Г.Дж.Райзер

КОМБИНАТОРНАЯ МАТЕМАТИКА

Автор ставит своей целью систематическое изложение основ комбинаторной математики, которая занимается изучением расположений элементов в множествах. В настоящее время эти методы находят многочисленные применения в важных практических задачах математической экономики, техники, кибернетики и т. п.

Книга будет полезной инженерам и научным работникам самых различных специальностей, а также студентам высших учебных заведений.

ОГЛАВЛЕНИЕ

ИМЕННОЙ УКАЗАТЕЛЬ

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

ПРЕДИСЛОВИЕ ПЕРЕВОДЧИКА

Развитие математики за последние 10—20 лет, в особенности бурный рост вычислительной техники, привел не только к расширению приложений этой науки, но и к перестройке ее содержания. Одной из основных черт этой перестройки является рост роли так называемой конечной математики, в частности, одной из важнейших ее частей — комбинаторных методов.

Комбинаторные идеи и методы всегда были тесно связаны с практическими задачами. Эта связь отчетливо выражена в большинстве книг и статей, посвящаемых комбинаторике. В качестве примера можно указать книгу Риордана „Введение в комбинаторный анализ“ (ИЛ, 1963), а также выпущенный в конце 1964 г. Калифорнийским университетом (США) сборник „Applied combinatorial mathematics“.

Теоретические основы комбинаторной математики, однако, развиты еще недостаточно и сильно отстают от требований практики. Значение предлагаемой вниманию читателей книги Райзера состоит прежде всего в том, что в ней рассматриваются теоретические проблемы комбинаторики. Книгу выгодно отличают общность исходных теоретических позиций, органическое единство в изложении материала, строгость математических суждений и доказательств.

Хотя автор и предуведомляет читателя, что от него не потребуется специальной подготовки в области комбинаторной математики, его книгу нельзя назвать элементарной. Написана она сжато, для успешного ее изучения необходим сравнительно высокий уровень математической культуры.

20 июля 1965 г. *К. А. Рыбников*

ИЗ ПРЕДИСЛОВИЯ АВТОРА

Для чтения данной монографии не требуется специальных знаний по комбинаторной математике. В первой главе мы рассматриваем элементарные свойства множеств и определяем понятия *перестановок*, *сочетаний* и *биномиальных коэффициентов*. Мы, конечно, рассматриваем эти понятия с современной точки зрения и с самого начала предполагаем, что читатель сможет оценить тонкости математических рассуждений. Наиболее глубокие исследования в области комбинаторной математики проводятся в рамках современной алгебры, и поэтому мы считаем, что читатель знаком с ее основными положениями и понятиями. Одно из центральных мест в аппарате современной алгебры занимают матрицы, и поэтому они не случайно используются во всех главах монографии, являясь одновременно их связующим звеном. Сначала это просто прямоугольные таблицы, и для понимания их не требуется специальной подготовки; затем они начинают занимать более видное место в изложении, и мы вводим обычные правила операций над ними. К теории чисел мы обращаемся редко, и в большинстве случаев для понимания происходящего вполне достаточно знакомства с общими положениями. Представления о полях и группах мы касаемся мимоходом и только в редких случаях выходим за рамки определения этих понятий.

Многие доказательства, приводимые нами, построены на рассуждениях вычислительного характера, на конечной индукции и на ряде других давно известных методов, однако это отнюдь не означает, что комбинаторная математика очень проста. Наоборот, этот раздел математики представляет значительные трудности как для усвоения, так и для изложения материала. Необходимость весьма

вдумчивого подхода к излагаемым результатам усугубляется тем, что приводимые нами определения и доказательства достаточно кратки. Но прилежание и острый ум ведут к мастерству, а наш предмет щедро вознаграждает тех, кто познает его тайны.

Некоторые разделы нашей науки мы излагаем очень подробно и выходим на передний край достижений современных исследований, но нам приходится расплачиваться за это — мы вынуждены отказаться от освещения многих интересных проблем.

В каждой главе приводится список литературы, который может служить руководством к дальнейшим исследованиям, однако мы далеко не претендуем на полноту этих списков.

На страницах этой книги мы касаемся ряда важных вопросов, на которые в настоящее время еще не найдены ответы. Но комбинаторная математика исключительно бурно развивается в наши дни, и мы верим, что ее важнейшие открытия еще впереди.

Я выражаю признательность математикам, которые оказали мне ту или иную помощь. Профессор М. Холл (младший) существенно помог мне и воодушевлял меня. Профессоры Р. П. Боас, И. Нивен и Р. Сильверман внесли много поправок в изложение материала. Большую помощь мне оказали также д-р Д. Р. Фалкерсон, д-р К. Гольдберг, д-р А. Дж. Хоффман, проф. Э. Клейнфельд, Д. Э. Кнут, д-р М. Ньюман, д-р Э. Т. Паркер, проф. Т. Радо и проф. А. У. Таккер. Профессор Г. М. Гехман и Ф. Г. Райзер помогли мне подготовить рукопись к печати.

Герберт Дж. Райзер

Сиракузский университет,
февраль 1963 г.

Глава 1

ОСНОВЫ КОМБИНАТОРНОЙ МАТЕМАТИКИ

1. Что такое комбинаторная математика? Комбинаторная математика, известная также под названием комбинаторного анализа или комбинаторики, является математической дисциплиной, возникшей в древние времена. Согласно одной легенде, китайский император Ю (примерно 2200 г. до н. э.) наблюдал магический квадрат

$$\begin{bmatrix} 4 & 9 & 2 \\ 3 & 5 & 7 \\ 8 & 1 & 6 \end{bmatrix}$$

на панцире некой божественной черепахи. Некоторые начальные сведения о перестановках появились в Китае еще до 1100 г. до н. э., а Бен Эзра (примерно 1140 г. н. э.), по-видимому, знал формулу для числа комбинаций из n элементов по r. Многие из самых ранних работ связаны с числовой мистикой. В течение нескольких последующих веков различные авторы подходили к комбинаторике с точки зрения математических развлечений. Широко известными примерами такого рода являются: задача Баше о взвешивании, задача Киркмана о школьницах и задача Эйлера о 36 офицерах [1]). Подобные задачи представляют интерес для упражнений интеллекта, а их решения иногда оказываются остроумными и изящными.

Многие из задач, которые изучали в прошлом для развлечения или в силу их эстетической привлекательности, приобрели в наше время большое значение как в теоретической, так и прикладной науке. Не так давно конечные проективные плоскости считались комбинатор-

[1]) См. также Кутлумуратов Дж., О развитии комбинаторных методов математики, Нукус, 1964. — *Прим. перев.*

ным курьезом. Сегодня же они служат исходными понятиями в основаниях геометрии, при анализе и планировании экспериментов. Новая техника с ее жизненно важными связями с дискретным придала развлекательной математике прошлого новые серьезные цели.

Гораздо более важным является то, что современная эпоха характеризуется возникновением широкого круга новых замечательных задач комбинаторики. Последние возникли в абстрактной алгебре, топологии, основаниях математики, теории графов, теории игр, линейном программировании и во многих других областях.

Комбинаторика всегда была многосторонней. В наши дни эта многосторонность особенно возросла. Однако многочисленные и разнообразные задачи комбинаторики не были успешно разработаны с позиций общей теории. Многое из того, о чем было сказано выше, в одинаковой степени приложимо к теории чисел, ибо комбинаторика и теория чисел являются родственными дисциплинами: они имеют определенные пересечения в общей системе математических знаний, и каждая из них существенно обогащает другую.

Комбинаторика затрагивает области многих разделов математики, и это обстоятельство затрудняет ее формальное определение. Но в основном она имеет дело с изучением расположения элементов в множества. Обычно число элементов конечно, а их расположение обусловлено определенными ограничительными условиями, вытекающими из условий исследуемой конкретной задачи.

В литературе, как правило, рассматриваются два общих типа задач. В первом из них существование предписанной конфигурации сомнительно, и исследование состоит в попытках доказать это существование. Такие задачи называются *проблемами существования*. Во втором типе задач существование конфигураций известно, а при исследованиях стремятся определить число конфигураций или дать их классификацию. Такие задачи мы называем *перечислительными*. В настоящей монографии упор сделан на задачи о существовании, но имеется и много перечислительных задач.

Можно заметить, что вторая категория задач есть не что иное, как усовершенствование или очевидное расши-

рение первой. Это так и есть. Но на практике получается, что если существование конфигурации требует интенсивного исследования, то почти ничего нельзя сказать о соответствующей перечислительной задаче. С другой стороны, если перечислительная задача поддается решению, то соответствующая задача существования обычно решается тривиально.

Проиллюстрируем эти замечания на элементарном примере. Удалим из шахматной 8×8-доски два квадратика из противоположных углов. Пусть имеется 31 кость домино, каждая из которых покрывает две клетки на доске. Задача состоит в том, чтобы покрыть всю доску этими костями. В этой задаче существование решения сомнительно. Покажем, что такое покрытие невозможно. В самом деле удалены два черных или два белых квадратика, и потому доска имеет неравное число черных и белых квадратиков. Но кость, положенная на доску, должна покрыть один белый и один черный квадрат. Следовательно, полное покрытие невозможно. Предположим, что квадраты, находящиеся на противоположных углах, не удалены; тогда покрыть доску 32 костями можно многими способами. При этих обстоятельствах приходим к перечислительной задаче об определении числа различных покрытий.

2. Множества. Пусть S — произвольное множество элементов $a, b, c, \ldots$. Обозначим тот факт, что s является элементом S, с помощью записи $s \in S$. Если каждый элемент множества A есть в то же время элемент множества S, то A есть *подмножество* S и мы обозначаем это символом $A \subseteq S$. Если $A \subseteq S$ и $S \subseteq A$, то эти два множества тождественны, и мы пишем $A = S$. Если $A \subseteq S$, но $A \neq S$, то A является *собственным* или *истинным* подмножеством множества S: $A \subset S$. Множество всех подмножеств множества S обозначают $P(S)$. Для удобства в символике пустое множество, или *нуль-множество* $\varnothing$, считается членом множества $P(S)$.

Пусть S и T — подмножества множества M. Множество элементов e, таких, что $e \in S$ и $e \in T$, называют *пересечением* $S \cap T$ множеств S и T. В более общем случае, если $T_1, T_2, \ldots, T_r$ суть подмножества множества M,

то $T_1 \cap T_2 \cap \ldots \cap T_r$ обозначает множество элементов e, таких, что $e \in T_i$ для всякого $i = 1, 2, \ldots, r$. Подмножества S и T множества M считаются *непересекающимися*, если они не имеют общих элементов. Равенство $S \cap T = \varnothing$ обозначает, что S и T не пересекаются. *Объединение* $S \cup T$ подмножеств S и T множества M есть множество элементов e, таких, что e принадлежит хотя бы одному из множеств S и T. В более общем случае, если $T_1, T_2, \ldots, T_r$ суть подмножества множества M, то $T_1 \cup T_2 \cup \ldots \cup T_r$ обозначает множество всех элементов e, таких, что $e \in T_i$ для одного по крайней мере $i = 1, 2, \ldots, r$. Подмножества $T_1, T_2, \ldots, T_r$ множества M образуют *разбиение* последнего при условии, что $M = T_1 \cup T_2 \cup \ldots \cup T_r$ и что $T_i \cap T_j = \phi$ для $i \neq j$ ($i, j = 1, 2, \ldots, r$). Разбиения M называются *упорядоченными*, если равенство разбиений

$$M = T_1 \cup T_2 \cup \ldots \cup T_r \quad \text{и} \quad M = T_1' \cup T_2' \cup \ldots \cup T_r'$$

означает, что $T_i = T_i'$ ($i = 1, 2, \ldots, r$), и *неупорядоченными*, если равенство разбиений означает, что каждое T_i равно некоторому T_j' [1]).

Множество S, содержащее только конечное число элементов, называется *конечным*. Конечное множество называется *множеством из n элементов*, если число его элементов равно в точности n. Употребляя эту терминологию, мы принимаем, что $n > 0$, и исключаем нуль-множество $\varnothing$. В дальнейшем в тексте мы будем называть множество из n элементов *n-множеством*. Таким образом, выражение „r-подмножество n-множества“ означает подмножество из r элементов множества из n элементов.

Многие вычислительные рассуждения широко используют следующие элементарные правила. Пусть S есть m-множество, а T есть n-множество. Если $S \cap T = \varnothing$, то $S \cup T$ есть $(m + n)$-множество. Это — *правило суммы*. *Обобщенное правило суммы* утверждает следующее: *если* T_i *есть* n_i*-множество* ($i = 1, 2, \ldots, r$) *и если* $M = T_1 \cup T_2 \cup \ldots \cup T_r$ *есть разбиение* M, *то* M *является* $(n_1 + n_2 + \ldots + n_r)$*-множеством*.

[1]) Порядок множеств равного объема при этом учитывается, так как такие множества взаимно заменяемы (в противном случае они оказываются неразличимыми). — *Прим. ред.*

Пусть S и T обозначают два множества, а (s, t) — упорядоченную пару элементов $s \in S$ и $t \in T$ [1]). Две пары (s, t) и (s^*, t^*) равны, если $s = s^*$ и $t = t^*$. Множество всех таких упорядоченных пар называется *произведением* S и T и обозначается $S \times T$. Пусть $M(S, T, n)$ обозначает множество упорядоченных пар вида (s, t), где s — произвольный элемент S, но каждый $s \in S$ попарно соединен в точности с n элементами $t \in T$. Различные элементы из S не должны быть попарно соединены элементами одного и того же n-подмножества множества T. Это понятие указывает, что T содержит по меньшей мере n элементов. Более того, $M(S, T, n) = S \times T$ тогда и только тогда, когда T есть n-множество. Пусть S есть m-множество. Тогда $M(S, T, n)$ есть (m, n)-множество. Это — *правило произведения. Обобщенное правило произведения* утверждает: *если* T_1 *есть* n_1*-множество и если* $M_2 = M(T_1, T_2, n_2)$, $M_3 = M(M_2, T_3, n_3)$ *и, наконец,* $M_r = M(M_{r-1}, T_r, n_r)$, *то* M_r *есть* $(n_1 n_2 \ldots n_r)$*-множество.*

3. Выборки. Пусть дано множество S и

$$(a_1, a_2, \ldots, a_r) \tag{3.1}$$

— упорядоченное r-множество элементов S, не обязательно различных. Два r-множества $(a_1, a_2, \ldots, a_r)$ и $(a_1^*, a_2^*, \ldots, a_r^*)$ равны, если $a_i = a_i^*$ $(i = 1, 2, \ldots, r)$. Назовем (3.1) *выборкой* из S. Эта выборка имеет *объем* r, и мы будем рассматривать (3.1) как r-выборку из S.

Теорема 3.1. *Число* r*-выборок из* n*-множества равно* n^r.

Доказательство. Пусть S есть n-множество. Настоящая теорема является частным случаем обобщенного правила произведения, где $T_1 = T_2 = \ldots = T_r = S$ и $n_1 = n_2 = \ldots = n_r = n$.

Пусть S есть n-множество и пусть компоненты a_i в r-выборке (3.1) различны. В таком случае r-выборку называют *r-перестановкой из n элементов*. В r-перестановке $r \leqslant n$; n-перестановка называется *перестановкой* n элементов.

[1]) То есть пара (s, t) отлична от пары (t, s). — *Прим. ред.*

Теорема 3.2. *Число r-перестановок из n элементов равно*

$$P(n, r) = n(n-1) \ldots (n-r+1). \qquad (3.2)$$

Доказательство. Эта теорема есть частный случай обобщенного правила произведения, когда $T_1 = T_2 = \ldots = T_r = S$ и $n_1 = n$, $n_2 = n-1$, ..., $n_r = n-r+1$. В соответствии с (3.2) введем $P(n, n)$ для обозначения произведения первых n натуральных чисел; $P(n, n)$ записывается $n!$ (читается „эн факториал"). Таким образом,

$$P(n, n) = n! = n(n-1) \ldots 1. \qquad (3.3)$$

Следствие 3.3. *Число перестановок n элементов равно* $n!$.

Отображение α (однозначное) множества S в множество T есть соответствие, в котором связывают с каждым $s \in S$ единственный элемент $t = s\alpha \in T$. Элемент $s\alpha$ называется *образом элемента s* при отображении α. Два отображения α и β множества S в множество T равны, если $s\alpha = s\beta$ для всех $s \in S$. Отображение α есть отображение S *на* T, если всякий элемент $t \in T$ является образом некоторого элемента $s \in S$. Отображение S на T будет взаимно однозначным, если различные элементы S имеют различные образы. Пусть теперь $G(S)$ будет множеством всех взаимно однозначных отображений S на себя. Пусть α и β входят в $G(S)$. Тогда отображение, переводящее $s \in S$ в $(s\alpha)\beta \in S$, есть взаимно однозначное отображение, называемое *произведением* отображений α и β. Множество $G(S)$ является алгебраической системой с бинарной операцией, называемой произведением, и можно убедиться, что $G(S)$ удовлетворяет аксиомам группы.

Пусть S есть n-множество элементов $1, 2, \ldots, n$. Тогда $G(S)$ называется *симметрической группой порядка n*. Она обозначается S_n. Пусть α — элемент S_n, который переводит i в $i\alpha$ $(i = 1, 2, \ldots, n)$. Взаимно однозначное отображение α характеризуется перестановкой

$$(1\alpha, 2\alpha, \ldots, n\alpha). \qquad (3.4)$$

Наоборот, всякая перестановка n элементов является в действительности взаимно однозначным отображением

элементов на себя. Число элементов в группе называется ее *порядком*. Теперь мы можем сформулировать следствие 3.3 в терминах теории групп.

Следствие 3.4. *Порядок S_n равен $n!$.*

Примеры. а) Число 2-перестановок из трех элементов равно $P(3, 2) = 3 \cdot 2 = 6$. Если перенумеровать элементы 1, 2, 3, то 2-перестановки суть:

$$(1, 2),\ (1, 3),\ (2, 1),\ (2, 3),\ (3, 1),\ (3, 2).$$

б) Число всевозможных слов, состоящих из пяти букв английского алфавита, равно 26^5. Если потребовать, чтобы буквы в этих словах были различными, то число слов будет равно

$$26 \cdot 25 \cdot 24 \cdot 23 \cdot 22 = 7\,893\,600.$$

в) S_{100} имеет порядок $(9{,}3326\ldots)\,10^{157}$. Эддингтоновская оценка числа электронов во вселенной составляет всего лишь $(136)\,2^{256}$.

г) Пусть A — матрица из m строк и n столбцов, составленная из нулей и единиц. Существует 2^{mn} таких матриц. Если $m = n = 100$, то это даст $2^{10\,000}$ матриц.

4. Неупорядоченные выборки. Пусть дано множество S и

$$\{a_1,\ a_2,\ \ldots,\ a_r\} \tag{4.1}$$

— неупорядоченная совокупность r элементов S, не обязательно различных. Число появлений элемента в этой совокупности называется *кратностью* элемента. Две таких совокупности $\{a_1,\ a_2,\ \ldots,\ a_r\}$ и $\{a_1^*,\ a_2^*,\ \ldots,\ a_r^*\}$ будут равны, если элементы с их соответствующими кратностями будут теми же самыми в обеих совокупностях. Назовем (4.1) *неупорядоченной выборкой* из S. Неупорядоченная выборка имеет здесь объем r, и мы будем рассматривать (4.1) как *r-выборку* из S. Если каждый элемент в (4.1) имеет кратность 1, то r-выборка является r-подмножеством множества S; r-подмножество n-множества называется также *r-сочетанием* из n элементов.

Для натуральных n (3.3) утверждает, что

$$n! = P(n,\ n). \tag{4.2}$$

Удобно определить

$$0! = 1, \tag{4.3}$$

так что для любого положительного целого n

$$n! = n(n-1)!. \tag{4.4}$$

Положим теперь, что n и r — натуральные числа и определим

$$\begin{aligned} C(n, r) &= \binom{n}{r} = \frac{n(n-1)\dots(n-r+1)}{r!}, \\ C(n, 0) &= \binom{n}{0} = 1, \\ C(0, r) &= \binom{0}{r} = 0, \\ C(0, 0) &= \binom{0}{0} = 1. \end{aligned} \tag{4.5}$$

Таким образом, (4.5) определяет $C(n, r)$ для всех неотрицательных целых n и r. Заметим, что если $r > n$, то $C(n, r) = 0$. Это означает, что если n фиксировано, то $C(n, r)$ принимает только конечное число различных значений. Числа $C(n, r)$, определенные соотношениями (4.5), — знакомые нам *биномиальные коэффициенты*. Им принадлежит немалая роль в перечислительных задачах.

Теорема 4.1. *Число r-подмножеств n-множества равно*

$$\binom{n}{r}.$$

Доказательство. По теореме 3.2 число r-перестановок из n элементов равно $P(n, r)$. Каждая r-перестановка может быть упорядочена $r!$ способами. Если пренебречь порядком, то число различимых расположений равно

$$C(n, r) = \frac{P(n, r)}{r!}. \tag{4.6}$$

Пусть дано n-множество S и пусть $P(S)$ обозначает множество всех подмножеств S. Обозначим через T мно-

жество всех n-выборок, получаемых из 2-множества целых чисел 0 и 1. Существует естественное взаимно однозначное отображение $P(S)$ на T. Так, если $X = \{a_{i_1}, a_{i_2}, \ldots, a_{i_r}\}$ входит в $P(S)$, то образом X при взаимно однозначном отображении является n-выборка с единицами на местах $i_1, i_2, \ldots, i_r$ и с нулями — на остальных местах. Теперь применим теорему 4.1, чтобы подсчитать число элементов в $P(S)$, и теорему 3.1 для подсчета числа элементов в множестве T. Приравнивая эти результаты, получаем

$$\binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{n} = 2^n. \tag{4.7}$$

Разумеется, тождество (4.7) элементарно. Но доказательство его демонстрирует способ, оказывающийся эффективным во многих комбинаторных исследованиях.

Теорема 4.2. *Число r-выборок из n-множества равно*

$$\binom{n+r-1}{n-1} = \binom{n+r-1}{r}. \tag{4.8}$$

Доказательство. Заменим n-множество S на n-множество S' натуральных чисел 1, 2, ..., n. Всякая r-выборка из множества S' может быть записана в виде

$$\{a_1, a_2, \ldots, a_r\}, \tag{4.9}$$

где

$$a_1 \leqslant a_2 \leqslant \ldots \leqslant a_r. \tag{4.10}$$

Пусть теперь S^* есть $(n+r-1)$-множество натуральных чисел 1, 2, ..., $n+r-1$. Тогда

$$(a_1+0,\ a_2+1,\ \ldots,\ a_r+r-1) \tag{4.11}$$

является r-подмножеством множества S^*. Более того, соответствие

$$\{a_1, a_2, \ldots, a_r\} \leftrightarrow \{a_1+0,\ a_2+1,\ \ldots,\ a_r+r-1\} \tag{4.12}$$

есть взаимно однозначное отображение r-выборки из множества S' на r-подмножество множества S^*. Но по тео-

реме 4.1 число r-подмножеств множества S^* равно

$$\binom{n+r-1}{r}.$$

Пусть дано разбиение n-множества S на r_i-подмножества T_i $(i=1, 2, \ldots, k)$:

$$S = T_1 \cup T_2 \cup \ldots \cup T_k. \tag{4.13}$$

Тогда

$$n = r_1 + r_2 + \ldots + r_k. \tag{4.14}$$

Разбиение (4.13) будем называть $(r_1, r_2, \ldots, r_k)$-*разбиением* множества S.

Теорема 4.3. *Число неупорядоченных*[1] $(r_1, r_2, \ldots, r_k)$-*разбиений n-множества равно*

$$\frac{n!}{r_1!\, r_2! \ldots r_k!}. \tag{4.15}$$

Доказательство. По теореме 4.1 и обобщенному правилу произведения число неупорядоченных $(r_1, r_2, \ldots, r_k)$-разбиений n-множества равно

$$\binom{n}{r_1}\binom{n-r_1}{r_2}\ldots\binom{n-r_1-\ldots-r_k}{r_k} = \frac{n!}{r_1!\, r_2! \ldots r_k!}. \tag{4.16}$$

Числа (4.15) называются *полиномиальными коэффициентами*. Из теоремы 4.3 следует, что число неупорядоченных $(1, 1, \ldots, 1)$-разбиений n-множества равно $n!$. В этом случае теорема 4.3 сводится к следствию 3.3. Число неупорядоченных $(r, n-r)$-разбиений n-множества равно

$$\frac{n!}{r!\,(n-r)!}.$$

В этом случае теорема 4.3 сводится к теореме 4.1.

Полиномиальные коэффициенты теоремы 4.3 имеют другую весьма полезную комбинаторную интерпретацию. Пусть S есть k-множество элементов $a_1, a_2, \ldots, a_k$ и

$$n = r_1 + r_2 + \ldots + r_k, \tag{4.17}$$

где r_i — натуральные числа. Пусть $(a_{i_1}, a_{i_2}, \ldots, a_{i_n})$ означает n-выборку из множества S, в которой a_i содер-

[1]) В оригинале — „упорядоченных", что неверно (см. определение и примечание к нему на стр. 11). — *Прим. ред.*

жится ровно r_i раз ($i = 1, 2, \ldots, k$). Обозначим через T множество всех таких выборок. Тогда число элементов множества T равно

$$\frac{n!}{r_1! r_2! \ldots r_k!}, \tag{4.18}$$

ибо в каждой выборке r_1 элементов a_1 могут быть заменены на r_1 различных элементов, отличающихся от элементов выборки. Затем эти r_1 элементов могут быть переставлены $r_1!$ способами, и таким образом каждая выборка дает $r_1!$ новых выборок. Применим эту процедуру замещения к новой совокупности выборок и заменим каждый из r_2 элементов a_2 на r_2 различных элементов, отличных от элементов выборки. Эта процедура ограничена тем, что всего имеется $n!$ перестановок. Следовательно, число элементов множества T задано выражением (4.18).

Примеры. а) Сдача карт при игре в бридж представляет выбор 13 карт из колоды в 52 карты. Порядок карт при сдаче несуществен. Значит, число различных сдач будет

$$\binom{52}{13} = 635\ 013\ 559\ 600.$$

б) В игре в бридж 52 карты колоды распределяются между четырьмя игроками. Каждый игрок получает 13 карт. Следовательно, число различных ситуаций за карточным столиком равно

$$\frac{52!}{(13!)^4} = (5{,}3645\ldots)\, 10^{28}.$$

в) Число слов, состоящих из 12 букв, которые могут быть образованы из четырех букв a, четырех букв b, двух букв c и двух букв d, будет равно

$$\frac{12!}{4!\,4!\,2!\,2!} = 207\,900.$$

г) Число слов из пяти букв, которые могут быть образованы из букв a, b и c и в которых буква a появляется самое большее дважды, буква b — самое большее один раз, а буква c — не более трех раз, будет равно

$$\frac{5!}{2!\,0!\,3!} + \frac{5!}{2!\,1!\,2!} + \frac{5!}{1!\,1!\,3!} = 60.$$

д) Бросание множества r игральных костей можно рассматривать как r-выборку из 6-множества. Число различных выпадений будет

$$\binom{r+5}{5} = \binom{r+5}{r}.$$

5. Биномиальные коэффициенты. Дано, что n и r — натуральные числа. Тогда

$$\binom{n}{r}=\binom{n-1}{r}+\binom{n-1}{r-1}. \tag{5.1}$$

Формула (5.1) представляет основное рекуррентное соотношение для биномиальных коэффициентов, являющееся непосредственным следствием определения (4.5). Исследования предыдущего параграфа показывают, что биномиальные коэффициенты — целые числа. Докажем теперь это утверждение с помощью математической индукции. Если $n=0$ или $r=0$, то оно верно непосредственно из (4.5). Если n и r положительны, то из предположения индукции вытекает, что два члена в правой части равенства (5.1) — целые. Следовательно, член в левой части (5.1) должен быть целым числом. Это утверждение может быть сформулировано в более яркой форме: *произведение r последовательных натуральных чисел делится на $r!$.*

Будем называть натуральное число, не равное 1, *простым*, если оно делится только на самого себя и на единицу.

Теорема 5.1. *Если p — простое, то числа*

$$\binom{p}{1}, \binom{p}{2}, \ldots, \binom{p}{p-1} \tag{5.2}$$

делятся на p.

Доказательство. Пусть r — целое число в интервале $1 \leqslant r \leqslant p-1$. Тогда

$$p(p-1)\ldots(p-r+1) \tag{5.3}$$

делится на $r!$. Но $r!$ просто по отношению к p, и, следовательно,

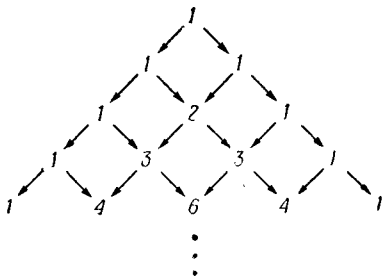
$$(p-1)(p-2)\ldots(p-r+1) \tag{5.4}$$

делится на $r!$. Таким образом,

$$\binom{p}{r}=p\frac{(p-1)(p-2)\ldots(p-r+1)}{r!} \tag{5.5}$$

делится на p.

Формула (5.1) подсказывает эффективный способ вычисления биномиальных коэффициентов. Схематически он иллюстрируется диаграммой (5.6)



(5.6)

известной под названием *треугольника Паскаля*. Мы рассматриваем стрелку в (5.6) как односторонний путь. Если можно пройти от одного биномиального коэффициента P до другого биномиального коэффициента Q в (5.6) по последовательности односторонних путей, начинающейся в P и заканчивающейся в Q, мы скажем, что P и Q связаны односторонним маршрутом. Пусть I обозначает единицу, расположенную в вершине треугольника. Тогда оказывается, что I и P связаны разными односторонними маршрутами. Биномиальный коэффициент P показывает число различных маршрутов. Эта интересная особенность треугольника Паскаля есть неотъемлемое свойство его построения из (5.1). Симметрия и монотонность горизонтальных строк в (5.6) следуют из соотношений

$$\binom{n}{r} = \binom{n}{n-r} \quad (0 \leqslant r \leqslant n), \tag{5.7}$$

$$\binom{2n}{0} < \binom{2n}{1} < \ldots < \binom{2n}{n}, \tag{5.8}$$

$$\binom{2n-1}{0} < \binom{2n-1}{1} < \ldots < \binom{2n-1}{n-1} = \binom{2n-1}{n}. \tag{5.9}$$

Пусть n — натуральное число. Тогда

$$(x+y)^n = \binom{n}{0} x^n + \binom{n}{1} x^{n-1}y + \ldots + \binom{n}{n} y^n. \tag{5.10}$$

Алгебраическое тождество (5.10) является хорошо известной биномиальной теоремой. Мы даем доказательство (5.10), основанное на идеях п. 4. Пусть S есть n-множество символов

$$(x+y)_1,\ (x+y)_2,\ \ldots,\ (x+y)_n. \tag{5.11}$$

Тогда для $r>0$ коэффициент при $x^{n-r}y^r$ в разложении $(x+y)^n$ равен числу r-подмножеств множества S. Но по теореме 4.1 это число равно

$$\binom{n}{r}, \tag{5.12}$$

следовательно, формула (5.10) справедлива.

Многие тождества для биномиальных коэффициентов легко выводятся из (5.1) и (5.10). Формула (5.1) идеальна для доказательства методом индукции заданного тождества. Разложение (5.10) подвергается формальным преобразованиям и является непосредственным источником многих соотношений между коэффициентами. Например, если в (5.10) мы положим $x=y=1$, то

$$\binom{n}{0}+\binom{n}{1}+\ \ldots\ +\binom{n}{n}=2^n. \tag{5.13}$$

С другой стороны, если положим $x=1$, а $y=-1$, то

$$\binom{n}{0}-\binom{n}{1}+\ \ldots\ +(-1)^n\binom{n}{n}=0. \tag{5.14}$$

Следующие типичные тождества часто встречаются в литературе и могут быть выведены элементарными методами:

$$\sum_{k=0}^{n}\binom{n}{k}^2=\binom{2n}{n}, \tag{5.15}$$

$$\sum_{k=1}^{n}k\binom{n}{k}=n\cdot 2^{n-1}, \tag{5.16}$$

$$\sum_{k=1}^{n}k^2\binom{n}{k}=n(n+1)\cdot 2^{n-2}, \tag{5.17}$$

$$\sum_{k=1}^{n}\frac{(-1)^{k-1}}{k}\binom{n}{k}=1+\frac{1}{2}+\ \ldots\ +\frac{1}{n}. \tag{5.18}$$

ЛИТЕРАТУРА

Свойства делимости биномиальных и полиномиальных коэффициентов рассматриваются в книге [1], гл. 9.

1. Dickson L. E., History of the Theory of Numbers, vol. 1, New York, 1952.
2. Feller W., Probability Theory and Its Applications, vol. 1, New York, 1950. (Русский перевод: Феллер В., Введение в теорию вероятностей и ее приложения, ИЛ, 1952; русский перевод второго издания, изд-во „Мир", 1964.)
3. Netto E., Lehrbuch der Combinatorik, Leipzig, 2 Aufl., 1927.
4. Riordan J., An Introduction to Combinatorial Analysis, New York, 1958. (Русский перевод: Риордан Дж., Введение в комбинаторный анализ, ИЛ, 1963.)

Глава 2

ПРИНЦИП ВКЛЮЧЕНИЯ И ИСКЛЮЧЕНИЯ

1. Основная формула. Пусть дано n-множество S; всякому $a \in S$ припишем единственный *вес* $w(a)$, где $w(a)$ — элемент некоторого поля F. Никаких ограничений на поле F или на выбор весов из этого поля не накладывается. Однако нередко сами комбинаторные задачи подсказывают какие-то естественные назначения весов. Во многих задачах каждому $a \in S$ приписан вес $w(a)$, равный единице. Пусть P обозначает N-множество свойств

$$P_1, P_2, \ldots, P_N, \tag{1.1}$$

связанных с элементами множества S, и пусть

$$\{P_{i_1}, P_{i_2}, \ldots, P_{i_r}\} \tag{1.2}$$

обозначает r-подмножество множества P. Пусть

$$W(P_{i_1}, P_{i_2}, \ldots, P_{i_r}) \tag{1.3}$$

равно сумме весов тех элементов из S, которые обладают каждым из свойств $P_{i_1}, P_{i_2}, \ldots, P_{i_r}$. Если в множестве S нет ни одного такого элемента, то выражению (1.3) приписывается значение, равное нулю. Далее, пусть

$$W(r) = \sum W(P_{i_1}, P_{i_2}, \ldots, P_{i_r}) \tag{1.4}$$

равно сумме значений (1.3) для всех r-подмножеств множества P.

Распространим (1.4) на случай $r = 0$ и положим $W(0)$ равным сумме весов элементов S. Теперь мы в состоянии сформулировать и доказать основную теорему включения и исключения.

Теорема 1.1. *Пусть $E(m)$ обозначает сумму весов элементов множества S, которые удовлетво-*

ряют в точности m свойствам (1.1). *Тогда*

$$E(m) = W(m) - \binom{m+1}{m} W(m+1) + \binom{m+2}{m} W(m+2) - \ldots + (-1)^{N-m} \binom{N}{m} W(N). \quad (1.5)$$

Доказательство. Пусть $a \in S$; a обладает весом $w(a)$ и удовлетворяет в точности t свойствам (1.1). Если $t < m$, то a дает нуль в правой части (1.5). С другой стороны, если $t = m$, то a дает в правой части (1.5) вес $w(a)$. Если же $t > m$, то a дает в правой части (1.5)

$$\left[\binom{t}{m} - \binom{m+1}{m}\binom{t}{m+1} + \binom{m+2}{m}\binom{t}{m+2} - \ldots + (-1)^{t-m}\binom{t}{m}\binom{t}{t}\right] w(a). \quad (1.6)$$

Но

$$\binom{k}{m}\binom{t}{k} = \binom{t}{m}\binom{t-m}{t-k} \qquad (m \leqslant k \leqslant t), \quad (1.7)$$

и, следовательно, (1.6) сводится к

$$\binom{t}{m}\left[\binom{t-m}{t-m} - \binom{t-m}{t-(m+1)} + \binom{t-m}{t-(m+2)} - \ldots + (-1)^{t-m}\binom{t-m}{t-t}\right] w(a). \quad (1.8)$$

Но вследствие (5.14) из гл. 1 выражение в скобках в (1.8) равно нулю. Следовательно, если $t > m$, то a дает нуль в правой части (1.5). Из этого вытекает, что правая часть (1.5) есть сумма весов элементов множества S, удовлетворяющих в точности m свойствам (1.1).

Теорема 1.2. *Пусть $E(0)$ обозначает сумму весов элементов множества S, не удовлетворяющих ни одному из свойств* (1.1). *Тогда*

$$E(0) = W(0) - W(1) + W(2) - \ldots + (-1)^N W(N). \quad (1.9)$$

Доказательство. Это частный случай теоремы 1.1, именно при $m = 0$.

Пусть каждому $a \in S$ приписан вес, равный $+1$. Тогда сумма весов равна числу слагаемых в сумме. В этом случае в теореме 1.2 имеем $W(0) = n$, а $E(0)$ есть число элементов множества S, не удовлетворяющих ни одному из свойств (1.1). Получающийся при этом частный вид равенства (1.9) называется *формулой решета*. Эта формула приписывается Да Сильве и Сильвестру. В действительности формула решета известна с давних времен и, возможно, уже была известна в том или другом виде еще кому-нибудь из семьи Бернулли. Следующие три пункта этой главы мы посвящаем различным приложениям теоремы 1.1.

2. Приложения к теории чисел. В этом пункте мы применяем формулу решета к избранным вопросам элементарной теории чисел.

Пусть x — действительное неотрицательное число. Обозначим через

$$[x] \tag{2.1}$$

наибольшее целое число, не превышающее x. Пусть также

$$(a, b) \tag{2.2}$$

— наибольший общий делитель двух целых чисел a и b, не равных нулю. Тогда $(a, b) = 1$ означает, что a и b взаимно просты. Будем писать

$$a \mid b, \tag{2.3}$$

если a делит b, и

$$a \nmid b, \tag{2.4}$$

если a не делит b.

Теорема 2.1. *Дано натуральное число a и натуральные числа $a_1, a_2, \ldots, a_N$, такие, что $(a_i, a_j) = 1$, если $i \neq j$. Тогда число целых чисел k, таких, что*

$$0 < k \leqslant n, \quad a_i \nmid k \qquad (i = 1, 2, \ldots, N) \tag{2.5}$$

равно

$$n - \sum_{1 \leqslant i \leqslant N} \left[\frac{n}{a_i}\right] + \sum_{1 \leqslant i < j \leqslant N} \left[\frac{n}{a_i a_j}\right] - \ldots$$
$$\ldots + (-1)^N \left[\frac{n}{a_1 a_2 \ldots a_N}\right]. \tag{2.6}$$

Доказательство. Пусть S есть n-множество натуральных чисел 1, 2, ..., n, а P_i — свойство, означающее, что элемент множества S делится на a_i ($i = 1, 2, \ldots, N$). По условию все a_i попарно взаимно просты. Следовательно, выражение

$$W(P_{i_1}, P_{i_2}, \ldots, P_{i_r}) \tag{2.7}$$

в формуле решета есть число таких целых чисел k, что

$$0 < k \leqslant n, \quad a_{i_1} a_{i_2} \ldots a_{i_r} \mid k. \tag{2.8}$$

Но это число равно

$$\left[\frac{n}{a_{i_1} a_{i_2} \ldots a_{i_r}} \right]. \tag{2.9}$$

Функция Эйлера $\varphi(n)$, где n — натуральное число, есть число таких целых чисел k, что

$$0 < k \leqslant n, \qquad (k, n) = 1. \tag{2.10}$$

Теорема 2.2. *Пусть n — натуральное число. Тогда*

$$\varphi(n) = n \prod_p \left(1 - \frac{1}{p}\right). \tag{2.11}$$

Произведение в (2.11) *распространено на все простые делители p числа n.*

Доказательство. В теореме (2.1) заменим a_i на p_i и предположим, что $p_1, p_2, \ldots, p_N$ — простые делители n. Тогда из (2.6) следует

$$\varphi(n) = n - \sum_{1 \leqslant i \leqslant N} \frac{n}{p_i} + \sum_{1 \leqslant i < j \leqslant N} \frac{n}{p_i p_j} - \ldots$$

$$\ldots + (-1)^N \frac{n}{p_1 p_2 \ldots p_N}. \tag{2.12}$$

Но это выражение эквивалентно (2.11).

Функция Мёбиуса $\mu(n)$ натурального аргумента n определена так:

$$\left.\begin{array}{ll} \mu(1)=1, & \\ \mu(n)=0, & \text{если } n \text{ делится на квадрат простого числа,} \\ \mu(p_1, p_2, \ldots, p_k)=(-1)^k, & \text{если простые числа } p_1, p_2, \ldots, p_k \text{ различны.} \end{array}\right\} \quad (2.13)$$

Функция Мёбиуса позволяет записать (2.12) в более изящном виде

$$\varphi(n)=n\sum_d \frac{\mu(d)}{d}. \quad (2.14)$$

Суммирование в (2.14) производится по всем d — положительным делителям n.

Пусть n — натуральное число. Если известны простые числа, не превышающие $\sqrt{n}$, то простые числа, не превышающие n, могут быть найдены следующим способом. Напишем последовательность

$$2, 3, \ldots, n. \quad (2.15)$$

Вычеркнем из (2.15) все числа, делящиеся на 2, затем — все числа, делящиеся на 3, на 5 и т. д., и, наконец, все числа, делящиеся на q, где q есть наибольшее простое число, не превышающее $\sqrt{n}$. Оставшиеся числа будут все простыми, бóльшими $\sqrt{n}$ и не превышающими n, потому что они не могут иметь простого множителя, не превышающего $\sqrt{n}$, а также не могут быть произведением двух чисел, бóльших $\sqrt{n}$.

Этот интересный метод построения простых чисел называется *решетом Эратосфена*.

Обозначим через $\pi(x)$ число простых чисел, не превышающих положительного действительного числа x. В результате применения решета Эратосфена к последовательности (2.15) остается

$$\pi(n)-\pi(\sqrt{n}) \quad (2.16)$$

целых чисел. Но число это можно подсчитать и другим способом. В теореме 2.1 заменим a_i на q_i и предположим,

что числа $q_1, q_2, \ldots, q_N$ все простые, не превосходящие $\sqrt{n}$. Тогда по теореме 2.1 искомое число равно

$$-1+n-\sum_{1\leqslant i\leqslant N}\left[\frac{n}{q_i}\right]+\sum_{1\leqslant i<j\leqslant N}\left[\frac{n}{q_iq_j}\right]-\ldots$$

$$\ldots+(-1)^N\left[\frac{n}{q_1q_2\ldots q_N}\right]. \quad (2.17)$$

Отсюда следует, что

$$\pi(n)-\pi(\sqrt{n})=-1+\sum_d \mu(d)\left[\frac{n}{d}\right]. \quad (2.18)$$

Суммирование в (2.18) производится по всем положительным делителям d произведения $q_1q_2\ldots q_N$, где $q_1, q_2, \ldots, q_N$ — простые числа, не превосходящие $\sqrt{n}$.

3. Беспорядки. Пусть

$$(a_1, a_2, \ldots, a_n) \quad (3.1)$$

является перестановкой n элементов $1, 2, \ldots, n$. Перестановка (3.1) называется *беспорядком*, если $a_i \neq i$ $(i=1, 2, \ldots, n)$. Таким образом, в беспорядке ни один элемент не занимает своего естественного места. Задача Монмора, хорошо известная под французским названием „задачи о встречах" (Le problème des recontres), состоит в том, чтобы подсчитать число таких беспорядков. Пусть D_n обозначает это число. Мы можем легко вычислить D_n по формуле решета. В самом деле, пусть S — множество $n!$ перестановок (3.1) и пусть P_i обозначает то свойство, что в перестановке (3.1) имеет место $a_i=i$ $(i=1, 2, \ldots, n)$. Тогда

$$W(P_{i_1}, P_{i_2}, \ldots, P_{i_r})=(n-r)! \quad (3.2)$$

и

$$W(r)=\binom{n}{r}(n-r)!=\frac{n!}{r!}. \quad (3.3)$$

Таким образом, мы получаем следующую формулу для D_n:

$$D_n=n!\left(1-\frac{1}{1!}+\frac{1}{2!}-\ldots+(-1)^n\frac{1}{n!}\right). \quad (3.4)$$

Формула (3.4) напоминает знакопеременный ряд для e^{-1}

$$e^{-1} = 1 - \frac{1}{1!} + \frac{1}{2!} - \ldots. \tag{3.5}$$

Фактически мы можем теперь записать (3.5) в виде

$$e^{-1} = \frac{D_n}{n!} + (-1)^{n+1} \frac{1}{(n+1)!} \pm \ldots, \tag{3.6}$$

а это означает, что $D_n/n!$ и e^{-1} отличаются друг от друга меньше чем на $1/(n+1)!$. Следовательно, $n!e^{-1}$ является весьма хорошим приближением для D_n.

Формула (3.4) имеет большое число довольно любопытных приложений. Предположим, например, что n мужчин пришли на вечер и оставили свои n шляп в передней. Вслед за тем шляпы были спутаны и возвращены гостям в случайном порядке. Вероятность того, что ни один мужчина не получит своей шляпы, равна $D_n/n!$. Это приложение имеет много разновидностей. Но удивительным свойством является то, что для всех практических целей вероятность равна e^{-1} и совсем несущественно, 10 человек присутствуют или 10 000. В задаче с более серьезным оттенком спрашивается о числе способов, которыми могут быть размещены на условной шахматной доске восемь ладей так, чтобы ни одна ладья не могла атаковать другую, а белая диагональ была бы свободной от ладей. Это может быть осуществлено $D_8 = 14\,833$ различными способами.

4. Перманент. В дальнейшем мы будем предполагать знакомство с элементами теории матриц и с этой целью введем здесь систему обозначений и терминов, которые будем использовать в тексте книги. Пусть дано множество S. *Прямоугольная таблица* (array), основанная на множестве S, есть конфигурация из m строк и n столбцов вида

$$A = \begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \cdot & \cdot & \cdot & \cdot \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{bmatrix}. \tag{4.1}$$

Элемент a_{ij}, находящийся в i-й строке и j-столбце таблицы A, должен быть элементом множества S; на само множество S не следует накладывать никаких ограничений. Мы будем говорить, что a_{ij} занимает (i, j)-*положение* в A. Всякий раз, когда мы пожелаем подчеркнуть тот факт, что A содержит m строк и n столбцов, мы будем упоминать об A как о $(m \times n)$-таблице, или, что равносильно, скажем, что A имеет *размер* $m \times n$. Если $m = n$, то A является *квадратной* таблицей и имеет *порядок* n. Если из A вычеркнуты $m - r$ строк и $n - s$ столбцов, то получившаяся прямоугольная таблица размера $r \times s$ называется *подтаблицей* A. Две $(m \times n)$-таблицы равны, если соответствующие элементы на (i, j)-положениях равны $(i = 1, 2, 3, \ldots, m;\ j = 1, 2, \ldots, n)$. В определенном смысле таблица (4.1) является не чем иным, как выборкой размера $m \times n$ из данного множества S. Но, с другой стороны, $(1 \times n)$-таблицу можно рассматривать как выборку размера n, и таким образом (4.1) оказывается естественным обобщением этого понятия. Теперь заменим довольно громоздкую символику (4.1) на

$$A = [a_{ij}] \quad (i = 1, 2, \ldots, m;\ j = 1, 2, \ldots, n). \tag{4.2}$$

Пусть $e = \min(m, n)$. В этом случае *главная диагональ* A состоит из элементов a_{ii}, находящихся в положении (i, i) для $i = 1, 2, \ldots, e$. *Транспонированной таблицей* A^T от A является $(n \times m)$-таблица, полученная из A путем отражения A относительно главной диагонали. Таким образом, A^T содержит a_{ji} в (i, j)-положениях $(i = 1, 2, \ldots, n;\ j = 1, 2, \ldots, m)$. Таблица A называется *симметрической*, если $A = A^T$.

Предположим теперь, что множество S есть некоторое поле F. Тогда прямоугольная таблица оказывается матрицей. Сложение и скалярное умножение для $(m \times n)$-матриц может быть определено обычным образом, и множество всех $(m \times n)$-матриц, элементы которых входят в поле F, образует векторное пространство размерности mn над F. Более того, $(m \times n)$-матрица может быть умножена на $(n \times t)$-матрицу по известному правилу умножения матриц. Матрица-произведение имеет размер $m \times t$. Заметим, что если A имеет размер $m \times n$, то мы можем всегда образовать произведения AA^T порядка m и A^TA порядка n.

Эти произведения в действительности являются симметрическими матрицами.

Пусть теперь дана матрица $A = [a_{ij}]$ размера $m \times n$, где $m \leqslant n$. Введем следующее определение *перманента* матрицы A:

$$\operatorname{per}(A) = \sum a_{1i_1} a_{2i_2} \ldots a_{mi_m}. \tag{4.3}$$

Суммирование в (4.3) производится по всем m-перестановкам $(i_1, i_2, \ldots, i_m)$ целых чисел $1, 2, \ldots, n$. Эта скалярная функция матрицы A нередко появляется в литературе по комбинаторному анализу в связи с определенными перечислительными и экстремальными задачами. Рассмотрим теперь некоторые формальные свойства $\operatorname{per}(A)$. Прежде всего, $\operatorname{per}(A)$ оказывается инвариантным относительно любых перестановок строк и столбцов в A. Таким образом, умножение одной строки A на скаляр a в F просто заменяет $\operatorname{per}(A)$ на $a \cdot \operatorname{per}(A)$. Рассмотрим далее важный частный случай, когда A является квадратной матрицей порядка n. В этом случае $\operatorname{per}(A)$ оказывается инвариантным также и относительно транспозиций, и мы можем записать

$$\operatorname{per}(A) = \operatorname{per}(A^T). \tag{4.4}$$

В этом случае $\operatorname{per}(A)$ является тем же, что и детерминант, $\det(A)$, если не говорить о множителях ± 1, предшествующих каждому произведению в правой части равенства (4.3). Это предполагает возможность вычислительной процедуры для $\operatorname{per}(A)$, аналогичной хорошо развитой теории для $\det(A)$. В самом деле, законы, определенные для детерминантов, аналогичны законам, определенным для перманентов. Например, разложение Лапласа для детерминантов целиком переносится и на перманенты. Но основной мультипликативный закон, справедливый для детерминантов:

$$\det(AB) = \det(A) \cdot \det(B), \tag{4.5}$$

глубоко ошибочен для перманентов. Прибавление строки A, умноженной на некоторое число, к другой строке также не оставляет $\operatorname{per}(A)$ инвариантным. Эти обстоятельства чрезвычайно затрудняют технику вычисления $\operatorname{per}(A)$; поэтому многие квадратные матрицы имеют легко вычи-

сляемые детерминанты и неопределяемые перманенты. Опишем теперь метод вычисления $\operatorname{per}(A)$.

Теорема 4.1. *Дана матрица A размера $m \times n$, где $m \leqslant n$. Пусть A_r обозначает матрицу, полученную из A заменой r ее столбцов на столбцы, составленные из нулей. Пусть $S(A_r)$ — произведение сумм строк A_r, а $\sum S(A_r)$ — суммы $S(A_r)$ по всем выборам для A_r. Тогда*

$$\operatorname{per}(A) = \sum S(A_{n-m}) - \binom{n-m+1}{1} \sum S(A_{n-m+1}) + \\ + \binom{n-m+2}{2} \sum S(A_{n-m+2}) - \dots \\ \dots + (-1)^{m-1} \binom{n-1}{m-1} \sum S(A_{n-1}). \quad (4.6)$$

Доказательство. Обозначим через S множество всех выборок объема m

$$(j_1, j_2, \dots, j_m) \quad (4.7)$$

целых положительных чисел 1, 2, ..., n. Пусть вес выборки (4.7) равен

$$a_{1j_1} a_{2j_2} \dots a_{mj_m}. \quad (4.8)$$

Пусть P_i означает то свойство, что выборка (4.7) не содержит целого числа i ($i = 1, 2, \dots, n$). Предположим теперь, что A_r получено из A заменой столбцов с номерами $i_1, i_2, \dots, i_r$ на столбцы, составленные из нулей. Тогда

$$W(P_{i_1}, P_{i_2}, \dots, P_{i_r}) = S(A_r), \quad (4.9)$$

и, следовательно,

$$W(r) = \sum S(A_r). \quad (4.10)$$

Функция $\operatorname{per}(A)$ равна сумме весов элементов S, удовлетворяющих $n - m$ свойствам P_i ($i = 1, 2, \dots, n$). Таким образом, (4.6) оказывается следствием теоремы 1.1.

Следствие 4.2. *Пусть дана квадратная матрица A порядка n. Тогда*

$$\operatorname{per}(A) = S(A) - \sum S(A_1) + \sum S(A_2) - \ldots \\ \ldots + (-1)^{n-1} \sum S(A_{n-1}). \quad (4.11)$$

Доказательство. Это частный случай теоремы 4.1 для $m = n$.

Пусть A — матрица, элементами которой являются либо 0, либо 1. Назовем такую матрицу (0, 1)-*матрицей*; 2^{mn} таких (0, 1)-матриц размера $m \times n$ имеют важное значение в комбинаторике; они будут играть ведущую роль и в нашем изложении предмета. Пока же мы ограничимся немногими элементарными замечаниями относительно перманентов некоторых весьма специальных (0, 1)-матриц. Пусть I — единичная матрица порядка n, а J—матрица порядка n, составленная целиком из единиц. Нетрудно проверить, что

$$\operatorname{per}(J) = n!, \quad (4.12)$$

$$\operatorname{per}(J - I) = D_n. \quad (4.13)$$

Заметим в заключение, что из (4.11) и (4.12) вытекает тождество

$$n! = \sum_{r=0}^{n-1} (-1)^r \binom{n}{r} (n-r)^n. \quad (4.14)$$

Кроме того, из (4.11) и (4.13) получается вторая формула для числа беспорядков, а именно

$$D_n = \sum_{r=0}^{n-1} (-1)^r \binom{n}{r} (n-r)^n (n-r-1)^{n-r}. \quad (4.15)$$

ЛИТЕРАТУРА

1. Feller W., Probability Theory and Its Applications, vol. 1, New York, 1950. (О русских переводах этой книги см. стр. 22).
2. Hardy G. H., Wright E. M., An Introduction to the Theory of Numbers, 3 ed., 1954.
3. Nagell T., Introduction to Number Theory, New York, 1951.
4. Riordan J., An Introduction to Combinatorial Analysis, New York, 1958. (О русском переводе этой книги см. стр. 22.)

РЕКУРРЕНТНЫЕ СООТНОШЕНИЯ

1. Некоторые элементарные рекуррентности. Простым примером рекуррентности является соотношение

$$\binom{n}{r} = \binom{n-1}{r} + \binom{n-1}{r-1}. \tag{1.1}$$

С помощью (1.1) подбором подходящих начальных значений можно вычислять биномиальные коэффициенты для всех неотрицательных целых n и r. Этот вычислительный процесс схематически иллюстрирует треугольник Паскаля. *Рекуррентностями* называются соотношения многих разных типов, и нет необходимости настаивать на формальном определении этого термина. Но в общем под рекуррентностью понимают специальный тип отношений, включающих количества с целочисленными параметрами. Это соотношение таково, что его можно использовать для вычисления значения величины шаг за шагом, исходя из заданных начальных значений и значений, предварительно подсчитанных. Рекуррентности естественным образом возникли во многих перечислительных задачах, и теория рекуррентностей имеет весьма обширную литературу. Этот предмет с большой тщательностью развит в недавно вышедшей книге Риордана, упоминаемой в литературе к настоящей главе. Мы не будем подробно останавливаться на этом, ограничившись обсуждением немногих простых рекуррентностей, представляющих для нас специальный интерес.

Начнем с одной задачи из элементарной геометрии. Предположим, что мы ищем число частей, на которые делится плоскость n прямыми линиями, расположенными произвольным образом. Обозначим это число через P_n.

Положим по определению

$$P_0 = 1. \tag{1.2}$$

Легко показать, что для любого натурального n

$$P_n = P_{n-1} + n. \tag{1.3}$$

Начальное условие (1.2) и рекуррентность (1.3) определяют P_n для всех неотрицательных целых n. Фактически из (1.2) и (1.3) следует

$$P_n = \frac{n(n+1)}{2} + 1. \tag{1.4}$$

Рассмотрим далее множество T всех выборок объема n, полученных из 2-множества, состоящего из 0 и 1. Попробуем выяснить, каково число выборок, не содержащих двух нулей подряд. Обозначим это число $f(n)$ и определим

$$f(0) = 1, \tag{1.5}$$

а также, что тривиально,

$$f(1) = 2. \tag{1.6}$$

Пусть теперь $n \geqslant 2$. Тогда существует $f(n-1)$ таких выборок с первым элементом, равным единице, и $f(n-2)$ таких выборок с нулем в качестве первого элемента. Следовательно,

$$f(n) = f(n-1) + f(n-2). \tag{1.7}$$

Начальные условия (1.5) и (1.6) и рекуррентность (1.7) определяют $f(n)$ для всех неотрицательных целых n. Числа $f(n)$ называются *числами Фибоначчи*. Они обладают многими замечательными арифметическими и комбинаторными свойствами.

Эйлер исследовал с точки зрения рекуррентностей задачу о беспорядках. Положим по определению

$$D_0 = 1 \tag{1.8}$$

и из тривиальных соображений

$$D_1 = 0. \tag{1.9}$$

Рассмотрим теперь беспорядок

$$(a_1, a_2, \ldots, a_n) \tag{1.10}$$

из n элементов, обозначенных 1, 2, ..., n, где $n \geqslant 2$. Первое место в (1.10) открыто для всех элементов, исключая 1, т. е. для $n-1$ элементов. Предположим теперь, что первым элементом в (1.10) выбран $a_1 = k$ $(k \neq 1)$. Тогда все беспорядки (1.10) делятся на два типа в зависимости от того, находится элемент 1 на k-м месте или нет. Если 1 находится на k-м месте, то число перестановок будет таким же, что и число перестановок из $n-2$ элементов, из которых ни один не находится на своем месте, т. е. D_{n-2}. С другой стороны, если 1 не находится на k-м месте, то допустимые перестановки таковы, что в них элементы 1, 2, ..., $k-1$, $k+1$, ..., n занимают места от 2-го до n-го, элемент 1 не занимает k-го места, а всякий другой элемент не находится на своем месте. Но это то же самое, что и перестановки из $n-1$ элементов, обозначенных 2, ..., n, причем каждый элемент не находится на своем месте. Число таких перестановок, очевидно, D_{n-1}. Из вышеприведенных рассуждений вытекает

$$D_n = (n-1)(D_{n-1} + D_{n-2}). \tag{1.11}$$

Рекуррентность (1.11) может быть использована для того, чтобы дать прямое доказательство по индукции следующей формулы:

$$D_n = n!\left(1 - \frac{1}{1!} + \frac{1}{2!} - \ldots + (-1)^n \frac{1}{n!}\right). \tag{1.12}$$

2. Числа размещений. Пусть U_n обозначает число перестановок из n элементов, обозначенных 1, 2, ..., n и таких, что элемент i не находится ни на i-м, ни на $(i+1)$-м местах, $i = 1, 2, \ldots, n-1$, а элемент n — ни на n-м, ни на 1-м местах. Иными словами, U_n есть число перестановок, противоречивых двум перестановкам

$$(1, 2, 3, \ldots, n), \quad (n, 1, 2, \ldots, n-1). \tag{2.1}$$

Пусть C обозначает (0, 1)-матрицу порядка n, в которой на местах (1, 2), (2, 3), (3, 4), ..., $(n, 1)$ находятся единицы, а на остальных местах — нули. Пусть, далее, J обозначает матрицу порядка n, каждым элементом которой будет единица, а I — единичную матрицу порядка n. Тогда легко вывести, что

$$U_n = \operatorname{per}(J - I - C). \tag{2.2}$$

Однако формула для перманента, выведенная в предыдущей главе, не позволяет непосредственно подсчитать числа U_n.

Числа U_n называются *числами размещений*. Основанием для такого названия является следующая „задача о размещении гостей", сформулированная Люка. Спрашивается, сколькими способами можно рассадить за круглым столом n супружеских пар, мужчин и женщин поочередно, однако так, чтобы ни одна жена не сидела рядом со своим мужем. Сначала могут быть рассажены жены, и это можно осуществить $2n!$ способами. После этого ни один муж не может занять ни одного из двух мест рядом со своей женой, но число способов рассадить мужей не зависит от рассаживания жен. Таким образом, если M_n означает число размещений в указанной задаче, то очевидно, что

$$M_n = 2n!\,U_n. \tag{2.3}$$

Следовательно, мы можем сконцентрировать наше внимание на числах размещений U_n.

Теорема 2.1. *Числа размещений U_n определяются по формуле*

$$U_n = n! - \frac{2n}{2n-1}\binom{2n-1}{1}(n-1)! + \\ + \frac{2n}{2n-2}\binom{2n-2}{2}(n-2)! - \ldots + (-1)^n \frac{2n}{n}\binom{n}{n}0! \quad (n > 1). \tag{2.4}$$

Эта замечательная формула для U_n была опубликована в сообщении Тушара. Приведенное ниже доказательство (2.4) является изящным рекуррентным рассуждением, принадлежащим Капланскому.

Лемма 2.2. *Пусть $f(n, k)$ обозначает число способов выбора k элементов, среди которых нет двух соседних, из n элементов, расположенных в ряд. Тогда*

$$f(n, k) = \binom{n-k+1}{k}. \tag{2.5}$$

Доказательство. Мы имеем начальные условия

$$f(n,\ 1)=\binom{n}{1}=n, \tag{2.6}$$

а для $n>1$

$$f(1,\ n)=\binom{1}{n}=0. \tag{2.7}$$

Пусть теперь $1<k<n$. Мы можем разбить выборки на те, которые включают в себя первый элемент, и на те, которые не включают его. Те выборки, что включают первый элемент, не могут включать второго, и их число будет

$$f(n-2,\ k-1). \tag{2.8}$$

Число же выборок, не включающих первый элемент, будет

$$f(n-1,\ k). \tag{2.9}$$

Следовательно, мы имеем рекуррентность

$$f(n,\ k)=f(n-1,\ k)+f(n-2,\ k-1). \tag{2.10}$$

Теперь мы можем доказать (2.5) по индукции. По предположению индукции

$$f(n-1,\ k)=\binom{n-k}{k},\quad f(n-2,\ k-1)=\binom{n-k}{k-1}. \tag{2.11}$$

Но тогда из (2.10) и (2.11) вытекает, что

$$f(n,\ k)=\binom{n-k}{k}+\binom{n-k}{k-1}, \tag{2.12}$$

что эквивалентно (2.5).

Лемма 2.3. *Пусть $g(n,\ k)$ обозначает число способов выбора k элементов, никакие два из которых не являются смежными, из n элементов, расположенных в круг. Тогда*

$$g(n,\ k)=\frac{n}{n-k}\binom{n-k}{k}\quad (n>k). \tag{2.13}$$

Доказательство. Разобьем, как мы это делали выше, все выборки на те, которые включают первый элемент, и те, которые его не включают. Выборки, вклю-

чающие первый элемент, не могут включать второй и последний элементы. Их число

$$f(n-3,\ k-1). \tag{2.14}$$

Число выборок, не включающих в себя первый элемент:

$$f(n-1,\ k). \tag{2.15}$$

Следовательно,

$$g(n,\ k)=f(n-1,\ k)+f(n-3,\ k-1), \tag{2.16}$$

и теперь (2.13) легко следует из леммы 2.2.

Возвратимся еще раз к перестановкам элементов, обозначенных 1, 2, ..., n. Пусть P_i обозначает то свойство, что перестановка имеет элемент i на i-м месте ($i=1,\ 2,\ \ldots,\ n$), а P_i' — то свойство, что перестановка содержит элемент i на $(i+1)$-м месте ($i=1,\ 2,\ \ldots,\ n-1$). При этом P_n' означает, что в перестановке элемент n занимает первое место. Расположим в ряд $2n$ свойств

$$P_1,\ P_1',\ P_2,\ P_2',\ \ldots,\ P_n,\ P_n'. \tag{2.17}$$

Выберем k из этих свойств и узнаем, каково число перестановок, удовлетворяющих каждому из этих k свойств. Ответ будет $(n-k)!$, если k свойств будут совместимыми, и 0 в других случаях. Обозначим через v_k число способов выбора k совместимых свойств из общего числа $2n$ свойств (2.17). Тогда по формуле решета

$$U_n=v_0 n!-v_1(n-1)!+v_2(n-2)!-\ \ldots\ +(-1)^n v_n 0! \tag{2.18}$$

Остается только вычислить v_k. Но мы замечаем, что если $2n$ свойств (2.17) расположены в круг, то несовместимыми свойствами являются только два последовательных. Следовательно, по лемме 2.3

$$v_k=\frac{2n}{2n-k}\binom{2n-k}{k}, \tag{2.19}$$

а это и доказывает теорему.

3. Латинские прямоугольники. Дано множество S из n элементов. *Латинский прямоугольник*, основанный на n-множестве S, есть прямоугольная $(r\times s)$-таблица

$$A=[a_{ij}]\quad (i=1,\ 2,\ \ldots,\ r;\ j=1,\ 2,\ \ldots,\ s), \tag{3.1}$$

удовлетворяющая условию: каждая строка (3.1) является s-перестановкой элементов S, а каждый столбец (3.1) — r-перестановкой элементов S. Из этого следует, что $r \leqslant n$ и $s \leqslant n$. Обозначим элементы S через $1, 2, \ldots, n$ и предположим, что $s = n$. Тогда латинский прямоугольник содержит в каждой строке перестановку элементов $1, 2, \ldots, n$, и эти перестановки выбраны таким образом, что ни один столбец не содержит повторяющихся элементов. Латинский прямоугольник такого типа считается *нормализованным*, если первая его строка записана в естественном порядке $1, 2, \ldots, n$. Если $L(r, n)$ обозначает число $r \times n$ латинских прямоугольников, а $K(r, n)$ — число нормализованных $r \times n$ латинских прямоугольников, то очевидно

$$L(r, n) = n!\,K(r, n). \tag{3.2}$$

Нормализованные $2 \times n$ латинские прямоугольники являются беспорядками, и, следовательно,

$$K(2, n) = D_n. \tag{3.3}$$

Очевидно также, что числа размещений U_n оказываются числами $3 \times n$ латинских прямоугольников с исходными строками

$$\begin{bmatrix} 1 & 2 & 3 \ldots & n \\ n & 1 & 2 \ldots & n-1 \end{bmatrix}. \tag{3.4}$$

В интересной формуле Риордана для $K(3, n)$ утверждается, что

$$K(3, n) = \sum_{k=0}^{m} \binom{n}{k} D_{n-k} D_k U_{n-2k}, \tag{3.5}$$

где $m = [n/2]$, а $U_0 = 1$. Однако задача о перечислении латинских прямоугольников, имеющих более трех строк, лишь едва затронута. В этой связи заслуживает упоминания важная асимптотическая формула Эрдёша и Капланского. В ней утверждается, что если $r < (\ln n)^{5/2}$, то

$$L(r, n) \sim n!^r e^{-\binom{r}{2}}. \tag{3.6}$$

Они предположили, что формула (3.6) остается справедливой для $r < n^{1/3}$; это было доказано Ямамото.

Если $r = s = n$, то латинский прямоугольник называют *латинским квадратом порядка n*. Такая конфигурация может быть рассмотрена как таблица умножения весьма общих алгебраических систем. Обращаем внимание читателя на то, что мультипликативная таблица конечных групп определяет латинский квадрат. Но построенный таким образом латинский квадрат обладает весьма специальными свойствами. Если теперь

$$L(n,\ n) = n!\,(n-1)!\,l_n, \tag{3.7}$$

то l_n обозначает число латинских квадратов порядка n, у которых элементы первой строки и первого столбца расположены в естественном порядке. Наши предыдущие рассуждения относительно $K(r,\ n)$ дают понять, что вычисление l_n не может быть легким. Это и на самом деле так. Следующая таблица показывает известные значения l_n:

n	1	2	3	4	5	6	7
l_n	1	1	1	4	56	9408	16 942 080

ЛИТЕРАТУРА

Риордан [5] дает полный обзор рекуррентностей со многими дополнительными литературными ссылками. Числа Фибоначчи исследованы у Диксона [1], гл. 17. Классические работы о числах размещений включают статьи Тушара [7] и Капланского [3]. Вывод формулы для $K(3,\ n)$ имеется у Риордана [4]. Асимптотические формулы для $L(r,\ n)$ рассмотрены у Эрдёша и Капланского [2] и у Ямамото [8]. Значением l_7 мы обязаны Сейду [6].

1. Dickson L. E., History of the Theory of Numbers, vol. 1, New York, 1952.
2. Erdös P., Kaplansky I., The asymptotic number of Latin rectangles, *Amer. Jour. Math.*, **68** (1946), 230—236.
3. Kaplansky I., Solution of the „Problème des ménages", *Bull. Amer. Math. Soc.*, **49** (1943), 784—785.
4. Riordan J., Three-line Latin rectangles — II, *Amer. Math. Monthly*, **53** (1946), 18—20.
5. Riordan J., An Introduction to Combinatorial Analysis, New York, 1958. (О русском переводе этой книги см. стр. 22.)
6. Sade A., Énumération des Carrés Latins. Application an 7-e Ordre, Conjecture pour les Ordres Supérieurs, Marseille, 1948.
7. Touchard J., Sur un problème de permutations, *C. R. Acad. Sci. Paris*, **198** (1934), 631—633.
8. Yamamoto K., On the asymptotic number of Latin rectangles, *Japan Jour. Math.*, **21** (1951), 113—119.

Глава 4

ТЕОРЕМА РАМСЕЯ

1. Основная теорема. Мы посвящаем этот пункт описанию и доказательству важной комбинаторной теоремы, возникшей из некоторых исследований в области оснований математики. Теорема эта названа по имени английского логика Ф. П. Рамсея. В математике принципом разбиения называется следующее утверждение: если множество достаточно большого числа элементов разбито на не очень большое число подмножеств, то по крайней мере одно из подмножеств должно содержать большое число элементов. Теорему Рамсея можно рассматривать как глубокое обобщение этого простого принципа. В доказательстве теоремы Рамсея широко используется аппарат рекуррентностей. Теорема имеет много разнообразных приложений, некоторые из них будут рассмотрены в следующем пункте.

Пусть дано n-множество S, и пусть $P_r(S)$ обозначает множество всех r-подмножеств множества S. Пусть, далее,

$$P_r(S) = A_1 \cup A_2 \cup \ldots \cup A_t \tag{1.1}$$

— произвольное упорядоченное разбиение $P_r(S)$ на t составляющих $A_1, A_2, \ldots, A_t$. Пусть, наконец, заданы целые числа $q_1, q_2, \ldots, q_t$, такие, что

$$1 \leqslant r \leqslant q_1, q_2, \ldots, q_t. \tag{1.2}$$

Если существует q_i-подмножество множества S, содержащее все r-подмножества из A_i, то будем его называть (q_i, A_i)-*подмножеством* множества S. Теорема Рамсея утверждает следующее.

Теорема 1.1. *Пусть заданы целые числа* $q_1, q_2, \ldots, q_t$ *и* r, *удовлетворяющие* (1.2). *Тогда существует минимальное натуральное число* $N(q_1, q_2, \ldots, q_t, r)$, *обладающее тем свойством, что для всех*

целых чисел $n \geqslant N(q_1, q_2, \ldots, q_t, r)$ *справедливо следующее. Дано* n*-множество* S *и произвольное упорядоченное разбиение* (1.1) *множества* $P_r(s)$ *на* t *составляющих* $A_1, A_2, \ldots, A_t$*; тогда* S *содержит* (q_i, A_i)*-подмножество для некоторого* i, $i = 1, 2, \ldots, t$.

Доказательство. Чтобы добиться лучшего понимания формулировки теоремы, рассмотрим вначале различные ее частные случаи. Начнем с замечания, что в случае $r = 1$ теорема сводится к принципу разбиения. В этом случае $P_r(S)$ совпадает с S, а (q_i, A_i)-подмножество множества S является некоторым q_i-подмножеством множества A_i. Отсюда вытекает[1]), что

$$N(q_1, q_2, \ldots, q_t, 1) = q_1 + q_2 + \ldots + q_t - t + 1. \quad (1.3)$$

Положим теперь $q_1 = q_2 = \ldots = q_t = q \geqslant r \geqslant 1$. В этом случае теорема выглядит следующим образом. Дано n-множество S, где n достаточно велико. Все r-подмножества множества S произвольным образом разбиты на t составляющих. Тогда существует q-подмножество множества S со всеми r-подмножествами одной из t составляющих. Из этого утверждения легко вывести теорему Рамсея в общем случае. Это можно выполнить, выбирая q равным максимуму чисел $q_1, q_2, \ldots, q_t$. Для $t = 1$ теорема Рамсея тривиальна, и в этом случае мы имеем $N(q_1, r) = q_1$. Предположим, что мы доказали теорему для $t = 2$. Тогда мы покажем, что теорема должна быть справедливой для $t = 3$. В самом деле, мы можем написать

$$P_r(S) = A_1 \cup (A_2 \cup A_3) \quad (1.4)$$

и положить

$$q_2' = N(q_2, q_3, r). \quad (1.5)$$

Теперь, если $n \geqslant N(q_1, q_2', r)$, то n-множество S должно содержать (q_1, A_1)-подмножество или $(q_2', A_2 \cup A_3)$-подмножество. Но если выполняется последняя альтернатива, то q_2'-подмножество множества S должно содержать или (q_2, A_2)-подмножество, или (q_3, A_3)-подмножество. Следо-

[1]) См. Холл М., Комбинаторный анализ, ИЛ, 1963, стр. 43—45, где приводится доказательство (1.3) для $t = 2$. — *Прим. ред.*

вательно, теорема справедлива для $t=3$; и очевидно, что по индукции теорема верна для всякого t. Следовательно, мы обязаны доказать эту теорему только для $t=2$; сосредоточим наше внимание на этом случае.

Из (1.3) мы знаем, что

$$N(q_1,\ q_2,\ 1)=q_1+q_2-1. \tag{1.6}$$

Более того, мы утверждаем, что

$$N(q_1,\ r,\ r)=q_1, \tag{1.7}$$
$$N(r,\ q_2,\ r)=q_2. \tag{1.8}$$

Чтобы доказать это, положим $q_2=r$ и $n\geqslant q_1$. Если A_2 не пусто, то n-множество S содержит $(r,\ A_2)$-подмножество. С другой стороны, если A_2 пусто, то $A_1=P_r(S)$, и S содержит $(q_1,\ P_r(S))$-подмножество. Тем самым доказано утверждение (1.7). Аналогичными рассуждениями доказывается равенство (1.8).

Чтобы завершить доказательство для $t=2$, применим индукцию. На основе (1.6), (1.7) и (1.8) мы можем принять, что данные числа q_1, q_2 и r удовлетворяют неравенству $1<r<q_1,\ q_2$. Примем в качестве предположения индукции существование целых чисел $N(q_1-1,\ q_2,\ r)$ и $N(q_1,\ q_2-1,\ r)$. Кроме того, включим в эту гипотезу существование целого числа $N(q_1',\ q_2',\ r-1)$ для всех $q_1',\ q_2'$, таких, что $1\leqslant r\leqslant q_1',\ q_2'$. Исходя из этих предположений, а также из (1.6), (1.7) и (1.8), мы устанавливаем существование целого числа $N(q_1,\ q_2,\ r)$. Эта индукция верна, кроме того, потому, что существуют следующие целые числа:

$$\begin{array}{lll} N(2,\ 2,\ 2), & N(2,\ 3,\ 2), & N(2,\ 4,\ 2),\ \ldots \\ N(3,\ 2,\ 2), & N(3,\ 3,\ 2), & N(3,\ 4,\ 2),\ \ldots \\ N(4,\ 2,\ 2), & N(4,\ 3,\ 2), & N(4,\ 4,\ 2),\ \ldots \\ \vdots & \vdots & \vdots \end{array} \tag{1.9}$$

В свою очередь это влечет существование целых чисел $N(q_1,\ q_2,\ 3)$ и т. д.

В силу предположения индукции существуют числа $p_1=N(q_1-1,\ q_2,\ r)$, $p_2=N(q_1,\ q_2-1,\ r)$ и $N(p_1,\ p_2,\ r-1)$.

Исходя из этого, мы доказываем существование $N(q_1, q_2, r)$. Фактически мы доказываем следующее неравенство:

$$N(q_1, q_2, r) \leqslant N(p_1, p_2, r-1)+1. \tag{1.10}$$

Пусть

$$n \geqslant N(p_1, p_2, r-1)+1. \tag{1.11}$$

Пусть a — фиксированный элемент n-множества S, а T есть $(n-1)$-множество остальных элементов S. Применим разбиение $P_r(S) = A_1 \cup A_2$ всех r-подмножеств множества S, чтобы определить разбиение

$$P_{r-1}(T) = B_1 \cup B_2 \tag{1.12}$$

множества $P_{r-1}(T)$ всех $(r-1)$-подмножеств множества T. Это делается следующим образом. Пусть R — какое-либо $(r-1)$-подмножество множества T. Если $R \cup a$ входит в A_1, мы помещаем R в B_1, а если $R \cup a$ входит в A_2, то — в B_2. Это и дает нам разбиение (1.12) множества $P_{r-1}(T)$.

Множество T содержит по крайней мере $N(p_1, p_2, r-1)$ элементов. Следовательно, T содержит или (p_1, B_1)-подмножество, или (p_2, B_2)-подмножество. Сначала рассмотрим случай, когда T содержит (p_1, B_1)-подмножество. Тогда T содержит p_1-подмножество U, все $(r-1)$-подмножества которого лежат в B_1. Теперь $p_1 = N(q_1-1, q_2, r)$ и U как подмножество множества S содержит или (q_1-1)-подмножество, все r-подмножества которого входят в A_1, или q_2-подмножество, все r-подмножества которого входят в A_2. Если имеет место последняя альтернатива, то q_2-подмножество удовлетворяет нашим требованиям; теорема доказана.

Предположим теперь, что U содержит (q_1-1)-подмножество V, все r-подмножества которого входят в A_1. Но в этом случае $W = V \cup a$ является q_1-подмножеством множества S. Если r-подмножество множества W не содержит a, то оно является r-подмножеством множества V и, следовательно, это r-подмножество входит в A_1. С другой стороны, если r-подмножество множества W содержит элемент a, то оно состоит из этого элемента a и из $(r-1)$-подмножества множества V. Множество V, поскольку оно является подмножеством множества U,

содержит все свои $(r-1)$-подмножества в B_1. Но тогда, по определению разбиения (1.12), такое r-подмножество множества W входит также в A_1. Таким образом, W есть q_1-подмножество множества S, все r-подмножества которого входят в A_1. Другой случай, в котором T содержит (p_2, B_2)-подмножество, может быть рассмотрен с помощью совершенно аналогичных рассуждений. Теперь доказательство теоремы Рамсея полностью выполнено.

Целые числа $N(q_1, q_2, r)$ имеют глубокий комбинаторный смысл. Но, к сожалению, для них неизвестно никакой рекуррентности, а рекуррентное неравенство (1.10) не очень действенно в большинстве случаев. Это доставляет серьезные затруднения при вычислении $N(q_1, q_2, r)$. Конечно, мы всегда получаем тривиальные значения (1.6), (1.7) и (1.8). Но, помимо них, все известные $N(q_1, q_2, r)$ укладываются в следующую симметрическую таблицу для $N(q_1, q_2, 2)$:

	3	4	5
3	6	9	14
4	9	18	
5	14		

(1.13)

Не удивительно, что еще меньше известно о случаях, когда $t > 2$. В этом случае наибольшая информация к настоящему времени содержится в следующем утверждении:

$$N(3, 3, 3, 2) = 17. \tag{1.14}$$

2. Приложения. Рассмотрим n точек, расположенных произвольным образом в пространстве трех измерений. Две различные точки определяют отрезок; каждый из этих отрезков окрашен в красный или синий цвет. 2-подмножества точек могут быть разбиты на множество A_1 красных отрезков и множество A_2 синих отрезков. Теперь, если q_1 и q_2 — целые числа, такие, что $2 \leqslant q_1, q_2$, и если $n \geqslant N(q_1, q_2, 2)$, то по теореме Рамсея должны существовать q_1 точек, образующих только красные отрезки, и q_2 точек, образующих только синие отрезки. Более того, $N(q_1, q_2, 2)$ есть минимальное целое число, обладающее этим свойством.

Следующее приложение теоремы Рамсея относится к выпуклым многоугольникам.

Теорема 2.1. *Дано целое число* $m \geqslant 3$. *Существует минимальное натуральное* N_m, *такое, что для всех целых* $n \geqslant N_m$ *выполняется следующее свойство: если среди* n *точек на плоскости никакие три точки не лежат на одной прямой, то* m *точек являются вершинами выпуклого* m*-угольника.*

Лемма 2.2. *Если среди пяти точек на плоскости никакие три точки не лежат на одной прямой, то четыре точки являются вершинами выпуклого четырехугольника.*

Доказательство. Пять точек определяют десять прямолинейных отрезков, а периметр этой конфигурации является выпуклым многоугольником. Если этот выпуклый многоугольник является пяти- или четырехугольником, то имеем тривиальный случай. Предположим, что выпуклый многоугольник оказался треугольником. Тогда две из пяти точек попадают внутрь треугольника. Две внутренние точки определяют прямую, а две из трех вершин треугольника лежат с одной стороны этой прямой. Тогда эти две вершины треугольника и две внутренних точки образуют выпуклый четырехугольник.

Лемма 2.3. *Если из* m *точек на плоскости никакие три не коллинеарны и если все четырехугольники, образованные из этих* m *точек, выпуклые, то* m *точек являются вершинами выпуклого* m*-угольника.*

Доказательство. Очевидно, что m точек определяют $m(m-1)/2$ прямолинейных отрезков, а периметр этой конфигурации есть выпуклый q-угольник. Занумеруем последовательно вершины q-угольника: $V_1, V_2, \ldots, V_q$. Если одна из наших точек попадает внутрь q-угольника, то она должна оказаться внутри одного из треугольников: $V_1V_2V_3$, $V_1V_3V_4$, $\ldots$, $V_1V_{q-1}V_q$. Но это противоречит условию, что все четырехугольники, образованные из точек, выпуклые. Следовательно, $q = m$, а m-угольник выпуклый.

Теперь теорема 2.1 оказывается нетрудным следствием теоремы Рамсея. Чтобы это доказать, положим $m \geqslant 4$ и

$n \geqslant N(5,\ m,\ 4)$. Разобьем 4-подмножества из n точек на выпуклые и невыпуклые четырехугольники. По теореме Рамсея существует или пятиугольник со всеми невыпуклыми четырехугольниками, или один m-угольник со всеми выпуклыми четырехугольниками. В силу леммы 2.2 первая альтернатива отпадает, а по лемме 2.3 m-угольник будет выпуклым.

Наши рассуждения показали, что

$$N_m \leqslant N(5,\ m,\ 4). \tag{2.1}$$

Известно, что $N_3 = 3 = 2 + 1$, $N_4 = 5 = 2^2 + 1$; было показано, что $N_5 = 9 = 2^3 + 1$. Это приводит к предположению, что

$$N_m = 2^{m-2} + 1, \tag{2.2}$$

но это утверждение еще не доказано.

Наше заключительное приложение касается (0, 1)-матриц. Подматрица порядка m матрицы A порядка n называется *главной*, если она получена вычеркиванием из A произвольных $n - m$ строк и стольких же столбцов.

Теорема 2.4. *Дано произвольное натуральное число m. Всякая* (0, 1)*-матрица A достаточно большого порядка n содержит главную подматрицу порядка m одного из следующих четырех видов*:

$$\begin{bmatrix} * & & 0 \\ & \ddots & \\ 0 & & * \end{bmatrix}, \quad \begin{bmatrix} * & & 0 \\ & \ddots & \\ 1 & & * \end{bmatrix}, \quad \begin{bmatrix} * & & 1 \\ & \ddots & \\ 0 & & * \end{bmatrix}, \quad \begin{bmatrix} * & & 1 \\ & \ddots & \\ 1 & & * \end{bmatrix}. \tag{2.3}$$

Звездочки на главной диагонали обозначают нули и единицы. Элементы же, расположенные выше или ниже главной диагонали, все либо нули, либо единицы, как показано в (2.3).

Доказательство. Пусть в теореме Рамсея n-множество S будет множеством n векторов-строк матрицы

$A = [a_{ij}]$. Обозначим строку i в A через α_i. Положим $i < j$ и свяжем с вектор-строками α_i и α_j в A вектор (a_{ji}, a_{ij}). Этот вектор будет (0, 0), (1, 0), (0, 1) или (1, 1). Следовательно, мы имеем разбиение 2-подмножеств множества S

$$P_2(S) = A_1 \cup A_2 \cup A_3 \cup A_4. \tag{2.4}$$

Предположим, что

$$n \geqslant N(m, m, m, m, 2). \tag{2.5}$$

Тогда по теореме Рамсея существует m-подмножество множества S, все 2-подмножества которого лежат в одной из четырех составляющих $P_2(S)$. Но из этого следует существование главной подматрицы одного из четырех видов, показанных в (2.3).

ЛИТЕРАТУРА

Теорема Рамсея в ее первоначальной форме дана в [8]. Приведенное здесь доказательство и результаты о выпуклых многоугольниках принадлежат Эрдёшу и Секерешу [4]. Подсчет значений для $N(q_1, q_2, 2)$ и $N(3, 3, 3, 2)$ дан в статье Гринвуда и Глисона [6].

1. Erdös P., Rado R., A combinatorial theorem, *Jour. London Math. Soc.*, **25** (1950), 249—255.
2. Erdös P., Rado R., Combinatorial theorems on classifications of subsets of a given set, *Proc. London Math. Soc.*, 3rd. ser., **2** (1952), 417—439.
3. Erdös P., Rado R., A partition calculus in set theory, *Bull. Amer. Math. Soc.*, **62** (1956), 427—489.
4. Erdös P., Szekeres G., A combinatorial problem in geometry *Compositio Mathematica*, **2** (1935), 463—470.
5. Goodman A. W., On sets of acqnaintances and strangers at any party, *Amer. Math. Monthly*, **66** (1959), 778—783.
6. Greenwood R. E., Gleason A. M., Combinatorial relations and chromatic graphs, *Canad. Jour. Math.*, **7** (1955), 1—7.
7. Rado R., Direct decomposition of partitions, *Jour. London Math. Soc.*, **29** (1954), 71—83.
8. Ramsey F. P., On a problem of formal logic, *Proc. London Math. Soc.*, 2nd series, **30** (1930), 264—286.
9. Skolem T., Ein kombinatorischer Satz mit Anwendung auf ein logisches Entscheidungsproblem, *Fundamenta Mathematicae*, **20** (1933), 254—261.

Глава 5

СИСТЕМЫ РАЗЛИЧНЫХ ПРЕДСТАВИТЕЛЕЙ

1. Основная теорема. Дано произвольное множество S. Пусть $P(S)$ обозначает множество всех подмножеств множества S. Пусть, далее,

$$D = (a_1,\ a_2,\ \ldots,\ a_m) \tag{1.1}$$

есть m-выборка из множества S, а

$$M(S) = (S_1,\ S_2,\ \ldots,\ S_m) \tag{1.2}$$

есть m-выборка из $P(S)$. Теперь предположим, что m элементов выборки D различны и что

$$a_i \in S_i \quad (i = 1,\ 2,\ \ldots,\ m). \tag{1.3}$$

В таком случае будем говорить, что элемент a_i *представляет* множество S_i и что подмножества S_1, S_2, $\ldots$, S_m имеют *систему различных представителей* (сокращенно: с. р. п.). Назовем выборку D с. р. п. для $M(S)$. Определение с. р. п. требует, чтобы $a_i \neq a_j$, как только $i \neq j$, но S_i и S_j не обязательно должны быть различными подмножествами множества S.

Дадим простую иллюстрацию понятия с. р. п. Пусть S есть 5-множество целых чисел 1, 2, 3, 4, 5. Положим $S_1 = (2, 5)$, $S_2 = (2, 5)$, $S_3 = (1, 2, 3, 4)$, $S_4 = (1, 2, 5)$. Тогда $D = (2, 5, 3, 1)$ есть с. р. п. для S_1, S_2, S_3, S_4. Если мы в этом примере заменим S_4 на $S_4' = (2, 5)$, то подмножества уже не будут иметь с. р. п., так как $S_1 \cup S_2 \cup S_4'$ есть 2-множество, а для того чтобы представлять S_1, S_2, S_4', требуется три элемента.

Необходимое и достаточное условие существования с. р. п. дает следующая теорема Ф. Холла.

Теорема 1.1. *Подмножества* $S_1, S_2, \ldots, S_m$ *имеют с. р. п. тогда и только тогда, когда множество* $S_{i_1} \cup S_{i_2} \cup \ldots \cup S_{i_k}$ *содержит по меньшей мере* k *элементов. Это должно выполняться для* $k = 1, 2, \ldots, m$ *и для всех* k*-сочетаний* $(i_1, i_2, \ldots, i_k)$ *целых чисел* $1, 2, \ldots, m$.

Необходимость этой фундаментальной теоремы очевидна. Докажем теперь усовершенствованный вариант условия достаточности, дающий нижнюю грань для числа с. р. п. Затем в следующих разделах книги мы обсудим дальнейшие разветвления и приложения наших результатов.

Теорема 1.2. *Пусть подмножества* $S_1, S_2, \ldots, S_m$ *удовлетворяют необходимому условию существования с. р. п. и пусть каждое из этих подмножеств состоит по меньшей мере из* t *элементов. Если* $t \leqslant m$, *то* $M(S)$ *имеет по меньшей мере* $t!$ *систем различных представителей, а если* $t > m$, *то* $M(S)$ *имеет по меньшей мере* $t!/(t-m)!$ *таких систем.*

Доказательство проводится посредством индукции относительно m. Для $m = 1$ теорема очевидна. В качестве предположения индукции примем, что теорема верна для всех m'-выборок из $P(S)$, где $m' < m$. Докажем теорему для m-выборок $M(S) = (S_1, S_2, \ldots, S_m)$. Доказательство разбивается на два случая.

В первом случае мы исходим из предположения, что множество $S_{i_1} \cup S_{i_2} \cup \ldots \cup S_{i_k}$ содержит по меньшей мере $k+1$ элементов. Это имеет силу для $k = 1, 2, \ldots, m-1$ и для всех k-сочетаний $(i_1, i_2, \ldots, i_k)$ целых чисел $1, 2, \ldots, m$. В этом случае поступаем таким образом.

Пусть a_1 — фиксированный элемент в S_1. Вычеркнем a_1 всюду, где бы он ни появлялся из множеств $S_2, S_3, \ldots, S_m$, и обозначим получившиеся множества $S_2', S_3', \ldots, S_m'$ соответственно; $(m-1)$-выборка

$$M'(S) = (S_2', S_3', \ldots, S_m') \tag{1.4}$$

удовлетворяет необходимому условию существования с. р. п., так как множество $S_{i_1} \cup S_{i_2} \cup \ldots \cup S_{i_k}$ содержит

по меньшей мере $k+1$ элементов. Теперь, если $t \leqslant m$, то $t-1 \leqslant m-1$ и по предположению индукции $M'(S)$ имеет по меньшей мере $(t-1)!$ с. р. п. Также, если $t > m$, то $t-1 > m-1$ и по той же причине $M'(S)$ имеет по меньшей мере $(t-1)!/(t-m)!$ систем различных представителей. Но a_1 и с. р. п. для $M'(S)$ дают нам с. р. п. для $M(S)$, где a_1 представляет S_1. Это справедливо для каждого из t выборов элемента a_1. Следовательно, мы получаем искомое число с. р. п. для $M(S)$.

Во втором случае существует k-подмножество множества S вида $S_{i_1} \cup S_{i_2} \cup \ldots \cup S_{i_k}$. Здесь k — целое число, лежащее в интервале $1 \leqslant k \leqslant m-1$, а $(i_1, i_2, \ldots, i_k)$ — определенное k-сочетание целых чисел $1, 2, \ldots, m$. Переименуем подмножества $S_1, S_2, \ldots, S_m$, так что $S_{i_1} \cup S_{i_2} \cup \ldots \cup S_{i_k}$ есть $S_1 \cup S_2 \cup \ldots \cup S_k$. Из существования этого k-подмножества вытекает, что $t \leqslant k$. Следовательно, по предположению индукции k-выборка $(S_1, S_2, \ldots, S_k)$ имеет по меньшей мере $t!$ с. р. п. Пусть $D^* = (a_1, a_2, \ldots, a_k)$ обозначает одну такую с. р. п. Вычеркнем элементы D^* всюду, где бы они ни появлялись, из множеств $S_{k+1}, S_{k+2}, \ldots, S_m$ и обозначим получившиеся множества $S^*_{k+1}, S^*_{k+2}, \ldots, S^*_m$ соответственно; $(m-k)$-выборка

$$M^*(S) = (S^*_{k+1}, S^*_{k+2}, \ldots, S^*_m) \tag{1.5}$$

удовлетворяет необходимому условию существования с. р. п., так как если, скажем, $S^*_{k+1} \cup S^*_{k+2} \cup \ldots \cup S^*_{k+k^*}$ содержит менее k^* элементов, то

$$S_1 \cup S_2 \cup \ldots \cup S_k \cup S_{k+1} \cup S_{k+2} \cup \ldots \cup S_{k+k^*} \tag{1.6}$$

содержит менее $k+k^*$ элементов, а это противоречит условию теоремы [1]). Следовательно, $M^*(S)$ имеет по меньшей мере одну с. р. п., и, следовательно, $M(S)$ имеет по меньшей мере $t!$ с. р. п. Это и доказывает теорему 1.2 а заодно и теорему 1.1.

---

[1]) То есть необходимому условию существования с. р. п. (теорема 1.1). — *Прим. ред.*

2. Разбиения. Пусть

$$T = A_1 \cup A_2 \cup \ldots \cup A_m \tag{2.1}$$

и

$$T = B_1 \cup B_2 \cup \ldots \cup B_m \tag{2.2}$$

обозначают два разбиения множества T, в которых ни одна из составляющих не является нуль-множеством $\varnothing$. Возьмем m-подмножество E множества T, такое, что каждое $A_i \cap E \neq \varnothing$ и каждое $B_j \cap E \neq \varnothing$. Тогда каждое из этих пересечений должно быть 1-множеством и множество E может быть названо *системой общих представителей* (сокращенно с. о. п.) разбиений (2.1) и (2.2). С. о. п. существует для этих разбиений тогда и только тогда, когда существует подходящая перенумерация составляющих (2.1), такая, что

$$A_i \cap B_i \neq \varnothing \quad (i = 1, 2, \ldots, m). \tag{2.3}$$

Используем теорию с. р. п. для того, чтобы получить следующее необходимое и достаточное условие существования с. о. п.

Теорема 2.1. *Разбиения* (2.1) *и* (2.2) *имеют с. о. п. тогда и только тогда, когда множество* $A_{i_1} \cup A_{i_2} \cup \ldots \cup A_{i_k}$ *содержит не более* k *из составляющих* $B_1, B_2, \ldots, B_m$. *Это должно выполняться для* $k = 1, 2, \ldots, m$ *и для всех* k*-сочетаний* $(i_1, i_2, \ldots, i_k)$ *целых чисел* $1, 2, \ldots, m$.

Доказательство. Необходимость условия, сформулированного в теореме, как и прежде, очевидна. Достаточность докажем следующим образом. Пусть S есть m-множество элементов $A_1, A_2, \ldots, A_m$. Пусть S_i — множество всех элементов A_j, таких, что $A_j \cap B_i \neq \varnothing$. Тогда $M(S) = (S_1, S_2, \ldots, S_m)$ является m-выборкой подмножеств множества S. Мы утверждаем, что множество $M(S)$ удовлетворяет необходимому условию существования с. р. п. Так как если, скажем, $S_1 \cup S_2 \cup \ldots \cup S_{k+1}$ содержит только k элементов $A_{i_1}, A_{i_2}, \ldots, A_{i_k}$, то $A_{i_1} \cup A_{i_2} \cup \ldots \cup A_{i_k}$ содержит $k+1$ составляющих $B_1, B_2, \ldots, B_{k+1}$, что противоречит условию теоремы. Следовательно, по теореме 1.1 существует с. р. п. для $M(S)$. Теперь мы

можем перенумеровать компоненты (2.1) так, чтобы эта с. р. п. была $D=(A_1, A_2, \ldots, A_m)$. Но тогда справедливо (2.3), что и доказывает теорему.

Теорема 2.2. *Пусть даны два разбиения множества* T: $T=A_1 \cup A_2 \cup \ldots \cup A_m$ *и* $T=B_1 \cup B_2 \cup \ldots \cup B_m$. *Если в этих разбиениях каждая составляющая* A_i *или* B_j *является* r*-подмножеством множества* T, *то разбиения имеют с. о. п.*

Доказательство. Это частный случай теоремы 2.1.

Из теоремы 2.2 вытекает следующее утверждение для $(r \times m)$-таблиц, элементами которых являются числа 1, 2, ..., rm. Пусть дано

$$A=\begin{bmatrix} 1 & 2 & \ldots & m \\ m+1 & m+2 & \ldots & 2m \\ \vdots & \vdots & & \\ \vdots & \vdots & & \\ \vdots & \vdots & & \\ (r-1)\,m+1 & (r-1)\,m+2 & \ldots & rm \end{bmatrix}. \quad (2.4)$$

Пусть теперь дана $(r \times m)$-таблица B, элементами которой являются тоже целые числа 1, 2, ..., rm, но расположенные в произвольном порядке. Тогда существует для B такая перестановка столбцов, что соответствующие столбцы A и B будут иметь по меньшей мере один общий элемент.

Следующая ниже иллюстрация требует знания элементарных свойств смежных классов в теории групп [1]). Но в этом случае теорема оказывается непосредственным следствием теоремы 2.2.

Теорема 2.3. *Дана конечная группа* G *и ее подгруппа* H. *Пусть* $G=Hx_1 \cup Hx_2 \cup \ldots \cup Hx_m$ *— разложение по правым смежным классам относительно* H, *а* $G=y_1H \cup y_2H \cup \ldots \cup y_mH$ *— разложение по левым смежным классам относительно* H [2]). *Тогда сущ-*

---

[1]) См., например, Холл М., Теория групп, ИЛ, 1962. — *Прим. ред.*

[2]) У Холла наоборот: xH — правый, а Hx — левый смежные по подгруппе H классы. — *Прим. ред.*

ствуют элементы $z_1, z_2, \ldots, z_m$ *группы* G, *такие, что*

$$G = Hz_1 \cup Hz_2 \cup \ldots \cup Hz_m = z_1H \cup z_2H \cup \ldots \cup z_mH. \tag{2.5}$$

3. Латинские прямоугольники. В этом разделе мы приложим теорию с. р. п. к латинским прямоугольникам. Пусть дан $r \times s$ латинский прямоугольник, составленный из n элементов $1, 2, \ldots, n$. Будем говорить, что латинский прямоугольник может быть *расширен* до латинского квадрата порядка n, если мы сможем присоединить к нему $n - r$ строк и $n - s$ столбцов так, чтобы окончательная конфигурация оказалась латинским квадратом n-го порядка. Причем новая конфигурация содержит старую в левом верхнем углу.

Теорема 3.1. *Дан* $r \times n$ *латинский прямоугольник, построенный из* n *элементов* $1, 2, \ldots, n$. *Он может быть расширен до латинского квадрата* n*-го порядка.*

Доказательство. Пусть дано n-множество S, состоящее из элементов $1, 2, \ldots, n$, и пусть S_i — множество всех тех элементов множества S, которые не появляются в i-м столбце латинского прямоугольника. Тогда каждое S_i есть $(n - r)$-подмножество множества S, а $M(S) = (S_1, S_2, \ldots, S_n)$ есть n-выборка подмножеств множества S. Докажем, что $M(S)$ удовлетворяет необходимому условию существования с. р. п. Пусть i является элементом множества S. В латинском прямоугольнике r появлений элемента i имеют место в различных столбцах. Следовательно, этот элемент находится точно в $n - r$-множествах из $S_1, S_2, \ldots, S_n$. Теперь, если, скажем, множество $S_1 \cup S_2 \cup \ldots \cup S_k$ содержит только $k - 1$ элемент, то в таком случае эти элементы появляются в множествах $S_1, S_2, \ldots, S_k$ не более чем $(n - r)(k - 1)$ раз. Но это противоречит тому факту, что каждое из этих множеств является $(n - r)$-подмножеством множества S. Следовательно, $M(S)$ имеет с. р. п. Обозначим последнюю через $D = (i_1, i_2, \ldots, i_n)$. Тогда D может быть присоединена к $r \times n$ латинскому прямоугольнику, чтобы получить $(r + 1) \times n$ латинский прямоугольник. Указанный

процесс может быть повторен, пока латинский прямоугольник не окажется расширенным до латинского квадрата порядка n.

Теорема 3.2. *Существует по меньшей мере*

$$n!(n-1)!\ldots(n-r+1)! \tag{3.1}$$

$r \times n$ латинских прямоугольников, и, следовательно, по крайней мере

$$n!(n-1)!\ldots 2!1! \tag{3.2}$$

$n \times n$ латинских квадратов.

Доказательство. Существует $n!$ латинских прямоугольников размерности $1 \times n$. По теоремам 3.1 и 1.2 каждый из них может быть расширен по меньшей мере до $(n-1)!$ латинских прямоугольников размерности $2 \times n$. Следовательно, существует по меньшей мере $n!(n-1)!$ латинских прямоугольников размерности $2 \times n$. Рассуждая далее аналогичным образом, докажем теорему.

Обозначим через l_n число латинских квадратов порядка n, у которых элементы первой строки и первого столбца расположены в естественном порядке. Тогда из теоремы 3.2 следует, что

$$l_n \geqslant (n-2)!(n-3)!\ldots 1!. \tag{3.3}$$

Приведем таблицу значений l_n и $b_n = (n-2)!(n-3)!\ldots 1!$ для $n = 3, 4, 5, 6, 7$:

n	3	4	5	6	7
l_n	1	4	56	9 408	16 942 080
b_n	1	2	12	288	34 560.

4. Матрицы, составленные из нулей и единиц. Дана матрица A размера $m \times n$, элементами которой являются нули и единицы. Такие (0, 1)-матрицы играют ведущую роль в решении многих комбинаторных вопросов. Одна из главных причин этого следующая. Пусть S есть n-множество элементов $a_1, a_2, \ldots, a_n$, а $M(S) = (S_1, S_2, \ldots, S_m)$ есть m-выборка подмножеств множества S. Теперь пусть $a_{ij} = 1$, если a_j принадлежит

множеству S_i, а если это не так, то $a_{ij}=0$. Тогда

$$A=[a_{ij}] \quad (i=1,\ 2,\ \ldots,\ m;\ j=1,\ 2,\ \ldots,\ n) \tag{4.1}$$

есть (0, 1)-матрица размера $m \times n$. Эта матрица называется *инцидентной* для подмножеств $S_1, S_2, \ldots, S_m$ множества S. Единицы в i-й строке матрицы A обозначают элементы, принадлежащие множеству S_i, а единицы в j-м столбце обозначают множества, содержащие элемент a_j. Таким образом, матрица A дает полное описание подмножеств $S_1, S_2, \ldots, S_m$ множества S. В свою очередь, если задана (0, 1)-матрица A размера $m \times n$ и если S есть произвольное n-множество, то существуют подмножества $S_1, S_2, \ldots, S_m$ этого множества, такие, что A является их инцидентной матрицей.

Из сказанного выше ясно, что (0, 1)-матрица A характеризует подмножества $S_1, S_2, \ldots, S_m$ множества S. Но мы можем характеризовать эти подмножества также матрицей, элементами которой будут $+1$ и -1 или вообще две разных величины x и y. Все такие характеристики являются вполне удовлетворительными, но они зачастую не имеют никакого преимущества перед характеристикой с помощью инцидентной матрицы A. В самом деле, выбор 0 и 1 в качестве элементов матрицы A особенно удобен вследствие простоты их поведения при сложении и умножении. Следующая теорема иллюстрирует это утверждение.

Теорема 4.1. *Даны подмножества* $S_1, S_2, \ldots, S_m$ *некоторого* n*-множества; пусть* $m \leqslant n$. *Введем для этих подмножеств инцидентную матрицу* A. *Тогда число систем различных представителей для* $M(S)=(S_1, S_2, \ldots, S_m)$ *равно* $\operatorname{per}(A)$.

Доказательство непосредственно следует из определений. Заметим, что определение $\operatorname{per}(A)$ и существование с. р. п. одинаково требуют $m \leqslant n$.

Перестановочная матрица[1]) P есть (0, 1)-матрица размера $m \times n$, такая, что $PP^T=I$, где P^T обозначает транспонированную матрицу P, а I — единичную матрицу

[1]) Или *матрица перестановки*. — *Прим. ред.*

m-го порядка. Из этого определения следует, что $m \leqslant n$. Перестановочная матрица порядка m имеет единственный элемент 1 в каждой строке и в каждом столбце, тогда как все другие элементы — нули. Предположим теперь, что в множестве S элементы и подмножества перенумерованы. В таком случае инцидентная матрица A заменяется другой инцидентной матрицей A' вида

$$A' = PAQ. \tag{4.2}$$

Здесь P — перестановочная матрица порядка m, определенная перенумерованием подмножеств, а Q — перестановочная матрица порядка n, определенная перенумерованием элементов. Многие исследования, включающие в себя (0, 1)-матрицу A, имеют дело с функциями, которые подобно $\mathrm{per}(A)$ остаются инвариантными относительно произвольных перестановок строк и столбцов матрицы A. Причина этого теперь очевидна. Подобные функции представляют интерес для комбинаторики потому, что они не зависят от того, как конкретно перенумерованы элементы и подмножества множества S.

5. Граничный ранг. Термин *линия* в матрице обозначает или строку, или столбец матрицы. *Следом* матрицы является сумма элементов, расположенных на ее главной диагонали. Рассмотрим теперь (0, 1)-матрицу A размера $m \times n$. *Граничным рангом* (term rank) матрицы A называется максимальное число единиц в A, расположенных так, что никакие две единицы не лежат на одной линии. Таким образом, граничный ранг матрицы A равен максимальному ее следу при произвольных перестановках строк и столбцов. Это эквивалентно максимальному числу квадратных подматриц в A с отличным от нуля перманентом. Понятие граничного ранга подсказывает удобное обобщение понятий с. р. п. для подмножеств $S_1, S_2, \ldots, S_m$ n-множества S. Ибо если A есть инцидентная матрица для этих подмножеств, то последние имеют с. р. п. тогда и только тогда, когда граничный ранг этой матрицы равен m.

Теорема 5.1. *Дана* (0, 1)-*матрица* A *размера* $m \times n$. *Минимальное число линий в* A, *содержащих*

все единицы, имеющиеся в A, равно граничному рангу A.

Доказательство. Пусть ρ' равно минимальному числу линий матрицы A, содержащих все единицы, а ρ равно граничному рангу A. Требуется доказать, что $\rho = \rho'$. Никакая линия не может содержать две единицы, которые числятся в ρ единицах граничного ранга. Следовательно, $\rho' \geqslant \rho$. Используем теорию с. р. п., чтобы доказать, что $\rho \geqslant \rho'$. Пусть минимальное покрытие единиц ρ' линиями состоит из e строк и f столбцов, так что $e + f = \rho'$. Как ρ, так и ρ' инвариантны относительно перестановок строк и столбцов в A. Следовательно, можем выбрать эти e строк и f столбцов в качестве начальных в матрице. Запишем матрицу так:

$$\begin{bmatrix} A_1 & A_2 \\ A_3 & A_4 \end{bmatrix}, \tag{5.1}$$

где A_1 имеет размер $e \times f$. Теперь граничный ранг A_2 будет e, так как мы можем рассматривать A_2 как инцидентную матрицу для подмножеств $S_1, S_2, \ldots, S_e$ из $(n-f)$-множества целых чисел $f+1, f+2, \ldots, n$. Эти подмножества должны удовлетворять необходимому условию существования с. р. п. Ибо если бы это условие не было выполнено, то мы могли бы заменить некоторые из e строк на меньшее число столбцов, сохранив покрытие всех единиц в A. Но в таком случае покрытие оказывается выполненным менее чем $e+f$ линиями, что противоречит условию минимальности ρ'. Что касается A_3, то мы можем рассматривать транспонированную матрицу A_3^T как инцидентную для подмножеств и показать аналогичными рассуждениями, что f будет граничным рангом A_3. Следовательно, $\rho \geqslant e + f = \rho'$ и теорема 5.1 таким образом доказана.

Теорема 5.1 имеет следующее непосредственное обобщение. Пусть дана матрица A размера $m \times n$, элементы которой являются элементами поля F. Минимальное число линий в A, содержащих все ненулевые элементы, равно максимальному числу ненулевых элементов A, никакие два из которых не лежат на одной линии.

Теорема 5.2. *Дана матрица A размера $m \times n$, элементами которой являются неотрицательные действительные числа; пусть $m \leqslant n$. Пусть сумма элементов каждой строки в A равна m', а сумма элементов каждого столбца — n'. Тогда*

$$A = c_1 P_1 + c_2 P_2 + \ldots + c_t P_t, \tag{5.2}$$

где каждое P_i есть перестановочная матрица, а коэффициенты c_i — неотрицательные действительные числа.

Доказательство. Если матрица A не квадратная, то заменим ее на

$$A' = \begin{bmatrix} & A & \\ \dfrac{m'}{n} & & J \end{bmatrix}, \tag{5.3}$$

где J — матрица размера $(n - m) \times n$, составленная из единиц. Матрица A' имеет порядок n, а ее элементы представляют собой неотрицательные действительные числа. Сумма элементов каждой строки и каждого столбца матрицы A' равна m'. Если A' — ненулевая матрица, то она имеет n положительных элементов, никакие два из которых не лежат на одной линии. Если бы A' не имела n таких элементов, то в соответствии с замечаниями, вытекающими из теоремы 5.1, мы могли бы покрыть положительные элементы A e строками и f столбцами, где $e + f < n$. Но тогда $m'n \leqslant m'(e + f) < m'n$, а это — явное противоречие. Пусть теперь P_1' — перестановочная матрица порядка n, в которой единицы занимают те же места, что и n положительных элементов матрицы A'. Пусть из этих элементов наименьшим будет c_1. Тогда $A' - c_1 P_1'$ есть матрица, элементами которой являются действительные неотрицательные числа. Кроме того, суммы элементов каждой строки и каждого столбца в матрице $A' - c_1 P_1'$ равны неотрицательному действительному числу $m' - c_1$. Но в $A' - c_1 P_1'$ появляется по меньшей мере на один нуль больше, нежели в A'. Поэтому теперь можно продолжать работать с $A' - c_1 P_1'$ и повторять вышеприведенные рассуждения до $A_1 = c_1 P_1' + c_2 P_2' + \ldots + c_t P_t'$,

Но это как раз и дает разложение вида (5.2) для матрицы A.

Теорема 5.2 имеет большое число интересных приложений.

Теорема 5.3. *Пусть дана* $(0, 1)$*-матрица* A *порядка* n, *такая, что суммы элементов по любой строке или любому столбцу равны целому положительному числу* k. Тогда

$$A = P_1 + P_2 + \ldots + P_k, \tag{5.4}$$

где все P_i *— перестановочные матрицы.*

Доказательство вытекает из доказательства теоремы 5.2. В этом случае любое $c_j = 1$ и процесс обрывается после $t = k$ шагов.

Теорема 5.3 позволяет дать утвердительный ответ на следующую задачу. Устроены танцы для n юношей и n девушек. Каждый юноша был предварительно представлен k девушкам, а каждая девушка — k юношам. Никто из них не пожелал расширить знакомства. Могут ли юноши и девушки быть соединенными в пары так, чтобы не было уже необходимости в новых знакомствах? Построим $(0, 1)$-матрицу $A = [a_{ij}]$, где $a_{ij} = 1$, если юноша j был предварительно представлен девушке i, и $a_{ij} = 0$ в противном случае. Тогда A удовлетворяет требованиям теоремы 5.3, а перестановочная матрица P_i из (5.4) дает желаемое распределение юношей и девушек по парам.

Матрица A порядка n называется *дважды стохастической*, если ее элементы представляют собой неотрицательные действительные числа, а суммы элементов по любой строке и по любому столбцу равны 1. Эти матрицы по праву подверглись широкому исследованию вследствие их значения в теории вероятностей перехода. Из теоремы 5.2 вытекает

Теорема 5.4. *Пусть дана дважды стохастическая матрица* A *порядка* n. *Тогда*

$$A = c_1 P_1 + c_2 P_2 + \ldots + c_t P_t, \tag{5.5}$$

где P_i *— перестановочные матрицы, а* c_j *— действительные положительные числа, такие, что*

$$c_1 + c_2 + \ldots + c_t = 1. \tag{5.6}$$

Пусть матрица A — дважды стохастическая. Ее элементы — действительные неотрицательные числа, так что $\operatorname{per} A$ не может превзойти произведения сумм элементов по строкам. Но так как каждая сумма элементов по строкам равна 1, то мы имеем

$$\operatorname{per}(A) \leqslant 1. \tag{5.7}$$

Равенство в (5.7) выполняется тогда и только тогда, когда дважды стохастическая матрица A является перестановочной. Из теоремы 5.4 очевидно, что если A — дважды стохастическая, то $\operatorname{per}(A) > 0$. Но если A — дважды стохастическая матрица порядка n, то определение минимального значения $\operatorname{per}(A)$ является трудной, еще не решенной задачей. В предположении Ван дер Вардена утверждается

$$\operatorname{per}(A) \geqslant \frac{n!}{n^n}. \tag{5.8}$$

Равенство в (5.8) получается, если $A = n^{-1}J$, где J — матрица порядка n, составленная из единиц. В действительности это может быть единственным случаем равенства. Следующее предположение является обобщением (5.8): если матрицы A и B — дважды стохастические, то

$$\operatorname{per}(AB) \leqslant \operatorname{per}(A), \operatorname{per}(B). \tag{5.9}$$

Частный случай $B = n^{-1}J$ эквивалентен (5.8).

ЛИТЕРАТУРА

Основная теорема 1.1 рассмотрена в [8], теорема 1.2 в [6]. Доказательство теоремы 1.2 содержится в [9] и [15]. Приложения к латинским прямоугольникам имеются в [5,6]. Многие из приложений к матрицам даны в [14]. Обширные исследования предположения Ван дер Вардена имеются в работах [17, 18].

1. Berge C., Théorie des Graphes et ses Applications, Paris, 1958. (Русский перевод: Берж К., Теория графов и ее применения, ИЛ, 1962.)
2. Everett C. J., Whaples G., Representations of sequences of sets, *Amer. Jour. Math.*, **71** (1949), 287—293.
3. Ford L. R., Jr., Fulkerson D. R., Network flows and systems of representatives, *Canad. Jour. Math.*, **10** (1958), 78—85.
4. Ford L. R., Jr., Fulkerson D. R., Flows in Networks, Princeton Univ. Press, 1962. (Русский перевод: Форд Л., Фалкерсон Д., Потоки в сетях, изд-во „Мир", в печати.)

5. Hall M., Jr., An existence theorem for Latin squares, *Bull. Amer. Math. Soc.*, **51** (1945), 387—388.
6. Hall M., Jr., Distinct representatives of subsets, *Bull. Amer. Math. Soc.*, **54** (1948), 922—926.
7. Hall M., Jr., An algorithm for distinct representatives, *Amer. Math. Monthly*, **63** (1956), 716—717.
8. Hall Ph., On representatives of subsets, *Jour. London Math. Soc.*, **10** (1935), 26—30.
9. Halmos P. R., Vaughan H. E., The marriage problem, *Amer. Jour. Math.*, **72** (1950), 214—215.
10. Higgins P. J., Disjoint transversals of subsets, *Canad. Jour. Math.*, **11** (1959), 280—285.
11. Hoffman A. J., Some recent applications of the theory of linear inequalities to extremal combinatorial analysis, *Proc. of Symposia in Applied Math.*, **10** (1960), 113—128.
12. Hoffman A. J., Kuhn H. W., Systems of distinct representatives and linear programming, *Amer. Math. Monthly*, **63** (1956), 455—460.
13. Hoffmann A. J., Kuhn H. W., On systems of distinct representatives, Annals of Math. Studies, v. 38, 1956, 199—206.
14. König D., Theorie der Endlichen und Unendlichen Graphen, New York, 1950.
15. Mann H. B., Ryser H. J., Systems of distinct representatives, *Amer. Math. Monthly*, **60** (1953), 397—401.
16. Marcus M., Minc H., On the relation between the determinant and the permanent, *Illinois Jour. Math.*, **5** (1961) 376—381.
17. Marcus M., Newman M., On the minimum of the permanent of a doubly stochastic matrix, *Duke Math. Journ*, **26** (1959), 61—72.
18. Marcus M., Newman M., Inequalities for the permanent function, *Ann. Math.*, **75** (1962), 47—62.
19. Mendelsohn N. S., Dulmage A. L., Some generalizations of the problem of distinct representatives, *Canad. Jour. Math.*, **10** (1958), 230—241.
20. Ore O., Graphs and matching theorems, *Duke Math. Jour.*, **22** (1955), 625—639.
21. Ore O., Theory of Graphs, Amer. Math. Soc. Collog. Publs., v. 38, 1962.
22. Rado R., Factorization of even graphs, *Quarterly Jour. Math.*, **20** (1949), 95—104.
23 Ryser H. J., A combinatorial theorem with an application to Latin rectangles, *Proc. Amer. Math. Soc.*, **2** (1951), 550—552.

Глава 6

МАТРИЦЫ ИЗ НУЛЕЙ И ЕДИНИЦ

1. Класс $\mathfrak{A}(R, S)$. Дана (0, 1)-матрица A размера $m \times n$. Обозначим через r_i сумму элементов i-й строки матрицы A, а через s_j — соответствующую сумму для j-го столбца. Назовем векторы

$$R = (r_1, r_2, \ldots, r_m) \tag{1.1}$$

и

$$S = (s_1, s_2, \ldots, s_n) \tag{1.2}$$

соответственно *вектором сумм строк* и *вектором сумм столбцов*. Будем говорить, что вектор R *монотонен*, если $r_1 \geqslant r_2 \geqslant \ldots \geqslant r_m$; аналогичное определение введем для S. Если τ обозначает число всех единиц в A, то очевидно, что

$$\tau = \sum_{i=1}^{m} r_i = \sum_{j=1}^{n} s_j. \tag{1.3}$$

Векторы R и S определяют класс

$$\mathfrak{A} = \mathfrak{A}(R, S), \tag{1.4}$$

состоящий из всех (0, 1)-матриц размера $m \times n$, имеющих вектор сумм строк R и вектор сумм столбцов S. В настоящей главе мы исследуем структуру класса $\mathfrak{A}$. Наши теоремы будут относиться к (0, 1)-матрицам, однако любой вывод может быть перефразирован в чисто комбинаторных терминах относительно множества и элемента, ибо (0, 1)-матрица размера $m \times n$ может быть интерпретирована как инцидентная матрица подмножеств $T_1, T_2, \ldots, T_m$ некоторого n-множества T.

Пусть теперь $R = (r_1, r_2, \ldots, r_m)$ и $S = (s_1, s_2 \ldots, s_n)$ — векторы, компоненты которых являются целыми

неотрицательными числами. Пусть $\mathfrak{A} = \mathfrak{A}(R, S)$ обозначает класс всех (0, 1)-матриц размера $m \times n$ с R в качестве вектора сумм строк и S в качестве вектора сумм столбцов. Исследуем условия, при которых класс $\mathfrak{A}$ будет непустым. Начнем с введения некоторых обозначений. Пусть

$$\delta_i = (1, 1, \ldots, 1, 0, 0, \ldots, 0) \quad (i = 1, 2, \ldots, m) \tag{1.5}$$

есть вектор из n составляющих с единицами на первых r_i местах и с нулями на остальных. Матрица вида

$$\overline{A} = \begin{bmatrix} \overline{\delta_1} \\ \delta_2 \\ \cdot \\ \cdot \\ \cdot \\ \underline{\delta_m} \end{bmatrix} \tag{1.6}$$

называется *максимальной матрицей* с R в качестве вектора сумм строк. Вектор сумм столбцов $\overline{S} = (\overline{s}_1, \overline{s}_2, \ldots, \overline{s}_n)$ матрицы $\overline{A}$ монотонен. Кроме того,

$$\sum_{i=1}^{m} r_i = \sum_{j=1}^{n} \overline{s}_j, \tag{1.7}$$

и класс $\mathfrak{A}(R, \overline{S})$ содержит только одну матрицу, а именно $\overline{A}$. Пусть даны два вектора: $S = (s_1, s_2, \ldots, s_n)$ и $S^* = (s_1^*, s_2^*, \ldots, s_n^*)$, компоненты которых — целые неотрицательные числа. Вектор S^* *мажорирует* вектор S:

$$S \prec S^*, \tag{1.8}$$

если при перенумерации индексов выполняются соотношения

$$s_1 \geqslant s_2 \geqslant \ldots \geqslant s_n, \quad s_1^* \geqslant s_2^* \geqslant \ldots \geqslant s_n^*, \tag{1.9}$$

$$s_1 + s_2 + \ldots + s_i \leqslant s_1^* + s_2^* + \ldots + s_i^* \quad (i = 1, 2, \ldots, n-1), \tag{1.10}$$

$$s_1 + s_2 + \ldots + s_n = s_1^* + s_2^* + \ldots + s_n^*. \tag{1.11}$$

Теорема 1.1. *Пусть* $R = (r_1, r_2, \ldots, r_m)$ *и* $S = (s_1, s_2, \ldots, s_n)$ — *два вектора с целыми неотрица-*

тельными компонентами. Пусть $\overline{A}$ — $m \times n$ *максимальная матрица с вектором сумм строк* R *и вектором сумм столбцов* $\overline{S}$. *Класс* $\mathfrak{A}(R, S)$ *будет непустым тогда и только тогда, когда*

$$S \prec \overline{S}. \tag{1.12}$$

Доказательство. Пусть класс $\mathfrak{A}$ содержит матрицу A. Последняя может быть построена из $\overline{A}$ посредством переноса единиц в строках матрицы $\overline{A}$. Таким образом, для S монотонного можем написать

$$s_1 + s_2 + \ldots + s_i \leqslant \overline{s}_1 + \overline{s}_2 + \ldots + \overline{s}_i \quad (i = 1, 2, \ldots, n-1), \tag{1.13}$$

$$s_1 + s_2 + \ldots + s_n = \overline{s}_1 + \overline{s}_2 + \ldots + \overline{s}_n, \tag{1.14}$$

откуда $S \prec \overline{S}$.

Теперь предположим, что $S \prec \overline{S}$. Перенумеруем индексы так, чтобы R и S сделались монотонными, и построим матрицу $\tilde{A}$ с вектором сумм строк R и вектором сумм столбцов S. Матрица $\tilde{A}$ строится из $\overline{A}$ последовательным перемещением единиц в строках $\overline{A}$ слева направо. Сначала опишем построение, а затем проверим, может ли оно быть выполнено. Построение начинается с перемещения последней единицы в некоторых строках матрицы $\overline{A}$ до столбца n. Потребуем, чтобы столбец n имел сумму s_n и чтобы единицы появлялись в тех строках, в которых $\overline{A}$ имеет s_n в качестве наибольшей из сумм строк. В случае когда суммы некоторых строк имеют равные значения, предпочтение отдается самым нижним положениям. Это дает нам матрицу вида

$$[\overline{A}_{n-1}, A_1]. \tag{1.15}$$

Здесь $\overline{A}_{n-1}$ есть $m \times (n-1)$ максимальная матрица с монотонными векторами сумм строк и сумм столбцов. Матрица же A_1 есть $(m \times 1)$-матрица с суммой столбца s_n. Оставим матрицу A_1 неизмененной и повторим описанное построение относительно $\overline{A}_{n-1}$. На $(n-f)$-м шаге построения мы уже будем иметь матрицу вида

$$[\overline{A}_f, A_{n-f}]. \tag{1.16}$$

Здесь $\overline{A}_f$ есть $m \times f$ максимальная матрица с монотонными векторами сумм строк и сумм столбцов, а матрица A_{n-f} — $[m \times (n-f)]$-матрица с монотонным вектором сумм столбцов $(s_{f+1}, s_{f+2}, \ldots, s_n)$.

Теперь перейдем к $(n-f+1)$-му шагу построения и убедимся, что он может быть выполнен. Предположим, что мы попытались преобразовать $\overline{A}_f$ в формуле (1.16) указанным выше способом и не смогли добиться того, чтобы столбец f имел сумму s_f. Пусть $(e_1, e_2, \ldots, e_f)$ — монотонный вектор сумм столбцов матрицы $\overline{A}_f$. Тогда мы должны иметь либо $e_1 < s_f$, либо $e_f > s_f$. Если $e_1 < s_f$, то

$$s_1 + s_2 + \ldots + s_f = e_1 + e_2 + \ldots + e_f \leqslant \\ \leqslant f e_1 < f s_f \leqslant s_1 + s_2 + \ldots + s_f, \qquad (1.17)$$

а это — очевидное противоречие. С другой стороны, если $e_f > s_f$, то $e_f > s_{f+1}, s_{f+2}, \ldots, s_n$, так что первые e_f строк матрицы A_{n-f} содержат по меньшей мере один нуль в каждом столбце. Матрица $\overline{A}_f$ — максимальная с монотонным вектором сумм строк. Но тогда по построению остальные $m - e_{f-1}$ строк матрицы A_{n-f} содержат только нули. Следовательно,

$$e_1 + e_2 + \ldots + e_{f-1} = \bar{s}_1 + \bar{s}_2 + \ldots + \bar{s}_{f-1}. \qquad (1.18)$$

Из (1.12) и (1.18) следует

$$s_1 + s_2 + \ldots + s_{f-1} + s_f = e_1 + e_2 + \ldots + e_{f-1} + e_f \leqslant \\ \leqslant \bar{s}_1 + \bar{s}_2 + \ldots + \bar{s}_{f-1} + s_f = \\ = e_1 + e_2 + \ldots + e_{f-1} + s_f. \qquad (1.19)$$

Но тогда $s_f \geqslant e_f$, а это противоречит тому, что $e_f > s_f$. Мы можем начать построение с n-го столбца, и процесс придет к автоматическому завершению в 1-м столбце. Это и доказывает теорему 1.1. Заметим теперь, что если R_i обозначает вектор сумм строк для первых i столбцов матрицы $\tilde{A}$, то R_i монотонен для всякого $i = 1, 2, \ldots, n$.

Описанное построение для случая $R = S = (3, 3, 1, 1)$ иллюстрирует матрица

$$\tilde{A} = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}. \tag{1.20}$$

Выше мы определили условия, при которых класс $\mathfrak{A}$ будет непустым. Гораздо более трудной оказывается задача подсчета числа матриц в классе. Несомненно, что это число является довольно сложной функцией от R и S.

2. Приложение к латинским прямоугольникам. Пусть дан $r \times s$ латинский прямоугольник, основанный на n элементах $1, 2, \ldots, n$. В настоящем разделе мы получим необходимое и достаточное условие для расширения латинского прямоугольника до латинского квадрата порядка n.

Теорема 2.1. *Дана* $(0, 1)$*-матрица* A *размера* $m \times n$, *причем* $m \leqslant n$. *Пусть эта матрица имеет вектор сумм строк* $R = (k, k, \ldots, k)$, *где* k *— натуральное число, а в векторе сумм столбцов* $S = (s_1, s_2, \ldots, s_n)$ *имеем*

$$0 \leqslant k - s_i \leqslant n - m \quad (i = 1, 2, \ldots, n). \tag{2.1}$$

Тогда

$$A = P_1 + P_2 + \ldots + P_k, \tag{2.2}$$

где P_i *— перестановочные матрицы.*

Доказательство. Мы можем принять, что $m < n$. В самом деле, если $m = n$, то теорема сводится к теореме 5.3 гл. 5. Пусть теперь существует $(0, 1)$-матрица A' размера $(n - m) \times n$ с вектором сумм строк $R' = (k, k, \ldots, k)$ и вектором сумм столбцов $S' = (k - s_1, k - s_2, \ldots, k - s_n)$. Пусть $\overline{S}'$ — вектор, первые k компонент которого равны $n - m$, а остальные $n - k$ компонент равны нулю. В силу (2.1) имеем $S' \prec \overline{S}'$. Следовательно, предыдущая теорема устанавливает суще-

ствование A'. Но тогда

$$\begin{bmatrix} A \\ A' \end{bmatrix} \tag{2.3}$$

есть $(n \times n)$-матрица, в которой суммы элементов строки или столбца равны k. Значит, эта матрица оказывается суммой k перестановочных матриц. Но тогда и A есть сумма перестановочных матриц.

Теорема 2.2. *Дан $r \times s$ латинский прямоугольник, построенный из n элементов* 1, 2, ..., n. *Обозначим через $N(i)$ число появлений элемента i в латинском прямоугольнике. Такой латинский прямоугольник может быть расширен до латинского квадрата n-го порядка тогда и только тогда, когда*

$$N(i) \geqslant r + s - n \quad (i = 1, 2, \ldots, n). \tag{2.4}$$

Доказательство. Пусть дано n-множество T элементов 1, 2, ..., n. Обозначим через T_j множество всех элементов T, которые не появляются в j-й строке латинского прямоугольника $(j = 1, 2, \ldots, r)$. Тогда каждое T_j есть $(n - s)$-подмножество множества T. Обозначим через $M(i)$ число появлений элемента i в множествах $T_1, T_2, \ldots, T_r$ $(i = 1, 2, \ldots, n)$. Если латинский прямоугольник может быть расширен до $n \times n$ латинского квадрата, то $M(i) \leqslant n - s$. Но $N(i) + M(i) = r$, откуда $N(i) \geqslant r + s - n$.

Обратно, предположим, что $N(i) \geqslant r + s - n$. Пусть A — инцидентная матрица для подмножеств $T_1, T_2, \ldots, T_r$ n-множества T. Матрица A размера $r \times n$ имеет вектор сумм строк $R = (n - s, n - s, \ldots, n - s)$ и вектор сумм столбцов $S = (M(1), M(2), \ldots, M(n))$. По предположению $N(i) = r - M(i) \geqslant r + s - n$, а поскольку наша конфигурация есть латинский прямоугольник, то $N(i) = r - M(i) \leqslant s$. Следовательно,

$$0 \leqslant n - s - M(i) \leqslant n - r \quad (i = 1, 2, \ldots, n), \tag{2.5}$$

и по теореме 2.1

$$A = P_1 + P_2 + \ldots + P_{n-s}, \tag{2.6}$$

где P_i — перестановочные матрицы. Но эти матрицы определяют r-перестановки элементов 1, 2, ..., n, а эти r-перестановки могут быть присоединены как столбцы к $r \times s$ латинскому прямоугольнику, чтобы получить $r \times n$ латинский прямоугольник. По теореме 3.1 гл. 5 эта конфигурация может быть расширена до $n \times n$ латинского квадрата. Можно избежать ссылки на упомянутую теорему и дополнить транспонированный $n \times r$ латинский прямоугольник до $n \times n$ латинского квадрата только что описанным методом. Условие на $N(i)$ в этом случае тривиально выполняется.

Предшествующая теорема допускает постановку следующей задачи: дана $(n \times n)$-таблица, основанная на элементах 1, 2, ..., n и одном неопределенном элементе x. При каких условиях подходящая замена элемента x элементами 1, 2, ..., n приводит к латинскому квадрату порядка n?

Настоящая теорема решает эту задачу в очень частном случае. В общем же виде эта задача никогда не была успешно решена.

3. Замены. Дана матрица A в классе $\mathfrak{A} = \mathfrak{A}(R, S)$ всех (0, 1)-матриц размера $m \times n$ с векторами сумм строк $R = (r_1, r_2, \ldots, r_m)$ и сумм столбцов $S = (s_1, s_2, \ldots, s_n)$. Рассмотрим (2×2)-подматрицы матрицы A вида

$$A_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad A_2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}. \tag{3.1}$$

Замена есть преобразование элементов матрицы A, которое переводит подматрицы типа A_1 в A_2, и наоборот, а все остальные элементы оставляет неизменными. Это в известном смысле самая элементарная операция, которая может быть применена к A, чтобы получить новую матрицу в классе $\mathfrak{A}$. Замены полезны во многих задачах, где речь идет о классе $\mathfrak{A}$. Начнем с установления теоремы о заменах.

Теорема 3.1. *Пусть матрицы A и A' входят в класс $\mathfrak{A}(R, S)$. Тогда матрица A может быть*

преобразована в матрицу A' с помощью конечного числа замен.

Доказательство. Примем, что R и S монотонны, а матрица A построена, как в первом разделе. Мы можем применить замены к A так, чтобы n-й столбец в ней был заменен n-м столбцом матрицы $\tilde{A}$. Это возможно потому, что столбец n в $\tilde{A}$ имеет свои единицы в тех строках, в которых наибольшей суммой является s_n. Теперь оставим столбец n преобразованной матрицы неизменным и сконцентрируем наше внимание на столбце $n-1$. Первые $n-1$ столбцов как в $\tilde{A}$, так и в преобразованной матрице суть матрицы с одним и тем же вектором сумм строк. Исходя из структуры $\tilde{A}$, мы можем применить замены к преобразованной матрице и заменить $(n-1)$-й столбец ее на $(n-1)$-й столбец матрицы $\tilde{A}$. Таким образом, мы преобразовываем матрицу A в матрицу $\tilde{A}$ посредством замен. Мы также можем преобразовать заменами матрицу A' в матрицу $\tilde{A}$. Пусть промежуточные матрицы, получающиеся при этом преобразовании, будут $A_1, A_2, \ldots, A_q$. Но в таком случае существует замена, переводящая $\tilde{A}$ в A_q. Существует также замена, переводящая A_q в A_{q-1} и т. д. Таким образом, матрица $\tilde{A}$ преобразуема заменами в матрицу A'. Следовательно, матрица A может быть преобразована заменами в матрицу A'. Заметим, что формула минимального числа замен, требуемых для преобразования A в A', является, очевидно, безнадежно сложной функцией от A и A'.

Пусть A — матрица из класса $\mathfrak{A}(R, S)$. Во многих исследованиях принимают без ограничения общности, что векторы сумм строк R и сумм столбцов S удовлетворяют условиям

$$r_1 \geqslant r_2 \geqslant \ldots \geqslant r_m > 0, \tag{3.2}$$

$$s_1 \geqslant s_2 \geqslant \ldots \geqslant s_n > 0. \tag{3.3}$$

Это означает, что мы исключили строки и столбцы, состоящие из нулей, и переставили оставшиеся строки и столбцы так, чтобы они были расположены монотонно. Непустой класс $\mathfrak{A}(R, S)$, в котором R и S удовлетворяют

условиям (3.2) и (3.3), называется *нормализованным*. В дальнейшем мы будем считать $\mathfrak{A}$ нормализованным.

Пусть дана матрица A нормализованного класса $\mathfrak{A}$. Элемент $a_{ef}=1$ матрицы A будем называть *инвариантной единицей*, если никакая последовательность замен, примененных к A, не заменяет этот элемент на нуль. Если $a_{ef}=1$ есть инвариантная единица матрицы A, то по теореме о заменах элементы, находящиеся на месте (e, f) во всех матрицах класса $\mathfrak{A}$, должны быть инвариантными единицами. Таким образом, или все матрицы класса $\mathfrak{A}$ содержат инвариантные единицы, или ни одна. Поэтому мы будем говорить, что класс $\mathfrak{A}$ либо имеет, либо не имеет инвариантной единицы.

Теорема 3.2. *Нормализованный класс $\mathfrak{A}$ имеет инвариантные единицы тогда и только тогда, когда всякая матрица этого класса имеет разложение вида*

$$A=\begin{bmatrix} J & * \\ * & 0 \end{bmatrix}. \tag{3.4}$$

Здесь J — матрица из единиц размера $e\times f$ $(0<e\leqslant m,\ 0<f\leqslant n)$, а 0 — нулевая матрица. Целые числа e и f не обязательно единственны, но они определены векторами сумм строк R и сумм столбцов S и не зависят от того, какая конкретная матрица A выбрана из класса $\mathfrak{A}$.

Доказательство. Очевидно, что в J всякая 1 инвариантна. Предположим далее, что нормализованный класс $\mathfrak{A}$ имеет инвариантные единицы. Положим, что a_{ef} есть инвариантная единица при $e+f$ максимальном и пусть

$$A=\begin{bmatrix} W & X \\ Y & Z \end{bmatrix}, \tag{3.5}$$

где W имеет размер $e\times f$. Если в W появился нуль, то при нормализации $\mathfrak{A}$ требуется самое большее две замены чтобы инвариантная единица сменилась на 0. Следовательно, $W=J$, и каждая единица в J инвариантна.

Теперь, поскольку $e+f$ максимально, мы можем выбрать матрицу A так, чтобы 0 появился в первом столбце X. Далее, если Z содержит 1 в t-й строке, то мы можем, если это необходимо, применить замену и получить, что в Z первый столбец содержит 1 в t-й строке. Но тогда Y в t-й строке будет содержать только единицы. В самом деле, если Y содержит 0 в t-й строке, то одна замена образует инвариантную единицу матрицы A. Фактически каждая единица в t-й строке матрицы Y является инвариантной. Но это противоречит условию максимальности $e+f$. Следовательно, $Z=0$ и матрица A имеет вид (3.4). А если это так, то всякая матрица A в классе $\mathfrak{A}$ имеет вид (3.4).

4. Максимальный граничный ранг. Пусть $\tilde{\rho}$ будет минимальным, а $\bar{\rho}$ — максимальным граничным рангом матриц нормализованного класса $\mathfrak{A}=\mathfrak{A}(R, S)$. Настоящий пункт мы посвятим изучению $\bar{\rho}$. Приведенные здесь теоремы интересны сами по себе, и, кроме того, они дают явное выражение для $\bar{\rho}$. Но метод, применяемый при выводе этих теорем, приложим к большому числу задач. Начнем с одного элементарного результата о промежуточных граничных рангах.

Теорема 4.1. *Пусть $\tilde{\rho}$ — минимальный, а $\bar{\rho}$ — максимальный граничный ранг матриц нормализованного класса $\mathfrak{A}$. Тогда $\mathfrak{A}$ содержит матрицу A_ρ, граничный ранг которой равен ρ, где ρ — произвольное целое число в отрезке*

$$\tilde{\rho} \leqslant \rho \leqslant \bar{\rho}. \tag{4.1}$$

Доказательство. Применение замены к матрице A класса $\mathfrak{A}$ изменяет ее граничный ранг на 1 или оставляет его неизменным. Но по теореме о заменах мы можем преобразовать матрицу $A_{\bar{\rho}}$ с граничным рангом $\bar{\rho}$ в матрицу $A_{\tilde{\rho}}$ с граничным рангом $\tilde{\rho}$. Из этого следует, что существует матрица A, граничный ранг которой равен ρ.

Теорема 4.2. *Нормализованный класс* $\mathfrak{A}$ *содержит матрицу* $A_{\bar{\rho}}$, *в которой* $\bar{\rho}$ *единиц находятся на местах*

$$(1, \bar{\rho}), \quad (2, \bar{\rho}-1), \ \ldots, \ (\bar{\rho}, 1).$$

Доказательство. Дана матрица $A_{\bar{\rho}}$ с максимальным граничным рангом $\bar{\rho}$. Выберем в ней множество из $\bar{\rho}$ единиц, никакие две из которых не находятся на одной линии, и назовем эти единицы *существенными* для матрицы $A_{\bar{\rho}}$. Все другие единицы матрицы $A_{\bar{\rho}}$ назовем *несущественными*. Мы можем выбрать матрицу $A_{\bar{\rho}}$, содержащую $\bar{\rho}$ существенных единиц в первых $\bar{\rho}$ строках. В самом деле предположим, что существенная единица находится на (i, j)-м месте и что строка i' не содержит существенных единиц ($i' \leqslant \bar{\rho} < i$). Тогда назовем единицу, находящуюся на месте (i', j), существенной, а единицу, находящуюся на месте (i, j), несущественной. С другой стороны, если на (i', j)-м месте находится 0, то в силу нормализации $\mathfrak{A}$ существует замена, которая помещает существенную единицу на (i', j)-е место и сохраняет граничный ранг $\bar{\rho}$. Таким способом мы получаем $A_{\bar{\rho}}$ с существенными единицами в первых $\bar{\rho}$ строках. Аналогичные рассуждения относительно столбцов приводят к матрице вида

$$A_{\bar{\rho}} = \begin{bmatrix} D & * \\ * & 0 \end{bmatrix}. \tag{4.2}$$

Здесь у D и порядок, и граничный ранг равны $\bar{\rho}$. Матрица 0 — нулевая, потому что граничный ранг матрицы $A_{\bar{\rho}}$ не может превосходить $\bar{\rho}$. Будем говорить, что $\bar{\rho}$ элементов матрицы, расположенных на местах $(1, \bar{\rho})$, $(2, \bar{\rho}-1)$, $\ldots$, $(\bar{\rho}, 1)$, образуют *побочную диагональ* матрицы D. Получим теперь матрицу $A_{\bar{\rho}}$, имеющую $\bar{\rho}$ существенных единиц на побочной диагонали D. Предположим, что существенные единицы имеются на местах $(1, \bar{\rho})$, $(2, \bar{\rho}-1)$, $\ldots$, $(d, \bar{\rho}-d+1)$, а на месте $(d+1, \bar{\rho}-d)$ существенной единицы нет. Тогда суще-

ственная единица в $(d+1)$-й строке и существенная единица в $(\bar{\rho}-d)$-м столбце определяет (2×2)-подматрицу матрицы D одного из следующих четырех видов

$$\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix},\quad \begin{bmatrix}1 & 0\\ 1 & 1\end{bmatrix},\quad \begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix},\quad \begin{bmatrix}1 & 1\\ 1 & 1\end{bmatrix}. \tag{4.3}$$

Единицы, расположенные в (4.3) на главной диагонали, соответствуют существенным единицам матрицы $A_{\bar{\rho}}$. В любом случае требуется не больше одной замены, чтобы поместить две единицы на места, соответствующие побочной диагонали в (4.3). Эти единицы можно рассматривать как существенные для матрицы $A_{\bar{\rho}}$. Это и дает нам существенную единицу на $(d+1,\ \bar{\rho}-d)$-м месте матрицы D. Таким образом, матрица $A_{\bar{\rho}}$, имеющая $\bar{\rho}$ существенных единиц на побочной диагонали, существует.

Пусть дана (0, 1)-матрица Q. Обозначим через $N_0(Q)$ число нулей, а через $N_1(Q)$ — число единиц в Q. Пусть A есть (0, 1)-матрица размера $m\times n$. Тогда в матрице A выполняется условие: $m,\ n>0$. Но если A разбита на блоки[1]), то удобно ввести вырожденные подматрицы W размера $e\times f$, где либо $e=0$, либо $f=0$[2]). В вырожденной подматрице W имеем $N_0(W)=N_1(W)=0$. После этих замечаний мы готовы высказать наше основное заключение относительно максимального граничного ранга $\bar{\rho}$ матриц в нормализованном классе $\mathfrak{A}$.

Теорема 4.3. *Всякая матрица A в нормализованном классе $\mathfrak{A}$ имеет разложение вида*

$$A=\begin{bmatrix}W & X\\ Y & Z\end{bmatrix}, \tag{4.4}$$

где W — подматрица размера $e\times f$ $(0\leqslant e\leqslant m,\ 0\leqslant f\leqslant n)$, Z — подматрица размера $(m-e)\times(n-f)$ и, кроме того,

$$N_0(W)+N_1(Z)=\bar{\rho}-(e+f). \tag{4.5}$$

[1]) То есть непересекающиеся подматрицы из некоторого числа столбцов. — *Прим. ред.*

[2]) То есть подматрицы нулевого порядка. — *Прим. ред.*

Целые числа e и f не обязательно единственны, но они определены векторами сумм строк R и сумм столбцов S и не зависят от выбора конкретной матрицы A в классе $\mathfrak{A}$. В частности, матрица $A_{\bar{\rho}}$ из теоремы (4.2) *удовлетворяет соотношению*

$$N_0(W) = 0, \quad N_1(Z) = \bar{\rho} - (e + f). \tag{4.6}$$

Доказательство. Если матрица A имеет вектор сумм строк $R = (r_1, r_2, \ldots, r_m)$ и вектор сумм столбцов $S = (s_1, s_2, \ldots, s_n)$, то из этого тотчас следует, что

$$N_0(W) + N_1(Z) = ef + (r_{e+1} + r_{e+2} + \ldots + r_m) - (s_1 + s_2 + \ldots + s_f). \tag{4.7}$$

Таким образом, сумма $N_0(W) + N_1(Z)$ не зависит от выбора матрицы A в классе $\mathfrak{A}$. Этого достаточно, чтобы доказать теорему для матрицы $A_{\bar{\rho}}$ теоремы 4.2. Сосредоточим наше внимание на $A_{\bar{\rho}}$ и применим индукцию относительно ее строк. Теорема справедлива для однострочной матрицы. Доказательство по индукции состоит в утверждении, что если теорема доказана для $(m-1)$-строчных матриц, то она справедлива и для матриц с m строками. Теперь, если $\bar{\rho} = m$, то теорема справедлива для $e = m$ и $f = 0$. Если же $\bar{\rho} = n$, то теорема верна в случае $e = 0$ и $f = n$. Следовательно, положим, что $\bar{\rho} < m, n$. Заметим, что в этом случае e и f доставляют собственное разложение[1]) матрицы $A_{\bar{\rho}}$ $(0 < e < m,\ 0 < f < n)$. Так как если $e = 0$ или m, либо $f = 0$ или n, то мы получим противоречие условию $\bar{\rho} < m, n$.

Пусть теперь матрица $A_{\bar{\rho}} = [a_{ij}]$ из теоремы 4.2 имеет граничный ранг $\bar{\rho} < m, n$. Нормализуем первую строку матрицы $A_{\bar{\rho}}$ заменами следующим образом. Если $s_i > s_j$, $a_{1i} = 0$, $a_{1j} = 1$, то применим замену, которая заменит a_{1i} на 1 и a_{1j} на 0. Если $i < \bar{\rho}$, то замену выбираем так, чтобы она не помещала существенную единицу на $(\bar{\rho} - i + 1, i)$-е место в $A_{\bar{\rho}}$. Таким же образом, если

[1]) То есть представление (4.2). — *Прим. ред.*

$s_i = s_j$ $(i < j)$, $a_{1i} = 1$, $a_{1j} = 0$, применим замену, в которой вместо a_{1i} появляется 0 и вместо a_{1j} — единица. Если $j < \bar{\rho}$, то эта замена не поместит существенную единицу на $(\bar{\rho} - j + 1, j)$-е место в $A_{\bar{\rho}}$. Если же этого не удастся избежать, то матрица имеет 1 на $(\bar{\rho} - i + 1, j)$-м месте, и вторая замена, включающая строки $(\bar{\rho} - i + 1)$ и и $(\bar{\rho} - j + 1)$, возвращает 1 на $(\bar{\rho} - j + 1, j)$-е место. Если мы применим все возможные замены описанного типа, то получим матрицу вида

$$M = \begin{bmatrix} \delta_1 & \delta_2 \\ A_{\bar{\rho}-1} & 0 \end{bmatrix}. \tag{4.8}$$

В (4.8) δ_1 есть вектор из n' компонент, а δ_2 — вектор из $n - n'$ единиц. Вырожденный случай $n = n'$ не исключен. Матрица $A_{\bar{\rho}-1}$ размера $(m - 1) \times n'$ имеет единицы на местах $(1, \bar{\rho} - 1)$, $(2, \bar{\rho} - 2)$, ..., $(\bar{\rho} - 1, 1)$ и порождает нормализованный класс $\mathfrak{A}'$. Матрица 0 — нулевая размера $(m - 1) \times (n - n')$.

Докажем, что $\bar{\rho} - 1$ есть максимальный граничный ранг матрицы класса $\mathfrak{A}'$. Пусть A' — матрица класса $\mathfrak{A}'$, имеющая $\bar{\rho}$ существенных единиц на местах $(1, \bar{\rho})$, $(2, \bar{\rho} - 1)$, ..., $(\bar{\rho}, 1)$. В (4.8) заменим матрицу $A_{\bar{\rho}-1}$ на A' и назовем получившуюся при этом матрицу M'. Матрица M' принадлежит классу $\mathfrak{A}$. Если это окажется необходимым, применим замену, чтобы поместить 1 на $(1, n)$-е место в матрице M'. Но в таком случае граничный ранг матрицы M' противоречит условию максимальности $\bar{\rho}$ для $\mathfrak{A}$. Таким образом, $A_{\bar{\rho}-1}$ имеет максимальный граничный ранг $\bar{\rho} - 1$, а ее существенные единицы располагаются на местах $(1, \bar{\rho} - 1)$, $(2, \bar{\rho} - 2)$, ..., $(\bar{\rho} - 1, 1)$. По предположению индукции

$$A_{\bar{\rho}-1} = \begin{bmatrix} W' & X' \\ Y' & Z' \end{bmatrix}, \tag{4.9}$$

где W' — матрица из единиц размера $e' \times f'$, а $N_1(Z') = \bar{\rho} - 1 - (e' + f')$. Выберем f' максимальным в том

смысле, что каждый столбец в X', помимо существенных единиц в Z', содержит один нуль. Нам известно, что $\bar{\rho}-1<m-1$, но возможно $\bar{\rho}-1=n'$. Последнее приводит к вырожденному разложению матрицы $A_{\bar{\rho}-1}$, в котором $e'=0$, $f'=n'$. Но во всех других разложениях $0<e'<m-1$, $0<f'<n'$.

Теперь в (4.8) предположим, что M имеет один нуль в δ_1 над некоторым столбцом из Y', и пусть этот столбец из Y' содержит несущественную единицу из $A_{\bar{\rho}-1}$. Тогда, проведя нормализацию первой строки M, получим, что $n'=n$ и что нули появляются на местах $f'+1$, $f'+2$, ..., n в δ_1. Теперь, если разложение $A_{\bar{\rho}-1}$ вырожденное, то это противоречит тому, что $\bar{\rho}-1=n'$, а если оно невырожденное, то получается противоречие с $r_1\geqslant r_2$. Следовательно, если M имеет нуль в δ_1 сверх столбца из Y', то этот столбец не содержит несущественных единиц из $A_{\bar{\rho}-1}$. Это означает, что разложение (4.9) может быть перестроено так, чтобы M не имела нулей в δ_1 над столбцами Y'. Если это будет необходимо, можно применить замену, чтобы поместить 1 на место $(1, \bar{\rho})$ в M. Это и даст нам разложение желаемого вида.

Нетрудным следствием из этой теоремы является замечательная формула, в которой $\bar{\rho}$ выражено через компоненты вектора сумм строк $R=(r_1, r_2, \ldots, r_m)$ и вектора сумм столбцов $S=(s_1, s_2, \ldots, s_n)$ матриц нормализованного класса $\mathfrak{A}(R, S)$.

Теорема 4.4. *Пусть*

$$t_{ij}=ij+(r_{i+1}+r_{i+2}+\ldots+r_m)-(s_1+s_2+\ldots+s_j)$$
$$(i=0, 1, \ldots, m;\ j=0, 1, \ldots, n). \qquad (4.10)$$

Тогда

$$\bar{\rho}=\min_{i,j}\{t_{ij}+(i+j)\} \qquad (4.11)$$
$$(i=0, 1, \ldots, m;\ j=0, 1, \ldots, n).$$

Доказательство. Пусть

$$A_{\bar{\rho}}=\begin{bmatrix} W & X \\ Y & Z \end{bmatrix} \qquad (4.12)$$

— матрица с максимальным граничным рангом $\bar{\rho}$ и пусть W — матрица размера $i \times j$. Теперь $\bar{\rho}$ линий достаточно, чтобы покрыть единицы в $A_{\bar{\rho}}$. Следовательно,

$$N_1(Z) + (i + j) \geqslant \bar{\rho}. \tag{4.13}$$

Но $N_0(W) \geqslant 0$, так что

$$t_{ij} + (i + j) \geqslant \bar{\rho}. \tag{4.14}$$

Равенство в формуле (4.14) достигается для тех значений e и f [1]), которые указаны в теореме 4.3. Таким образом, теорема 4.4 доказана.

Указанная формула пригодна и для вычисления $\tilde{\rho}$, но мы не будем здесь на этом останавливаться. Следующая теорема дает нам условия, при которых $\tilde{\rho} < \bar{\rho}$.

Теорема 4.5. *Дан нормализованный класс* $\mathfrak{A}$, *не имеющий инвариантных единиц; пусть* $\bar{\rho} < m, n$. *Тогда* $\tilde{\rho} < \bar{\rho}$.

Доказательство. По предположению $\bar{\rho} < m, n$. Следовательно, e и f из теоремы 4.3 находятся соответственно в интервалах $0 < e < m$ и $0 < f < n$. По условию элемент матрицы $A_{\bar{\rho}}$ из теоремы 4.3, находящийся на месте (1,1), не является инвариантной единицей. Но по теореме 4.3 имеем $N_0(W) + N_1(Z) = \bar{\rho} - (e + f)$. Это означает, что в классе $\mathfrak{A}$ существуют матрицы с числом единиц в Z, меньшим, чем $\bar{\rho} - (e + f)$. Но тогда единицы в такой матрице могут быть покрыты менее чем $\bar{\rho}$ линиями. Следовательно, $\tilde{\rho} < \bar{\rho}$.

Заметим, что теорема 4.5 может не удовлетворяться, если отбросить предположение об инвариантных единицах. Класс, содержащий максимальную матрицу A, имеет $\tilde{\rho} = \bar{\rho}$. Ограничение $\bar{\rho} < m, n$ не может быть устранено. Например, класс из $n!$ перестановочных матриц порядка n имеет $\tilde{\rho} = \bar{\rho}$. Интересной нерешенной задачей является

[1]) То есть i и j. — *Прим. ред.*

четкая классификация всех классов $\mathfrak{A}(R, S)$, для которых $\tilde{\rho} = \bar{\rho}$.

5. Задачи. Предыдущий раздел был посвящен анализу граничного ранга матрицы A нормализованного класса $\mathfrak{A}$. Мы можем связать с A другие подходящие функции и исследовать их поведение, когда матрица A распространяется на весь их класс[1]). В некоторых случаях подобные исследования были выполнены. Например, пусть $\tilde{\sigma}$ — минимальный, а $\bar{\sigma}$ — максимальный следы матриц нормализованного класса $\mathfrak{A}$. Тогда можно доказать, что

$$\tilde{\sigma} = \max_{i,\,j} \{\min(i,\ j) - t_{ij}\} \tag{5.1}$$

$$(i = 0,\ 1,\ \ldots,\ m;\ \ j = 0,\ 1,\ \ldots,\ n),$$

$$\bar{\sigma} = \min_{i,\,j} \{t_{ij} + \max(i,\ j)\} \tag{5.2}$$

$$(i = 0,\ 1,\ \ldots,\ m;\ \ j = 0,\ 1,\ \ldots,\ n).$$

Эти формулы носят черты большого сходства с формулой для $\bar{\rho}$ в п. 4, а их вывод производится довольно сходными путями.

Однако многие экстремальные задачи этого вида не могут быть рассмотрены с такой тщательностью. Пусть дана матрица A в нормализованном классе $\mathfrak{A}(R, S)$ и пусть α — целое число, расположенное в отрезке $1 \leqslant \alpha \leqslant r_m$. Пусть E есть $(m \times \varepsilon)$-подматрица матрицы A, и сумма элементов каждой строки матрицы E равна по меньшей мере α. Минимальное значение ε, обладающее этим свойством, назовем α-*шириной* $\varepsilon(\alpha)$ матрицы A. Целое число α и матрица A единственным образом определяют $\varepsilon(\alpha)$. Теперь пусть $\tilde{\varepsilon}(\alpha)$ — минимальная, а $\bar{\varepsilon}(\alpha)$ — максимальная α-ширины матриц класса $\mathfrak{A}$. Можно доказать, что матрица $\tilde{A}$, построенная в первом разделе, имеет α-ширину $\tilde{\varepsilon}(\alpha)$ для всякого $\alpha = 1,\ 2,\ \ldots,\ r_m$. В самом деле, оказывается, что α-я единица в последней строке матрицы $\tilde{A}$ попадает в столбец $\tilde{\varepsilon}(\alpha)$. Это замечательное свойство

[1]) Имеется в виду класс функций с одной и той же матрицей A. — *Прим. ред.*

матрицы $\tilde{A}$ дает эффективный способ вычисления $\tilde{\varepsilon}(\alpha)$. Но относительно поведения $\bar{\varepsilon}(\alpha)$ известно очень мало. Больше информации можно получить о его предельном значении. В гл. 8 это сделается очевидным. Там мы рассмотрим взаимосвязь между $\bar{\varepsilon}(1)$ и конечными проективными плоскостями.

Для некоторых классов частных видов существуют задачи, интересные сами по себе. Пусть $\mathfrak{A}(K, K)$ обозначает класс, в котором $m = n$, а также

$$R = S = K = (k, k, \ldots, k), \tag{5.3}$$

где k — фиксированное целое число, расположенное в отрезке $1 \leqslant k \leqslant n$. Таким образом, $\mathfrak{A}(K, K)$ есть класс всех (0, 1)-матриц порядка n, в каждой строке и каждом столбце которых имеется точно k единиц. В случае $k = 1$ класс состоит из $n!$ перестановочных матриц порядка n, а в случае $k = n$ — из матриц J порядка n. Из теоремы 5.3 гл. 5 следует, что в классе $\mathfrak{A}(K, K)$

$$\tilde{\rho} = \bar{\rho} = m = n. \tag{5.4}$$

При этих условиях естественно задать вопрос о минимальном и максимальном значениях перманента матриц класса $\mathfrak{A}(K, K)$. Однако ни то ни другое значение еще не определены. Задача определения минимального значения может иметь важное комбинаторное значение. Соответствующая задача для дважды стохастических матриц приводит к предположению Ван дер Вардена (см. гл. 5).

ЛИТЕРАТУРА

Теорема 1.1 принадлежит Гейлу [9] и Райзеру [13], а теорема 4.2 — Хаберу [10]. Остальные теоремы в §§ 2, 3 и 4 доказаны Райзером [12, 13, 14]. В п. 3 при изложении доказательств мы следовали Хаберу [10]. Минимальный граничный ранг $\tilde{\rho}$ рассмотрен в [10, 11]. Следы матриц изучены в [5] и [15], а α-ширины — в [6, 7, 8].

1. Dulmage A. L., Mendelsohn N. S., Coberings of bipartite graphs, *Canad. Jour. Math.*, **10** (1958), 517—534.
2. Dulmage A. L., Mendelsohn N. S., The term and stochastic ranks of a matrix, *Canad. Jour. Math.*, **11** (1959), 269—279.

3. Evans T., Embedding incomplete Latin squares, *Amer. Math Monthly*, **67** (1960), 958—961.
4. Ford L. R., Jr., Fulkerson D. R., Flows in Networks, Princeton Univ. Press, 1962. (О русском переводе этой книги см. стр. 62.)
5. Fulkerson D. R., Zero-one matrices with zero trace, *Pacific Jour. Math.*, **10** (1960), 831—836.
6. Fulkerson D. R., Ryser H. J., Widths and heights of (0,1)-matrices, *Canad. Jour. Math.*, **13** (1961), 239—255.
7. Fulkerson D. R., Ryser H. J., Multiplicities and minimal widths for (0, 1)-matrices, *Canad. Jour. Math.*, **14** (1962), 498—508.
8. Fulkerson D. R., Ryser H. J., Width sequences for special classes of (0, 1)-matrices, *Canad. Jour. Math.*, **15** (1963), № 3, 371—396.
9. Gale D., A theorem on flows in Networks, *Pacific Jour. Math.*, **7** (1957), 1073—1082.
10. Haber R. M., Term rank of (0, 1)-matrices, *Rend. Sem. Math. Padova*, **30** (1960), 24—51.
11. Haber R. M., Minimal term rank of a class of (0, 1)-matrices, *Canad. Jour. Math.*, **15** (1963), 188—192.
12. Ryser H. J., A combinatorial theorem with an application to Latin rectangles, *Proc. Amer. Math. Soc.*, **2** (1951), 550—552.
13. Ryser H. J., Combinatorial properties of matrices of zeros and ones, *Canad. Jour. Math.*, **9** (1957), 371—377.
14. Ryser H. J., The term rank of a matrix, *Canad. Jour. Math.*, **10** (1958), 57—65.
15. Ryser H. J., Traces of matrices of zeros and ones, *Canad. Jour. Math.*, **12** (1960), 463—476.
16. Ryser H. J., Matrices of zeros and ones, *Bull. Am r. Math. Soc.*, **66** (1960), 442—464.

Глава 7

ОРТОГОНАЛЬНЫЕ ЛАТИНСКИЕ КВАДРАТЫ

1. Теоремы существования. Пусть $A_1 = (a_{ij}^{(1)})$ и $A_2 = (a_{ij}^{(2)})$ обозначают два $n \times n$ латинских квадрата, основанных на n элементах $1, 2, \ldots, n$, и пусть $n \geqslant 3$. Латинские квадраты A_1 и A_2 называются *ортогональными*, если все n^2 2-выборок

$$(a_{ij}^{(1)}, a_{ij}^{(2)}) \quad (i, j = 1, 2, \ldots, n) \tag{1.1}$$

различны. Иными словами, предположим, что один из латинских квадратов наложен на другой. Тогда получающаяся конфигурация будет $(n \times n)$-таблицей (n by n array), состоящей из упорядоченных пар чисел $1, 2, \ldots, n$, а требование ортогональности латинских квадратов означает, что все элементы этой таблицы различны. Эта $(n \times n)$-таблица 2-выборок, составленная из пары ортогональных латинских квадратов, в литературе часто называется *греко-латинским* или *эйлеровским квадратом*. Приведем пример пары ортогональных латинских квадратов 3-го порядка:

$$A_1 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix}, \quad A_2 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix}. \tag{1.2}$$

В более общей постановке, пусть $A_1, A_2, \ldots, A_t$ — множество двух или более латинских квадратов порядка $n \geqslant 3$. В этом множестве латинские квадраты называются *ортогональными*, а все множество $A_1, A_2, \ldots, A_t$ — *ортогональным множеством*, если A_i ортогонален A_j для всяких $i \neq j$. В настоящей главе мы изучаем ортогональные множества. Эти конфигурации имеют длинную историю и одно время подвергались исследованию ради развлечения. Но в наши дни мы осознаем их важность при изучении конечных проективных плоскостей и при-

мыкающих к ним вопросов. Начнем со следующего элементарного результата.

Теорема 1.1. *Пусть дано множество t ортогональных латинских квадратов $A_1, A_2, \ldots, A_t$ порядка $n \geqslant 3$. Тогда*

$$t \leqslant n - 1. \tag{1.3}$$

Доказательство. Перенумеруем элементы каждого латинского квадрата так, чтобы первая строка каждого из латинских квадратов состояла из элементов 1, 2, ..., n именно в таком порядке. Это не нарушает ортогональности множества. Рассмотрим теперь t элементов, находящихся на месте (2,1) этих латинских квадратов. Эти t элементов должны быть различными, потому что в противном случае мы получили бы противоречие с условием ортогональности множества. Ни один из этих элементов не равен 1. Следовательно, $t \leqslant n - 1$.

Если в (1.3) имеет место равенство, то ортогональное множество называется *полным*. Множество (1.2) является полным.

Здесь мы предполагаем, что читатель знает элементарные свойства конечных полей. Это поля, составленные из конечного числа элементов. Если n обозначает число элементов поля, то хорошо известно, что $n = p^\alpha$, где p — простое, а α — натуральное число. Обратно, для любого простого p и натурального α существует поле из $n = p^\alpha$ элементов. Более того, два поля из $n = p^\alpha$ элементов определяются единственным образом с точностью до изоморфизма. Поле из $n = p^\alpha$ элементов носит название *поля Галуа* и обозначается символом $GF(p^\alpha)$. Если $\alpha = 1$, то элементы поля Галуа могут быть выбраны в виде полной системы вычетов 0, 1, ..., $p - 1$ по модулю p. Операции над полем — сложение и умножение — осуществляются по модулю p. Ниже мы докажем теорему существования для полного множества ортогональных латинских квадратов. В доказательстве используется существование поля Галуа $GF(p^\alpha)$.

Теорема 1.2. *Пусть $n = p^\alpha$, где p — простое, а α — натуральное числа. Тогда для $n \geqslant 3$ сущест-*

вует полное множество из $n-1$ ортогональных латинских квадратов порядка n.

Доказательство. Обозначим элементы поля Галуа $GF(p^\alpha)$ так: $a_0=0$, $a_1=1$, $a_2, \ldots, a_{n-1}$. Определим $n-1$ матриц порядка n

$$A_e=\left[a_{ij}^{(e)}\right] \quad (i, j=0, 1, \ldots, n-1;\ e=1, 2, \ldots, n-1), \tag{1.4}$$

где

$$a_{ij}^{(e)}=a_e a_i+a_j. \tag{1.5}$$

Здесь каждая матрица A_e является латинским квадратом. В самом деле, если A_e имеет два одинаковых элемента в одной и той же строке, то существуют j и j' такие, что

$$a_e a_i+a_j=a_e a_i+a_{j'}. \tag{1.6}$$

Но из этого следует $a_j=a_{j'}$ и $j=j'$. Аналогично, если A_e имеет два одинаковых элемента в одном и том же столбце, то существуют i и i' такие, что

$$a_e a_i+a_j=a_e a_{i'}+a_j. \tag{1.7}$$

Но поскольку $a_e\neq 0$, отсюда вытекает, что $a_i=a_{i'}$ и $i=i'$. Следовательно, каждая матрица A_e есть латинский квадрат. Теперь пусть $1\leqslant e<f\leqslant n-1$. В таком случае A_e и A_f ортогональны. Действительно, положим, что

$$\left(a_{ij}^{(e)}, a_{ij}^{(f)}\right)=\left(a_{i'j'}^{(e)}, a_{i'j'}^{(f)}\right). \tag{1.8}$$

Тогда

$$a_e a_i+a_j=a_e a_{i'}+a_{j'}, \tag{1.9}$$

$$a_f a_i+a_j=a_f a_{i'}+a_{j'}. \tag{1.10}$$

Вычитание (1.10) из (1.9) дает

$$a_i(a_e-a_f)=a_{i'}(a_e-a_f). \tag{1.11}$$

Поскольку $a_e\neq a_f$, имеем $a_i=a_{i'}$ и $i=i'$. Но тогда подстановка в (1.9) дает $a_j=a_{j'}$ и $j=j'$. Следовательно, множество (1.4) ортогонально.

Теорема 1.3. *В случае $n\geqslant 3$ и $t\geqslant 2$ множество t ортогональных латинских квадратов порядка n*

эквивалентно $[n^2 \times (t+2)]$-*таблице.*

$$A = [a_{ij}] \quad (i = 1, 2, \ldots, n^2;\ j = 1, 2, \ldots, t+2). \quad (1.12)$$

Элементы a_{ij} *таблицы* A *нумеруются* $1, 2, \ldots, n$, *а строки каждой* $(n^2 \times 2)$-*подтаблицы таблицы* A *представляют* n^2 2-*выборок из* $1, 2, \ldots, n$.

Доказательство. Дана таблица A. Переставим в ней строки таким образом, чтобы элементы строк в первых двух столбцах находились в естественном порядке $(1, 1), (1, 2), \ldots, (1, n), \ldots, (n, 1), (n, 2), \ldots, (n, n)$. Для каждого $e = 3, 4, \ldots, t+2$ построим $(n \times n)$-таблицу A_e следующим образом. Первая строка A_e состоит из первых n элементов столбца e таблицы A, вторая строка A_e из следующих n элементов столбца e таблицы A и т. д. до последней строки, состоящей из последних n элементов столбца e таблицы A. Тогда $A_3, A_4, \ldots, A_{t+2}$ образуют множество t ортогональных латинских квадратов порядка n. В самом деле, предположение относительно A таково, что каждая из таблиц является латинским квадратом. Действительно, по виду первого столбца таблицы A устанавливаем, что A_e не имеет двух одинаковых элементов в строке, а по виду второго столбца таблицы A — что A_e не имеет двух одинаковых элементов в столбце. Итак, если $e \neq f$, то A_e и A_f ортогональны в силу способа построения столбцов e и f таблицы A. Обратное предложение доказывается аналогично.

Например, с латинскими квадратами (1.2) связана такая таблица:

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 2 & 2 \\ 1 & 3 & 3 & 3 \\ 2 & 1 & 2 & 3 \\ 2 & 2 & 3 & 1 \\ 2 & 3 & 1 & 2 \\ 3 & 1 & 3 & 2 \\ 3 & 2 & 1 & 3 \\ 3 & 3 & 2 & 1 \end{bmatrix}. \quad (1.13)$$

Теорема 1.4. *Если существует множество из t ортогональных латинских квадратов порядка n и если существует множество из t ортогональных латинских квадратов порядка n', то существует и множество из t ортогональных латинских квадратов порядка nn'.*

Доказательство. Представим оба множества t ортогональных латинских квадратов порядка n и n' посредством $[n^2 \times (t+2)]$-таблицы A и соответственно $[n'^2 \times (t+2)]$-таблицы A'. Обе эти таблицы A и A' имеют вид, описанный в теореме 1.3, и построены из элементов, занумерованных соответственно $1, 2, \ldots, n$ и $1, 2, \ldots, n'$. Обозначим соответственно строку i таблицы A и строку j таблицы A' через

$$(a_{i1}, a_{i2}, \ldots, a_{i,t+2}), \tag{1.14}$$

$$(a'_{j1}, a'_{j2}, \ldots, a'_{j,t+2}). \tag{1.15}$$

Соединим (1.14) и (1.15) в строку из $t+2$ компонент вида

$$((a_{i1}, a'_{j1}), (a_{i2}, a'_{j2}), \ldots, (a_{i,t+2}, a'_{j,t+2})). \tag{1.16}$$

Тогда $(nn')^2$ строк вида (1.16) образуют $[(nn')^2 \times (t+2)]$-таблицу. Элементами этой таблицы являются nn' 2-выборок вида

$$(1, 1), (1, 2), \ldots, (1, n'), \ldots, (n, 1), (n, 2), \ldots, (n, n'). \tag{1.17}$$

Из построения таблиц A и A' следует, что строками каждой $[(nn')^2 \times 2]$-подтаблицы нашей последней таблицы являются $(nn')^2$ 2-выборок элементов (1.17). Тогда по теореме 1.3 эта таблица размера $(nn')^2 \times (t+2)$ эквивалентна множеству из t ортогональных латинских квадратов порядка nn'.

Теорема 1.5. *Пусть дано разложение произвольного натурального числа n по натуральным сте-*

пеням α_i *различных простых чисел* p_i, *а именно* $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_N^{\alpha_N}$. *Пусть*

$$t = \min\left(p_i^{\alpha_i} - 1\right) \quad (i = 1, 2, \ldots, N). \tag{1.18}$$

Тогда для $t \geqslant 2$ *существует множество из* t *ортогональных латинских квадратов порядка* n.

Доказательство. По теореме 1.2 существует множество из t ортогональных латинских квадратов порядка $p_i^{\alpha_i}$ для каждого $i = 1, 2, \ldots, N$. Доказательство настоящей теоремы получается многократным приложением теоремы 1.4.

Предыдущая теорема устанавливает существование пары ортогональных латинских квадратов порядка $n \not\equiv 2 \pmod 4$. В следующем пункте мы исследуем ортогональные латинские квадраты порядка $n \equiv 2 \pmod 4$.

2. Предположение Эйлера. Эйлер предложил задачу о 36 офицерах. Она состояла в требовании расположить 36 офицеров 6 рангов и из 6 полков в каре. Каждая шеренга и каждая колонна этого каре должны содержать одного и только одного офицера каждого ранга и одного и только одного офицера из каждого полка. Мы можем занумеровать полки и ранги цифрами 1, 2, ..., 6 и обозначить каждого офицера 2-выборкой целых чисел от 1 до 6. Первая компонента 2-выборки обозначает ранг офицера, а вторая — его полк. Задача Эйлера, таким образом, сводится к построению пары ортогональных латинских квадратов порядка 6. В 1782 г. Эйлер высказал предположение, что не существует пары ортогональных латинских квадратов порядка $n \equiv 2 \pmod 4$. Тэрри примерно в 1900 г. подтвердил путем систематического пересчета справедливость предположения Эйлера для $n = 6$. Однако совсем недавно объединенные усилия Боса, Шрикханде и Паркера привели к следующей теореме.

Теорема 2.1. *Пусть* $n \equiv 2 \pmod 4$ *и пусть* $n > 6$. *Тогда существует пара ортогональных латинских квадратов порядка* n.

Эта теорема показывает, что действительное положение дел как раз противоположно предполагаемому; она демонстрирует опасность перехода к общим выводам на основании ограниченного числа эмпирических данных. Мы не можем входить здесь в подробности доказательства теоремы 2.1. Однако мы дадим простое и изящное построение для частного случая этой теоремы.

Теорема 2.2. *Пусть* $n \equiv 10 \pmod{12}$. *Тогда существует пара ортогональных латинских квадратов порядка* n.

Доказательство. Пусть m — целое число, для которого пара ортогональных латинских квадратов порядка m существует. Введем числа $i = 0, 1, \ldots, 2m$ и определим векторы

$$\begin{aligned} A_i &= (i, i, \ldots, i), \\ B_i &= (i+1, i+2, \ldots, i+m), \\ C_i &= (i-1, i-2, \ldots, i-m). \end{aligned} \tag{2.1}$$

Каждый из этих векторов имеет m компонент, а эти компоненты могут быть рассмотрены как целые числа по модулю $(2m+1)$. Образуем теперь разности по модулю $(2m+1)$:

$$\begin{aligned} D &= A_i - B_i = (2m, 2m-1, \ldots, m+1), \\ D' &= B_i - A_i = (1, 2, \ldots, m), \\ E &= A_i - C_i = (1, 2, \ldots, m), \\ E' &= C_i - A_i = (2m, 2m-1, \ldots, m+1), \\ F &= B_i - C_i = (2, 4, \ldots, 2m), \\ F' &= C_i - B_i = (2m-1, 2m-3, \ldots, 1). \end{aligned} \tag{2.2}$$

В (2.2) очевидно, что $2m$ компонент в D и D' суть $1, 2, \ldots, 2m \pmod{2m+1}$, и то же самое имеет место для E и E', F и F'. Это выполняется для каждого $i = 0, 1, \ldots, 2m$. Из векторов (2.1) построим векторы

$$\begin{aligned} A &= (A_0, A_1, \ldots, A_{2m}), \\ B &= (B_0, B_1, \ldots, B_{2m}), \\ C &= (C_0, C_1, \ldots, C_{2m}). \end{aligned} \tag{2.3}$$

Тогда в силу (2.2)

$$A-B=(D,\ D,\ \ldots,\ D), \qquad B-A=(D',\ D',\ \ldots,\ D'),$$
$$A-C=(E,\ E,\ \ldots,\ E), \qquad C-A=(E',\ E',\ \ldots,\ E'),$$
$$B-C=(F,\ F,\ \ldots,\ F), \qquad C-B=(F',\ F',\ \ldots,\ F'). \tag{2.4}$$

Каждый из векторов (2.3) и (2.4) имеет $m(2m+1)$ компонент. Введем перестановку из m элементов

$$X=(x_1,\ x_2,\ \ldots,\ x_m). \tag{2.5}$$

Из нее построим $m(2m+1)$-выборку

$$Y=(X,\ X,\ \ldots,\ X). \tag{2.6}$$

Теперь из A, B, C и Y построим таблицу размера $4\times 4m(2m+1)$

$$G=\begin{bmatrix} A & B & C & Y \\ B & A & Y & C \\ C & Y & A & B \\ Y & C & B & A \end{bmatrix}. \tag{2.7}$$

Из G выделим $[2\times 4m(2m+1)]$-подтаблицу G'. Она содержит одну из подтаблиц

$$\begin{bmatrix} A & Y \\ Y & A \end{bmatrix}, \quad \begin{bmatrix} B & Y \\ Y & B \end{bmatrix}, \quad \begin{vmatrix} C & Y \\ Y & C \end{vmatrix}. \tag{2.8}$$

Если учитывать структуру A, B, C и Y, то это означает, что G' содержит столбцы

$$\begin{pmatrix} i \\ x_j \end{pmatrix} \quad \text{и} \quad \begin{pmatrix} x_j \\ i \end{pmatrix}. \tag{2.9}$$

Здесь $i=0,\ 1,\ \ldots,\ 2m \pmod{2m+1}$, а $j=1,\ 2,\ \ldots,\ m$. Кроме того, G' содержит одну из подтаблиц

$$\begin{bmatrix} A & B \\ B & A \end{bmatrix}, \quad \begin{bmatrix} A & C \\ C & A \end{bmatrix} \text{ или } \begin{bmatrix} B & C \\ C & B \end{bmatrix}. \tag{2.10}$$

Если $i \neq j$, то $i - j \pmod{2m+1}$ является компонентой D или D'; то же самое имеет место для E или E', а также для F или F'.

Если, скажем, компонента $i - j \pmod{2m+1}$ появляется в качестве компоненты D, то она появляется $2m+1$ раз в $A - B$. Места $i - j \pmod{2m+1}$ в $A - B$ таковы, что G' содержит столбец вида

$$\begin{pmatrix} i \\ j \end{pmatrix}. \tag{2.11}$$

Такая же ситуация имеет место во всех случаях, а это означает, что G' содержит (2.11) для всех $i \neq j$, $i, j = 0, 1, \ldots, 2m \pmod{2m+1}$.

По условию, выдвинутому в начале доказательства, целое число m таково, что существует пара ортогональных латинских квадратов порядка m. Пусть H — $(4 \times m^2)$-таблица из элементов $x_1, x_2, \ldots, x_m$, а транспонированная к ней имеет вид, описанный в теореме 1.3. Построим таблицу

$$Z = \left[\begin{array}{cc} G & H \end{array}\right] \begin{array}{c} \left[\begin{array}{cccc} 0 & 1 & \ldots & 2m \end{array}\right. \\ \left[\begin{array}{cccc} 0 & 1 & \ldots & 2m \end{array}\right. \\ \left[\begin{array}{cccc} 0 & 1 & \ldots & 2m \end{array}\right. \\ \left[\begin{array}{cccc} 0 & 1 & \ldots & 2m \end{array}\right. \end{array}. \tag{2.12}$$

Эта таблица имеет четыре строки и

$$4m(2m+1) + m^2 + 2m + 1 = (3m+1)^2 \tag{2.13}$$

столбцов. Столбцы каждой $[2 \times (3m+1)^2]$-подтаблицы таблицы Z суть $(3m+1)^2$ 2-выборок из элементов $0, 1, \ldots, 2m \pmod{2m+1}$ и $x_1, x_2, \ldots, x_m$. Следовательно, таблица, полученная транспонированием Z, имеет вид, описанный в теореме 1.3. Таким образом, существует пара ортогональных латинских квадратов порядка $n = 3m+1$. По теореме 1.5 мы можем положить $m \equiv 3 \pmod 4$, что даст нам $n \equiv 10 \pmod{12}$. Выбор других значений для m приведет к значениям n, предварительно рассмотренным в теореме 1.5.

Рассмотренное здесь построение дает следующую пару ортогональных латинских квадратов 10-го порядка:

$$A = \begin{vmatrix} 0 & 6 & 5 & 4 & x_3 & x_2 & x_1 & 1 & 2 & 3 \\ x_1 & 1 & 0 & 6 & 5 & x_3 & x_2 & 2 & 3 & 4 \\ x_2 & x_1 & 2 & 1 & 0 & 6 & x_3 & 3 & 4 & 5 \\ x_3 & x_2 & x_1 & 3 & 2 & 1 & 0 & 4 & 5 & 6 \\ 1 & x_3 & x_2 & x_1 & 4 & 3 & 2 & 5 & 6 & 0 \\ 3 & 2 & x_3 & x_2 & x_1 & 5 & 4 & 6 & 0 & 1 \\ 5 & 4 & 3 & x_3 & x_2 & x_1 & 6 & 0 & 1 & 2 \\ 2 & 3 & 4 & 5 & 6 & 0 & 1 & x_1 & x_2 & x_3 \\ 4 & 5 & 6 & 0 & 1 & 2 & 3 & x_2 & x_3 & x_1 \\ 6 & 0 & 1 & 2 & 3 & 4 & 5 & x_3 & x_1 & x_2 \end{vmatrix}$$

$$B = \begin{vmatrix} 0 & x_1 & x_2 & x_3 & 1 & 3 & 5 & 2 & 4 & 6 \\ 6 & 1 & x_1 & x_2 & x_3 & 2 & 4 & 3 & 5 & 0 \\ 5 & 0 & 2 & x_1 & x_2 & x_3 & 3 & 4 & 6 & 1 \\ 4 & 6 & 1 & 3 & x_1 & x_2 & x_3 & 5 & 0 & 2 \\ x_3 & 5 & 0 & 2 & 4 & x_1 & x_2 & 6 & 1 & 3 \\ x_2 & x_3 & 6 & 1 & 3 & 5 & x_1 & 0 & 2 & 4 \\ x_1 & x_2 & x_3 & 0 & 2 & 4 & 6 & 1 & 3 & 5 \\ 1 & 2 & 3 & 4 & 5 & 6 & 0 & x_1 & x_2 & x_3 \\ 2 & 3 & 4 & 5 & 6 & 0 & 1 & x_3 & x_1 & x_2 \\ 3 & 4 & 5 & 6 & 0 & 1 & 2 & x_2 & x_3 & x_1 \end{vmatrix}.$$

3. Конечные проективные плоскости. Мы начинаем исследование конечных проективных плоскостей. С первого взгляда эти системы кажутся совершенно не относящимися к ортогональным латинским квадратам, рассматриваемым в предыдущих разделах. Однако в п. 4 мы покажем, что эти два вопроса известным образом взаимосвязаны. *Проективная плоскость* π — это математическая система, составленная из элементов, называемых „точками", и из других элементов, называемых „прямыми". Точки и линии связаны „отношением инцидентности". А именно мы предполагаем,

что существует вполне определенное соотношение „точка P лежит на прямой L“, или эквивалентное: „прямая L проходит через точку P“, удовлетворяющее следующим постулатам:

(3.1) две различные точки π лежат на одной и только одной прямой π;

(3.2) две различные прямые π проходят через одну и только одну точку π;

(3.3) существует четыре различных точки π, никакие три из которых не лежат на одной прямой.

Постулаты (3.1) и (3.2) являются целиком основными для системы. Постулат (3.3) служит для того, чтобы исключить некоторые вырожденные системы, удовлетворяющие только (3.1) и (3.2). Из этих постулатов вытекает следующий:

(3.4) существует четыре различных прямых в π, никакие три из которых не проходят через одну и ту же точку.

Теперь ясно, что всякое предложение, относящееся к проективной плоскости, имеет двойственное предложение, получающееся соответствующей заменой слов „точка“ и „прямая“ и выражений „точка P лежит на прямой L“ и „прямая L проходит через точку P“. Постулат (3.2) двойствен постулату (3.1), а (3.4) двойствен (3.3). Этот „принцип двойственности“ имеет фундаментальное значение в теории проективных плоскостей.

Теорема 3.1. *Даны две различные точки P и P' и две различные прямые L и L' на плоскости π. Существуют взаимно однозначные отображения: точек, лежащих на прямой L, на точки прямой L'; прямых, проходящих через точку P, на прямые, проходящие через точку P'; точек прямой L на прямые, проходящие через P.*

Доказательство. Обозначим через PQ единственную прямую, проходящую через две различные точки P и Q плоскости π. Пусть L и L' — две различные прямые на π. Существует точка O на π, не лежащая ни на L, ни на L'. В самом деле, если бы все точки плоскости π лежали на L и на L', то существовали бы точки A, B прямой L и точки C, D прямой L', такие, что A, B,

C, D удовлетворяли бы требованиям (3.3). Но из этого следовало бы, что прямые AB и CD проходят через точки, не лежащие на L или L'. А теперь из точки O, не лежащей на L или L', мы можем установить взаимно однозначное соответствие точек прямой L с точками прямой L', так как если P лежит на прямой L, то единственная прямая OP проходит через единственную точку P' на прямой L'. Это взаимно однозначное отображение всех точек L на все точки L'.

Второе утверждение теоремы двойственно первому. Пусть O — точка плоскости π, не лежащая на L. Тогда существует взаимно однозначное отображение точек, лежащих на прямой L, на прямые, проходящие через точку O. Это справедливо также, если точка лежит на прямой L' вследствие второго утверждения теоремы. Заметим, что мы показали, что на каждой прямой плоскости π лежат по меньшей мере три различные точки, а также, что по меньшей мере три различные прямые проходят через каждую точку плоскости π.

Проективная плоскость π называется *конечной*, если она содержит только конечное число точек. Конечные проективные плоскости имеют фундаментальное значение в комбинаторной математике, и в дальнейшем изложении этого предмета они будут играть ведущую роль. Пусть L — прямая на конечной проективной плоскости π, и пусть число всех точек, лежащих на прямой L, равно $n+1$. Натуральное число n называется *порядком* плоскости π и является основным инвариантом для π.

Теорема 3.2. *Пусть задана конечная проективная плоскость π порядка n. Тогда число точек, лежащих на любой прямой плоскости π, как и число прямых, проходящих через любую точку плоскости π, равно $n+1$. Более того, плоскость π имеет всего n^2+n+1 точек и столько же прямых.*

Доказательство. Первое утверждение теоремы непосредственно следует из теоремы 3.1 и из определения порядка. Зададим точку O на плоскости π. Существует $n+1$ прямых, проходящих через O, и на каждой из этих прямых имеется в точности n точек, кроме точки O. Сле-

довательно, плоскость π имеет всего $1+n(n+1)=n^2+n+1$ точек. Двойственное утверждение состоит в том, что плоскость π имеет всего n^2+n+1 прямых.

Для конечной проективной плоскости порядка n возможны различные эквивалентные системы постулатов. Например, пусть π — математическая система, удовлетворяющая постулатам (3.2) и (3.3). Пусть π имеет всего n^2+n+1 точек, где точно $n+1$ точек лежат на каждой прямой и в точности $n+1$ прямых проходят через каждую точку. Тогда система π является конечной проективной плоскостью порядка n. Потому что если O — точка на π, то через нее проходит как раз $n+1$ прямых, а на каждой прямой, кроме точки O, имеется n точек. Это объясняет, почему на π имеется всего n^2+n+1 точек. Следовательно, две различные точки π лежат на одной прямой. Это доказывает (3.1), и значит π оказывается конечной проективной плоскостью порядка n.

Заметим, наконец, что во многих исследованиях удобно рассматривать прямые на конечной проективной плоскости порядка n как некоторые $(n+1)$-подмножества точек. „Наименьшая“ проективная плоскость имеет порядок $n=2$. Следующие 3-подмножества элементов 1, 2, ..., 7 показывают семь прямых проективной плоскости порядка 2

$$L_1=\{1, 2, 4\},\quad L_2=\{2, 3, 5\},\quad L_3=\{3, 4, 6\},$$
$$L_4=\{4, 5, 7\},\quad L_5=\{5, 6, 1\},\quad L_6=\{6, 7, 2\},$$
$$L_7=\{7, 1, 3\}.$$

4. Проективные плоскости и латинские квадраты. В настоящем разделе мы установим связь между конечными проективными плоскостями и полными множествами латинских квадратов.

Теорема 4.1. *Пусть $n\geqslant 3$. Построить проективную плоскость порядка n можно тогда и только тогда, когда можно построить полное множество $n-1$ ортогональных латинских квадратов порядка n.*

Доказательство. Пусть дана проективная плоскость π порядка n. Пусть L — некоторая прямая

плоскости π, а $P_1, P_2, \ldots, P_{n+1}$ — точки на ней. Остальные n^2 точек, не лежащих на прямой L, обозначим через $Q_1, Q_2, \ldots, Q_{n^2}$. Занумеруем произвольным образом через $1, 2, \ldots, n$ прямые, проходящие через точку P_j, и пусть эта нумерация проведена для каждого $j = 1, 2, \ldots, n+1$. В частности, пусть Q_iP_j занумерована a_{ij}. Тогда

$$A = [a_{ij}] \quad (i = 1, 2, \ldots, n^2; \quad j = 1, 2, \ldots, n+1) \quad (4.1)$$

есть $[n^2 \times (n+1)]$-таблица из элементов $1, 2, \ldots, n$. Строки каждой $(n^2 \times 2)$-подтаблицы, выбранной из A, суть n^2 2-выборок из элементов $1, 2, \ldots, n$. Так как если мы предположим, что $a_{ij} = a_{i'j}$ и $a_{ik} = a_{i'k}$, где $i \neq i'$ и $j \neq k$, то $Q_iP_j = Q_{i'}P_j$ и $Q_iP_k = Q_{i'}P_k$. Но в таком случае $Q_iQ_{i'}$ должна проходить через точки P_j и P_k, так что $Q_iQ_{i'} = L$, а это противоречит тому факту, что точки Q_i и $Q_{i'}$ не лежат на прямой L. Следовательно, (4.1) есть таблица типа, описанного в теореме (1.3), а она дает полное множество $n-1$ ортогональных латинских квадратов порядка n.

Обратно, пусть (4.1) — таблица типа, описанного в теореме 1.3. В ней n^2 строк пусть обозначают „обычные“ точки $Q_1, Q_2, \ldots, Q_{n^2}$, и пусть $P_1, P_2, \ldots, P_{n+1}$ — „идеальные“ точки. „Обычная“ прямая L_{ij} проходит через P_j и обычные точки с элементом i в столбце j таблицы A. „Идеальная“ прямая L проходит через идеальные точки $P_1, P_2, \ldots, P_{n+1}$. Таким образом мы определили конфигурацию π, состоящую из n^2+n+1 точек. Каждая точка лежит как раз на $n+1$ прямых, а каждая прямая проходит точно через $n+1$ точек. Пусть L_{ij} и $L_{i'k}$ — две обычные прямые, причем $j \neq k$. Эти прямые проходят через единственную точку с элементом i в столбце j и элементом i' в столбце k таблицы A. Пусть, далее, L_{ij} и $L_{i'j}$ — две обычные прямые, причем $i \neq i'$. Эти прямые проходят через единственную точку P_j. Обычная прямая L_{ij} и идеальная прямая L также проходят через единственную точку P_{ij}. Это доказывает (3.2). Четыре точки: (1, 1), (1, 2), (2, 1), (2, 2) — в первых двух положениях удовле-

творяют постулату (3.3). В силу замечаний, вытекающих из доказательства теоремы 3.2, выясняется, что π есть конечная проективная плоскость порядка n.

Теорема 4.2. *Пусть* $n = p^\alpha$, *где* p — *простое, а* α — *натуральное числа. Тогда существует конечная проективная плоскость* π *порядка* n.

Доказательство. Эта теорема является следствием теорем 1.2 и 4.1. Плоскость порядка 2 требует специального рассмотрения, что было проделано в предыдущем пункте.

Пусть даны натуральное число n и наибольший квадрат d, делящий n. Напишем $n = n'd$ и назовем n' *свободной от квадрата частью* числа n. Если $d = 1$, то само n является числом, свободным от квадрата, а если $n' = 1$, то n является квадратом. Теперь мы в состоянии сформулировать теорему Брука—Райзера о несуществовании конечных проективных плоскостей.

Теорема 4.3. *Пусть* $n \equiv 1$ *или* $2 \pmod 4$, *и пусть свободная от квадрата часть числа* n *содержит по меньшей мере один простой множитель* $p \equiv 3 \pmod 4$. *В таком случае конечной проективной плоскости* π *порядка* n *не существует.*

Мы докажем обобщение этой теоремы в гл. 8. Очевидно, что теорема исключает возможность построения геометрий для бесконечно большого числа значений n, например для $n = 2p$, где p — простое и $p \equiv 3 \pmod 4$. Разумеется, теоремы 4.2 и 4.3 оставляют вопрос нерешенным для бесконечно большого числа значений n. Но до сего времени никаких значений n, кроме упомянутых в теоремах, не было ни добавлено, ни исключено. Это привело к развитию двух противоположных точек зрения. Одни настаивают, что плоскость π порядка n существует тогда и только тогда, когда $n = p^\alpha$, а другие считают, что если n не удовлетворяет условиям теоремы 4.3, то плоскость обязательно существует. Определение точных оценок для n есть одна из главных нерешенных проблем комбинаторики в наши дни. Первым неопределенным случаем является $n = 10$. Существование плоскости 10-го порядка требует построения множества из 9 ортогональных

латинских квадратов 10-го порядка. Однако еще никто не построил множества из трех ортогональных латинских квадратов порядка 10.

ЛИТЕРАТУРА

В статьях [8, 9] содержится материал, относящийся к п. 1 этой главы. Фундаментальные работы относительно предположения Эйлера включают [2, 3, 11, 12]. Наше изложение теоремы 2.2 имеется в [4]. Тэрри [18] исследовал случай $n = 6$. Теорема 4.1, представлена в [1, 17], теорема 4.2 — в [19], а теорема 4.3 — в [5].

1. Bose R. C., On the application of the properties of Galois fields to the problem of construction on hyper-Graeco-Latin-squares, *Sankhyā*, 3 (1938), 323—338.
2. Bose R. C., Shrikhande S. S., On the falsity of Enler's conjecture about the non-existence of two orthogonal Latin squares of order $4t + 2$, *Proc. Nat. Acad. Sci. U.S.A.*, **45** (1959), 734—737.
3. Bose R. C., Shrikhande S. S., On the construction of sets of mutually orthogonal Latin squares and the falisity of a conjecture of Euler, *Trans. Amer. Math. Soc.*, **95** (1960), 191—209.
4. Bose R. C., Shrikhande S. S., Parker E. T., Further results on the construction of mutually orthogonal Latin squares and the falsity of Euler's conjecture, *Canad. Jour. Math.*, **12** (1960), 189—203.
5. Bruck R. H., Ryser H. J., The nonexistence of certain finite projective planes, *Canad. Jour. Math.*, **1** (1949), 88—93.
6. Hall M., Jr., Projective planes, *Trans. Amer. Math. Soc.*, **54** (1943), 229—277.
7. Hall M., Jr., Projective planes and Related Topics, California Institute of Technology, 1954.
8. MacNeish H. F., Euler squares, *Ann. Math.*, **23** (1922), 221—227.
9. Mann H. B., The construction of orthogonal Latin squares, *Ann. Math. Stat.*, **13** (1942), 418—423.
10. Mann H. B., On orthogonal Latin squares, *Bull. Amer. Math. Soc.*, **50** (1944), 249—257.
11. Parker E. T., Construction of some sets of mutually orthogonal Latin squares, *Proc. Amer. Math. Soc.*, **10** (1959), 946—949.
12. Parker E. T., Orthogonal Latin squares, *Proc. Nat. Acad. Sci. U.S.A.*, **45** (1959), 859—862.
13. Parker E. T., Nonextendibility conditions on mutually orthogonal Latin squares, *Proc. Amer. Math. Soc.*, **13** (1962), 219—221.

14. Pickert G., Projective Ebenen, Berlin, 1955.
15. Ryser H. J., Geometries and incidence matrices, Slaught Memorial Papers, № 4, 1955, 25—31.
16. Скорняков Л. А., Проективные плоскости, *УМН*, **6**, № 6 (1951), 112—154.
17. Stevens W. L., The completely orthonalized Latin square, *Ann. Eugen.*, **9** (1939), 82—93.
18. Tarry G., Le probleme de 36 officieurs, *Comptes Rendu de l'Association Francaise pour l'Avancement de Science Naturel*, **1** (1900), 122—123; **2** (1901), 170—203.
19. Veblen O., Bussey W. H., Finite projective geometries, *Trans. Amer. Math. Soc.*, **7** (1906), 241—259.

Глава 8

КОМБИНАТОРНЫЕ СХЕМЫ

1. (b, v, r, k, λ)-конфигурация. В настоящем пункте мы введем комбинаторные конфигурации, являющиеся обобщением конечных проективных плоскостей, описанных в предыдущей главе. Пусть задано v-множество X элементов $x_1, x_2, \ldots, x_v$, и пусть $X_1, X_2, \ldots, X_b$ — b различных подмножеств X. Эти подмножества называются *уравновешенной неполной блок-схемой*, если они удовлетворяют следующим требованиям:

(1.1) Каждое X_i является k-подмножеством множества X.

(1.2) Каждая пара элементов множества X является 2-подмножеством точно λ множеств из $X_1, X_2, \ldots, X_b$.

(1.3) Целые числа v, k, λ удовлетворяют условиям $0 < \lambda$ и $k < v - 1$.

Требования (1.1) и (1.2) — основные при определении уравновешенных неполных блок-схем, а требование (1.3) введено для того, чтобы исключить некоторые вырожденные конфигурации. Уравновешенные неполные блок-схемы имеют большое значение в той области статистики, которая имеет дело с анализом и планированием экспериментов. Там элементы называются *многообразиями*[1] (varieties), а множества — *блоками* (blocks). Эта номенклатура объясняет, почему именно мы ввели буквы v и b. Пусть $x \in X$, и пусть x входит в r из подмножеств $X_1, X_2, \ldots, X_b$. Теперь рассмотрим $v - 1$ 2-подмножеств множества X, содержащих x. Требования (1.1) и (1.2) могут быть использованы для подсчета числа появлений этих $v - 1$ 2-подмножеств в $X_1, \ldots, X_b$. Если приравн-

[1] Также *обработками*. — *Прим. ред.*

нять результаты подсчета, то получим

$$r(k-1)=\lambda(v-1). \tag{1.4}$$

Это показывает, что r является другим инвариантом уравновешенных неполных блок-схем, который обозначает число повторных появлений элемента в подмножествах $X_1, X_2, \ldots, X_b$. Поскольку каждый из v элементов появляется точно r раз и поскольку каждое X_i есть k-подмножество множества X, то отсюда следует, что

$$bk=vr. \tag{1.5}$$

Уравновешенная неполная блок-схема включает в себя пять основных параметров b, v, r, k, λ; в дальнейшем мы будем ее называть (b, v, r, k, λ)-*конфигурацией*. Указанные пять чисел не являются независимыми. Они связаны соотношениями (1.4) и (1.5). Однако эти соотношения ни в коем случае не являются единственными необходимыми условиями для существования (b, v, r, k, λ)-конфигурации. Фактически центральной задачей при изучении этих конфигураций является определение точной области значений b, v, r, k, λ, при которых конфигурации существуют. Эта задача еще не решена, а отдельные частные случаи ее имеют сами по себе большое значение.

Пусть дана инцидентная матрица

$$A=[a_{ij}] \quad (i=1, 2, \ldots, b;\ j=1, 2, \ldots, v) \tag{1.6}$$

для (b, v, r, k, λ)-конфигурации. Это означает, разумеется, что A есть (0, 1)-матрица размера $b \times v$, в которой $a_{ij}=1$, если $x_j \in X_i$, и $a_{ij}=0$, если $x_j \notin X_i$.
Основные свойства (b, v, r, k, λ)-конфигураций:

$$AJ=kJ', \tag{1.7}$$

$$A^TA=(r-\lambda)I+\lambda J. \tag{1.8}$$

Здесь A^T обозначает транспонированную матрицу A. Матрица J есть матрица порядка v, составленная из единиц, J' — матрица размера $b \times v$, составленная из единиц, а I — единичная матрица порядка v. Обратно, пусть дано, что $0<\lambda$ и $k<v-1$. Тогда, если A есть (0, 1)-матрица размера $b \times v$ и если A удовлетворяет (1.7) и (1.8),

то мы утверждаем, что (b, v, r, k, λ)-конфигурация с инцидентной матрицей A существует.

Если в (0, 1)-матрице заменить нули на единицы и наоборот, то получающаяся при этом матрица называется *дополнением* первоначальной матрицы. Пусть A — матрица инцидентности для (b, v, r, k, λ)-конфигурации, а A' — ее дополнение. Нетрудно проверить, что

$$A'J = k'J', \tag{1.9}$$

$$A'^{T}A' = (r' - \lambda')I + \lambda'J, \tag{1.10}$$

где $r' = b - r$, $k' = v - k$, $\lambda' = b - 2r + \lambda$. Из последнего соотношения и из (1.4) и (1.5) следует, что $(b - r)(v - k - 1) = \lambda'(v - 1)$. Следовательно, при $0 < \lambda$ и $k < v - 1$ имеем $0 < \lambda'$ и $k' < v - 1$. Таким образом, A' определяет (b, v, r', k', λ')-конфигурацию. Она называется *дополнением* (b, v, r, k, λ)-конфигурации.

Пусть A_1 и A_2 — матрицы инцидентности для двух (b, v, r, k, λ)-конфигураций. Две конфигурации считаются *изоморфными*, если существуют перестановочные матрицы P порядка b и Q порядка v, такие, что

$$A_1 = PA_2Q. \tag{1.11}$$

Всякий раз, когда мы пытаемся классифицировать (b, v, r, k, λ)-конфигурации для отдельных множеств параметров, мы учитываем только конфигурации, различные в смысле изоморфизма. Этот метод вполне оправдан, так как изоморфные конфигурации отличаются только нумерацией элементов и подмножеств. Матрицы инцидентности дают нам мощное средство исследования (b, v, r, k, λ)-конфигураций. Проиллюстрируем это путем применения матриц инцидентности для доказательства неравенства Фишера.

Теорема 1.1. *Для (b, v, r, k, λ)-конфигурации выполняется неравенство*

$$b \geqslant v.$$

Доказательство. Пусть A — матрица инцидентности (b, v, r, k, λ)-конфигурации. Известно, что A имеет размеры $b \times v$. Предположим, что $b < v$. Присоединим $v - b$ строк, составленных из нулей, к матрице A, получим

квадратную матрицу A^* порядка v, такую, что

$$A^{*T}A^* = (r-\lambda)I + \lambda J. \qquad (1.12)$$

Вычислим теперь $\det(A^{*T}A^*)$ двумя разными способами. Матрица A^* содержит строку нулей, так что $\det(A^{*T}A^*) = \det(A^{*T})\det(A^*) = 0$. Матрица $(r-\lambda)I + \lambda J$ имеет порядок v, имеет r на главной диагонали и λ на всех других местах. Возьмем эту матрицу и вычтем 1-й столбец из каждого из остальных столбцов. Затем прибавим к первой строке строки 2, 3, ..., v. Полученная матрица имеет нули на главной диагонали. Более того, получаем, что

$$\det((r-\lambda)I + \lambda J) = (r+(v-1)\lambda)(r-\lambda)^{v-1}, \qquad (1.13)$$

Следовательно, $\det(A^{*T}A^*) \neq 0$, а это противоречит нашему предыдущему утверждению. Следовательно, $b \geqslant v$.

Из (1.4) и (1.5) вытекает, что (b, v, r, k, λ)-конфигурация в случае, когда $k = 2$, $\lambda = 1$, имеет $b = v(v-1)/2$, $r = v-1$. Следовательно, конфигурация оказывается множеством всех 2-подмножеств v-множества. Гораздо более интересное положение возникает в случае $k = 3$, $\lambda = 1$. Пусть дано v-множество X, где $v \geqslant 3$. *Штейнеровой системой троек порядка v* называется множество всех 3-подмножеств, или *троек*, из X, такое, что всякое 2-подмножество из X оказывается подмножеством только одной тройки. Штейнеровы системы троек порядков 3, 7 и 9 таковы:

$$\begin{aligned}
(v=3)&: \{1, 2, 3\};\\
(v=7)&: \{1, 2, 4\},\ \{2, 3, 5\},\ \{3, 4, 6\},\\
&\quad \{4, 5, 7\},\ \{5, 6, 1\},\ \{6, 7, 2\},\ \{7, 1, 3\};\\
(v=9)&: \{1, 2, 3\},\ \{4, 5, 6\},\ \{7, 8, 9\},\\
&\quad \{1, 4, 7,\},\ \{2, 5, 8\},\ \{3, 6, 9\},\\
&\quad \{1, 5, 9,\},\ \{2, 6, 7\},\ \{3, 4, 8\},\\
&\quad \{1, 6, 8,\},\ \{2, 4, 9\},\ \{3, 5, 7\}.
\end{aligned}$$

Заметим, что система троек Штейнера порядка 7 есть то же самое, что и проективная плоскость порядка 2 (см. предыдущую главу). Ясно, что системы троек Штейнера порядка $v > 3$ являются (b, v, r, k, λ)-конфигура-

циями с $k=3$, $\lambda=1$. Следовательно, в силу (1.4) и (1.5)

$$b=\frac{v(v-1)}{6}; \qquad r=\frac{v-1}{2}. \tag{1.14}$$

Отсюда вытекает, что *система троек Штейнера имеет порядок* $v \geqslant 3$ *и что* $v \equiv 1$ *или* $3 \pmod 6$. Для всех этих значений v тройки Штейнера построены. Райсс получил такое построение еще в 1859 г., затем было получено много последующих построений. Для $v=3, 7$ и 9 системы оказались единственными. Существуют точно две системы 13-го порядка и 80 систем 15-го порядка. Для $v>15$ число различных систем неизвестно. Ограничим наше изложение следующим элементарным построением.

Теорема 1.2. *Если существуют системы троек Штейнера* S_1 *порядка* v_1 *и* S_2 *порядка* v_2, *то существует штейнерова система троек* S *порядка* $v_1 v_2$.

Доказательство. Пусть дано, что $\{a_i, a_j, a_k\} \in S_1$, а $\{b_r, b_s, b_t\} \in S_2$. Образуем $v_1 v_2$-множество элементов c_{ij} $(i=1, 2, \ldots, v_1;\ j=1, 2, \ldots, v_2)$ и положим, что тройка $\{c_{ir}, c_{js}, c_{kt}\}$ входит в S, если: 1) $r=s=t$ и тройка $\{a_i, a_j, a_k\} \in S_1$, либо 2) $i=j=k$ и $\{b_r, b_s, b_t\} \in S_2$, либо 3) $\{a_i, a_j, a_k\} \in S_1$ и $\{b_r, b_s, b_t\} \in S_2$. Нетрудно проверить, что эти правила характеризуют S как штейнерову систему троек порядка $v_1 v_2$. Те тройки S, для которых $r=s=t=1$, изоморфны системе S_1, а тройки S_1, для которых $i=j=k=1$, изоморфны S_2.

Пусть число n — целое неотрицательное. *Системой троек Киркмана порядка* $v=6n+3$ называют систему троек Штейнера порядка $v=6n+3$ со следующим дополнительным условием. Множество из $b=(2n+1)\times$ $\times(3n+1)$ троек разбито на $3n+1$ компонент, каждая из которых представляет собой $(2n+1)$-подмножество троек, а каждый из $v=6n+3$ элементов системы троек появляется в каждой компоненте в точности один раз. Система троек Штейнера порядка 3 есть вырожденная система троек Киркмана при $n=0$. Указанная выше система троек Штейнера порядка 9 есть система троек Киркмана при $n=1$. Здесь 12 троек разбиты на 4 компоненты. Каждая из них записана в строку из 3 троек;

каждый из 9 элементов появляется в каждой строке в точности один раз.

Знаменитая задача Киркмана о 15 школьницах может быть сформулирована следующим образом. Учительница выводит свой класс из 15 девочек на ежедневную прогулку. Школьницы построены по трое в пять рядов, так что каждая из них имеет двух компаньонок. Задача состоит в том, чтобы так строить класс, чтобы в течение семи дней подряд ни одна из школьниц не гуляла с каждой из своих подруг по тройке более одного раза. Эта задача эквивалентна требованию построить систему троек Киркмана для случая $n = 2$. Всем этим требованиям удовлетворяет следующая система:

{1, 2, 5},	{3, 14, 15},	{4, 6, 12},	{7, 8, 11},	{9, 10, 13},
{1, 3, 9},	{2, 8, 15},	{4, 11, 13},	{5, 12, 14},	{6, 7, 10},
{1, 4, 15},	{2, 9, 11},	{3, 10, 12},	{5, 7, 13},	{6, 8, 14},
{1, 6, 11},	{2, 7, 12},	{3, 8, 13},	{4, 9, 14},	{5, 10, 15},
{1, 8, 10},	{2, 13, 14},	{3, 4, 7},	{5, 6, 9},	{11, 12, 15},
{1, 7, 14},	{2, 4, 10},	{3, 5, 11},	{6, 13, 15},	{8, 9, 12},
{1, 12,13},	}2, 3, 6},	{4, 5, 8},	{7, 9, 15},	}10, 11, 14}.

2. (v, k, λ)-конфигурация. Пусть дано v-множество X элементов $x_1, x_2, \ldots, x_v$, и пусть $X_1, X_2, \ldots, X_v$ будут подмножествами множества X. Эти подмножества образуют (v, k, λ)-*конфигурацию*, если они удовлетворяют следующим требованиям:

(2.1) Каждое подмножество X_i есть k-подмножество.

(2.2) Каждое пересечение $X_i \cap X_j$ при $i \neq j$ есть λ-подмножество.

(2.3) Целые числа v, k, λ удовлетворяют условию $0 < \lambda < k < v - 1$.

Пусть

$$A = [a_{ij}] \quad (i, j = 1, 2, \ldots, v) \tag{2.4}$$

— матрица инцидентности для (v, k, λ)-конфигурации. Тогда A является (0,1)-матрицей порядка v, из (2.1) и (2.2) следует

$$AA^T = B = (k - \lambda) I + \lambda J. \tag{2.5}$$

Здесь A^T обозначает транспонированную матрицу A. Матрица J составлена из единиц и имеет порядок v, а мат-

рица I — единичная матрица того же порядка. Наоборот, пусть $0 < \lambda < k < v - 1$. Тогда, если A есть (0,1)-матрица порядка v и если A удовлетворяет (2.5), то мы можем утверждать, что существует (v, k, λ)-конфигурация с матрицей инцидентности A.

Матрица, составленная из действительных чисел, называется *нормальной*, если она перестановочна со своей транспонированной матрицей при умножении.

Теорема 2.1. *Матрица инцидентности A любой (v, k, λ)-конфигурации нормальна. Так что*

$$AA^T = A^TA = B. \tag{2.6}$$

Доказательство. Пусть A — матрица инцидентности (v, k, λ)-конфигурации. Из (1.13) известно, что

$$\det(B) = (k + (v-1)\lambda)(k-\lambda)^{v-1}. \tag{2.7}$$

Следовательно, $\det(AA^T) = \det(A)\det(A^T) = \det(B) \neq 0$, и, значит, $\det(A) \neq 0$. Это означает, что матрица A — невырожденная и имеет обратную матрицу, обозначенную A^{-1}. Известно, что $AJ = kJ$. Следовательно, отсюда вытекает, что $A^{-1}J = k^{-1}J$. Более того,

$$AA^TJ = BJ = (k - \lambda + \lambda v)J \tag{2.8}$$

и

$$A^TJ = (k - \lambda + \lambda v)k^{-1}J. \tag{2.9}$$

Транспонировав теперь обе части (2.9), получим

$$JA = (k - \lambda + \lambda v)k^{-1}J. \tag{2.10}$$

Следовательно,

$$JAJ = (k - \lambda + \lambda v)k^{-1}vJ. \tag{2.11}$$

Но также

$$JAJ = kvJ, \tag{2.12}$$

откуда следует, что

$$k - \lambda = k^2 - \lambda v. \tag{2.13}$$

Подставив этот результат в (2.10), получим

$$JA = kJ. \tag{2.14}$$

Наконец,

$$A^TA = A^{-1}(AA^T)A = A^{-1}BA = \\ = (k-\lambda)I + \lambda A^{-1}JA = (k-\lambda)I + \lambda J = B, \quad (2.15)$$

а это и есть желаемый результат.

Теорема 2.2. *(v, k, λ)-конфигурация эквивалентна (b, v, r, k, λ)-конфигурации, в которой $b = v$ и $r = k$.*

Доказательство. Эта теорема является непосредственным следствием теоремы 2.1.

В статистике (v, k, λ)-конфигурация называется *симметрической уравновешенной неполной блок-схемой*. Эти конфигурации встречаются во многих областях чистой и прикладной математики. Остальную часть этой главы мы посвятим их изучению.

Теорема 2.3. *Конечная проективная плоскость порядка n эквивалентна (v, k, λ)-конфигурации с параметрами $v = n^2 + n + 1$, $k = n + 1$, $\lambda = 1$.*

Доказательство. Эта теорема следует из результатов п. 3 гл. 7 и из теоремы 2.1.

В гл. 7 мы установили существование проективной плоскости порядка $n = p^\alpha$, где p — простое, а α — натуральное числа. Мы также отметили, что до сих пор были построены конечные проективные плоскости только порядков, являющихся степенями простого числа. Известно, что проективные плоскости порядков $n = 2, 3, 4, 5, 7$ и 8 единственны. Число проективных плоскостей порядка $n = p^\alpha$ для $n > 8$ неизвестно.

Изучим теперь другой важный класс (v, k, λ)-конфигураций. Матрица H порядка n, составленная из элементов $+1$ и -1, называется *матрицей Адамара* (или адамаровой), если

$$HH^T = nI, \quad (2.16)$$

где H^T обозначает транспонированную матрицу H, а I — единичную матрицу порядка n. Из матричного равенства (2.16) следует, что

$$\text{абс. знач. } \det(H) = n^{n/2}. \quad (2.17)$$

Упомянем попутно, что матрицы Адамара появляются весьма естественно из следующих рассуждений. Если элементы некоторой матрицы действительны и абсолютное значение каждого элемента не превосходит 1, то знаменитое неравенство Адамара утверждает, что абсолютное значение детерминанта этой матрицы не превосходит $n^{n/2}$. Более того, можно доказать, что значение $n^{n/2}$ достигается тогда и только тогда, когда матрица — адамарова.

Из матричного равенства (2.16) следует, что

$$H^{-1} = n^{-1}H^T. \tag{2.18}$$

Следовательно, H — нормальная матрица и

$$HH^T = H^TH = nI. \tag{2.19}$$

Если строку или столбец матрицы Адамара умножить на -1, то матрица сохраняет свойство быть адамаровой. Следовательно, мы всегда можем принять, что элементы первой строки и первого столбца являются положительными единицами. Такая матрица Адамара называется *нормализованной*. Например, нормализованные матрицы Адамара порядков 1 и 2 суть:

$$[1], \quad \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

Рассмотрим теперь нормализованную матрицу Адамара порядка $n \geqslant 3$. Мы можем переставить столбцы ее так, чтобы во второй строке первая половина членов состояла из положительных единиц, а вторая — из отрицательных. Пусть t обозначает число положительных единиц на первых $n/2$ местах в третьей строке, а t' — число положительных единиц на остальных $n/2$ местах третьей строки. Тогда в силу (2.16) имеем $2t + 2t' = n$ и $2t - 2t' = 0$. Следовательно, $n = 4t$; тем самым мы показали, что порядок матрицы Адамара $n = 1, 2$ или $n \equiv 0 \pmod 4$.

Предполагается, что матрицы Адамара существуют для всех порядков $n \equiv 0 \pmod 4$. Для их построения пригодны разнообразные методы. Например, для $n \leqslant 200$ матрицы Адамара были построены для всех порядков $n \equiv 0 \pmod 4$, за исключением $n = 116$, 156 и 188. Ниже мы опишем одно очень несложное построение. Пусть $A = [a_{ij}]$ — мат-

рица порядка n, а $A' = [a'_{ij}]$ — матрица порядка n'. Элементы этих матриц пусть находятся в поле F. *Прямым произведением* матриц A и A' называется матрица

$$A \times A' = \begin{bmatrix} a_{11}A' & a_{12}A' & \dots & a_{1n}A' \\ a_{21}A' & a_{22}A' & & a_{2n}A' \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ a_{n1}A' & a_{n2}A' & \dots & a_{nn}A' \end{bmatrix}. \qquad (2.20)$$

Это матрица порядка nn'.

Теорема 2.4. *Прямое произведение двух матриц Адамара будет снова матрицей Адамара.*

Доказательство. Даны адамаровы матрицы H порядка n и H' порядка n'. Можно проверить последовательность внутренних произведений $H \times H'$ и убедиться, что требования для матрицы Адамара выполняются. Дальнейшие альтернативные суждения используют некоторые важные формальные свойства символа прямого произведения. Так,

$$(H \times H')(H \times H')^T = (H \times H')(H^T \times H'^T) =$$
$$= HH^T \times H'H'^T = nI_n \times n'I_{n'} = nn'I_{nn'}, \qquad (2.21)$$

где I_n, $I_{n'}$, $I_{nn'}$ — единичные матрицы порядков n, n', nn' соответственно. Заметим, что мы установили существование матриц Адамара порядка $n = 2^\alpha$, где α — произвольное целое положительное число.

Теперь установим взаимосвязь между матрицами Адамара и (v, k, λ)-конфигурациями.

Теорема 2.5. *Нормализованная матрица Адамара порядка $n = 4t \geqslant 8$ эквивалентна (v, k, λ)-конфигурации с параметрами $v = 4t - 1$, $k = 2t - 1$, $\lambda = t - 1$.*

Доказательство. Положим, что H — нормализованная матрица Адамара порядка $n = 4t \geqslant 8$. Вычеркнем первую строку и первый столбец этой матрицы и заменим все -1 нулями. Получим (0,1)-матрицу A порядка

$v = 4t - 1$. Поскольку H — нормализованная матрица Адамара, то оказывается, что A удовлетворяет матричному равенству

$$AA^T = tI + (t - 1)\, J. \tag{2.22}$$

Следовательно, A является матрицей инцидентности (v, k, λ)-конфигурации с параметрами $x = 4t - 1$, $k = 2t - 1$, $\lambda = t - 1$. Все рассуждение обратимо, и мы можем применить матрицу инцидентности A (v, k, λ)-конфигурации с параметрами $v = 4t - 1$, $k = 2t - 1$, $\lambda = t - 1$ к тому, чтобы построить нормализованную матрицу Адамара порядка $n = 4t$.

Дополнением к (v, k, λ)-конфигурации с параметрами $v = 4t - 1$, $k = 2t - 1$, $\lambda = t - 1$ является (v, k', λ')-конфигурация с параметрами $v = 4t - 1$, $k' = 2t$, $\lambda' = t$. Назовем обе эти конфигурации *адамаровыми*. Интересно отметить, что (v, k, λ)-конфигурация с параметрами $v = 7$, $k = 3$, $\lambda = 1$ играет в нашем изложении единственную в своем роде роль. Эта конфигурация одновременно является системой троек Штейнера, конечной проективной плоскостью и адамаровой конфигурацией.

3. Теорема несуществования. Начнем с некоторых предварительных замечаний. Пусть $S = (s_{ij})$ и $S' = (s'_{ij})$ — две симметричные $(n \times n)$-матрицы с элементами, принадлежащими полю F. Будем говорить, что S и S' *конгруэнтны* над F, или $S \overset{c}{=} S'$, если существует невырожденная $(n \times n)$-матрица P с элементами из F такая, что

$$P^T S P = S', \tag{3.1}$$

где P^T обозначает транспонированную матрицу P. Нетрудно проверить, что конгруэнтность матриц удовлетворяет обычным требованиям, предъявляемым к соотношению равенства. Таким образом, из $S \overset{c}{=} S$ и $S \overset{c}{=} S'$ следует, что $S' \overset{c}{=} S$, а из $S \overset{c}{=} S'$ и $S' \overset{c}{=} S^*$ следует: $S \overset{c}{=} S^*$.

Пусть $S = (s_{ij})$ — симметрическая $(n \times n)$-матрица с элементами в F и пусть

$$f = f(x_1, x_2, \ldots, x_n) = \sum_{i,\, j=1}^{n} x_i s_{ij} x_j \tag{3.2}$$

— квадратичная форма неизвестных $x_1, x_2, \ldots, x_n$. Назовем f ***квадратичной формой*** матрицы S. Предположим, что $S' = (s'_{ij})$ — симметричная $(n \times n)$-матрица с элементами в F и что $S \overset{c}{=} S'$ над F. Тогда мы знаем, что существует невырожденная матрица $P = (p_{ij})$ с элементами в F, такая, что $P^T S P = S'$. Положим, что $y_1, y_2, \ldots, y_n$ — другое множество неизвестных, и запишем

$$x_i = \sum_{j=1}^{n} p_{ij} y_j \quad (i = 1, 2, \ldots, n). \tag{3.3}$$

Матрица P — невырожденная, поэтому она имеет обратную матрицу $P^{-1} = Q = (q_{ij})$ и формула (3.3) эквивалентна

$$y_i = \sum_{j=1}^{n} q_{ij} x_j \quad (i = 1, 2, \ldots, n). \tag{3.4}$$

Если теперь мы подставим (3.3) в (3.2), то получим новую квадратичную форму f' неизвестных $y_1, y_2, \ldots, y_n$. Непосредственным подсчетом можно проверить, что

$$f' = f'(y_1, y_2, \ldots, y_n) = \sum_{i,j=1}^{n} y_i s'_{ij} y_j. \tag{3.5}$$

Иными словами, f' есть квадратичная форма матрицы S'. Квадратичные формы f и f' называются ***конгруэнтными*** над F. Мы показали, что если $x'_1, x'_2, \ldots, x'_n$ — произвольные элементы F и если

$$y'_i = \sum_{j=1}^{n} q_{ij} x'_j \quad (i = 1, 2, \ldots, n), \tag{3.6}$$

то

$$f(x'_1, x'_2, \ldots, x'_n) = f'(y'_1, y'_2, \ldots, y'_n) \tag{3.7}$$

справедливо в F. Кроме того, если $y^*_1, y^*_2, \ldots, y^*_n$ — произвольные элементы F и если

$$x^*_i = \sum_{j=1}^{n} p_{ij} y^*_j \quad (i = 1, 2, \ldots, n), \tag{3.8}$$

то

$$f(x_1^*, x_2^*, \ldots, x_n^*) = f'(y_1^*, y_2^*, \ldots, y_n^*) \tag{3.9}$$

тоже выполняется в F.

Если A — матрица порядка n, A' — матрица порядка n' и если элементы этих матриц — элементы поля F, то *прямой суммой* матриц A и A' является матрица порядка $n+n'$, определенная следующим образом:

$$A \dotplus A' = \begin{bmatrix} A & 0 \\ 0 & A' \end{bmatrix}, \tag{3.10}$$

где нули обозначают нулевые матрицы. Если $S_1 \overset{c}{=} S_1'$, $S_2 \overset{c}{=} S_2'$, то отсюда без труда следует, что

$$S_1 \dotplus S_2 \overset{c}{=} S_1' \dotplus S_2'. \tag{3.11}$$

Усложнения в теории конгруэнтности матриц зависят от того, насколько широки предположения о природе поля F. В классической работе Сильвестра рассматривается задача для случая поля действительных чисел, и это не очень трудно. Но в случае поля рациональных чисел положение делается гораздо более сложным. Дело в том, что этот предмет тесно связан с глубокими проблемами теории чисел. Сделаем некоторые элементарные замечания о конгруэнтностях над полем рациональных чисел. Пусть m — натуральное число. По теореме Лагранжа о 4 квадратах [1])

$$m = a_1^2 + a_2^2 + a_3^2 + a_4^2, \tag{3.12}$$

где a_1, a_2, a_3, a_4 — целые числа. Для наших целей достаточно знать, что эти 4 количества — рациональные числа. Обозначим через I_n единичную матрицу порядка n и определим

$$H = \begin{bmatrix} a_1 & a_2 & a_3 & a_4 \\ a_2 & -a_1 & a_4 & -a_3 \\ a_3 & -a_4 & -a_1 & a_2 \\ a_4 & a_3 & -a_2 & -a_1 \end{bmatrix}. \tag{3.13}$$

[1]) См., например, Арнольд И. В., Теория чисел, Госучпедгиз, 1939. — *Прим. ред.*

Тогда, если мы умножим H на транспонированную матрицу H^T, получим

$$HH^T = mI_4. \tag{3.14}$$

Следовательно, мы показали, что

$$mI_4 \overset{c}{=} I_4 \tag{3.15}$$

над рациональным полем. В силу (3.11), отсюда следует

$$mI_n \overset{c}{=} I_n \tag{3.16}$$

для всех $n \equiv 0 \pmod 4$.

Возвратимся к (v, k, λ)-конфигурациям. Центральной проблемой при их изучении является определение точной области значений v, k, λ, для которых конфигурация существует. По определению v, k, λ — целые и такие, что $0 < \lambda < k < v - 1$, а (2.13) утверждает

$$k - \lambda = k^2 - \lambda v. \tag{3.17}$$

Это необходимые условия относительно v, k, λ, для того чтобы конфигурация существовала. Всякий раз, когда мы будем обсуждать вопрос о существовании этих конфигураций, мы будем предполагать, что параметры удовлетворяют этим требованиям. Ниже мы дадим теорему, содержащую дальнейшие необходимые условия. Другие необходимые условия неизвестны, так что можно предполагать, что (v, k, λ)-конфигурации существуют, если только они не подпадают под исключения, сформулированные в теореме 3.1.

Теорема 3.1. *Пусть v, k, λ — целые числа, для которых существует (v, k, λ)-конфигурация. Если v — четное, то $(k - \lambda)$ — квадрат. Если же v — нечетное, то диофантово уравнение*

$$x^2 = (k - \lambda)\, y^2 + (-1)^{\frac{v-1}{2}} \lambda z^2 \tag{3.18}$$

имеет решение в целых ненулевых x, y, z.

Доказательство. Пусть A — матрица инцидентности (v, k, λ)-конфигурации. В силу матричного равен-

ства (2.5) имеем

$$AA^T = B = (k-\lambda)I + \lambda J. \tag{3.19}$$

Учитывая (2.7) и (3.17), отсюда получаем

$$(\det(A))^2 = \det(B) = k^2(k-\lambda)^{v-1}. \tag{3.20}$$

Следовательно, число $k^2(k-\lambda)^{v-1}$ — квадрат. Если теперь v — четное число, то $(k-\lambda)$ — квадрат. Первое утверждение теоремы доказано.

Далее, пусть v — нечетно. По (3.19)

$$B \overset{c}{=} I \tag{3.21}$$

над полем рациональных чисел. Рассмотрим сначала случай $v \equiv 1 \pmod 4$. В силу (3.11) и (3.16)

$$B \overset{c}{=} (k-\lambda)I_{v-1} \dot{+} I_1, \tag{3.22}$$

или в терминах квадратичных форм

$$\begin{aligned}(k-\lambda)(x_1^2 + x_2^2 + \ldots + x_v^2) + \\ + \lambda(x_1 + x_2 + \ldots + x_v)^2 = \\ = (k-\lambda)(y_1^2 + y_2^2 + \ldots + y_{v-1}^2) + y_v^2.\end{aligned} \tag{3.23}$$

Здесь

$$x_i = p_{i1}y_1 + p_{i2}y_2 + \ldots + p_{iv}y_v \qquad (i = 1, 2, \ldots, v), \tag{3.24}$$

где элементы матрицы $P = [p_{ij}]$ рациональны, а сама матрица P — невырожденная.

В (3.24), если $p_{11} \neq 1$, положим $x_1 = y_1$, а если $p_{11} = 1$, то положим $x_1 = -y_1$. Из этого следует

$$y_1 = e_2y_2 + e_3y_3 + \ldots + e_vy_v, \tag{3.25}$$

где $e_2, e_3, \ldots, e_v$ — рациональны. В силу (3.24) имеем $x_2 = p_2y_2 + p_3y_3 + \ldots + p_vy_v$, где $p_2, p_3, \ldots, p_v$ — рациональны. В свою очередь, если $p_2 \neq 1$, мы положим $x_2 = y_2$, а если $p_2 = 1$, то положим $x_2 = -y_2$. Это влечет соотношение

$$y_2 = f_3y_3 + f_4y_4 + \ldots + f_vy_v, \tag{3.26}$$

где f_3, f_4, ..., f_v — рациональные. Продолжим эти рассуждения до момента, когда

$$y_{v-2} = g_{v-1}y_{v-1} + g_v y_v, \tag{3.27}$$

где g_{v-1} и g_v — рациональные. Согласно (3.24) имеем $x_{v-1} = q_{v-1}y_{v-1} + q_v y_v$, где q_{v-1} и q_v — рациональные. Наконец, положим $x_{v-1} = \pm y_{v-1}$, и это даст нам $y_{v-1} = h_v y_v$, где h_v — рациональное. До сих пор мы оставляли y_v неуточненным; теперь положим, что y_v — рациональное число, не равное нулю. Тогда y_{v-1}, y_{v-2}, ..., y_1 определены единственным образом посредством указанных выше соотношений, а x_1, x_2, ..., x_v определены также единственным образом соотношением (3.24). Кроме того, $x_i^2 = y_i^2$ $(i = 1, 2, \ldots, v-1)$. Если мы подставим эти рациональные числа в (3.23), то получим

$$(k-\lambda)x_v^2 + \lambda(x_1 + x_2 + \ldots + x_v)^2 = y_v^2, \tag{3.28}$$

что и доказывает теорему для случая $v \equiv 1 \pmod 4$.

Пусть теперь $v \equiv 3 \pmod 4$. Доказательство в этом случае потребует только внесения небольших изменений в изложенные выше рассуждения. Из (3.21), (3.11) и (3.16) получаем

$$B \dotplus I_1 \overset{c}{=} (k-\lambda) I_{v+1}. \tag{3.29}$$

В терминах квадратичных форм это означает

$$\begin{aligned}(k-\lambda)(x_1^2 + x_2^2 + \ldots + x_v^2) + \\ + \lambda(x_1 + x_2 + \ldots + x_v)^2 + x_{v+1}^2 = \\ = (k-\lambda)(y_1^2 + y_2^2 + \ldots + y_{v+1}^2).\end{aligned} \tag{3.30}$$

Здесь

$$\begin{aligned}x_i = p'_{i1}y_1 + p'_{i2}y_2 + \ldots + p'_{i,\,v+1}y_{v+1} \\ (i = 1, 2, \ldots, v+1),\end{aligned} \tag{3.31}$$

где элементы матрицы $P' = [p'_{ij}]$ — рациональные числа, а сама матрица невырождена. Положим, как и прежде, $x_1 = \pm y_1$ и получим соотношение

$$y_1 = e'_2 y_2 + e'_3 y_3 + \ldots + e'_{v+1}y_{v+1}, \tag{3.32}$$

где e_2', e_3', ..., e_{v+1}' — рациональные числа. Положим $x_2 = \pm y_2$ и получим

$$y_2 = f_3' y_3 + f_4' y_4 + \ldots + f_{v+1}' y_{v+1}, \qquad (3.33)$$

где f_3', f_4', ..., f_{v+1}' — рациональные. Так мы продолжим до

$$y_{v-1} = g_v' y_v + g_{v+1}' y_{v+1}, \qquad (3.34)$$

где g_v' и g_{v+1}' — рациональные. Согласно (3.31), имеем $x_v = q_v' y_v + q_{v+1}' y_{v+1}$, где q_v' и q_{v+1}' — рациональные. Наконец, положим $x_v = \pm y_v$, а это даст нам $y_v = h_{v+1}' y_{v+1}$, где h_{v+1}' — рациональное. Теперь будем считать, что y_{v+1} — рациональное число, не равное нулю. В таком случае y_v, y_{v-1}, ..., y_1, а также x_1, x_2, ..., x_{v+1} определены единственным образом. Кроме того, $x_i^2 = y_i^2$ $(i = 1, 2, \ldots, v)$. Если мы подставим эти рациональные числа в (3.30), то получим

$$\lambda (x_1 + x_2 + \ldots + x_v)^2 + x_{v+1}^2 = (k - \lambda) y_{v+1}^2, \qquad (3.35)$$

что и доказывает теорему для $v \equiv 3 \pmod 4$.

Пусть a и m — натуральные числа, взаимно простые. Если сравнение $x^2 \equiv a \pmod m$ имеет решение, то a называется *квадратичным вычетом* m; если же решения нет, то a называется *квадратичным невычетом* m. Пусть даны натуральные числа a, b, c, свободные от квадратов, попарно взаимно простые и не все одного и того же знака. Диофантово уравнение

$$ax^2 + by^2 + cz^2 = 0, \qquad (3.36)$$

коэффициенты a, b, c которого удовлетворяют указанным требованиям, называется *уравнением Лежандра*. Классическая теорема Лежандра утверждает, что уравнение (3.36) имеет целочисленные ненулевые решения x, y, z тогда и только тогда, когда величины $-bc$, $-ac$, $-ab$ являются квадратичными вычетами a, b, c соответственно. Необходимые условия теоремы очевидны: если уравнение (3.36) имеет решения x, y, z целочисленные и не все равные нулю, то мы можем утверждать, что эти три целых числа не имеют общих простых множителей. Отсюда следует,

что если простое число p делит a, то оно не делит z. В самом деле, если $p \mid z$, то $p \mid y$, $p^2 \mid ax^2$ и $p \mid x$. Таким образом, (3.36) означает, что $(bz^{-1}y)^2 \equiv -bc \pmod{a}$. Другие необходимые условия получаются симметричными рассуждениями. Существенным в теореме Лежандра является утверждение, что эти необходимые условия являются также достаточными. Эта часть доказательства далеко не очевидна [1]).

Легко превратить уравнение (3.18) в уравнение Лежандра. Пусть $(k-\lambda)'$ и λ' обозначают соответственно свободные от квадратов части для $k-\lambda$ и λ. Пусть теперь $d = ((k-\lambda)', \lambda')$, где этот символ означает положительный наибольший общий делитель чисел $(k-\lambda)'$ и λ'. Тогда (3.18) имеет решение в целых x, y, z, не равных нулю одновременно, тогда и только тогда, когда уравнение

$$dx^2 = \frac{(k-\lambda)'}{d} y^2 + (-1)^{\frac{v-1}{2}} \frac{\lambda'}{d} z^2 \qquad (3.37)$$

имеет ненулевое решение в целых x, y, z. Более того, уравнение (3.37) есть уравнение Лежандра. Таким образом, если v — нечетное и если (v, k, λ)-конфигурация существует, то величины

$$(-1)^{\frac{v+1}{2}} \frac{\lambda'(k-\lambda)'}{d^2}, \quad (-1)^{\frac{v-1}{2}} \lambda', \quad (k-\lambda)' \qquad (3.38)$$

являются квадратическими вычетами d, $\frac{(k-\lambda)'}{d}$, $\frac{\lambda'}{d}$ соответственно. Многие важные (v, k, λ)-конфигурации имеют нечетное v и $(k, \lambda) = 1$. У них $(k-\lambda, \lambda) = 1$ и, следовательно, $d = 1$. Ясно, что для этих конфигураций первое из необходимых условий тривиально. Третье необходимое условие также тривиально, потому что мы всегда имеем $k^2 = (k-\lambda) + \lambda v$, а это означает, что $k-\lambda$ есть квадратический вычет λ. Но отсюда следует, что $(k-\lambda)'$ является квадратическим вычетом λ'. Таким образом, полностью теорема 3.1 для (v, k, λ)-конфигураций при v

[1]) Подробное доказательство этой теоремы см., например, в книге Дирихле Лежен П. Г., Лекции по теории чисел, ОНТИ, 1935. — *Прим. ред.*

нечетном и при $(k, \lambda) = 1$ формулируется так: *для* (v, k, λ)*-конфигурации с нечетным* v *и* $(k, \lambda) = 1$ *число* $(-1)^{\frac{v-1}{2}} \lambda'$ *является квадратичным вычетом для* $(k - \lambda)'$.

Теперь мы подготовлены к тому, чтобы доказать теорему 4.3 гл. 7.

Теорема 3.2. *Пусть* $n \equiv 1$ *или* $2 \pmod 4$, *а свободная от квадрата часть* n *содержит по меньшей мере один простой множитель* $p \equiv 3 \pmod 4$. *Тогда конечной проективной плоскости* π *порядка* n *не существует.*

Доказательство. Конечная проективная плоскость порядка n есть (v, k, λ)-конфигурация с параметрами $v = n^2 + n + 1$, $k = n + 1$, $\lambda = 1$. У нас v нечетно и $(k, \lambda) = 1$. Предположение, что $n \equiv 1$ или $2 \pmod 4$ означает, что $\frac{v-1}{2}$ нечетно. Следовательно, если плоскость существует, то -1 есть квадратичный вычет p. Из элементарной теории чисел [1]) мы знаем, однако, что -1 есть квадратичный невычет простого числа $p \equiv 3 \pmod 4$.

Существование матриц Адамара предполагается для всех $n \equiv 0 \pmod 4$. При этих обстоятельствах мы бы не стали прибегать к теореме 3.1, чтобы исключить адамаровы конфигурации, и это совершенно верно. Адамарова конфигурация имеет параметры $v = 4t - 1$, $k = 2t - 1$, $\lambda = t - 1$ или $v = 4t - 1$, $k' = 2t$, $\lambda' = t$. Эти значения приводят к диофантовым уравнениям:

$$x^2 = ty^2 - (t - 1)z^2; \quad x^2 = ty^2 - tz^2. \tag{3.39}$$

Первое из них имеет решение $x = y = z = 1$, а второе — $x = 0$, $y = z = 1$.

4. Матричное уравнение $AA^T = B$. В этом пункте мы изучаем матричное уравнение $AA^T = B$. Повсюду в дальнейшем A будет обозначать матрицу порядка v с рациональными или целыми элементами, а A^T — транс-

[1]) См. сноску на стр. 112, 117. — *Прим. ред.*

понированную матрицу A. Матрица B имеет порядок v и определяется соотношением

$$B = (k - \lambda) I + \lambda J. \tag{4.1}$$

В этом выражении I — единичная матрица порядка v, а J — матрица порядка v, составленная из единиц. Положим, что k и λ целые и такие, что $0 < \lambda < k < v - 1$ и

$$k - \lambda = k^2 - \lambda v. \tag{4.2}$$

Начнем с такой теоремы.

Теорема 4.1. *Пусть A — матрица с рациональными элементами, такая, что $AA^T = B$. Тогда*

$$A^T A = (k - \lambda) I + \frac{\lambda}{k^2} A^T J A. \tag{4.3}$$

Доказательство. В п. 2 мы указали, что матрица B — невырожденная. Теперь мы утверждаем, что матрица, обратная B, задается соотношением

$$B^{-1} = \frac{1}{k - \lambda} I - \frac{\lambda}{k^2 (k - \lambda)} J. \tag{4.4}$$

Это верно потому, что если мы умножим (4.4) слева на B и применим (4.2), то получим $BB^{-1} = I$. Предположим теперь, что $AA^T = B$. Тогда $A\left(A^T B^{-1}\right) = I$, и, поскольку сама матрица и обратная ей перестановочны, получим

$$A^T B^{-1} A = I. \tag{4.5}$$

Тогда в силу (4.4)

$$A^T \left(\frac{1}{k - \lambda} I - \frac{\lambda}{k^2 (k - \lambda)} J \right) A = I, \tag{4.6}$$

откуда

$$A^T A = (k - \lambda) I + \frac{\lambda}{k^2} A^T J A. \tag{4.7}$$

Из теоремы 4.1 вытекает много интересных следствий. Пусть s_i обозначает сумму элементов i-го столбца матрицы A, а t_i обозначает сумму квадратов элементов i-го столбца

матрицы A. Подсчетом можно проверить, что

$$A^T JA = [s_i s_j] \quad (i, j = 1, 2, \ldots, v). \tag{4.8}$$

Следовательно, из теоремы 4.1 вытекает, что

$$k^2 t_i = \lambda s_i^2 + k^2 (k - \lambda) \quad (i = 1, 2, \ldots, v). \tag{4.9}$$

Затем мы обнаруживаем, что если A — матрица, составленная из рациональных элементов и такая, что $AA^T = B$, и если $JA = kJ$, то $A^T A = B$. Это утверждение является непосредственным следствием теоремы 4.1. Были проведены широкие исследования матричной конгруэнтности $B \overset{c}{=} I$ над полем рациональных чисел. Здесь мы не можем входить в детали этих исследований. Мы просто отметим, что, как известно, мы всегда имеем $B \overset{c}{=} I$ над полем рациональных чисел, за исключением тех значений v, k, λ, для которых (v, k, λ)-конфигурации исключены условиями теоремы 3.1. Известно также, что если $B \overset{c}{=} I$ над рациональным полем, то существует матрица A с рациональными элементами, такая, что $AA^T = A^T A = B$. Эти исследования имеют сами по себе существенный интерес, но они не дают новой информации относительно условий несуществования (v, k, λ)-конфигураций.

Естественно было бы изучить матричное уравнение $AA^T = B$ для случая, когда A составлена из целочисленных элементов. Начнем с элементарных наблюдений. Пусть дана матрица A с целочисленными элементами, такая, что $AA^T = A^T A = B$. Тогда мы утверждаем, что матрицей инцидентности для (v, k, λ)-конфигурации является или матрица A, или матрица $-A$. В самом деле, из $A^T A = B$ следует, что $t_i = k$, а в силу (4.9) мы имеем $s_i^2 = k^2$. Теперь из $t_i = k$, $s_i = k$ следует, что элементы i-го столбца матрицы A суть нули и единицы, а из $t_i = k$, $s_i = -k$ вытекает, что элементы i-го столбца матрицы A суть нули и отрицательные единицы. Каждый элемент матрицы B, не лежащий на главной диагонали, равен натуральному числу λ, а это означает, что обе разновидности столбцов не встречаются. Следовательно, A или $-A$ будет матрицей инцидентности (v, k, λ)-конфигурации.

Пусть S и S' — две симметрические $(n \times n)$-матрицы с элементами из кольца целых чисел. Матрица S *вполне*

представляет матрицу S', если существует матрица P порядка n с целыми элементами и такая, что

$$P^T S P = S', \tag{4.10}$$

где P^T обозначает транспонированную матрицу P. В частности, единичная матрица I порядка n вполне представляет S' в случае, если существует матрица P порядка n с целыми элементами и такая, что

$$P^T P = S'. \tag{4.11}$$

Ясно, что если (v, k, λ)-конфигурация существует, то единичная матрица I порядка v вполне представляет B. Ниже мы докажем обратное предложение для некоторых значений v, k, λ. К сожалению, задача определения того, будет или нет одна матрица вполне представлять другую, остается вообще неразрешенной проблемой. Дальнейшие продвижения здесь могут доставить нам более глубокое понимание (v, k, λ)-конфигураций.

Пусть дана матрица A с целыми элементами, такая, что $AA^T = B$. Если мы перемножим на -1 элементы какого-либо столбца матрицы A, то мы не нарушим матричного уравнения $AA^T = B$. Следовательно, мы можем выбрать матрицу A таким образом, чтобы суммы их элементов в столбцах были неотрицательными. О матрице A, в которой эти требования выполняются, говорят, что она имеет *нормализованный вид*.

Теорема 4.2. *Пусть A — матрица с целыми элементами, такая, что $AA^T = B$. Запишем A в нормализованном виде. Если (k, λ) свободно от квадрата и если $(k - \lambda)$ нечетно, то A — матрица инцидентности для (v, k, λ)-конфигурации.*

Доказательство. Снова обозначим через s_i сумму элементов i-го столбца в матрице A, а через t_i — сумму квадратов элементов того же столбца. Матрица A записана в нормализованном виде, так что каждое $s_i \geqslant 0$. Из уравнения (4.9) следует

$$\lambda s_i^2 \equiv 0 \pmod{k^2} \quad (i = 1, 2, \ldots, v). \tag{4.12}$$

Поскольку (k, λ) свободно от квадрата, то из (4.12) и (4.2) нетрудно вывести, что каждое $s_i \equiv 0 \pmod{k}$. Запишем $s_i = u_i k$; тогда равенство (4.9) примет вид

$$t_i = \lambda u_i^2 + (k - \lambda) \quad (i = 1, 2, \ldots, v). \tag{4.13}$$

Предположим, что некоторое $u_i = 0$. Тогда $s_i = 0$, и в силу (4.13) $t_i = k - \lambda$. Но

$$s_i^2 \equiv t_i \equiv k - \lambda \equiv 0 \pmod{2}, \tag{4.14}$$

а это противоречит нашему условию, что $(k - \lambda)$ нечетно. Следовательно, каждое $u_i \neq 0$. Но из $JAA^TJ = JBJ$ следует

$$s_1^2 + s_2^2 + \ldots + s_v^2 = k^2 v, \tag{4.15}$$

откуда

$$u_1^2 + u_2^2 + \ldots + u_v^2 = v. \tag{4.16}$$

Но если каждое $u_i \neq 0$, то каждое $u_i = 1$, а каждое $s_i = k$. Таким образом, каждое $t_i = k$. Но отсюда следует, что A есть матрица инцидентности (v, k, λ)-конфигурации.

Ограничение теоремы 4.2, заключающееся в том, что (k, λ) должно быть свободно от квадрата, не очень существенно. Многие важные (v, k, λ)-конфигурации удовлетворяют этому требованию, например конечные проективные плоскости и адамаровы конфигурации с параметрами $v = 4t - 1$, $k = 2t - 1$, $\lambda = t - 1$ и с условием $(k, \lambda) = 1$. С другой стороны, ограничение, заключающееся в том, что $(k - \lambda)$ должно быть нечетным, исключает из рассмотрения многие конфигурации. Но мы теперь знаем, что теорема 4.2 не обязательно верна для $(k - \lambda)$ целого и четного. В этом случае из того, что (k, λ) свободно от квадрата, все еще следует, что каждое $s_i \equiv 0 \pmod{k}$. Но мы не можем, вообще говоря, заключить, что каждое $u_i \neq 0$.

Пусть H — адамарова матрица порядка $n = 2$ или $n \equiv 0 \pmod{4}$. Выберем H так, чтобы ее первый столбец был составлен только из положительных единиц, и образуем прямую сумму

$$H' = H \dotplus H \dotplus \ldots \dotplus H \ (n + 1 \text{ слагаемых}). \tag{4.17}$$

Получится матрица порядка n^2+n. Пусть теперь δ — вектор-строка из n компонент с 1 на первом месте и 0 на всех остальных местах. Окаймим матрицу H' начальным вектором-строкой

$$\delta' = (\delta, \delta, \ldots, \delta) \text{ (всего } n+1 \text{ компонент } \delta). \quad (4.18)$$

Ясно, что δ' имеет всего n^2+n компонент. Затем окаймим полученную таблицу начальным вектором-столбцом из n^2+n+1 компонент. Этот вектор имеет 0 на первом месте и единицы на всех остальных местах.

Получающаяся при этом матрица A имеет порядок n^2+n+1; легко проверить, что она удовлетворяет матричному уравнению $AA^T = nI+J$. При этом матрица A записана в нормализованном виде. Но A не является матрицей инцидентности проективной плоскости порядка n.

Заметим, что решение только что описанного вида и матрица инцидентности проективной плоскости существуют одновременно, если $n = 2^\alpha$. Покажем эти решения для случая $n = 2$:

$$\begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & -1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & -1 \end{bmatrix}, \quad (4.19)$$

$$\begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}. \quad (4.20)$$

Далее покажем, что целые решения также существуют для $n = 10$. Определим

$$H^* = \left[\begin{array}{cc|cccc|cccc}
1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\
1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
\hline
1 & 1 & \multicolumn{4}{c|}{\multirow{4}{*}{$3I - J$}} & \multicolumn{4}{c}{\multirow{4}{*}{I}} \\
1 & 1 & & & & & & & & \\
1 & 1 & & & & & & & & \\
1 & 1 & & & & & & & & \\
\hline
1 & -1 & \multicolumn{4}{c|}{\multirow{4}{*}{$-I$}} & \multicolumn{4}{c}{\multirow{4}{*}{$3I - J$}} \\
1 & -1 & & & & & & & & \\
1 & -1 & & & & & & & & \\
1 & -1 & & & & & & & &
\end{array}\right], \tag{4.21}$$

где I обозначает единичную матрицу четвертого порядка, а J — матрицу четвертого порядка, состоящую из единиц. Тогда H^* — матрица порядка 10; нетрудно проверить, что она удовлетворяет соотношению $H^*H^{*T} = 10I$, где I — единичная матрица порядка 10. Теперь мы можем выполнить построение, описанное в предыдущем разделе, заменив лишь H на H^*. Это дает матрицу A порядка 111, удовлетворяющую матричному уравнению $AA^T = 10I + J$. Но A ни в коем случае не является матрицей инцидентности проективной плоскости порядка 10. По-видимому, существует широкое разнообразие целочисленных решений, которые не сводятся в их нормализованном виде к матрицам инцидентности. Фактически мы предполагаем, что для $v = n^2 + n + 1$, $k = n + 1$, $\lambda = 1$ такие решения всегда существуют, имея только в виду, что n четно и что $nI + J \overset{c}{=} I$ над полем рациональных чисел.

Выше мы заметили, что существование матриц Адамара предположено для всех $n \equiv 0 \pmod 4$. Покажем, что это предположение могло бы быть доказано, если бы теория целочисленных представлений матриц была более полной. Существует матрица Адамара порядка 2^α, а прямое произведение двух адамаровых матриц есть тоже адамарова матрица. Следовательно, существование матриц

Адамара всех порядков вида $4t$, где t нечетно, влечет за собой существование матриц Адамара всех порядков вида $n \equiv 0 \pmod 4$. Но матрица Адамара порядка $4t \geqslant 8$ эквивалентна адамаровой конфигурации с параметрами $v = 4t - 1$, $k = 2t - 1$, $\lambda = t - 1$. Эти конфигурации для случая t нечетного рассмотрены в теореме 4.2. Следовательно, проблема существования матриц Адамара всех порядков вида $n \equiv 0 \pmod 4$ может рассматриваться как проблема относительно целочисленных представлений.

5. Экстремальные задачи. До сих пор наше изучение (v, k, λ)-конфигурации было сосредоточено на задаче определения точных областей значений v, k, λ, для которых эти конфигурации существуют. Гораздо более трудная задача определения точного числа различных конфигураций для каждого выбора значений v, k, λ значительно превышает уровень развития современных методов. Упомянем в этой связи высказанное ранее предположение, что всякая проективная плоскость простого порядка единственна.

Существуют также важные задачи о (v, k, λ)-конфигурациях, которые непосредственно не относятся к этим двум основным задачам. В некоторых из них речь идет о выявлении свойств, присущих самим конфигурациям. Например, дана матрица инцидентности A проективной плоскости порядка n. Существуют ли перестановочные матрицы $P \neq I$ и Q, такие, что $PAQ = A$? Это — нерешенная задача. Положительный ответ имел бы важные следствия в геометрии и указал бы, что всякая конечная проективная плоскость обладает нетривиальной коллинеацией.

Много важных задач относится к существованию и классификации частных видов конфигураций с теми или иными дополнительными требованиями, налагаемыми на них. Упомянем об одном особенно интересном примере. Матрица порядка n вида

$$A = \begin{bmatrix} a_0 & a_1 & a_2 & a_{n-1} \\ a_{n-1} & a_0 & a_1 & a_{n-2} \\ \cdots & \cdots & \cdots & \cdots \\ a_1 & a_2 & a_3 & a_0 \end{bmatrix} \tag{5.1}$$

называется *циркулянтом*. Матрица инцидентности (4.20) проективной плоскости порядка 2 является циркулянтом. Матрицы инцидентности некоторых (v, k, λ)-конфигураций могут быть преобразованы в циркулянты перестановками строк и столбцов. Эти конфигурации эквивалентны совершенному разностному множеству в теории чисел и будут исследованы в гл. 9. Однако сначала обсудим некоторые экстремальные задачи, которые объединяют (v, k, λ)-конфигурации и некоторые из понятий, введенных в настоящей монографии ранее.

Пусть даны фиксированные целые числа v и k, такие, что

$$1 \leqslant k \leqslant v, \tag{5.2}$$

и пусть $\mathfrak{A}(K, K)$ — класс всех (0, 1)-матриц порядка v, имеющих в каждой строке и в каждом столбце ровно k единиц. В гл. 6 мы отмечали, что каждая матрица A в классе $\mathfrak{A}(K, K)$ имеет $\operatorname{per}(A) > 0$. Но для матриц этого класса мало что известно о минимальном значении $\operatorname{per}(A)$. Если $\mathfrak{A}(K, K)$ содержит матрицу инцидентности (v, k, λ)-конфигурации, то можно на основании очень ограниченных данных предполагать, что перманент этой матрицы мал или даже минимален в классе $\mathfrak{A}(K, K)$. Вычисления здесь делаются практически невозможными, даже для малых значений v. Аналогичная задача относительно дважды стохастических матриц приводит к предположению Ван дер Вардена (см. гл. 5).

Не так уж много известно о перманенте матрицы инцидентности (v, k, λ)-конфигурации. Однако, чтобы выполнить большие выкладки в этой области, были применены электронные вычислительные машины. Было подсчитано, что проективные плоскости порядков 2, 3 и 4 имеют перманенты, равные соответственно 24, 3852 и 18 534 400. Перманент матрицы инвариантен относительно перестановок строк, столбцов и относительно транспозиций. Пусть A и A' обозначают матрицы инцидентности двух (v, k, λ)-конфигураций с одними и теми же параметрами v, k и λ. Пусть, однако, эти матрицы будут таковы, что они не переводятся одна в другую только что описанными операциями. Тогда мы предполагаем, что

перманенты этих матриц различны. Их детерминанты, разумеется, равны по абсолютной величине.

Обозначим через Z матрицу инцидентности проективной плоскости 2-го порядка. Эта матрица имеет порядок 7 и обладает замечательным свойством

$$\operatorname{per}(Z) = \text{абс. знач. } \det(Z) = 24. \tag{5.3}$$

Теперь приведем без доказательства одну интересную теорему, которая покажет особую роль матрицы Z в теории перманентов.

Теорема 5.1. *Пусть A — циркулянт в классе $\mathfrak{A}(K, K)$. Если $k > 3$, то*

$$\operatorname{per}(A) > \text{абс. знач. } \det(A). \tag{5.4}$$

Если $k = 3$ и если

$$\operatorname{per}(A) = \text{абс. знач. } \det(A), \tag{5.5}$$

то перестановками строк и столбцов матрица A преобразуется в прямую сумму матриц Z, взятых e раз. Следовательно, $v = 7e$, а $\operatorname{per}(A) = (24)^e$.

Матрицы инцидентности (v, k, λ)-конфигураций возникают также в экстремальных задачах относительно детерминантов.

Теорема 5.2. *Пусть Q — $(0, 1)$-матрица порядка v, содержащая τ единиц. Определим k и λ следующим образом:*

$$\tau = kv, \tag{5.6}$$

$$\lambda = \frac{k(k-1)}{v-1} \tag{5.7}$$

и предположим, что $0 < \lambda < k < v - 1$. Тогда

$$\text{абс. знач. } \det(Q) \leqslant k(k-\lambda)^{\frac{v-1}{2}}; \tag{5.8}$$

при этом равенство достигается тогда и только тогда, когда Q — матрица инцидентности (v, k, λ)-конфигурации.

Мы опускаем доказательство теоремы 5.2. Фактически эта теорема может быть обобщена в нескольких направлениях. Кажется неправдоподобным, что неравенства

вида (5.8) будут решать глубокие арифметические проблемы, связанные с (v, k, λ)-конфигурациями. Однако такие неравенства интересны сами по себе. Заметим, что из теоремы 5.2 следует, что если класс $\mathfrak{A}(K, K)$ содержит матрицу инцидентности (v, k, λ)-конфигурации, то детерминант этой матрицы максимален по абсолютному значению в сравнении с матрицами этого класса. Это довольно неожиданно, потому что наши прежние замечания указывали, что перманент такой матрицы мог, по-видимому, быть минимальным относительно матриц этого класса.

Укажем на интересную связь между конечными проективными плоскостями и 1-шириной, определенной в гл. 6.

Теорема 5.3. *Пусть* $\mathfrak{A}(K, K)$ *— класс с параметрами* $v = n^2 + n + 1$, $k = n^2$, *и пусть* $n \geqslant 2$. *Матрицы в* $\mathfrak{A}(K, K)$, *которые являются дополнениями матриц инцидентности проективных плоскостей порядка* n, *имеют* 1*-ширину* $\varepsilon(1) = 3$, *а все другие матрицы в* $\mathfrak{A}(K, K)$ *имеют* 1*-ширину* $\varepsilon(1) = 2$.

Доказательство. Оно получается почти непосредственно. Дано, что A — матрица в классе $\mathfrak{A}(K, K)$. Образуем $A^T A$, где A^T — транспонированная матрица A. Обозначим через λ' минимальное и через λ — среднее значение элементов $A^T A$, не лежащих на главной диагонали $A^T A$. Очевидно, что

$$\lambda = \frac{n^2(n^2-1)}{n^2+n} = n(n-1). \tag{5.9}$$

Предположим, что $\lambda' = \lambda$. Тогда A есть дополнение матрицы инцидентности проективной плоскости порядка n. В этом случае из равенств $v = n^2 + n + 1$, $k = n^2$, $\lambda = n(n-1)$ следует, что всякая $(v \times 2)$-подматрица матрицы A имеет точно одну строку, состоящую из нулей. Но это означает, что A имеет 1-ширину $\varepsilon(1) = 3$. С другой стороны, предположим, что $\lambda' < \lambda$. Тогда из равенств $v = n^2 + n + 1$, $k = n^2$ следует, что $\lambda' = \lambda - 1$. Но это означает, что некоторая $(v \times 2)$-подматрица матрицы A не имеет строки, состоящей из нулей. Следовательно, A имеет 1-ширину $\varepsilon(1) = 2$.

Пусть $\bar{\varepsilon}(1)$ — максимальная 1-ширина матриц A в классе $\mathfrak{A}(K, K)$ из теоремы 5.3. Тогда отсюда следует, что $\bar{\varepsilon}(1) = 3$, если проективная плоскость порядка n существует, и $\bar{\varepsilon}(1) = 2$ в противном случае. В гл. 6 мы обозначили через $\tilde{\varepsilon}(\alpha)$ минимальную, а через $\bar{\varepsilon}(\alpha)$ — максимальную α-ширины матриц A в нормализованном классе $\mathfrak{A}(R, S)$. Мы отмечали, что для вычисления $\bar{\varepsilon}(\alpha)$ пригоден один весьма эффективный метод, однако относительно поведения $\bar{\varepsilon}(\alpha)$ известно очень мало. Теорема 5.3 показывает большую сложность $\bar{\varepsilon}(\alpha)$.

ЛИТЕРАТУРА

Классической работой о (b, v, r, k, λ)-конфигурациях является [3]. Наше доказательство неравенства Фишера имеется в [4]. О системах штейнеровских троек написано в [12], [17], [21], [34], [36], [40], [42], [52]. Теорема 2.1 впервые появилась в [43]. Единственность плоскости 8-го порядка доказана в [20]. Матрицы Адамара рассмотрены в работах [2], [6], [10], [14], [38], [56], [57, 58]. Пункт 3 основан на работах [8] и [7]. Рассмотрение уравнения Лежандра имеется в [35]. Пункт 4 в большей части следует работе [44]. Чтобы познакомиться со смежными вопросами, см. [1], [13], [19], [28]. Материал, служащий основой п. 4, см. в [29] и [54]. Вычисление перманентов рассмотрено в [37]. Теоремой 5.1 мы обязаны работе [55]. Теорема 5.2 появилась в статьях [45, 46], а обобщение этих работ рассмотрено в [33].

1. Albert A. A., Rational normal matrices satisfying the incidence equation, *Proc. Amer. Math. Soc.*, **4** (1953), 554—559.
2. Baumert L., Golomb S. W., Hall M., Jr., Discovery of an Hadamard matrix of order 92, *Bull. Amer. Math. Soc.*, **68** (1962), 237—238.
3. Bose R. C., On the construction of balanced incomplete block designs, *Ann. Eugen.*, **9** (1939), 353—399.
4. Bose R. C., A note on Fisher's inequality for balanced incomplete block designs, *Ann. Math. Stat.*, **20** (1949), 619—620.
5. Bose R. C., Mesner D. M., On linear associative algebras corresponding to association schemes of partically balanced designs, *Ann. Math. Stat.*, **30** (1959), 21—38.
6. Brauer A., On a new class of Hadamard determinants, *Math. Zeit.*, **58** (1953), 219—225.
7. Bruck R. H., Ryser H. J., The nonexistence of certain finite projective planes, *Canad. Jour. Math.*, **1** (1949), 88—93.

8. Chowla S., Ryser H. J., Combinatorial problems, *Canad. Jour. Math.*, **2** (1950), 93—99.
9. Connor W. S., On the structure of balanced incomplete block designs, *Ann. Math. Stat.*, **23** (1952), 57—71.
10. Dade E., Goldberg K., The construction of Hadamard matrices, *Michigan Math. Jour.*, **6** (1959), 247—250.
11. Fischer R. A., Yates F., Statistical Tables for Biological, Agricultural, and Medical Research, London, 2 ed., 1943.
12. Fort M. K., Jr., Hedlund G. A., Minimal coverings of pairs by triples, *Pacific Jour. Math.*, **8** (1958), 709—719.
13. Goldhaber J. K., Integral p-adic normal matrices satisfying the incidence equation, *Canad. Jour. Math.*, **12** (1960), 126—133.
14. Gruner W., Einlagerung des regularen n-Simplex in den n-dimensionalen Würfel, *Comment. Math. Helv.*, **12** (1939—1940), 149—152.
15. Hall M., Jr., Some Aspects of Analysis and Probability, New York, 1958, 35—104.
16. Hall M., Jr., Theory of Groups, New York, Macmillan, 1959. (Русский перевод: М. Холл, Теория групп, ИЛ, 1962.)
17. Hall M., Jr., Automorphisms of Steiner triple systems, *IBM Jour. Research and Dev.*, **4** (1960), 460—472.
18. Hall M., Jr., Connor W. S., An embedding theorem for balanced incomplete block designs, *Canad. Jour. Math.*, **6** (1953), 35—41.
19. Hall M., Jr., Ryser H. J., Normal completions of incidence matrices, *Amer. Jour. Math.*, **76** (1954), 581—589.
20. Hall M., Jr., Swift J. D., Walker R. J., Uniqueness of the projective plane of order eight, *Math. Tables Aids Comput.*, **10** (1956), 186—194.
21. Hanani H., A note on Steiner triple systems, *Math. Scand.*, **8** (1960), 154—156.
22. Hanani H., The existence and construction of balanced incomplete block designs, *Ann. Math. Stat.*, **32** (1961), 361—386.
23. Hoffman A. J., Newman M., Straus E. G., Taussky O., On the number of absolute points of a correlation, *Pacific Jour. Math.*, **6** (1956), 83—96.
24. Hoffman A. J., Richardson M., Block design games, *Canad. Jour. Math.*, **13** (1961), 110—128.
25. Hughes D. R., Collineations and generalized incidence matrices, *Trans. Amer. Math. Soc.*, **86** (1957), 284—296.
26. Hughes D. R., Generalized incidence matrices over group algebras, *Illinois Jour. Math.*, **1** (1957), 545—551.
27. Isbell J. R., A class of simple games, *Duke Math. Jour.*, **25** (1958), 423—439.

28. Johnsen E. C., Matrix rational completions satisfying generalized incidence equations, and integral solutions to the incidence equation for finite projective plane cases of orders $n \equiv 2 \pmod 4$. Doctoral dissertation, Ohio State University, 1961.

29. Jones B. W., The Arithmetic Theory of Quadratic Forms, Carus Math. Monograph, № 10, New York, 1950.

30. Kleinfeld E., Finite Hjelmslev planes, *Illinois Jour. Math.*, **3** (1959), 403—407.

31. Majumdar K. N., On some theorems in combinatorics relating to incomplete block designs, *Ann. Math. Stat.*, **24** (1953), 377—389.

32. Mann H. B., Analysis and Design of Experiments, New York, 1949.

33. Marcus M., Gordon W. R., Generalizations of some inequalities of H. J. Ryser, *Illinois Jour. Math.*, **7** (1963), № 4, 582—592.

34. Moore E. H., Concerning triple systems, *Math. Ann.*, **43** (1893), 271—285.

35. Nagell T., Introduction to Number Theory, New York, 1951.

36. Netto E., Lehrbuch der Combinatorik, Leipzig, 2 Aufl., 1927.

37. Nikolai P. J., Permanents of incidence matrices, *Math. Comp.*, **14** (1960), 262—266.

38. Paley R. E. A.C., On orthogonal matrices, *Jour. Math. and Physics*, **12** (1933), 311—320.

39. Parker E. T., On collineations of symmetric designs, *Proc. Amer. Math. Soc.*, **8** (1957), 350—351.

40. Reiss M., Über eine Steinersche combinatorische Aufgabe welche im 45sten Bande dieses Journals, Seite 181, gestellt worden ist, *Crelle's Jour.*, **56** (1859), 326—344.

41. Richardson M., On finite projective planes, *Proc. Amer. Math. Soc.*, **7** (1956), 458—465.

42. Rouse Ball W. W., Mathematical Recreations and Essays (revised by H. S. M. Coxeter), New York, 1947.

43. Ryser H. J., A note on a combinatorial problem, *Proc. Amer. Math. Soc.*, **1** (1950), 422—424.

44. Ryser H. J., Matrices with integer elements in combinatorial investigations, *Amer. Jour. Math.*, **74** (1952), 769—773.

45. Ryser H. J., Inequalities of compound and induced matrices with applications to combinatorial analysis, *Illinois Jour. Math.*, **2** (1958) 240—253.

46. Ryser H. J., Compound and induced matrices in combinatorial analysis, Proc. of Symposia in Applied Math., **10** (1960), 149—168.

47. Ryser H. J., Matrices of zeros and ones, *Bull. Amer. Math. Soc.*, **66** (1960), 442—464.

48. Schützenberger M. P., A non-existence theorem for an infinite family of symmetrical block designs, *Ann. Eugen.*, 14 (1949), 286—287.

49. Shrikhande S. S., The impossibility of certain symmetrical balanced incomplete block designs, *Ann. Math. Stat.*, 21 (1950), 106—111.

50. Shrikhande S. S., The non-existence of certain affine resolvable balanced incomplete block designs, *Canad. Jour. Math.*, 5 (1953), 413—420.

51. Silverman R., A metrization for power sets with applications to combinatorial analysis, *Canad. Jour. Math.*, 12 (1960), 158—176.

52. Skolem T., Some remarks on the triple systems of Steiner, *Math. Scand.*, 6 (1958), 273—280.

53. Sprott D. A., Note on balanced incomplete block designs, *Canad. Jour. Math.*, 6 (1954), 341—346.

54. Taussky O., Matrices of rational integers, *Bull. Amer. Math. Soc.*, 66 (1960), 327—345.

55. Tinsley M. F., Permanents of cyclic matrices, *Pacific Jour. Math.*, 10 (1960), 1067—1082.

56. Todd J. A., A combinatorial problem, *Jour. Math. Phys.*, 12 (1933), 321—333.

57. Williamson J., Hadamard's determinant theorem and the sum of four squares, *Duke Math. Jour.*, 11 (1944), 65—81.

58. Williamson J., Note on Hadamard's determinant theorem, *Bull. Amer. Math.* Soc., 53 (1947), 608—613.

СОВЕРШЕННЫЕ РАЗНОСТНЫЕ МНОЖЕСТВА

1. Совершенные разностные множества. Пусть $D = \{d_1, d_2, \ldots, d_k\}$ — k-множество целых чисел по модулю v и такое, что всякое число $a \not\equiv 0 \pmod{v}$ может быть выражено λ способами в виде

$$d_i - d_j \equiv a \pmod{v}, \tag{1.1}$$

где d_i и d_j — элементы D. Предположим далее, что

$$0 < \lambda < k < v - 1. \tag{1.2}$$

Эти неравенства служат только для того, чтобы исключить некоторые вырожденные конфигурации. Множество D, для которого эти требования выполняются, называется *совершенным разностным множеством* или, короче, *разностным множеством*. Нетрудно проверить, что

$$\lambda = \frac{k(k-1)}{v-1}. \tag{1.3}$$

Это утверждение непосредственно вытекает из следующей теоремы:

Теорема 1.1. *Совершенное разностное множество D эквивалентно (v, k, λ)-конфигурации с циркулянтом в качестве инцидентной матрицы.*

Доказательство. Дано v-множество X целых по модулю v чисел: $0, 1, \ldots, v-1$, а также задано разностное множество D. Определим v разностных множеств

$$D_e = \{d_1 + e, d_2 + e, \ldots, d_k + e\} \qquad (e = 0, 1, \ldots, v-1), \tag{1.4}$$

где каждое D_e есть k-подмножество множества X, а $D = D_0$. Из определения разностного множества сразу следует, что каждое пересечение $D_e \cap D_f$ при $e \neq f$ является

λ-подмножеством множества X. Следовательно, подмножества (1.4) являются (v, k, λ)-конфигурациями. Более того, матрица инцидентности для подмножеств $D_0, D_1, \ldots, D_{v-1}$ множества X есть циркулянт. Нетрудно доказать и обратное предложение.

Из предыдущей теоремы ясно, что разностные множества могут быть рассмотрены как частные виды (v, k, λ)-конфигураций, и, следовательно, теорема 3.1 гл. 8 справедлива для разностных множеств. Однако произвольная (v, k, λ)-конфигурация, вообще говоря, не соответствует разностному множеству. В самом деле, известны различные значения v, k и λ, для которых (v, k, λ)-конфигурации существуют, а разностные множества — нет. Для построения разностных множеств применимо большое число разных методов. Разностное множество, для которого $\lambda = 1$, называется *плоским*. Плоское разностное множество, для которого $n = k - \lambda$, приводит к проективной плоскости порядка n. Проективная плоскость этого вида называется *циклической*. Зингер построил циклические проективные плоскости всех порядков вида $n = p^\alpha$, где p — простое, а α — натуральное числа. Есть предположение, что всякая конечная циклическая проективная плоскость должна иметь порядок $n = p^\alpha$. Справедливость этого предположения установлена для $n \leqslant 1600$. Упомянем попутно и о другом предположении, что каждая конечная циклическая проективная плоскость есть дезаргезиан. В самом деле, из этого предположения следует, что $n = p^\alpha$, но мы не пытаемся здесь продолжать обсуждение интересной темы о дезарговых плоскостях. Следующая таблица показывает плоские разностные множества для нескольких первых значений n:

n	v	Плоское разностное множество
2	7	{0, 1, 3}
3	13	{0, 1, 3, 9}
2^2	21	{0, 1, 4, 14, 16}
5	31	{0, 1, 3, 8, 12, 18}
7	57	{0, 1, 3, 13, 32, 36, 43, 52}
2^3	73	{0, 1, 3, 7, 15, 31, 36, 54, 63}
3^2	91	{0, 1, 3, 9, 27, 49, 56, 61, 77, 81}
11	133	{0, 1, 3, 12, 20, 34, 38, 81, 88, 94, 104, 109}.

Обзор разностных множеств с параметрами v, k, λ был проделан для k, лежащего в отрезке

$$3 \leqslant k \leqslant 50. \tag{1.5}$$

Пусть v, k, λ — целые параметры, удовлетворяющие (1.3), (1.5) и

$$k < \frac{v}{2}. \tag{1.6}$$

Последнее утверждение не ведет к ограничению общности, поскольку дополнение к разностному множеству само есть разностное множество. Указанным требованиям удовлетворяют 268 выборов значений v, k и λ. Теорема 3.1 гл. 8 исключает (v, k, λ)-конфигурации в 101 случае. Разумеется, это означает, что разностные множества для этих 101 случаев не существуют. В оставшихся 167 случаях доказано существование разностных множеств в 46 и несуществование в 109 выборках. Таким образом, существование разностных множеств осталось невыясненным только в 12 случаях.

Построению разностных множеств посвящено большое число теорем. Докажем здесь следующий элементарный результат.

Теорема 1.2. *Пусть дано простое число* $p \geqslant 7$, *такое, что* $p \equiv 3 \pmod 4$. *Тогда множество* D, *составленное из* $k = (p-1)/2$ *различных квадратичных вычетов* $d_1, d_2, \ldots, d_k \pmod p$, *образует разностное множество с параметрами* $v = p = 4t - 1$, $k = 2t - 1$, $\lambda = t - 1$.

Доказательство. Пусть c — квадратичный вычет p, d_i и d_j — элементы множества D и пусть $d_i - d_j \equiv 1 \pmod p$. Тогда числа $d_i' \equiv c\, d_i \pmod p$ и $d_j' \equiv c\, d_j \pmod p$ также входят в D и удовлетворяют соотношению $d_i' - d_j' \equiv c \pmod p$. С другой стороны, положим, что d_i' и d_j' входят в множество D и пусть

$$d_i' - d_j' \equiv c \pmod p.$$

Тогда числа $d_i \equiv c^{-1} d_i' \pmod p$ и $d_j \equiv c^{-1} d_j' \pmod p$ тоже являются элементами D и удовлетворяют соотноше-

нию $d_i - d_j \equiv 1 \pmod{p}$. Таким образом, совокупность чисел d_i и d_j множества D такая, что $d_i - d_j \equiv 1 \pmod{p}$ является такой же, как и совокупность чисел d_i' и d_j', входящих в D, для которых $d_i' - d_j' \equiv c \pmod{p}$. Более того, если $p \equiv 3 \pmod{4}$ и если c распространяется на $(p-1)/2$ различных квадратичных вычетов по модулю p, то $-c$ распространяется на $(p-1)/2$ различных квадратичных невычетов по модулю p. Итак, $d_i - d_j \equiv c \pmod{p}$ эквивалентно $d_j - d_i \equiv -c \pmod{p}$, чем доказано, что D есть разностное множество.

Разностное множество D порождает адамарову конфигурацию. Матрица инцидентности A этой конфигурации является циркулянтом. Это не означает, что матрица Адамара H порядка $p+1 = 4t$, связанная с A, есть циркулянт. Граничное условие, примененное при получении H из A, разрушает циркулянтное свойство H. Отклонимся немножко и заметим, что матрица Адамара четвертого порядка

$$\begin{bmatrix} 1 & -1 & -1 & -1 \\ -1 & 1 & -1 & -1 \\ -1 & -1 & 1 & -1 \\ -1 & -1 & -1 & 1 \end{bmatrix} \tag{1.7}$$

является циркулянтом. Предполагается, что матрица Адамара порядка $n > 4$ не может быть циркулянтом. Мы докажем, что если H — матрица Адамара порядка n, а H — циркулянт, то n должно быть точным квадратом. В самом деле, пусть J — матрица порядка n, составленная из единиц. Поскольку H — матрица Адамара порядка n, мы имеем $HH^T = nI$, где H^T — транспонированная матрица H. Поскольку H является циркулянтом, имеем $HJ = JH = eJ$, где e — целое число. Следовательно,

$$HH^TJ = e^2J = nJ, \tag{1.8}$$

а это указывает на то, что $n = e^2$.

2. Теорема о множителе. Пусть X есть v-множество целых чисел по модулю v: $0, 1, \ldots, v-1$, и пусть $D = \{d_1, d_2, \ldots, d_k\}$ и $D' = \{d_1', d_2', \ldots, d_k'\}$ суть разностные множества с одними и теми же параметрами v, k, λ.

Зададим целое число t, такое, что $(t, v) = 1$, и произвольное целое s. Тогда $E = \{td_1, td_2, \ldots, td_k\}$ и $E' = \{d_1' + s, d_2' + s, \ldots, d_k' + s\}$, поскольку они являются k-подмножествами множества X, суть разностные множества. Будем теперь искать такие целые числа t и s, чтобы E и E' были одним и тем же k-подмножеством множества X. Предположим, что такие целые числа могут быть определены. Тогда при классификации разностных множеств естественно определить D и D' как одно и то же в смысле изоморфизма разностное множество. Заметим, что такие целые числа t и s не обязательно существуют. Например, нетрудно показать, что для $v = 31$ квадратичные вычеты по модулю 31

$$D = \{1, 2, 4, 5, 7, 8, 9, 10, 14, 16, 18, 19, 20, 25, 28\} \quad (2.1)$$

и разностное множество

$$D' = \{1, 2, 3, 4, 6, 8, 12, 15, 16, 17, 23, 24, 27, 29, 30\} \quad (2.2)$$

не могут быть преобразованы только что описанным методом в одно и то же разностное множество. Здесь мы не будем пытаться исследовать единственность разностных множеств. Однако предшествующие рассуждения имели в виду обосновать идею множителя разностного множества; теперь мы исследуем это понятие несколько подробнее.

Целое число t называется *множителем* разностного множества $D = \{d_1, d_2, \ldots, d_k\}$, если существует целое число s, такое, что $E = \{td_1, td_2, \ldots, td_k\}$ и $E' = \{d_1 + s, d_2 + s, \ldots, d_k + s\}$ являются одним и тем же k-подмножеством множества X. Множитель t должен удовлетворять сравнению $td_i - td_j \equiv 1 \pmod{v}$ для каких-либо i и j; следовательно, всякий множитель удовлетворяет условию

$$(t, v) = 1. \quad (2.3)$$

В терминах предшествующего рассмотрения ясно, что множитель устанавливает изоморфизм разностного множества с самим собой. Всегда имеется тривиальный множитель $t = 1$. Более того, легко проверить, что множи-

тели по модулю v образуют мультипликативную группу. Эта группа называется *группой множителей* разностного множества. Множители были введены в исследование разностных множеств М. Холлом и оказались очень сильным средством для вывода теорем как существования, так и несуществования. К сожалению, теория, которую мы излагаем, не имеет известных аналогий с (v, k, λ)-конфигурациями.

Начнем наше исследование множителей с некоторых общих замечаний о сравнениях. Пусть даны полиномы $f(x)$, $g(x)$, $h(x)$ с целыми коэффициентами. Будем писать

$$f(x) \equiv g(x) \pmod{h(x)}, \tag{2.4}$$

если существует полином $k(x)$ с целыми коэффициентами, такой, что $f(x) - g(x) = k(x)\,h(x)$. Пусть теперь заданы произвольные целые числа a и b и натуральное число m. Зададим натуральные числа a' и b', такие, что $a \equiv a' \pmod{m}$ и $b \equiv b' \pmod{m}$. Тогда получим, что $a \equiv b \pmod{m}$ тогда и только тогда, когда $a' \equiv b' \pmod{m}$. Более того, сравнение

$$a \equiv b \pmod{m} \tag{2.5}$$

эквивалентно полиномиальному сравнению

$$x^{a'} \equiv x^{b'} \pmod{x^m - 1}. \tag{2.6}$$

Заменим обозначения в (2.6) на

$$x^a \equiv x^b \pmod{x^m - 1}. \tag{2.7}$$

„Отрицательный“ показатель степени в (2.7) не должен быть причиной путаницы, потому что (2.7) лишь поясняет (2.6). Таким образом, (2.5) справедливо для целых чисел a и b тогда и только тогда, когда (2.7) выполняется для тех же чисел.

Пусть теперь задано разностное множество $D = \{d_1, d_2, \ldots, d_k\}$ с параметрами v, k, λ. Определим

$$\theta(x) \equiv x^{d_1} + x^{d_2} + \ldots + x^{d_k} \pmod{x^v - 1}. \tag{2.8}$$

Поскольку D есть разностное множество, то из этого следует, что

$$\theta(x)\,\theta(x^{-1}) \equiv k + \lambda x + \lambda x^2 + \ldots + \lambda x^{v-1} \pmod{x^v - 1}. \tag{2.9}$$

В самом деле, правая часть (2.9) есть сумма членов вида $x^{d_i - d_j}$ и содержит $x^0 = 1$ точно k раз, а каждую степень x, x^2, ..., x^{v-1} точно λ раз. Положим

$$T(x) = 1 + x + \ldots + x^{v-1}. \tag{2.10}$$

Тогда мы можем переписать (2.9) в виде

$$\theta(x)\,\theta(x^{-1}) \equiv k - \lambda + \lambda T(x) \pmod{x^v - 1}. \tag{2.11}$$

Заметим, что если ε есть v-й корень из единицы и если $\varepsilon \neq 1$, то отсюда следует, что $T(\varepsilon) = 0$ и из (2.11) следует

$$k - \lambda = \theta(\varepsilon)\,\theta(\varepsilon^{-1}). \tag{2.12}$$

Это равенство интересно само по себе: оно показывает нам, что разностные множества приводят к задаче разложения на множители (факторизации), включающей v-е корни из единицы. Возвратимся к множителю t и заметим, что t будет множитель разностного множества D тогда и только тогда, когда

$$\theta(x^t) \equiv x^s \theta(x) \pmod{x^v - 1}. \tag{2.13}$$

В самом деле, показатели степеней в левой части сравнения суть td_1, td_2, ..., $td_k \pmod v$, а в правой — $d_1 + s$, $d_2 + s$, ..., $d_k + s \pmod v$. Теперь мы подготовлены к тому, чтобы доказать следующую теорему.

Теорема 2.1. *Пусть дано разностное множество D с параметрами v, k, λ. Пусть p — простой делитель $k - \lambda$, такой, что $p \nmid v$ и $p > \lambda$. Тогда p является множителем разностного множества D.*

Доказательство. Поскольку D — разностное множество, мы имеем

$$\theta(x)\,\theta(x^{-1}) \equiv k - \lambda + \lambda T(x) \pmod{x^v - 1}. \tag{2.14}$$

Пусть $f(x)$ — произвольный полином с целыми коэффициентами. Из определения $T(x)$ следует

$$f(x)T(x) \equiv f(1)T(x) \pmod{x^v - 1}. \quad (2.15)$$

По условию $p \mid k - \lambda$ и $p \nmid v$. Известно также, что $k - \lambda = k^2 - \lambda v$. Отсюда следует, что $p \nmid k$, так как в противном случае $p \mid \lambda v$ и $p \mid \lambda$, поскольку $p > \lambda$. Таким образом,

$$k^{p-1} \equiv 1 \pmod{p}. \quad (2.16)$$

Все коэффициенты в разложении $\theta(x^p)$, за исключением коэффициентов при x^{pd_1}, x^{pd_2}, ..., x^{pd_k}, делятся на p. Умножим теперь (2.14) на $\theta(x^{p-1})$ и применим (2.15) и (2.16). Тогда мы можем записать результат в виде

$$\theta(x^p)\theta(x^{-1}) \equiv \lambda T(x) + pR(x) \pmod{x^v - 1}, \quad (2.17)$$

где $R(x)$ — полином с целыми коэффициентами. Выражение $\theta(x^p)\theta(x^{-1})$ в формуле (2.17), рассматриваемое как полином степени, меньшей, чем v, имеет целые неотрицательные коэффициенты. Далее, $p > \lambda$, а это означает, что $R(x)$ в той же формуле, рассматриваемое как полином степени, меньшей v, имеет целые неотрицательные коэффициенты. Умножим (2.17) на $\theta(x)$ и применим (2.14) и (2.15). Это даст

$$(k - \lambda)\theta(x^p) \equiv pR(x)\theta(x) \pmod{x^v - 1}. \quad (2.18)$$

Выражения $\theta(x^p)$, $R(x)$ и $\theta(x)$ в этой формуле, рассматриваемые как полиномы степени, меньшей v, имеют целые неотрицательные коэффициенты. Более того, структура (2.18) указывает, что $R(x)$ не может иметь более одного ненулевого члена. Следовательно, $R(x) = ax^s$, где a и s — целые неотрицательные числа. В формуле (2.18) мы можем положить $x = 1$, откуда получается $k - \lambda = pR(1)$. Следовательно,

$$(k - \lambda)\theta(x^p) \equiv (k - \lambda)x^s\theta(x) \pmod{x^v - 1}, \quad (2.19)$$

где p — множитель.

Теорема 2.1 доказывает существование нетривиального множителя для всякого плоского разностного множества, поскольку требования $p \nmid v$ и $p > \lambda$ определенно удовлетворяются в этом случае. В выводе теоремы 2.1 исполь-

зуется ограничение $p > \lambda$. Однако мы предполагаем, что это ограничение не составляет существенной части предположения. К тому же все известные разностные множества имеют $(k - \lambda, v) = 1$, так что можно предполагать, что всякий делитель $k - \lambda$ есть множитель разностного множества.

Сформулируем без доказательства следующее обобщение теоремы о множителе.

Теорема 2.2. *Пусть дано разностное множество D с параметрами v, k, λ. Положим, что d есть делитель $k - \lambda$, что $(d, v) = 1$ и что $d > \lambda$. Пусть t — такое целое число, что для каждого p, простого делителя d, существует целое число j, такое, что $p^j \equiv t \pmod{v}$. Тогда t — множитель разностного множества D.*

Из понятия множителя может быть выведено большое число теорем, заслуживающих внимания. Мы не будем изучать эти результаты. Закончим тем, что на небольшом числе примеров покажем, как можно применить понятие множителя, чтобы решить вопрос о существовании или несуществовании определенных разностных множеств.

Примеры. а) Существует разностное множество с параметрами $v = 37$, $k = 9$, $\lambda = 2$. Пусть $D = \{d_1, d_2, \ldots, d_k\}$ — разностное множество с произвольными параметрами v, k, λ. Будем говорить, что D *фиксировано* множителем t, если $D = \{td_1, td_2, \ldots, td_k\}$. Предположим, что $(t - 1, v) = 1$. Тогда мы утверждаем, что существует u, такое, что разностное множество $D_u = \{d_1 + u, d_2 + u, \ldots, d_k + u\}$ фиксировано t. В самом деле, множитель t отображает разностное множество D_u на разностное множество

$$D_{s+tu} = \{d_1 + s + tu, d_2 + s + tu, \ldots, d_k + s + tu\}. \quad (2.20)$$

Следовательно, множитель оставляет фиксированным разностное множество при u, определенном сравнением

$$(t - 1)u \equiv -s \pmod{v}. \quad (2.21)$$

Рассмотрим теперь разностное множество с параметрами $v = 37$, $k = 9$, $\lambda = 2$. Мы имеем $p = k - \lambda = 7$, $7 \nmid 37$ и $7 > 2$. Следовательно, по теореме 2.1 $p = 7$ есть множитель. Кроме того, $(6, 37) = 1$, так что разностное множество фиксировано числом 7. Мы можем умножить элементы этого разностного множества на соответствующий множитель так, чтобы один элемент

разностного множества был равен 1. Тогда следующие степени числа 7 (mod 37)

$$\{1, 7, 9, 10, 12, 16, 26, 33, 34\} \tag{2.22}$$

должны быть членами разностного множества. Это фактически и есть желаемое разностное множество. Итак, само построение показало, что разностное множество с этими параметрами единственно в смысле изоморфизма.

б) Существует разностное множество с параметрами $v = 23$, $k = 11$, $\lambda = 5$. В этом случае $k - \lambda = 6$, а два простых делителя 6 оба меньше 5. Следовательно, мы не можем применить теорему 2.1 непосредственно. Однако мы имеем $9 \equiv 2^5 \pmod{23}$ и $9 \equiv 3^2 \pmod{23}$. Из этого следует, что $d = 6$ и $t = 9$ удовлетворяют требованиям теоремы 2.2. Следовательно, 9 есть множитель разностного множества. Кроме того, $(8,23) = 1$, так что существует разностное множество, фиксированное числом 9. Мы можем потребовать, чтобы 1 была элементом этого разностного множества. Тогда следующие степени 9 (mod 23)

$$\{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\} \tag{2.23}$$

должны быть членами разностного множества. Это еще один пример единственного разностного множества с заданными параметрами. Нетрудно убедиться, что как 2, так и 3 являются множителями этого разностного множества.

в) Не существует плоского разностного множества с параметрами $v = 111$, $k = 11$, $\lambda = 1$. Это случай циклической проективной плоскости порядка 10. Следуя теореме 2.1, мы узнаем, что $p = 2$ есть множитель. Кроме того, $(1, 111) = 1$, так что существует разностное множество, фиксированное числом 2. Если мы применим множитель 2 к этому разностному множеству, то получим

$$\theta(x^2) \equiv \theta(x) \pmod{x^{111} - 1}. \tag{2.24}$$

Пусть теперь ε — кубический корень из единицы и $\varepsilon \neq 1$. Так как $111 = 3 \cdot 37$, то

$$\theta(\varepsilon^2) = \theta(\varepsilon). \tag{2.25}$$

Из этого следует, что $\theta(\varepsilon) = \theta(\varepsilon^{-1})$ — рациональное. Но тогда по формуле (2.12) выходит, что $k - \lambda = 10$ является квадратом. Следовательно, циклическая проективная плоскость порядка 10 не существует.

ЛИТЕРАТУРА

Классические работы по разностным множествам включают статьи [12] и [4]. Материал п. 2 основан на работах [4] и [6]. Доказательство теоремы 2.2 находится в работе [5].

1. Bruck R. H., Difference sets in a finite group, *Trans. Amer. Math. Soc.*, 78 (1955), 464—481.

2. Evans T. A., Mann H. B., On simple difference sets, *Sankhyā*, **11** (1951), 357—364.
3. Gordon B., Mills W. H., Welch L. R., Some new difference sets, *Canad. Jour. Math.*, **14** (1962), 614—625.
4. Hall M., Jr., Cyclic projective planes, *Duke Math. Jour.*, **14** (1947), 1079—1090.
5. Hall M., Jr., A survey of difference sets, *Proc. Amer. Math. Soc.*, **7** (1956), 975—986.
6. Hall M., Jr., Ryser H. J., Cyclic incidence matrices, *Canad. Jour. Math.*, **3** (1951), 495—502.
7. Hoffman A. J., Cyclic affine planes, *Canad. Jour. Math.*, **4** (1952), 295—301.
8. Hughes D. R., Partial difference sets, *Amer. Jour. Math.*, **78** (1956), 650—674.
9. Lehmer E., On residue difference sets, *Canad. Jour. Math.*, **5** (1953), 425—432.
10. Mann H. B., Some theorems on difference sets, *Canad. Jour. Math.*, **4** (1952), 222—226.
11. Ostrom T. G., Concerning difference sets, *Canad. Jour. Math.*, **5** (1953), 421—424.
12. Singer J., A theorem in finite projective geometry and some applications to number theory, *Trans. Amer. Math. Soc.*, **43** (1938), 377—385.
13. Stanton R. G., Sprott D. A., A family of difference sets, *Canad. Jour. Math.*, **10** (1958), 73—77.
14 Turyn R., Storer J., On binary sequences, *Proc. Amer. Math. Soc.*, **12** (1961), 394—399.
15. Whiteman A. L., A family of difference sets, *Illinois Jour. Math.*, **6** (1962), 107—121.

СПИСОК ОБОЗНАЧЕНИЙ

$s \in S$	s является элементом S
$A \subseteq S$	A есть подмножество множества S
$A \subset S$	A есть собственное подмножество множества S
$P(S)$	Множество всех подмножеств множества S
$\varnothing$	Нулевое множество
$S \cap T$	Пересечение множеств S и T
$S \cup T$	Объединение множеств S и T
n-множество	Конечное множество из $n > 0$ элементов
$S \times T$	Произведение множеств S и T
$(a_1, a_2, \ldots, a_r)$	Упорядоченное r-множество, называемое выборкой объема r, или r-выборкой; r-перестановка из n элементов в случае, когда компоненты различны и выбраны из n-множества
$P(n, r)$	Число r-перестановок из n элементов
$n!$	n-факториал
$G(S)$	Множество всех взаимно однозначных отображений в S на себя
S_n	Симметрическая группа порядка n
$\{a_1, a_2, \ldots, a_r\}$	Неупорядоченная выборка r элементов, не обязательно различных, объема r, или r-выборка; r-подмножество, если компоненты раз-

	личны, r-сочетание из n элементов, если компоненты различны и выбраны из n-множества
$C(n, r) = \binom{n}{r}$	Биномиальный коэффициент
$w(a)$	Вес элемента a
$[x]$	Наибольшее целое число, не превосходящее x
(a, b)	Положительный общий наибольший делитель чисел a и b
$a \mid b$	a делит b
$a \nmid b$	a не делит b
$\varphi(n)$	Эйлеровская φ-функция
$\mu(n)$	Функция Мёбиуса
$\pi(x)$	Число простых чисел, не превышающих x
D_n	Число беспорядков из n элементов
$A = [a_{ij}]$	Прямоугольная таблица, называемая матрицей, если элементы a_{ij} выбраны из поля
A^T	Транспонированная матрица A
$\mathrm{per}(A)$	Перманент матрицы A
$\det(A)$	Детерминант матрицы A
(0,1)-матрица	Матрица, элементами которой являются нули и единицы
I	Единичная матрица
J	Матрица, составленная из единиц
U_n	Числа размещений
C	(0,1)-матрица, в которой единицы расположены на местах: (1,2), (2,3), (3,4), ..., (n, 1), а нули — на всех остальных местах
l_n	Число латинских квадратов порядка n, в которых элементы первой строки и первого столбца расположены в естественном порядке
$P_r(S)$	Множество всех r-подмножеств множества S
$N(q_1, \ldots, q_t, r)$	Минимальное натуральное число в теореме Рамсея

N_m	Минимальное натуральное число в теореме о выпуклых многоугольниках
с. р. п.	Система различных представителей
с. о. п.	Система общих представителей
ρ	Граничный ранг
$R=(r_1,\ r_2,\ \ldots,\ r_m)$	Вектор сумм строк
$S=(s_1,\ s_2,\ \ldots,\ s_n)$	Вектор сумм столбцов
τ	Общее число единиц в (0,1)-матрице
$\mathfrak{A}=\mathfrak{A}(R,\ S)$	Класс всех (0,1)-матриц, вектор сумм строк которых R, а вектор сумм столбцов — S
$\overline{A}$	Максимальная матрица
$S \prec S^*$	S^* мажорирует S
$\widetilde{A}$	Специальная матрица, построенная в $\mathfrak{A}$
$\widetilde{\rho}$	Минимальный граничный ранг матриц в нормализованном классе $\mathfrak{A}$
$\overline{\rho}$	Максимальный граничный ранг матриц в нормализованном классе $\mathfrak{A}$
$N_0(Q)$	Число нулей в (0,1)-матрице Q
$N_1(Q)$	Число единиц в (0,1)-матрице Q
$\widetilde{\sigma}$	Минимальный след матриц в нормализованном классе $\mathfrak{A}$
$\overline{\sigma}$	Максимальный след матриц в нормализованном классе $\mathfrak{A}$
$\varepsilon(\alpha)$	α-ширина
$\widetilde{\varepsilon}(\alpha)$	Минимальная α-ширина матриц в нормализованном классе $\mathfrak{A}$
$\overline{\varepsilon}(\alpha)$	Максимальная α-ширина матриц в нормализованном классе $\mathfrak{A}$
$\mathfrak{A}(K,\ K)$	Класс, в котором $R=S=K=(k,\ k,\ \ldots,\ k)$
$GF(p^a)$	Поле Галуа
π	Проективная плоскость

B	Матрица порядка v, в которой элементы на главной диагонали равны k, а все остальные элементы равны λ
H	Матрица Адамара
$A \times A'$	Прямое произведение A и A'
$S \overset{c}{=} S'$	S конгруентна S'
$A \dot{+} A'$	Прямая сумма A и A'
$D = \{d_1, d_2, \ldots, d_k\}$	Совершенное разностное множество
t	Множитель разностного множества
$\theta(x)$	$x^{d_1} + x^{d_2} + \ldots + x^{d_k} \pmod{x^v - 1}$
$T(x)$	$1 + x + \ldots + x^{v-1}$.

ИМЕННОЙ УКАЗАТЕЛЬ

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

ОГЛАВЛЕНИЕ

Г. Дж. Райзер

КОМБИНАТОРНАЯ МАТЕМАТИКА