – подстановки одного цикленного типа, то в силу предложения 5 из [16] подстановки $(g_i, h) \in S_n \times S_n$ и $(g_j, h) \in S_n \times S_n$ также являются подстановками одного цикленного типа, и поэтому $f_{g_i,n,n} = f_{g_j,n,n}$. Если k_{p_i} – это количество подстановок множества S_n, имеющих такой же цикленный тип, как и подстановка g_i, то, учитывая что в S_n количество различных цикленных типов подстановок совпадает с $p(n)$ (9) можно переписать так:

$$\alpha_n = \frac{1}{(n!)^2} \sum_{i=1}^{p(n)} f_{g_i,n,n} k_{p_i}. \tag{10}$$

Так как, в соответствии с предложением 2, вычисление $f_{g,n,n}$ требует выполнения $O(n^4)$ операций и сумма в правой части формулы (10) содержит $p(n)$ слагаемых, то количество α_n орбит множества P_n требует выполнения $O(p(n)n^4)$ операций. Доказательство завершено.

Алгоритм развертки по вычислению количества орбит множества P_n, представленного в [16], требует выполнения $O(p_1)$ $p_1 = p^2(n)n^2 \log(n)$ арифметических операций. Алгоритм нахождения числа орбит множества P_n, предлагаемый в данной работе, предполагает выполнение $O(p_2)$, $p_2 = p(n)n^4$, арифметических операций. В следующей таблице представлены p_1 и p_2 при различных значениях *n*. При вычислении p_1 основание логарифма бралось равным 2.

n	p_1	p_2	p_1 / p_2
10	585988	420000	1.39521
50	$5.88489 \cdot 10^{14}$	$1.27641 \cdot 10^{12}$	461.049
10^2	$2.41283 \cdot 10^{21}$	$1.90569 \cdot 10^{16}$	126611
10^3	$5.76973 \cdot 10^{69}$	$2.40615 \cdot 10^{43}$	$2.39791 \cdot 10^{26}$
10^4	$1.73813 \cdot 10^{222}$	$3.61673 \cdot 10^{122}$	$4.8058 \cdot 10^{99}$
10^5	$1.255511301760969 \cdot 10^{704}$	$2.749351056977570 \cdot 10^{366}$	$4.56657325944103 \cdot 10^{337}$
10^6	$4.316892130888775 \cdot 10^{2227}$	$1.471684986358223 \cdot 10^{1131}$	$2.933299021804384 \cdot 10^{1096}$

Из таблицы следует, что, начиная с $n \geq 10^3$ предлагаемый в данной работе алгоритм дает довольно значительный выигрыш в количестве операций, которые необходимо выполнить при вычислении количества орбит множества P_n.

Пример. 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 $g_1 = (1)(2)(3)(4)$, $g_2 = (12)(3)(4)$, $g_3 = (12)(34)$, $g_4 = (123)(4)$, $g_5 = (1234)$. В соответствии с предложением 7 из [16], если в подстановке из n элементов имеется c_i циклов длины $l_i, i = \overline{1,k}$, то количество подстановок такого же цикленного типа равно $n!\prod_{i=1}^{k}\left(c_i!\,l_i^{c_i}\right)^{-1}$. Поэтому 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 $k_{p_1} = \frac{4!}{4!\cdot 1^4} = 1$, $k_{p_2} = \frac{4!}{2!\cdot 1^2\cdot 1!\cdot 2^1} = 6$, $k_{p_3} = \frac{4!}{2!\cdot 2^2} = 3$, $k_{p_4} = \frac{4!}{1!\cdot 1^2\cdot 1!\cdot 3^1} = 8$, $k_{p_5} = \frac{4!}{1!\cdot 4^1} = 6$. Используя формулы (4) и (7), найдем $f_{g_1,4,4} = 3192$, $f_{g_2,4,4} = 648$, $f_{g_3,4,4} = 312$, $f_{g_4,4,4} = 96$, $f_{g_5,4,4} = 72$. Применим формулу (10) для вычисления α_4:

$$\alpha_4 = \frac{1}{(4!)^2}\left(3192\cdot 1 + 648\cdot 6 + 312\cdot 3 + 96\cdot 8 + 72\cdot 6\right) = 16.$$

Полученное значение α_4 совпадает с четвертым членом последовательности A049311 [18].

Код программы на языке Python для вычисления α_n при различных n доступен по ссылке https://github.com/NuM314/thesis-codes/tree/master/solution-pn-n4.

Заключение

В работе рассматривается модификация предложенного ранее авторами алгоритма развертки для 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. Предлагаемая модификация алгоритма имеет вычислительную сложность $O(p(n)n^4)$, в то время как вычислительная сложность исходного алгоритма составляет $O(p^2(n)n^2\log(n))$.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. ***Кострикин, 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. ***Липницкий, В. А.*** Алгоритм развертки при подсчете количества S_n^2-орбит кэмеровских матриц / В. А. Липницкий, А. И. Сергей, Н. В. Спичекова // Веснік Магілёўскага дзяржаўнага ўніверсітэта імя А. А. Куляшова. Серыя В. Прыродазнаўчыя навукі. – 2017. – № 2(50). – С. 23–37.
17. ***Кормен, Т. Х.*** Алгоритмы: построение и анализ / Т. Х. Кормен, Ч. И. Лейзерсон, Р. Л. Риверст, К. Штайн. – Москва : ООО “И. Д. Вильямс”, 2013. – 1328 с.
18. The On-Line Encyclopedia of Integer Sequences. – [Электронный ресурс]. – Режим доступа: http://oeis.org/. – Дата доступа: 07.02.2017.

Поступила в редакцию 08.11.2017 г.
Контакты: valipnitski@yandex.ru (Липницкий Валерий Антонович)

Lipnitski V., Sergey A., Spichekova N. DYNAMIC PROGRAMMING IN UNWINDING ALGORITHM TO SOLVE THE THIRD CAMERON’S PROBLEM.

In the article a modification of the unwinding algorithm that was previously offered by the authors is constructed. The unwinding algorithm is designed to calculate number of orbits in the set of binary square matrices of the 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 algorithm proposed in this paper requires* $O(p(n)n^4)$ *of arithmetic operations where p(n) equals to number of unordered partitions of n.*

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