УДК 004.056.55; 621.391.26

ДЕЙСТВИЕ КВАДРАТА СИММЕТРИЧЕСКОЙ ГРУППЫ НА СПЕЦИАЛЬНОМ КЛАССЕ (0;1)-МАТРИЦ. ОТСУТСТВИЕ ПОЛНЫХ ОРБИТ

В.К. КОНОПЕЛЬКО, В.А. ЛИПНИЦКИЙ*, Н.В. СПИЧЕКОВА

Белорусский государственный университет информатики и радиоэлектроники
П.Бровки,6 Минск, 220013, Беларусь

**Военная академия Республики Беларусь*
Минск–57,220057, Беларусь

Поступила в редакцию 3 октября 2010

Изучается действие симметрической группы на строках и столбцах квадратных матриц порядка n, $n \geq 2$, с элементами 0 и 1, содержащих в точности n единиц. Исследуется строение и мощность возникающих при этом действии орбит. Доказывается отсутствие полных орбит при всех значениях n, за исключением $n = 3, 4$.

Ключевые слова: распознавание образов, помехоустойчивый линейный код, действие группы на множестве, матрица, симметрическая группа, орбита, полная орбита.

Постановка задачи

На экране в n^2 пикселей «вспыхивает» n точек. Требуется дать описание возникающих в результате образов. Подобная задача типична в теории и практике распознавания образов и изображений; она важна для радиолокации – распознать наблюдаемые летящие объекты по принципу «свой – чужой» или распределить их по типам и классам летающих объектов; данная задача существенную роль играет и в медицине – например, при распознавании и подсчёте тех или иных видов микроорганизмов в бактометре. Сводится к данной задаче и проблема декодирования кратных ошибок в кодах-произведениях, в итерационных кодах с большим кодовым расстоянием.

Конечно, вспыхивающие пиксели могут иметь разную окраску. В первом приближении цвет будем игнорировать. В таком случае экран можно однозначно отождествить с квадратной матрицей порядка n. Каждому пикселю соответствует тот или иной элемент матрицы, «спящему» пикселю ставим в соответствие 0, «вспыхнувшему» – 1. При таком сопоставлении очередному образу на экране соответствует своя квадратная матрица порядка n с элементами 0 в количестве $(n-1)n$ и с n элементами 1. В дальнейшем все многообразие данных матриц будем обозначать символом P или P_n, если потребуется уточнять значение параметра n.

Всякая классификация предполагает возможность отождествления некоторых объектов исследуемого многообразия. Отождествление предполагает наличие определённых, в каком-то смысле «тождественных» преобразований одного объекта в другой. Отсюда ещё в 1872 году Феликс Клейн в своей знаменитой «Эрлангенской программе» пришёл к выводу, что в основе всякой классификации геометрических объектов конкретного пространства лежит та или иная группа преобразований, действующая на данном пространстве [1].

По общему соглашению, в рамках данной задачи перечень «тождественных преобразований» задаёт следующее

Определение 1. *Две матрицы из множества* P_n *считаются эквивалентными, если они отличаются друг от друга перестановкой строк и/или столбцов.*

Всевозможные перестановки строк квадратных матриц порядка n порождаются элементами симметрической группы S_n и только ими. То же верно и для столбцов. Поэтому из определения 1 следует, что на множестве матриц P_n действует прямое произведение двух групп S_n, другими словами, – группа $S_n \times S_n = S_n^2$ – декартов квадрат симметрической группы порядка n. Предполагаем, что для каждого элемента $(f, g) \in S_n^2$ первая координата f действует на строках каждой матрицы $A \in P_n$, а вторая координата g действует на столбцах матрицы $f(A)$.

Таким образом, исходная задача равносильна задаче исследования действия группы S_n^2 на множестве P_n, описанию всех S_n^2 – орбит, на которые разбивается P_n под действием группы S_n^2. Следует отметить, что симметрическая группа или группа подстановок S_n – это исторически первый объект теории групп, начало исследованию свойств которой положили еще в XVIII веке Лагранж и Гаусс, хотя само понятие группы было сформулировано лишь в 1831 году Эваристом Галуа. Определённый вклад в изучение подгрупп симметрической группы внесла в XX веке и белорусская алгебраическая школа [2].

Следует отметить, что определённый вклад в решение данной задачи уже сделан (см., в частности, публикации [3–6]).

Общие сведения об орбитах

Действие произвольной группы G на произвольном множестве M определяет отношение эквивалентности на M (см., например, [7] или [8]), которое разбивает M на непересекающиеся классы M_i, называемые G – орбитами. Каждая G – орбита M_i однозначно определяется любым своим фиксированным представителем $x_i \in M_i$: $M_i = \{g(x_i) \mid g \in G\}$, то есть M_i состоит из всех элементов $g(x_i)$ множества M, которые получаются действием на x_i всех элементов $g \in G$. Множество M совпадает с объединением своих орбит: $M = \bigcup M_i$, а следовательно, имеет место равенство для мощностей: $|M| = \sum |M_i|$. Следует отметить, что те $g \in G$, для которых $g(x_i) = x_i$, образуют подгруппу $St(x_i) \subset G$, называемую стабилизатором элемента $x_i \in M_i$. При этом $|M_i| = [G : St(x_i)]$ – мощность орбиты M_i совпадает с индексом стабилизатора $St(x_i)$ в группе G. Получаем выражение мощности множества M полностью через параметры группы G:

$$|M| = \sum [G : St(x_i)]. \qquad (1)$$

Может оказаться, что $St(x_i) = \{e\}$ для нейтрального элемента e группы G. Тогда $|M_i| = |G|$ – имеет максимально возможное значение, такая орбита, обычно, называется полной. Отсюда и из теоремы Лагранжа о конечных группах следует, что, если G – конечная группа, то мощность любой G – орбиты либо совпадает с $|G|$, либо является делителем $|G|$. Отметим также, что стабилизаторы элементов одной G – орбиты сопряжены друг с другом: если $y = g(x_i) \in M_i$ для некоторого $g \in G$, то $St(y) = gSt(x_i)g^{-1}$.

Структура орбит целиком зависит от группы G. Так для группы $G = \Gamma$ циклических сдвигов координат векторов конечномерного пространства подавляющее большинство Γ – ор-

бит являются полными [9]. Цель данной работы – показать, что полных S_n^2 – орбит не существует, за исключением двух случаев, когда $n = 3, 4$.

Предварительные сведения об S_n^2 – орбитах

Применительно к рассматриваемому случаю, множество $M = P_n$ является конечным и состоит из $C_{n^2}^n = \dfrac{n^2!}{n!(n^2-n)!} = |P_n|$ квадратных матриц порядка n, $G = S_n^2$ – группа из $(n!)^2$ элементов, порядок которой имеет исключительно много делителей. Поскольку элементы каждой матрицы из множества P_n не одинаковы, то легко заметить, что каждая S_n^2 – орбита содержит более одной матрицы.

Можно отметить два основных метода формирования S_n^2 – орбит. Первый из них – априорный метод, заключается он в выборе конкретных матриц $A_i \in M = P_n$ с последующим составлением порождаемых ими орбит $< A_i >$ непосредственной перестановкой строк и столбцов выбранной матрицы.

Пример 1. Построим S_n^2 – орбиту матрицы $B = \begin{pmatrix} 1 & 0 & \ldots & 0 \\ 1 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 1 & 0 & \ldots & 0 \end{pmatrix} \in P_n$. Легко видеть, любые перестановки строк данной матрицы не меняют её. Всевозможные перестановки столбцов матрицы B передвигают столбец из единиц на другие места и дают в точности $n-1$ новых матриц, которые вместе с матрицей B образуют следующую S_n^2 – орбиту мощностью n:

$$< B >= \left\{ \begin{pmatrix} 1 & 0 & \ldots & 0 \\ 1 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 1 & 0 & \ldots & 0 \end{pmatrix}; \begin{pmatrix} 0 & 1 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 1 & \ldots & 0 \end{pmatrix}; \ldots; \begin{pmatrix} 0 & \ldots & 0 & 1 \\ 0 & \ldots & 0 & 1 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & \ldots & 0 & 1 \end{pmatrix} \right\}.$$

Ясно, что такую же мощность имеет и орбита $< B^T >$.

Базовое условие полноты списка S_n^2 – орбит

Множество всех орбит, на которое разбивается произвольное множество M под действием группы G принято обозначать через M / G. В соответствии с этим множество всех S_n^2 – орбит, на которое разбивается множество $(0,1)$ – матриц P_n, следует обозначать P_n / S_n^2.

Занимаясь составлением списка S_n^2 – орбит, переходя к построению следующей орбиты, следует проверять, что она не пересекается ни с одной из уже построенных орбит. Существенную помощь в этой проверке оказывают необходимые условия принадлежности матриц одной орбите. Составление полного списка орбит завершается, когда непересекающиеся орбиты суммарно исчерпают все элементы множества P_n, то есть при выполнении равенства

$$C_{n^2}^n = \frac{n^2!}{n!(n^2-n)!} = |P_n| = \sum_{i=1}^{l} |< A_i >| \qquad (2)$$

для подходящего целого l. Конечно, для построения полного списка орбит для реальных значений n требуются компьютерные ресурсы.

Формулы (1) и (2) подсказывают другой – теоретико-групповой метод составления орбит, который естественно назвать «методом стабилизаторов». Суть этого метода в вычислении групп $St(A_i)$ для тех или иных матриц A_i, их мощностей и индексов в группе $G = S_n^2$. Иногда этот метод реализуется легче и быстрее априорного.

S_n^2 – орбита единичной матрицы

Всевозможные перестановки строк (столбцов) единичной матрицы $E_n = \begin{pmatrix} 1 & 0 & ... & 0 \\ 0 & 1 & ... & 0 \\ ... & ... & ... & ... \\ 0 & 0 & ... & 1 \end{pmatrix}$ приводят к образованию $n!$ различных матриц, называемых перестановочными. Они образуют группу относительно матричного умножения, изоморфную группе S_n (детали см., например, в [7] или [10]).

Лемма 1. Пусть f – произвольная подстановка из S_n. Тогда элемент $(f, f) \in S_n^2$ принадлежит группе $St(E_n)$.

Доказательство. Для каждого целого i, $1 \le i \le n$, диагональный элемент a_{ii} матрицы E_n равен 1. Для доказательства леммы достаточно показать, что у матрицы, получаемой действием (f, f) на матрицу E_n, на главной диагонали также стоят только 1. Пусть $f = f_1 f_2 \cdot ... \cdot f_s$ – разложение f в произведение независимых циклов. Пусть цикл f_k содержит элемент i. Если $f_k = (i)$, то подстановка (f, f) оставляет элемент a_{ii} на месте. Если $f_k = (ij)$ – транспозиция, то подстановка (f, f) поменяет у матрицы E_n элементы $a_{ii} = 1$ и $a_{jj} = 1$ местами. Пусть $f_k = (...sij...)$ – цикл длиной $t \ge 3$. Тогда первая координата подстановки (f, f) переместит $a_{ii} = 1$ на место элемента a_{ji}, а $a_{ss} = 1$ переместит на место a_{is}. После этого вторая координата подстановки (f, f) i – й столбец только что преобразованной матрицы поставит на место j – ого столбца, а s – й на место i – ого. В итоге элемент $a_{ss} = 1$, стоящий на месте a_{is} – го, переместится на место элемента $a_{ii} = 1$. В силу произвольности i получаем, что подстановка (f, f) диагональ единичной матрицы в целом оставляет на месте. А это означает, что $(f, f) \in St(E_n)$. Лемма доказана.

Из леммы 1 непосредственно вытекает

Предложение 1. S_n^2 – орбита $< E_n >$ имеет мощность $n!$

Доказательство. Как уже отмечено выше, S_n^2 – орбита $< E_n >$ имеет как минимум $n!$ элементов. Лемма 1 утверждает, что диагональная подгруппа $D = \{(f, f) \mid f \in S_n\}$ мощностью $n!$ принадлежит группе $St(E_n)$. Индекс подгруппы D в группе S_n^2 равен $n!$. Если $|St(E_n)| > |D|$, то индекс $|S_n^2 : St(E_n)|$ должен быть меньше индекса $|S_n^2 : D| = n!$, что невозможно, так как S_n^2 – орбита $< E_n >$ уже имеет как минимум $n!$ элементов. Следовательно, $|< E_n >| = n!$.

Предложение полностью доказано.

Условия нетривиальности стабилизатора

Весом строки (столбца) матрицы $A \in P_n$ назовём количество единиц в этой строке (в этом столбце).

Предложение 2. Пусть матрица $A \in P_n$ удовлетворяет хотя бы одному из следующих условий:

а) имеет $k \geq 2$ одинаковых строк (столбцов);

б) имеет по $k \geq 2$ строк и столбцов весом 1, на пересечении которых расположена перестановочная матрица порядка k.

Тогда $|St(A)| > 1$.

Доказательство. В условиях первой части предложения всякая нетождественная перестановка $h \in S_n$ одинаковых строк (столбцов), оставляющая на месте остальные строки (столбцы), оставляет на месте матрицу A. Тогда для тождественной подстановки $e \in S_n$ пара (h, e) (пара (e, h)) из группы S_n^2 принадлежит $St(A)$.

Пусть названные в условиях второй части предложения строки и столбцы весом 1, на пересечении которых расположена перестановочная матрица порядка k, имеют номера $i_1, i_2, ..., i_k$ и $j_1, j_2, ..., j_k$ соответственно. Переставим отмеченные строки таким образом, чтобы на пересечении указанных строк и столбцов получилась единичная матрица E_k. Получим новую матрицу B, принадлежащую $S_n^2 -$орбите $< A >$. Тогда, в силу леммы 1, для каждой перестановки $g \in S_n$, действующей только на строках с номерами $i_1, i_2, ..., i_k$ и на остальных строках действующей тождественно пара $(g, g) \in S_n^2$ принадлежит стабилизатору $St(B)$. Имеется $k!$ названных подстановок g. Следовательно, $|St(B)| \geq k! \geq 2! > 1$. Как отмечалось выше, группа $St(A)$ сопряжена с группой $St(B)$, а поэтому у этих групп порядки совпадают. Значит, $|St(A)| > 1$, что и требовалось доказать.

О полноте $S_n^2 -$ орбит

Исчерпывающее описание полных $S_n^2 -$орбит во всех множествах P_n обеспечивает

Теорема 1. При $n = 2$ и при $n \geq 5$ полных $S_n^2 -$орбит на множестве P_n не существует. При $n = 3$ и при $n = 4$ множества P_3 и P_4 имеют по одной полной $S_n^2 -$орбите $\left\langle \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \right\rangle$ и $\left\langle \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \right\rangle$ соответственно.

Доказательство. Утверждение теоремы 1 для $n = 2, 3, 4$ проверяется непосредственно. Пусть $n \geq 5$. Полная $S_n^2 -$орбита может быть порождена лишь той матрицей $A \in P_n$, которая не удовлетворяет условиям предложения 2, в первую очередь – не имеет одинаковых строк и не имеет одинаковых столбцов. В частности, матрица A может иметь не более одной нулевой строки и не более одного нулевого столбца. Таким образом, относительно возможного наличия нулевой строки и нулевого столбца у матрицы A мы имеем 4 возможности.

(1, 1) – имеется одна нулевая строка и один нулевой столбец.

(1, 0) – имеется одна нулевая строка и нет нулевых столбцов.

(0, 1) – нет нулевых строк, но имеется нулевой столбец.

(0, 0) – нет нулевой строки и нет нулевого столбца.

Последняя ситуация возможна тогда и только тогда, когда в каждой строке и в каждом столбце матрицы A имеется в точности по одной единице. Это означает, что A – перестановочная матрица. Согласно предложению 1 матрица A принадлежит S_n^2 – орбите $< E_n >$ мощностью $n!$ и, следовательно, S_n^2 – орбита $< A >$ полной быть не может.

Вторая ситуация означает, что n единиц в матрице A расположены в $n-1$ ненулевых строках и по одной в каждом столбце. Значит, неизбежно найдётся строка с двумя единицами. Но тогда столбцы с этими единицами будут одинаковыми. Тогда, согласно предложению 2, $|St(A)| > 1$ и S_n^2 – орбита $< A >$ не может быть полной.

Третья ситуация аналогична второй.

Рассмотрим первую ситуацию. В её условиях матрица A эквивалентна матрице B, у которой в первой строке расположены 2 единицы, последняя строка – нулевая, а в остальные строки имеют вес, равный 1. При этом столбцы матрицы B, содержащие единицы из первой строки должны быть различными в силу предложения 2. Это возможно только в случае, когда один из данных столбцов содержит одну единицу, а второй – две единицы. Если столбец с двумя единицами не является первым, то поменяем его с первым столбцом. При этом ещё раз переставим строки, чтобы вторая единица первого столбца оказалась во второй строке. Аналогично вторым столбцом поставим столбец со второй единицей первой строки. Третьим столбцом поставим столбец с единицей в третьей строке, четвёртым столбцом поставим столбец с 1 в четвёртой строке и так далее. В итоге получим матрицу $C \in < B >$ вида

$$C = \begin{pmatrix} 1 & 1 & 0 & 0 & ... & 0 & 0 \\ 1 & 0 & 0 & 0 & ... & 0 & 0 \\ 0 & 0 & 1 & 0 & ... & 0 & 0 \\ 0 & 0 & 0 & 1 & ... & 0 & 0 \\ ... & ... & ... & ... & ... & ... & ... \\ 0 & 0 & 0 & 0 & ... & 1 & 0 \\ 0 & 0 & 0 & 0 & ... & 0 & 0 \end{pmatrix}.$$ При $n \geq 5$ матрица C удовлетворяет второй части предложения 2, а следовательно, имеет ненулевой стабилизатор. Это означает, что S_n^2 – орбита $< C >=< B >=< A >$ не может быть полной.

Теорема полностью доказана.

Заключение

На пути описания спектра S_n^2 – орбит множества $(0,1)$ – матриц P_n установлено отсутствие полных S_n^2 – орбит, за исключением лишь двух малых значений n. Это свидетельствует о наличии глубоких симметрий внутри множества n – точечных образов. Теперь на повестку дня встаёт вопрос о максимально возможных длинах S_n^2 – орбит при $n \geq 5$, о возможных закономерностях распределения максимальных длин орбит в зависимости от размеров рассматриваемых матриц.

ACTION OF THE SQUARE OF THE SYMMETRIC GROUP ON A SPECIAL CLASS OF (0;1)-MATRICES. ABSENCE OF COMPLETE ORBITS

V.K. KONOPELKO, V.A. LIPNITSKI, N.V. SPICHEKOVA

Abstract

The action of the symmetric group on the rows and columns of square matrices of order *n*, $n \geq 2$, with elements 0 and 1, containing exactly *n* units is studied. The structure and power of orbits arising in this action is analyzed. The absence of complete orbits for all values except $n = 3,4$ is proved.

Литература

1. *Клейн Ф.* Сравнительное обозрение новейших геометрических исследований («Эрлангенская программа»). М., 1956.
2. *Супруненко Д.А.* Группы подстановок. Минск, 1996.
3. *Конопелько В.К., Смолякова О.Г.* // Докл. БГУИР. 2008. № 7.
4. *Смолякова О.Г., Фам Хак Хоан.* // Докл. БГУИР. 2008. № 1.
5. *Смолякова О.Г.* // Автореф. канд. дисс. Минск, 2009.
6. *Смолякова О.Г., Макейчик Е.Г., Конопелько И.В.* // Докл. БГУИР. 2009. № 5.
7. *Кострикин А.И.* Введение в алгебру. М., 1977.
8. *Ленг С.* Алгебра. М., 1968.
9. *Липницкий В.А., Конопелько В.К.* Норменное декодирование помехоустойчивых кодов и алгебраические уравнения. Минск, 2007.
10. *Дворников В.Д., Конопелько В.К., Липницкий В.К.* Теория и практика низкоскоростных кодов. Минск, 2002.