SURVEYS IN APPLIED MATHEMATICS
IV: SOME ASPECTS OF ANALYSIS AND PROBABILITY
A SURVEY OF COMBINATORIAL ANALYSIS

BY

MARSHALL HALL, JR.,

(The Ohio State University)

NEW YORK

JOHN WILEY AND SONS, INC.

1958

БИБЛИОТЕКА СБОРНИКА «МАТЕМАТИКА»

М. ХОЛЛ

КОМБИНАТОРНЫЙ АНАЛИЗ

Перевод с английского
К. А. РЫБНИКОВА

ИЗДАТЕЛЬСТВО
ИНОСТРАННОЙ ЛИТЕРАТУРЫ
Москва 1963

В комбинаторном анализе исходят из рассмотрения множеств дискретных элементов, к которым применяются комбинаторные операции упорядочения и выбора. Формирование общей теории комбинаторного анализа, способной охватить огромное количество задач, которые решаются в различных отделах математики применением комбинаторных суждений, еще не завершено. Литературы на русском языке по комбинаторному анализу еще нет.

Настоящая книга Маршалла Холла младшего — американского математика, известного советскому читателю по переводу его книги „Теория групп",— является обзором современного состояния теории комбинаторного анализа в области теорем перечисления и выбора, а также построения различных схем. Автор отметил задачи и направления, наиболее перспективные с его точки зрения. В тексте рассматриваются задачи из теории чисел, теории конечных групп, геометрии и топологии.

Книга представляет интерес для широкого круга математиков-специалистов, в особенности для тех, кто занимается прикладными вопросами и желает применить комбинаторный аппарат современной математики.

Редакция литературы по математическим наукам

ПРЕДИСЛОВИЕ К РУССКОМУ ИЗДАНИЮ

Комбинаторный анализ — новая математическая дисциплина. Он вырастает из совокупности приложений методов комбинаторного характера в различных областях математики: теории вероятностей, геометрии, теории чисел, вычислительной математики и др. Исходной позицией комбинаторного анализа является рассмотрение множеств дискретных элементов, относительно которых введены комбинаторные операции упорядочения и выбора. Многочисленность и разнообразие задач, для решения которых в наше время применяется комбинаторный анализ, придают этому разделу математики многоплановость.

Роль комбинаторного анализа в математике быстро возрастает. Она определяется теоретической и практической значимостью, которую комбинаторные методы приобрели как часть так называемой конечной математики.

Строго говоря, называть комбинаторный анализ новым отделом математики можно только условно. Издавна известные приемы элементарной комбинаторики к концу XVII века преобразовались в математический аппарат логических суждений (Г. В. Лейбниц) и теории вероятностей (Я. Бернулли). Примерно через сто лет, в конце XVIII — начале XIX века, в германских государствах Европы была предпринята попытка создать комбинаторный анализ как единую математическую науку. Этому отдали много сил немецкие математики (К. Ф. Гинденбург, Я. Штейнер, Эшенбах, Роте и др.). Несоответствие, обнаружившееся между громоздким символическим аппаратом и слабыми еще оперативно-вычислительными возможностями, приостановило развитие этой науки. Комбинаторная школа к середине XIX века распалась, и само название „комбинаторный анализ“ постепенно было забыто.

Предлагаемый советскому читателю обзор [1], составленный американским математиком Маршаллом Холлом, приоткрывает возможности возрождаемого комбинаторного анализа и указывает направления, в которых, по мнению автора, наиболее важен и вероятен успех. В этом основное значение настоящего издания.

Обзор неполон. В нем не нашли отражения комбинаторный аппарат теории вероятностей, теории программирования и многие другие вопросы. Сведения о состоянии работ в области современного комбинаторного анализа отрывочны. Однако необходимо учитывать, что комбинаторный анализ находится в стадии формирования, что этот процесс протекает бурно и что в направлении консолидации его структуры предстоит еще большая работа.

По нашему мнению, неудачно написана гл. I, являющаяся по характеру изложения скорее заключительной, нежели вводной. Однако мы сохранили ее текст, чтобы советские читатели могли познакомиться с мыслями автора и со структурой комбинаторного анализа in statu nascendi.

К. А. Рыбников

---

[1]) Обзор опубликован в IV томе серии Surveys in applied mathematics, вышедшем под названием «Some aspects of analysis and probability».

ГЛАВА I

ВВЕДЕНИЕ И РЕЗЮМЕ

1. Введение

Содержание комбинаторного анализа нелегко определить Его можно сравнить с теорией чисел в том отношении, что он возник из совокупности разнообразных задач, которые даже в наше время не охватываются никакой единой теорией или методом. Делая попытку дать определение, будем говорить, что в комбинаторном анализе рассматриваются задачи о расположениях элементов в соответствии с точно определенными правилами и выясняется, сколькими путями такие расположения могут быть осуществлены.

Настоящая работа состоит из трех основных разделов: а) методы перечисления; б) теоремы выбора; в) существование и построение схем.

В комбинаторной задаче, указывая правила, согласно которым строятся расположения, логически мы обязаны поставить вопрос, можно ли такие расположения вообще осуществить; если можно, то как перейти к построению расположений, и, наконец, сколько существует различных решений. Если задача состоит в том, чтобы записать положительное целое число в виде суммы трех целых положительных чисел, то как вопрос о существовании решений, так и метод нахождения их являются по существу тривиальными. Таким образом, основной задачей является нахождение числа решений. При этом мы должны условиться о том, какие решения считать различными; так, в примере, который мы рассматриваем, должно быть точно указано, будем ли мы различать суммы трех целых чисел, отличающиеся лишь порядком слагаемых.

Большинство задач о перечислении таковы, что для них вопрос о существовании и построении решений по существу тривиален. Однако следует оговориться, что тривиальные методы построений могут оказаться чересчур

трудоемкими. Как и следует ожидать, для отыскания менее громоздких методов необходимы дополнительная теория и значительное мастерство. Именно в этом состоит трудность задачи о коммивояжере. В этой задаче дана таблица расстояний между всеми парами из n городов. Требуется отыскать такой циклический маршрут, пересекающий все города и возвращающийся в начальную точку, который был бы минимальным по общему расстоянию. Тривиальный метод состоит в испробовании всех $(n-1)!$ маршрутов и выборе кратчайшего. Но проблема нахождения решения с помощью меньшего числа испытаний не решена.

Теоремы выбора являются по своей природе теоремами существования. Дано множество объектов и требуется выбрать подмножество с некоторыми твердо установленными свойствами. В упомянутых теоремах рассматриваются необходимые и достаточные условия того, чтобы этот выбор был возможным.

Так, в теореме о различных представителях, доказанной Филиппом Холлом, утверждается, что если даны n множеств $S_1, S_2, \ldots, S_n$ некоторых объектов, то будут существовать различные представители $a_1, a_2, \ldots, a_n$ этих множеств, где a_i — элемент S_i и $a_i \neq a_j$, если $i \neq j$, при соблюдении, очевидно, необходимого условия, что среди всех элементов любых k множеств $(1 \leqslant k \leqslant n)$ найдутся по меньшей мере k различных.

Эти теоремы интересны сами по себе, а также важны для построения расположений. Гофман недавно показал, что многие из этих теорем вытекают из теоремы двойственности в линейном программировании.

В задачах о существовании и построении схем мы имеем дело по большей части с тактическими конфигурациями. В тактической конфигурации мы хотим построить из v объектов b блоков, каждый из которых состоит из k объектов, таких, что всякая комбинация объектов будет встречаться одинаково часто в каждом блоке. Эти схемы могут быть охарактеризованы определенными параметрами; относительно параметров существует несколько необходимых условий, обычно легко находимых. В некоторых случаях необходимые условия являются также достаточными, а в других — заведомо нет. В случае уравновешенной неполной блок-схемы требуется расположить v объектов в b бло-

ках по k объектов в каждом, так что каждый объект будет встречаться в r блоках, а каждая пара объектов будет попадаться всего λ раз. Здесь необходимые условия $bk = vr$ и $r(k-1) = \lambda(v-1)$ легко находятся. Первое — подсчетом всего количества появлений объектов в схеме (учитывая, с одной стороны, что b блоков содержат по k объектов каждый, а с другой стороны, что объектов всего v и каждый из них встречается r раз). Чтобы найти второе условие, заметим, что отдельный объект встречается в r блоках с $k-1$ другими объектами; с другой стороны, требуется, чтобы он встречался λ раз с $v-1$ оставшимися объектами, отсюда $r(k-1) = \lambda \times \times (v-1)$. Например, в случае систем троек Штейнера $k=3$, $\lambda=1$, и мы имеем $3b = vr$, $2r = v-1$. Здесь $r = (v-1)/2$, $b = v(v-1)/3$.

Следовательно, v должно быть вида $6t+1$ или $6t+3$. Справедливо и обратное: для каждого числа v вида $6t+1$ или $6t+3$ существует система троек Штейнера. С другой стороны, для конечных проективных плоскостей порядка n мы имеем $\lambda=1$; $k=r=n+1$; $v=b=n^2+n+1$. Здесь возможен не всякий порядок n. Если n — простое число или степень простого, то существует по меньшей мере одно решение; до настоящего времени неизвестны решения для чисел n другого вида. Установлено, что существует бесконечно много порядков, которые невозможны, начиная с $n=6$, 14, 21, 22 .... Это целые числа, сравнимые с 1 или 2 по модулю 4 и не имеющие вида $n=x^2+y^2$, при целых x и y. Первый неопределенный случай — это $n=10$; вплоть до настоящего времени он остался неразрешимым даже с помощью быстродействующих вычислительных машин.

Следует заметить, хотя это и будет очевидным для читателя, что настоящий обзор не является исчерпывающим. Материал подобран с таким расчетом, чтобы проиллюстрировать задачи и методы рассматриваемой области математики. Наибольшее внимание уделено недавним исследованиям, которые, по-видимому, обещают дать далеко идущие результаты.

2. Общие направления и итоги

Комбинаторный анализ является относительно новой ветвью математики, и справедливо было бы утверждать, что только в последние десять лет были развиты достаточно общие и эффективные методы. Некоторые из ранее существовавших задач предлагались как курьезы, например задача о 36 офицерах, поставленная Эйлером в 1779 г. Интерес к системам троек вырос из проблем алгебраической геометрии, восходящих к Штейнеру. Позже блок-схемы были использованы для статистического исследования контрольных испытаний. Исследования по основаниям геометрии привели к изучению конечных геометрических систем, которые сами являются комбинаторными схемами. Многие проблемы теории групп, в частности исследование мультипликативных транзитивных групп, по своей природе являются комбинаторными.

В последние годы были подвергнуты активному исследованию комбинаторные задачи весьма практического характера. Так, в Университете Дж. Вашингтона были изучены транспортные задачи, в частности составление расписания движения судов. «Дженерал электрик компани» использует быстродействующие вычислительные машины для составления плана распределения своей продукции. Была решена задача о распределении должностей, что явилось шагом к решению задачи о коммивояжере, которая интенсивно изучалась в «Рэнд корпорейшен». К этим задачам были применены методы теории игр и линейного программирования.

Первые работы по применению быстродействующих вычислительных машин к отдельным задачам были выполнены Лемерсом и Томпкинсом. Для проектного задания, предложенного летом 1955 г. Национальным научным фондом, автору удалось использовать машину СВАК [1] в Калифорнийском университете (Лос-Анжелес), чтобы построить большое число новых комбинаторных схем.

На первом этапе развития комбинаторного анализа ком-

---

[1] SWAC — National Bureau of Standarts, Western Automatic Computer.— *Прим. перев.*

бинаторные методы включали тождества для биномиальных коэффициентов, весьма ограниченные технические приемы и рекуррентные методы. Для этой части теории наилучшим источником является книга Нетто [7]. В конце XIX века школа английских математиков, в которой наиболее выдающейся фигурой был Мак-Магон старший, добилась существенного продвижения, используя производящие функции и операторы для получения формальных алгебраических и аналитических выражений комбинаторных величин. Хотя этот подход был весьма общим, он не мог рассматриваться как эффективный, за исключением некоторых специальных случаев. Если производящая функция оказывается элементарной или, как в случае функции распределения, принадлежит к хорошо известному классу трансцендентных функций, то может быть сделано многое. Но в большинстве случаев непосредственная погоня за построением формального аппарата более утомительна, нежели простое перечисление.

Школа индийских статистиков с 1935 г. проделала большую работу в области блок-схем. Их методы были весьма искусными и эффективными. С тех пор как Бозе перешел в Университет Северной Каролины, многие из его американских учеников, в особенности Коннор, добились значительных успехов.

Число американских математиков, которые начали в течение последних нескольких лет заниматься комбинаторным анализом, возрастает. Некоторые из них, включая Брука, Ризера и автора, пришли к этому кругу вопросов, исходя из исследований по основаниям геометрии и соответствующих задач в неассоциативных алгебрах. Лемерса привела к этим проблемам теория чисел. Другие, в особенности Томпкинс, Флуд, Кун и Гофман, встретились с комбинаторным анализом, изучая логику, линейное программирование и теорию игр.

Интерес русских к комбинаторному анализу, по-видимому, невелик, насколько об этом можно судить по опубликованным работам. Хотя Л. А. Скорняков и другие были весьма активны в исследованиях по основаниям геометрии, они мало сделали в области финитной геометрии, которая имеет истинно комбинаторный характер. П. К. Рашевский выполнил одну работу по конфигурациям

Фано элементарной природы. Наиболее обширная работа комбинаторного характера — это работа М. А. Гаврилова о релейно-контактных схемах. Он написал большое число статей и собрал их в книгу „Теория релейно-контактных схем", опубликованную Издательством Академии наук в Москве в 1950 г. В этой книге много места уделено декодированию цепей и применениям булевой алгебры к анализу цепей.

ГЛАВА II

МЕТОДЫ ПЕРЕЧИСЛЕНИЯ

1. Общие замечания

Главными средствами для подсчета числа решений комбинаторных задач являются: 1) перестановки и сочетания; 2) производящие функции; 3) рекуррентные методы и 4) графические методы. В задачах, решения которых легко построить, могут тем не менее возникнуть большие трудности при подсчете числа решений в связи с различным определением эквивалентности решений. Так, задача представления целого числа n в виде суммы неотрицательных целых чисел

$$n = a_1 + a_2 + \ldots + a_r \quad (r = 1, \ldots, n), \tag{1}$$

как нетрудно показать, имеет 2^{n-1} решений, если целые числа $a_1, a_2, \ldots, a_r$ рассматриваются как упорядоченное множество. Но, если они берутся в виде неупорядоченного множества, то число представлений $p(n)$ является гораздо более сложной функцией. По-видимому, имеет место общее правило, по которому упорядоченные решения задачи легче перечислить, нежели неупорядоченные. Наконец, в задачах перечисления всегда возникает вопрос о том, какие из ответов являются подходящими. Для функции $p(n)$ существуют рекуррентные формулы, хорошо приспособленные для вычисления ее последовательных значений, а также бесконечные ряды. Рекуррентные формулы наиболее полезны для составления таблиц значений $p(n)$, тогда как ряды дают информацию о порядке величины $p(n)$, а также удобны для вычисления отдельных значений.

2. Перестановки и сочетания

Упорядоченное множество r объектов $a_1, \ldots, a_r$, выбранных из множества n объектов, называется перестановкой n элементов, взятых по r. Если все выбранные объекты раз-

личны, число перестановок будет

$$_nP_r = n(n-1)(n-2)\ldots(n-r+1).$$

Если допускаются повторения, то этим числом будет n^r. Так, число перестановок из 5 букв *abcde*, взятых по три, есть $5\cdot4\cdot3=60$, если буквы выбираются различными, и $5^3=125$, если допускаются повторения. Неупорядоченное множество r объектов, выбранных из множества n объектов, называется сочетанием из n элементов по r. Если мы отыскиваем число сочетаний различных объектов, то, поскольку каждое сочетание встречается $r!$ раз в перестановке, число их будет равно

$$_nC_r = \frac{n(n-1)\ldots(n-r+1)}{r(r-1)\ldots1} = \frac{n!}{r!\,(n-r)!} = \binom{n}{r}, \qquad (2)$$

т. е. биномиальному коэффициенту. Но если допускаются повторения, мы не можем найти это число, деля n^r на соответствующие делители, так как перестановки приводят к сочетаниям различной кратности. Так, в сочетаниях из 5 букв по 3 сочетание *aaa* возникает из единственной перестановки, *aab* — из 3 перестановок и *abc* — из 6 перестановок. Чтобы найти это число, мы вынуждены прибегнуть к некоторому искусственному приему. Присоединим все множество к каждому сочетанию и перепишем полученное множество в порядке следования букв. Так, исходя из сочетания *bbc*, выбранного из множества *abcde*, мы получаем запись *abbbccde*. Эта запись полностью определяется помещением в $n+r-1$ интервалов между буквами $n-1$ отметок, разделяющих различные буквы таким образом: $a\,|\,bbb\,|\,cc\,|\,d\,|\,e$. Число способов, которыми можно это проделать, будет равно

$$\binom{n+r-1}{n-1} = \binom{n+r-1}{r}, \qquad (3)$$

и это есть, следовательно, число сочетаний из n по r с допущением повторений. Эта задача может также рассматриваться, как задача о разбиении, так как если x_i есть число, показывающее, сколько раз берется i-й элемент, то требуется определить число решений уравнения

$$r = x_1 + x_2 + \ldots + x_n \qquad (4)$$

в неотрицательных целых x_i (порядок следования чисел x существен). Если мы добавим единицу к каждому x и положим $y_i = x_i + 1$, то задача будет состоять в том, чтобы найти число решений уравнения

$$n + r = y_1 + y_2 + \ldots + y_n \tag{5}$$

в положительных целых $y_1, \ldots, y_n$. Если мы возьмем $n + r$ точек и сделаем $n - 1$ отметок в $n + r - 1$ интервалах между ними, то мы можем рассматривать y_1 как число точек первого множества, y_2 — второго и т. д., снова получая число $\binom{n+r-1}{n-1}$.

Тот же способ мы можем применить к задаче нахождения r-сочетаний чисел 1, 2, ..., n, не содержащих двух последовательных чисел. Поставим отметки после каждого выбранного числа. Если перед первой отметкой находится x_1 чисел, между первой и второй отметкой — x_2 чисел и, наконец, после последней отметки — x_{r+1} чисел, то мы имеем

$$n = x_1 + x_2 + \ldots + x_{r+1}, \tag{6}$$

где x_1 целое число, не меньшее единицы, $x_2 \ldots x_{r-1}$ суть по меньшей мере два, а x_{r+1} — неотрицательное число. Соответственно

$$\begin{aligned} n - r + 2 &= x_1 + (x_2 - 1) + \ldots + (x_r - 1) + (x_{r+1} + 1) = \\ &= y_1 + \ldots + y_r + y_{r+1}, \end{aligned} \tag{7}$$

что является представлением числа $n - r + 2$ в виде суммы $r + 1$ положительных целых чисел, а число таких представлений равно $\binom{n-r+1}{r}$. Если мы рассматриваем 1, 2, ..., n как цикл, то чтобы получить число выборок r элементов, не содержащих двух последовательных, мы должны исключить из вышеуказанного числа выборок те, которые включают единицу и n. Это — решения для случая $y_1 = 1$ и $y_{r+1} = 1$, и мы получаем уравнение $n - r = y_2 + \ldots + y_r$, которое имеет $\binom{n-r-1}{r-2}$ решений в натуральных числах. Таким образом, в циклическом случае возможны $\frac{n}{r}\binom{n-r-1}{r-1}$ выборок.

Итак, многие перечисления могут быть найдены посредством подсчета сочетаний, соответствующих прямо или косвенно данной задаче. Они приводят к биномиальным или полиномиальным коэффициентам. Многие задачи могут быть разбиты на несколько отдельных задач, решениями каждой из которых служат некоторые биномиальные коэффициенты, так что решение первоначально поставленной задачи является суммой биномиальных коэффициентов. Поэтому даже решение простой задачи может потребовать вычисления таких сумм. Существует много тождеств, включающих биномиальные коэффициенты. Таково, например, тождество

$$\sum_{k=0}^{2n} (-1)^k \binom{2n}{k}^3 = \frac{(-1)^n (3n)!}{(n!)^3}, \tag{8}$$

впервые доказанное Диксоном [3] в 1890 г. и более просто — Лунгреном [5] в 1947 г. Приведем некоторые простые и полезные тождества:

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n, \tag{9a}$$

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0, \tag{9b}$$

$$\sum_{k=1}^{n} k (-1)^k \binom{n}{k} = 0, \quad n \geqslant 1, \tag{9c}$$

$$\sum_{k=r}^{n} k(k-1) \ldots (k-r+1)(-1)^k \binom{n}{k} = 0, \quad n \geqslant r. \tag{9d}$$

Первые два тождества следуют из соотношения $(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k$, если положить в нем сначала $x=1$, а затем $x=-1$. Для получения третьего соотношения мы дифференцируем исходное соотношение, а затем полагаем $x=-1$; четвертое же получается r-кратным дифференцированием, после чего x полагается равным -1.

Перестановки и сочетания могут быть применены к перечислениям и косвенным образом, если применить важ-

ную общую формулу, выведенную Сильвестром. Предположим, что n объектов рассматриваются по отношению к некоторым свойствам $A_1, A_2, \ldots, A_n$. Пусть N_i $(i=1, \ldots, N)$ объектов имеют свойство A_i, N_{ij} объектов имеют как свойство A_i, так и A_j, а в более общем виде $N_{i_1 i_2 \ldots i_s}$ объектов имеют все свойства $A_{i_1}, A_{i_2}, \ldots, A_{i_s}$. Тогда, если $N(0)$ есть число объектов, не имеющих ни одного из свойств, то

$$N(0)=n-\sum_i N_i+\sum_{i<j} N_{ij}+\ldots+$$
$$+(-1)^s \sum_{i_1<\ldots<i_s} N_{i_1 \ldots i_s}+\ldots+(-1)^N N_{12\ldots N}. \quad (10)$$

Это доказывается легко[1]. Объект считается один раз в n, если не имеет никаких свойств, и совсем не учитывается во всех остальных членах. Рассмотрим объект, который имеет в точности $t \geqslant 1$ свойств. Тогда он принимается за 1 в общем числе n, за $-t$ в $-\sum_i N_i$, за $\binom{t}{2}$ в $\sum_{i<j} N_{ij}$ и вообще за $(-1)^s \binom{t}{s}$ в члене $(-1)^s \sum_{i_1<\ldots<i_s} N_{i_1 i_2 \ldots i_s}$. Но для $t \geqslant 1$ из тождества (9b) мы имеем

$$1-t+\binom{t}{2}+\ldots+(-1)^s\binom{t}{s}+\ldots=0. \quad (11)$$

Таким образом, всякий объект, не обладающий никаким из свойств, вносит 1 в правую часть формулы (10), а объект, обладающий $t \geqslant 1$ свойствами, вносит 0. Это доказывает формулу. Таким же образом, если $N(r)$ есть число объектов, обладающих точно r свойствами, то

$$N(r)=\sum_{i_1<\ldots<i_r} N_{i_1 \ldots i_r}+\ldots+$$
$$+(-1)^{s-r}\binom{s}{r}\sum_{i_1<\ldots<i_s} N_{i_1 \ldots i_s}+\ldots. \quad (12)$$

[1] Метод, основанный на использовании тождества (10), известен давно. Он известен под различными названиями: метод включения и исключения, метод решета, символический метод, метод перекрестной классификации.— *Прим. перев.*

Здесь объект, обладающий точно r свойствами, вносит 1 в первую сумму и ничего не вносит в остальные. Объект, имеющий в точности $t>r$ свойств, вносит $(-1)^{s-r}\binom{s}{r}\binom{t}{s}$ в сумму $(-1)^{s-r}\binom{s}{r}\sum_{i_1<\ldots<i_s} N_{i_1\ldots i_s}$. Но

$$\sum(-1)^{s-r}\binom{s}{r}\binom{t}{s}=0, \quad t>r, \tag{13}$$

что получается, если в (9d) положить $n=t$ и разделить обе части на $(-1)^r r!$ Таким образом, объекты, имеющие более чем r свойств, вносят 0 в правую часть формулы (12), и эта формула доказана.

Одним из приложений формулы (10) является решение задачи о беспорядке[1]. Мы ищем число перестановок

$$a_1\ a_2\ \ldots\ a_n \tag{14}$$

n чисел $1, 2, \ldots, n$, таких, что $a_i\neq i$ для всех $i=1, 2, \ldots, n$. Рассмотрим множество S всех $n!$ перестановок $b_1\ b_2\ \ldots\ b_n$, и пусть свойство A_i состоит в том, что $b_i=i$. Тогда для всяких $i_1<\ldots<i_s$

$$N_{i_1\ldots i_s}=(n-s)!,$$

поскольку они являются перестановками, в которых s объектов закреплены в своих позициях, а остальные объекты свободны. Здесь число беспорядков есть число $N(0)$, и применение формулы (10) дает равенство

$$N(0)=n!-n(n-1)!+\binom{n}{2}(n-2)!+\ldots+$$
$$+(-1)^s\binom{n}{s}(n-s)!\ldots, \tag{15}$$

которое после упрощений имеет вид

$$N(0)=n!\left(1-1+\frac{1}{2!}-\frac{1}{3!}+\ldots+\frac{(-1)^n}{n!}\right), \tag{16}$$

а это есть целое число, ближайшее к $\frac{n!}{e}$.

---

[1] Она называется также задачей о встречах.— *Прим. перев.*

3. Рекуррентные формулы и производящие функции

Число беспорядков для n элементов было впервые найдено Эйлером рекуррентным методом, который можно найти у Нетто [7], стр. 66. Пусть u_n будет числом беспорядков для 1, 2, ..., n. Находим непосредственно, что $u_1=0$, $u_2=1$, $u_3=2$. Предположим, что $a_1, a_2, \ldots, a_n$ — некоторый беспорядок. Тогда $\begin{pmatrix}1 & 2 & \ldots & n\\ a_1 & a_2 & \ldots & a_n\end{pmatrix}$ есть перестановка, переставляющая все буквы. Здесь a_1 может принимать какое-либо одно из $n-1$ значений 2, ..., n. При фиксированном выборе $a_1=j$ мы имеем частичную перестановку

$$\begin{pmatrix}2, & \ldots, & j, & \ldots, & n\\ a_2, & \ldots, & a_j, & \ldots, & a_n\end{pmatrix},$$

где $a_2 \ldots a_n$ суть числа 1, 2, ..., $j-1, j+1, \ldots, n$. Такие частичные перестановки бывают двух типов: те, в которых $a_j \neq 1$, и те, для которых $a_j=1$. Эти типы полностью исчерпывают все виды перестановок и взаимно исключают друг друга. В первом типе мы имеем перестановку

$$\begin{pmatrix}2, & \ldots, & i, & \ldots, & j, & \ldots, & n\\ a_2, & \ldots, & 1, & \ldots, & a_j, & \ldots, & a_n\end{pmatrix} \quad i \neq j,$$

которую можно ассоциировать с беспорядком 2, ..., n

$$\begin{pmatrix}2, & \ldots, & i, & \ldots, & j, & \ldots, & n\\ a_2, & \ldots, & j, & \ldots, & a_j, & \ldots, & a_n\end{pmatrix}.$$

Обратно, если в каком-либо беспорядке 2, ..., n мы заменим нижнее j на 1, то получим частичную перестановку первого типа. Следовательно, их число будет u_{n-1}. Что касается перестановок второго типа $\begin{pmatrix}2, & \ldots, & j, & \ldots, & n\\ a_2, & \ldots, & 1, & \ldots, & a_n\end{pmatrix}$, то, если мы вычеркнем $\begin{pmatrix}j\\ 1\end{pmatrix}$, останется беспорядок 2, ..., $j-1, j+1, \ldots, n$ и число беспорядков будет u_{n-2}. Поскольку u_{n-1} и u_{n-2} не зависят от выбора j и j может принимать $n-1$ различных значений, мы получим $u_n=(n-1)\times(u_{n-1}+u_{n-2})$. Формула приводит к тому же результату, что и другие методы. Обобщая этот метод, Джейкоб

[2] и позднее Керавала [4] нашли рекуррентный прием для нахождения числа трехстрочных латинских прямоугольников. Это число равно $n!\,u_n$, где u_n удовлетворяет соотношению

$$\begin{aligned}(n+3)\,u_{n+5} = {} & (n+4)(n^2+8n+17)\,u_{n+4} + \\ & + (n+3)(n+4)(n^2+8n+17)\,u_{n+3} + \\ & + (n+3)(n+4)(n^2+8n+13)\,u_{n+2} + \\ & + 2(n+2)(n+3)(n+4)(n^2+5n+3)\,u_{n+1} - \\ & - 4(n+1)(n+2)(n+3)(n+4)^2\,u_n,\end{aligned}$$

а первыми значениями будут

$$u_1 = 0,\quad u_2 = 0,\quad u_3 = 2,\quad u_4 = 24,\quad u_5 = 552.$$

Метод Джейкоба и Керавала состоит в исследовании трехстрочных таблиц

$$\begin{array}{cccc} a_1 & a_2 & \dots & a_n, \\ b_1 & b_2 & \dots & b_n, \\ c_1 & c_2 & \dots & c_n, \end{array}$$

в которых во второй и третьей строках используются не обязательно все те же самые буквы, что в первой и второй, но две из этих букв могут быть заменены новыми. Можно рассмотреть шесть различных вариантов таблицы с неповторяющимися значениями в столбце, и для каждого из них будут существовать числа u_n, v_n и т. д. беспорядков. Между ними найдены соотношения, которые и привели к указанному выше рекуррентному приему.

С последовательностью чисел $u_0, u_1, u_2, \dots, u_n, \dots$ мы можем связать степенной ряд $f(x) = u_0 + u_1 x + u_2 x^2 + \dots + u_n x^n + \dots$, который называется *производящей функцией* для u_n. Рекуррентные соотношения для u_n будут часто приводить к определенным соотношениям для $f(x)$, и если нам удастся найти явное выражение этой функции, то мы тогда сможем вычислить u_n. Наоборот, знание свойств функции может привести к рекуррентным соотношениям для u_n; рассматривая $f(x)$ как аналитическую функцию, мы можем применить теорему Коши для вычисления u_n точно или приближенно. На этом этапе комбинаторные задачи становятся по существу аналогичными многим задачам аналитической теории чисел. Иногда более удобно рассматривать

ряды $f(x)=u_0+u_1x+u_2x^2/2!+\ldots+u_nx^n/n!+\ldots$ или даже ряды других типов, включая ряды Дирихле и ряды Ламберта.

Приведем пример, иллюстрирующий этот метод. Отыщем число способов u_n образования бинарного, но неассоциативного произведения n сомножителей, взятых в порядке $a_1a_2\ldots a_n$. Здесь $u_2=1$, а для трех сомножителей мы имеем $(a_1a_2)a_3$ и $a_1(a_2a_3)$, откуда $u_3=2$. Положим формально, что $u_1=1$. Если бинарное произведение является соединением первых r букв, умноженным на некоторое соединение оставшихся $n-r$ букв $(a_1\ldots a_r)(a_{r+1}\ldots a_n)$, то первые r букв можно скомбинировать u_r способами, а остальные $n-r$ букв — u_{n-r} способами. Таким образом, мы получаем рекуррентную формулу для $n\geqslant 2$, $u_n=u_1u_{n-1}+u_2u_{n-2}+\ldots+u_{n-1}u_1$ [1]). Этому соотношению удовлетворяет и соглашение $u_1=1$. Положим, что $f(x)=u_1x+u_2x^2+\ldots+u_nx^n+\ldots$, и, отбросив предосторожности, продолжим рассуждения формально, игнорируя все вопросы о сходимости. Полученная рекуррентная формула эквивалентна формальному соотношению $[f(x)]^2=-x+f(x)$. Решая его как квадратное уравнение, получим $f(x)=(1-\sqrt{1-4x})/2$, где мы ставим знак минус, чтобы иметь ряды без постоянного члена. Теперь, представляя эту функцию степенным рядом, мы найдем, что коэффициент при x^n будет

$$v_n=-\frac{\left(\frac{1}{2}\right)\left(-\frac{1}{2}\right)\cdots\left(\frac{3-2n}{2}\right)(-4)^n}{n!}.$$

Эта формула упрощается и приводится к виду $v_n=[(2n-2)!]/[n!\,(n-1)!]$. Мы можем теперь провести рассуждения в обратном порядке, чтобы проверить себя и заключить, что $u_n=v_n$. Функция $f(x)=(1-\sqrt{1-4x})/2$ — аналитическая в круге $|x|<\frac{1}{4}$, и, следовательно, в ее степенном ряде коэффициент при x^n есть v_n. Теперь внутри круга сходимости функция $[f(x)]^2$ — также аналитическая и, так как $[f(x)]^2=f(x)-x$, мы получаем, сравнивая

[1]) Это выражение иногда называется конволюцией или сверткой.— *Прим. перев.*

коэффициенты при x^n, $n \geqslant 2$, что $v_n = v_1 v_{n-1} + \ldots + v_{n-1} v_1$. Так как $u_1 = v_1 = 1$ и рекуррентное соотношение то же, что и выше, то $u_n = v_n = [(2n-2)!]/[n!\,(n-1)!]$ для всех $n \geqslant 2$.

Если мы имеем линейную рекуррентную формулу с постоянными коэффициентами $u_{n+r} = a_1 u_{n+r-1} + \ldots + a_r u_n$, то легко видеть, что производящая функция $f(x) = u_0 + u_1 x + \ldots + u_n x^n + \ldots$ является рациональной:

$$f(x) = \frac{b_0 + b_1 x + \ldots + b_{r-1} x^{r-1}}{1 - a_1 x - \ldots - a_r x^r},$$

где формулы

$$\begin{aligned} u_0 &= b_0, \\ u_1 &= b_1 - a_1 b_0, \\ u_2 &= b_2 - a_1 b_1 - a_2 b_2, \\ &\ldots\ldots\ldots\ldots \\ u_{r-1} &= b_{r-1} - a_1 b_{r-2} \ldots a_{r-1} b_0 \end{aligned}$$

выражают соотношения между исходными значениями $u_0, \ldots, u_{r-1}$ и производящей функцией. Если $a_r = 0$, мы можем рассматривать рекуррентное соотношение низшего порядка. Взяв

$$\chi(x) = x^r - a_1 x^{r-1} - \ldots - a_r = (x - \alpha_1)^{e_1} \ldots (x - \alpha_s)^{e_s}$$

в качестве характеристического полинома, мы сможем показать, что общее решение задачи дается в виде

$$u_n = A_1(n)\,\alpha_1^n + \ldots + A_s(n)\,\alpha_s^n,$$

где $A_i(n)$ — произвольный полином относительно n степени $e_i - 1$, (e_i — кратность корня α_i).

Мак-Магон в своей двухтомной книге [6] широко развил теорию рекуррентных методов и производящих функций. Здесь нет возможности дать сколько-нибудь удовлетворительное описание этой работы. Однако, быть может, нам удастся передать некоторые особенности его методов.

Если $\alpha_1, \ldots, \alpha_n$ — некоторые неопределенные величины, то

$$f(x) = (x - \alpha_1) \ldots (x - \alpha_n) = x^n - a_1 x^{n-1} + \ldots + (-1)^n a_n,$$

где $a_1, a_2, \ldots, a_n$ — хорошо известные элементарные сим-

метрические функции

$$a_1 = \alpha_1 + \alpha_2 + \ldots + \alpha_n,$$
$$a_2 = \alpha_1\alpha_2 + \ldots + \alpha_{n-1}\alpha_n,$$
$$\ldots\ldots\ldots\ldots$$
$$a_r = \alpha_1\alpha_2 \ldots \alpha_r + \ldots + \alpha_{n-r+1} \ldots \alpha_n,$$
$$\ldots\ldots\ldots\ldots$$
$$a_n = \alpha_1\alpha_2 \ldots \alpha_n.$$

Если $m = c_1 + c_2 + \ldots + c_s$, где $c_1 \geqslant c_2 \geqslant \ldots \geqslant c_s$, есть разбиение целого числа m, то существует симметрическая функция от величин α, связанная с этим разбиением, $h(c_1, \ldots, c_s) = \sum \alpha_{i_1}^{c_1}\alpha_{j_2}^{c_2} \ldots \alpha_s^{c_s}$, где мы берем в точности один член каждого вида. Если мы теперь обозначим h_m сумму $h_m = \sum h(c_1, \ldots, c_s)$, где суммирование ведется по всем разбиениям m, то получим основную симметрическую функцию степени m. Теперь соотношение между h и a не зависит от n:

$$\frac{1}{1 - a_1x - a_2x^2 - a_3x^3 - \ldots} = 1 + h_1x + h_2x^2 + h_3x^3 + \ldots.$$

Отсюда мы вычисляем:

$$h_1 = a_1,$$
$$h_2 = a_1^2 - a_2,$$
$$h_3 = a_1^3 - 2a_1a_2 + a_3,$$
$$h_4 = a_1^4 - 3a_1^2a_2 + a_2^2 + 2a_1a_3 - a_4.$$

Мы можем выразить комбинаторные величины как коэффициенты, возникающие в результате действий над величинами h. Так, если мы хотим, следуя Мак-Магону, найти число способов разбиения семи элементов α, α, α, β, β, γ, δ на множества из четырех и оставшихся трех элементов, то это будет коэффициент $h(3, 2, 1, 1)$ в произведении h_4h_3, где h_4 и h_3 суть функции от четырех неопределенных величин α, β, γ, δ. Этот коэффициент равен 11. Трудность здесь, как и в других случаях, состоит в том, что, хотя комбинаторная величина и представлена как коэффициент, нет никаких указаний на то, как найти его значение. Чтобы дать различные выражения для получаемых здесь функций, необходимы некоторые тождества и теоремы.

Теорема, которую Мак-Магон называет главной теоремой, такова:

Главная теорема. *Если* $X_1, X_2, \ldots, X_n$ *заданы посредством соотношения* $(X_1, X_2, \ldots, X_n) = A(x_1, \ldots, x_n)$, *где* $A = (a_{ij})$ *есть* $n \times n$*-матрица, то коэффициент при* $x_1^{c_1} \ldots x_n^{c_n}$ *в разложении произведения* $X_1^{c_1} \ldots X_n^{c_n}$ *равен коэффициенту при* $x_1^{c_1} \ldots x_n^{c_n}$ *в разложении дроби*

$$\frac{1}{|(1 - a_1x_1)(1 - a_2x_2) \ldots (1 - a_nx_n)|},$$

где знаменатель символический и в его разложении член $a_ia_j \ldots a_t$ *должен быть заменен минором* A, *образованным из* i*-х,* j*-х, ...,* t*-х строк и столбцов* A.

В качестве приложения этой теоремы Мак-Магон вычислил биномиальную сумму $\sum_{k=0}^{2n} (-1)^k \binom{2n}{k}^3$, найденную первоначально Диксоном [3] в 1890 г. и не так давно (в 1947 г.) Лунггреном [5]. Мак-Магон заметил, что $\sum_{k=0}^{m} (-1)^k \binom{m}{k}^3$ — это коэффициент при $x^m y^m z^m$ в выражении $(y-z)^m (z-x)^m (x-y)^m$ и главная теорема применяется для случая $A = \begin{pmatrix} 0 & -1 & 1 \\ 1 & 0 & -1 \\ -1 & 1 & 0 \end{pmatrix}$.

Разлагая знаменатель $|(1 - a_1x)(1 - a_2y)(1 - a_3z)|$ согласно условию, принятому в теореме, получим

$$1 - |a_1|x - |a_2|y - |a_3|z + |a_1a_2|xy + |a_1a_3|xz + |a_2a_3|yz - |a_1a_2a_3|xyz$$

или, после вычисления миноров, $1 + xy + xz + yz$. Следовательно, нам надо отыскать коэффициент при $x^m y^m z^m$ в разложении

$$\frac{1}{1 + xy + xz + yz} = 1 + \sum_{t=1}^{\infty} (-1)^t (xy + yz + xz)^t.$$

Так как каждый член имеет четную степень, то сумма

$\sum_{k=0}^{m}(-1)^k\binom{m}{k}^3$ равна нулю, если m не является четным. Если $m=2n$, т. е. четно, то положим $yz=u^2$, $zx=v^2$, $xy=w^2$, так что $xyz=uvw$, и в разложении дроби $1/(1+u^2+v^2+w^2)$ будем искать коэффициент при $u^{2n}v^{2n}w^{2n}$. Он должен получиться из члена $(-1)^{3n}(u^2+v^2+w^2)^{3n}$, и с помощью полиномиальной теоремы мы сможем найти результат Диксона:

$$\sum_{k=0}^{2m}(-1)^k\binom{2n}{k}^3=(-1)^n\frac{[(3n)!]}{[(n)!^3]}.$$

В качестве частного примера выражения комбинаторных величин через коэффициенты Мак-Магон ([6], т. I, стр. 253) представил как коэффициент число латинских квадратов вида $n\times n$. Если это число обозначить через L_n, то будем иметь

$$\left(\sum a_1a_2^2a_3^4\ldots a_n^{2^{n-1}}\right)^n=\sum\ldots+L_n(a_1\ldots a_n)^{2^{n-1}}+\ldots.$$

Этот результат был выведен посредством операторов. Однако он недостаточно хорошо приспособлен для вычислений, зависящих от n-х степеней суммы $n!$ членов. Большая часть сочинения Мак-Магона посвящена исследованию операторов. Мы вынуждены ограничиться упоминанием двух операторов Хаммонда. Если a_1, ..., a_i являются, как и выше, элементарными симметрическими функциями, то

$$d_s=\frac{d}{(da_s)}+a_1\frac{d}{(da_{s+1})}+a_2\frac{d}{(da_{s+2})}+\ldots$$

есть дифференциальный оператор, применяемый к функциям от a, рассматриваемым как независимые переменные. В свою очередь, если

$$m=e_1p_1+e_2p_2+\ldots+e_rp_r\quad(p_1\geqslant p_2\geqslant\ldots\geqslant p_r)$$

есть разбиение числа m, где e_i — множитель при p_i, то мы введем обозначения $(p_1^{e_1}\ p_2^{e_2}\ldots p_r^{e_r})$ для соответствующей симметрической функции. Тогда операторы D_s определяются так, что

$$D_s(p_1^{e_1}\ p_2^{e_2}\ldots p_r^{e_r})=0,\quad\text{если } s\neq p_i,\ i=1,\ldots,r,$$

и

$$D_{p_i}(p_1^{e_1}\ p_2^{e_2}\ldots p_r^{e_r})=(p_1^{e_1}\ldots p_i^{e_i-1}\ldots p_r^{e_r}).$$

Зависимость между операторами d_s и операторами D_s точно такая же, как зависимость между степенными суммами $P_i = \sum_j a_j^i$ и элементарными симметрическими функциями. Именно, по правилу Ньютона,

$$P_m - a_1 P_{m-1} + a_2 P_{m-2} + \ldots + (-1)^m m a_m = 0,$$
$$d_m - D_1 d_{m-1} + D_2 d_{m-2} + \ldots + (-1)^m m d_m = 0.$$

Существует много взаимозависимостей между этими и другими операторами, но автор не смог найти достаточно примеров, где эти операторы вели бы к результатам, которые легко вычислить.

4. Разбиения

Разбиение положительного целого числа n есть представление этого числа в виде суммы целых положительных чисел $n = a_1 + a_2 + \ldots + a_k$. Здесь почти никогда не возникает вопроса о существовании разбиения; задача обычно состоит в отыскании числа распределений. Интересным примером проблемы существования является гипотеза Гольдбаха о том, что каждое целое четное число $\geqslant 4$ может быть записано как сумма двух простых чисел; однако она, собственно, относится к области теории чисел, хотя при исследовании разбиений трудно разграничить комбинаторные и теоретико-числовые задачи. Мы можем искать число распределений n на определенное число k частей или же оставить это число неуточненным. Мы можем считать существенным или несущественным порядок частей $a_1, a_2, \ldots, a_k$. В силу этого возникают четыре разных вопроса о числе распределений. На два из них, в случаях когда порядок частей существен, ответить легко. Другие два вопроса гораздо более трудны.

Если мы расположим в ряд n единиц и сделаем $k-1$ отметок в $k-1$ промежутках между ними, то ряд единиц разделится на k частей и мы таким образом получим $n = a_1 + a_2 + \ldots + a_k$, где $a_1, a_2, \ldots, a_k$ — числа единиц в каждом отрезке. Следовательно, число решений в данном случае является биномиальным коэффициентом $\binom{n-1}{k-1}$.

Если мы не будем задавать число частей k, то сможем получить упорядоченное распределение, делая отметки либо в каждом промежутке между единицами, либо не в каждом. Это может быть проделано 2^{n-1} способами; следовательно, число упорядоченных разбиений равно 2^{n-1}.

Мы не можем получить число неупорядоченных разбиений, деля число упорядоченных разбиений на подходящий делитель, так как разбиение с повторяющимися частями не дает стольких разбиений, сколько их дает разбиение с тем же числом различных частей.

Назовем $P_k(n)$ число разбиений n на k (неупорядоченных) частей. Очевидно, что $n=n$ есть единственное разбиение на одну часть, так что $P_1(n)=1$. Мы можем найти двойную рекуррентную формулу для $P_k(n)$ следующим образом. Если $n=a_1+a_2+\ldots+a_k$ — разбиение n на k неупорядоченных частей, $n-k=(a_1-1)+(a_2-1)+\ldots+(a_k-1)$ — разбиение $n-k$ на k или меньше частей, так как если $a_i=1$, то $a_i-1=0$. Это соответствие взаимно однозначное, так что $P_k(n)=\sum_{i=1}^{k} P_i(n-k)$. Очевидно, $P_k(k)=1$, так как $k=a_1+\ldots+a_k$ имеет в качестве единственного положительного решения $a_1=a_2=\ldots=a_k=1$. Таким образом, мы можем без труда заполнить таблицу для $P_k(n)$.

k \ n	1	2	3	4	5	6	7	8	9	10
1	1	1	1	1	1	1	1	1	1	1
2		1	1	2	2	3	3	4	4	5
3			1	1	2	3	4	5	7	8
4				1	1	2	3	5	6	9
5					1	1	2	3	5	7
6						1	1	2	3	5
7							1	1	2	3
8								1	1	2
9									1	1
10										1
	1	2	3	5	7	11	15	22	30	42

Из рекуррентных соотношений мы можем найти значения $P_k(n)$ для малых k. Так:

$$P_1(n)=1; \quad P_2(n)=\frac{n}{2}+\frac{1}{4}[(-1)^n-1];$$

$$=\frac{n}{2}, \qquad n\equiv 0\,(2)$$

$$=\frac{n-1}{2}, \qquad n\equiv 1\,(2)$$

$$P_3(n)=\frac{n^2}{12}, \qquad n\equiv 0\,(6)$$

$$=\frac{n^2}{12}-\frac{1}{12}, \quad n\equiv 1\,(6)$$

$$=\frac{n^2}{12}-\frac{1}{3}, \quad n\equiv 2\,(6)$$

$$=\frac{n^2}{12}+\frac{1}{4}, \quad n\equiv 3\,(6)$$

$$=\frac{n^2}{12}-\frac{1}{3}, \quad n\equiv 4\,(6)$$

$$=\frac{n^2}{12}-\frac{1}{12}, \quad n\equiv 5\,(6).$$

Доказательство того, что $p_k(n)=\sum_{i=1}^{k} P_i(n)$ приблизительно равно $\frac{1}{k!}\binom{n-1}{k-1}$, дал Аулук [1] в 1942 г. Этим подтверждается то, что можно было ожидать, а именно: так как для больших значений n в большинстве разбиений n на k частей все части различные, число упорядоченных разбиений, которое равно $\binom{n-1}{k-1}$, приблизительно в $k!$ раз больше, чем число неупорядоченных разбиений.

Общее число $p(n)$ неупорядоченных разбиений n, очевидно, равно $\sum_{i=1}^{n} P_k(n)$. Но это не наилучший способ вычисления $p(n)$. Мы имеем производящую функцию

$$\sum_{0}^{\infty} p(n)\,x^n=\left(\frac{1}{(1-x)}\right)\left(\frac{1}{(1-x^2)}\right)\left(\frac{1}{(1-x^3)}\right)\cdots\left(\frac{1}{(1-x^i)}\right)\cdots.$$

Если мы положим $n=a_1+a_2+\ldots+a_n$, где a_i есть число частей равных i в разбиении n, то непосредственно видно, что в разложении бесконечного произведения

$$(1-x)^{-1}(1-x^2)^{-1}\ldots(1-x^i)^{-1}\ldots=$$
$$=(1+x+x^2+\ldots)(1+x^2+$$
$$+x^4+\ldots)(1+x^3+x^6+\ldots)\ldots(1+x^i+x^{2i}+\ldots)$$

содержится член $x^n=x^{a_1}(x^2)^{a_2}\ldots(x^i)^{a_i}\ldots$, где каждый $(x^i)^{a_i}$ вносится соответствующим множителем $(1-x^i)^{-1}$ и, следовательно, для каждого разбиения имеется в точности один член. Таким образом, доказывается формальное равенство рядов $\sum_0^{\infty} p(n)x^n$ и бесконечного произведения $\prod_{i=1}^{\infty}(i-x^i)^{-1}$. Это равенство будет справедливо, так как бесконечное произведение сходится и является аналитической функцией внутри единичного круга.

Мы уже немного знаем о порядке величины $p(n)$. Теперь заметим, что в упорядоченных разбиениях n на k частей одно неупорядоченное разбиение соответствует самое большее $k!$ упорядоченным распределениям. Следовательно, $P_k(n)>\frac{1}{k!}\binom{n-1}{k-1}$. Так как $p(n)\geqslant\frac{1}{k!}\binom{n-1}{k-1}$ для всякого $k<n$, то $p(n)>C_k n^k$ для некоторой постоянной C_k. Таким образом, $p(n)$ растет быстрее, чем любая степень n. С другой стороны, если бы для некоторой положительной постоянной C и числа $\alpha>1$ мы имели $p(n)>C\alpha^n$, то ряд $\sum p(n)x^n$ расходился бы вне круга радиуса $1/\alpha$, а это противоречит тому факту, что он должен сходиться внутри единичного круга. Таким образом, $p(n)$ возрастает быстрее, чем всякая степень n, и медленнее, чем любая экспоненциальная функция α^n для $\alpha>1$.

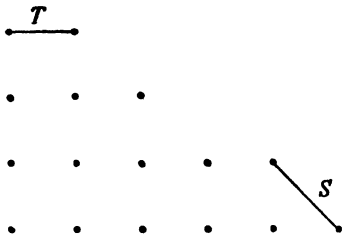
Мы уже заметили, что $\sum p(n)x^n$ эквивалентна бесконечному произведению $\prod_1^{\infty}(1-x^m)$. А это произведение само является производящей функцией $\sum c_n x^n$, где коэффициент c_n имеет комбинаторный смысл.

Очевидно, $c_n=A(n)-B(n)$, где $A(n)$ есть число разбиений n на четное число различных частей, а $B(n)$ есть

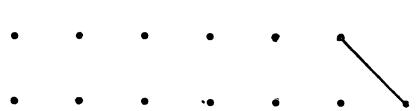
число разбиений n на нечетное число различных частей. Эйлер впервые доказал замечательный факт, что c_n почти всегда есть нуль. Более строго,

$$\prod_{k=1}^{\infty}(1-x^k)=1+\sum_{k=1}^{\infty}(-1)^k x^{(3k^2\pm k)/2}.$$

Приведем здесь комбинаторное доказательство тождества Эйлера, найденное Дж. Франклином [9]. Представим разбиение n на неравные части точечной схемой, где частями будут строки, самая короткая из которых будет наверху, самая длинная — внизу, а левые концы строк образуют вертикальный столбец. Так, разбиение $16=6+5+3+2$ изображается на схеме так:



Буквой T обозначим „верхнюю линию“ и проведем „боковую линию“ S, состоящую из всех точек на прямой, начинающейся с правого конца основания и образующей угол 45° с основанием. В данном случае как T, так и S имеют по две точки. Исходя из этой схемы, мы можем построить любую другую схему одним из двух методов: 1) если $T\leqslant S$, переместить верхнюю линию так, чтобы образовать новую боковую линию; 2) если $T>S$, переместить боковую линию так, чтобы образовать новую верхнюю линию. К приведенной выше схеме применим первый метод и, передвигая верхнюю линию, чтобы образовать новую боковую, получим схему



Она соответствует разбиению $16=7+6+3$. Здесь $T=3$, $S=2$, и, следовательно, применим второй метод, приводящий снова к распределению $16=6+5+3+2$. Эти методы взаимно обратны и, если они применимы, устанавливают взаимно однозначное соответствие между четными и нечетными разбиениями. Для большей точности заметим, что метод 1 применяется, когда $T<S$ или когда $T=S$ и верхняя линия не пересекается с боковой линией; метод 2 применяется, если $T>S+1$ или если $T=S+1$ и верхняя линия не пересекается с боковой. Таким образом, мы имеем взаимно однозначное соответствие между четными и нечетными распределениями на неравные части с двумя исключениями. Первый исключительный случай ($T=S$ и верхняя линия пересекается с боковой) соответствует разбиению вида

$$k+(k+1)+(k+2)+\ldots+(2k-1)=n=\frac{3k^2-k}{2},$$

четность которого совпадает с четностью k. Во втором исключительном случае ($T=S+1$ и верхняя линия пересекается с боковой) разбиение имеет вид

$$(k+1)+(k+2)+\ldots+2k=n=\frac{3k^2+k}{2};$$

четность этого разбиения также совпадает с четностью k. Отсюда $c_n=A(n)-B(n)=0$, если n не имеет вида $(3k^2\pm k)/2$, когда $c_n=(-1)^k$. Это доказывает тождество Эйлера.

Произведя умножение в левой части тождества

$$\left[1+\sum_{k=1}^{\infty}(-1)^k x^{\frac{(3k^2\pm k)}{2}}\right]\cdot[1+p(1)x+p(2)x^2+\ldots$$
$$\ldots+p(n)x^n\ldots]=1,$$

найдем рекуррентное соотношение для $p(n)$:

$$p(n)=p(n-1)+p(n-2)-p(n-5)-p(n-7)+\ldots$$
$$\ldots+(-1)^{k-1}p\left(n-\frac{3k^2\pm k}{2}\right)+\ldots,$$

удобное для вычисления последовательных значений $p(n)$:

$$\begin{aligned}
p(0)&=1,\\
p(1)&=1, & p(11)&=56,\\
p(2)&=2, & p(12)&=77,\\
p(3)&=3, & p(13)&=101,\\
p(4)&=5, & p(14)&=135,\\
p(5)&=7, & p(15)&=176,\\
p(6)&=11, & p(16)&=231,\\
p(7)&=15, & p(17)&=297,\\
p(8)&=22, & p(18)&=385,\\
p(9)&=30, & p(19)&=490,\\
p(10)&=42, & p(20)&=627.
\end{aligned}$$

Изучая значения $p(n)$, индийский математик Рамануджан высказал и впоследствии доказал любопытные предложения:

$$p(5n+4)\equiv 0 \pmod 5; \quad p(7n+5)\equiv 0 \pmod 7;$$
$$p(11n+6)\equiv 0 \pmod{11}.$$

Первые два из них нетрудно доказать, если, кроме тождества Эйлера, мы возьмем другое тождество того же рода, найденное Якоби:

$$\prod_{k=1}^{\infty}(1-x^k)^3 = 1-3x+5x^3-7x^6+\ldots = \sum_{k=0}^{\infty}(-1)^k(2k+1)\,x^{\frac{k(k+1)}{2}}.$$

Обозначим

$$K(x)=x\prod_{k=1}^{\infty}(1-x^k)^4 = x\prod_{k=1}^{\infty}(1-x^k)\prod_{k=1}^{\infty}(1-x^k)^3 = x\sum_{k=-\infty}^{+\infty}(-1)^k x^{\frac{3k^2+k}{2}}\sum_{t=0}^{\infty}(-1)^t(2t+1)\,x^{\frac{t(t+1)}{2}}.$$

Здесь в ряде для $K(x)$ мы имеем член с x^{5n+5}, когда

$$\frac{3k^2+k}{2}+\frac{t(t+1)}{2}+1=5n+5\equiv 0 \pmod 5.$$

Это приводит к соотношению

$$2(k+1)^2+(2t+1)^2\equiv 0 \pmod 5,$$

где как $k+1$, так и $2t+1$ сравнимы с 0 по модулю 5. Но коэффициент при таком члене равен $(-1)^{k+t}(2t+1)$, и, таким образом, он кратен 5. Отсюда в $K(x)$ коэффициент каждого члена с x^{5n+5} кратен 5. Теперь $(1-x^k)^5\equiv$ $\equiv(1-x^{5k}) \pmod 5$, а из этого следует, что $\frac{1-x^{5k}}{(1-x^k)^5}\equiv$ $\equiv 1 \pmod 5$. Это означает, что коэффициенты степенного ряда $K(x)$ суть целые и кратные 5, за исключением свободного члена, который равен единице. Следовательно, коэффициент при x^{5n+5} в разложении

$$\frac{x(1-x^5)(1-x^{10})\dots}{(1-x)(1-x^2)\dots}=$$

$$=x(1-x)^4(1-x^2)^4\dots\left(\frac{(1-x^5)(1-x^{10})\dots}{(1-x)^5(1-x^2)^5\dots}\right)$$

кратен 5 так же, как и коэффициент при x^{5n+5} в разложении

$$\frac{x}{(1-x)(1-x^2)(1-x^3)\dots},$$

который равен $p(5n+4)$, откуда $p(5n+4)\equiv 0 \pmod 5$.

Таким же способом мы можем доказать, что $p(7n+5)\equiv$ $\equiv 0 \pmod 7$, рассматривая в правой части разложения

$$x^2[(1-x)(1-x^2)\dots]^6=x^2(1-3x+5x^2-7x^6\dots)^2$$

член с показателем $7n+7$, возникающим из показателей $2+\frac{k(k+1)}{2}+\frac{t(t+1)}{2}$, и с коэффициентом, равным $(-1)^{k+t}(2k+1)(2t+1)$. Но здесь из сравнения

$$2+\frac{k(k+1)}{2}+\frac{t(t+1)}{2}\equiv 0 \pmod 7$$

вытекает, что

$$(2k+1)^2+(2t+1)^2\equiv 0 \pmod 7,$$

откуда

$$2k+1\equiv 2t+1\equiv 0 \pmod 7.$$

Дальнейшие рассуждения проходят аналогично. Столь же простого доказательства сравнения

$$p(11n+6)\equiv 0 \pmod{11},$$

по-видимому, не существует. Это зависит от более глубоких свойств эллиптических и модулярных функций.

Существуют и другие любопытные арифметические свойства $p(n)$. Тождества Роджера — Рамануджана выражают два из них:

$$1+\frac{x}{1-x}+\frac{x^4}{(1-x)(1-x^2)}+\ldots+\frac{x^{m^2}}{(1-x)(1-x^2)\ldots(1-x^m)}+\ldots=\frac{1}{(1-x)(1-x^6)\ldots(1-x^4)(1-x^9)\ldots}$$

и

$$1+\frac{x^2}{1-x}+\frac{x^6}{(1-x)(1-x^2)}+\ldots+\frac{x^{m(m+1)}}{(1-x)(1-x^2)\ldots(1-x^m)}+\ldots=\frac{1}{(1-x^2)(1-x^7)\ldots(1-x^3)(1-x^8)\ldots}.$$

Показатели в знаменателях справа образуют в каждом случае две арифметические прогрессии с разностью 5. Эти прогрессии были найдены в 1894 г. английским математиком Роджером, а позднее независимо — Рамануджаном. Харди [10] в своих лекциях о Рамануджане подчеркивает, что удивительное в этих формулах заключается в числе 5; ряды слева имеют сравнительно хорошо известный вид. Правая часть первого тождества перечисляет разбиения n на части вида $5k+1$, $5k+4$, а левая часть — разбиения n на части с минимальной разностью 2. В левой части член с показателем степени n появляется тогда, когда $n=m^2+a_1+2a_2+\ldots+ma_m$, что соответствует разбиению

$$n=(m-1+a_m+a_{m-1}+\ldots+a_2+a_1)+(m-3+a_m+a_{m-1}+\ldots+a_2)+\ldots\ldots+(3+a_m+a_{m-1})+(1+a_m),$$

которое является разбиением n на m частей с минимальной

разностью 2, и, наоборот, разбиение на части с минимальной разностью 2 имеет единственное представление этого вида. Аналогично, так как $m(m+1)=2+4+\ldots+2m$, левая сторона второго тождества перечисляет разбиения на части с минимальной разностью 2, где наименьшая часть будет по крайней мере 2, и тождество указывает, что число таких разбиений равно числу разбиений n на части вида $5k+2$, $5k+3$.

Одной из наиболее интересных частей теории разбиений является исследование асимптотического поведения $p(n)$. Мы будем следовать лекциям Харди о Рамануджане, где дан превосходный обзор работ в этой области. Первым приближением является $p(n) \sim \exp\left(\pi \sqrt{\frac{2}{3}} n^{1/2}\right)$.

Если $F(x)=\frac{1}{(1-x)(1-x^2)\ldots}$, то функция $F(x)$ — аналитическая внутри единичного круга и единичный круг является ее естественной границей. В качестве стандартного приема аналитической теории чисел мы применяем теорему Коши, чтобы найти

$$p(n)=\frac{1}{2\pi i}\int_C \frac{F(x)}{x^{n+1}}\,dx,$$

где C — контур, охватывающий начало координат. Точка $x=1$ является нулем каждого из сомножителей произведения $(1-x)(1-x^2)\ldots(1-x^k)\ldots$; таким образом, 1 можно рассматривать как полюс весьма высокого порядка для $F(x)$. Аналогично $x=-1$ является нулем для половины сомножителей, и, более общо, $x=\exp\frac{2\pi ip}{q}$ является нулем для каждого q-го сомножителя. Таким образом, оказывается, что $x=1$ — самая сильная особенность для $F(x)$ на единичной окружности и что точки $\exp\frac{2\pi ip}{q}$ являются особенностями, интенсивность которых убывает по мере возрастания q. Так как $F(x)$ — эллиптическая модулярная функция, то существуют функциональные уравнения, которым она удовлетворяет. Так, если

$$x^1=\exp\left\{\frac{-4\pi^2}{6\log\frac{1}{x}}\right\},$$

то

$$F(x)=\frac{x^{1/24}}{(2\pi)^{1/2}}\left(\log\frac{1}{x}\right)^{1/2}\exp\left\{\frac{\pi^2}{6\log\frac{1}{x}}\right\}F(x^1),$$

где x — действительное число, близкое к 1, тогда x^1 очень близко к нулю, а $F(x^1)$ весьма близко к 1. Таким образом, меняя $F(x^1)$ на 1, получаем очень хорошее приближение для $F(x)$ вблизи особенности $x=1$. Аналогичные тождества дают хорошие приближения для $F(x)$ вблизи каждой рациональной точки на единичной окружности. Если мы проводим аппроксимацию вблизи рациональных точек со знаменателями q, не превышающими некоторого Q, и выбираем в качестве C окружность, лежащую внутри единичного круга, радиус которого зависит от n и Q, то аппроксимирующие функции будут элементарными. Их можно точно проинтегрировать и, при достаточной тщательности, оценить ошибку. Первый результат, доказанный Харди и Рамануджаном, дает остаточный член порядка $\exp(\delta n^{1/2})$ для всякого положительного δ, когда взято достаточное число членов. Мак-Магон, применив рекуррентные формулы, вычислил значения $p(n)$ вплоть до $n=200$, найдя, что $p(200)=3\,972\,999\,029\,388$. Восемь членов формулы Харди — Рамануджана дали это значение с ошибкой порядка только 0,004, которая, естественно, была гораздо меньшей, чем они рассчитывали получить. Это подсказало им мысль проверить член, дающий ошибку, более внимательно, и они нашли, что при подходящих константах α и M, если $Q=\alpha n^{1/2}$, остаток не превышает $Mn^{-1/4}$.

Радемахер [8], пытаясь упростить анализ Харди — Рамануджана, внес небольшие изменения в их рассуждения и был поражен, найдя сходящийся ряд для $p(n)$:

$$p(n)=\sum_{q=1}^{\infty}L_q(n)\,\psi_q(n),$$

где

$$\psi_q(n)=\frac{q^{1/2}}{\pi\sqrt{2}}\cdot\frac{d}{dn}\left[\frac{\operatorname{sh}\pi\sqrt{\frac{2}{3}}\frac{\sqrt{n-\frac{1}{24}}}{q}}{\sqrt{n-\frac{1}{24}}}\right],$$

а

$$L_q(n) = \sum w_{p,q} \exp\left(-\frac{2np\pi i}{q}\right),$$

где $w_{p,q}$ — корень 24-й степени из единицы. Здесь p пробегает все целые числа, взаимно простые с q и не превосходящие q.

ЛИТЕРАТУРА

1. Аулук (Auluck F. C.), An asymptotic formula for $p_k(n)$, *J. Indian Math. Soc.* (N_1S_1), **6**, 113—114 (1942).
2. Джейкоб (Jacob S. M.), Latin rectangles of depth three, *Proc. London Math. Soc.* (2), **31**, 329—354 (1930).
3. Диксон (Dixon A. C.), On the sum of the cubes of the coefficients in a certain expansion by the binomial theorem, *Messenger of Math.*, **20**, 79—80 (1890).
4. Керавала (Kerawala S. M.), The enumeration of the latin rectangles of depth three by means of a difference equation, *Bull. Calcutta Math. Soc.*, **33**, 119—127 (1941).
5. Лунггрен (Ljunggren W.), An elementary proof of a formula of A. C. Dixon, *Norsk. Mat. Tidsskr.*, **29**, 35—38 (1947).
6. Мак-Магон (MacMahon P.), Combinatory Analysis, Cambridge University Press, Cambridge (1915).
7. Нетто (Netto E.), Lehrbuch der Combinatorik, B. G. Teubner, Leipzig, 1901.
8. Радемахер (Rademacher H.), A convergent series for the partition function $p(n)$, *Proc. Nat. Acad. Sci.*, **23**, 78—84 (1937).
9. Франклин (Franklin J.), Sur le développement du produit infini $(1-x)(1-x^2)\ldots$, *C. R. Acad. Fr.*, **92**, 448—450 (1881).
10. Харди (Hardy G. H.), Ramanujan, Cambridge University Press, Cambridge (1940).

ГЛАВА III

ТЕОРЕМЫ ВЫБОРА

1. Основные теоремы

Мы рассмотрим здесь несколько теорем, которые гарантируют существование определенных выборов при соответствующих предположениях. Они интересны сами по себе и могут быть использованы в качестве теорем существования в различных комбинаторных задачах.

Теорема о различных представителях. *Если для каждого индекса i в системе индексов I имеется конечное подмножество S_i множества S, то различные представители множеств, именно элементы a_i, такие, что $a_i \in S_i$ для всех i и $a_i \neq a_j$, если $i \neq j$, найдутся тогда и только тогда, когда удовлетворяется следующее условие.*

Условие С. *Среди элементов любого конечного числа k множеств S_i имеется по меньшей мере k различных.*

Заметим, что в этой теореме подмножества S_i и S_j при $i \neq j$ могут в действительности содержать в точности одни и те же элементы и отличаться, таким образом, только своими индексами. Если общее число n множеств конечно, а сами множества бесконечны, то теорема остается в силе, так как можно, очевидно, отбросить все, кроме n, элементы в каждом S_i, не нарушая условия С. Эта теорема впервые была выведена Ф. Холлом [12] и обобщена разными авторами [11, 3, 7].

Аналогичная теорема относительно матриц была доказана Кёнигом [5]. Мы будем употреблять термин „линия" матрицы, понимая под ним как строки, так и столбцы.

Теорема о матрицах. *Если элементы прямоугольной матрицы — нули и единицы, то минимальное число линий, которые содержат все единицы, равно максимальному числу единиц, которые могут быть выбраны таким образом, чтобы среди них не нашлось двух расположенных на одной и той же линии.*

Конечный случай теоремы Ф. Холла эквивалентен теореме Кёнига; каждая из этих теорем может легко быть

выведена из другой. Следующая теорема гарантирует, что мы можем осуществить ту или иную из двух выборок в случае, когда ясно, что ни одна из них в отдельности не может быть гарантирована.

Теорема Рамсея. *Пусть S — множество, содержащее N элементов; предположим, что семейство T всех подмножеств S, содержащих в точности r элементов, разделено на два семейства α и β, взаимно исключающих друг друга. Пусть $p \geqslant r$, $q \geqslant r$, $r \geqslant 1$. Тогда, если $n(p, q, r) \leqslant N$ есть число, зависящее только от целых чисел p, q, r и не зависящее от множества S, то либо существует подмножество A из p элементов, в котором все r-подмножества принадлежат семейству α, либо существует подмножество B из q элементов, в котором все r-подмножества входят в семейство β.*

Мы начнем с построения алгоритма для теоремы о различных представителях в случае конечного числа множеств. Практически в конкретном случае нелегко установить, выполняется условие С или нет. Очевидно, что условие С есть необходимое условие, потому что если различные представители существуют, то для любых k множеств представителями будут k различных элементов, содержащихся в этих множествах. С помощью нашего алгоритма мы, не производя никаких предварительных испытаний, либо найдем множество различных представителей, либо получим k множеств, которые содержат меньше чем k элементов, что нарушает условие С и доказывает, что не существует множества различных представителей.

Допустим, что множества $S_1, S_2, \ldots, S_n$ записаны по порядку. Выберем произвольный элемент a_1 из S_1 и до тех пор, пока это возможно, будем выбирать произвольные a_i из S_i, отличные от ранее выбранных элементов a. Если этот процесс удастся довести до S_n, то мы получим совокупность различных представителей. Мы можем, однако, достичь множества S_r, все элементы которого $b_1, b_2, \ldots, b_t$ были использованы как представители некоторых $S_1, \ldots, S_{r-1}$. Тогда мы построим несколько вспомогательных множеств $T_0, T_1, \ldots$. Множество T_0 состоит из элементов $b_1, b_2, \ldots, b_t$, которые мы считаем упорядоченными. Множество T_1 состоит из элементов множества, представителем которого является b_1, за исключением

самого b_1 и всех остальных использованных элементов. T_1 может быть пустым, но если оно непусто, то его элементы, обозначенные как $b_{t+1}, \ldots, b_s$, непосредственно следуют за $b_1, \ldots, b_t$. Далее, если i-й элемент b_i есть представитель множества S_j, мы построим множество T_i, состоящее из тех элементов S_j, которые еще не использованы, и запишем эти элементы после элементов, уже использованных. Мы продолжаем так поступать до тех пор, пока не случится одно из двух: 1) мы достигнем некоторого b_i, который не является представителем, или 2) последовательность исчерпывается элементами $b_1, \ldots, b_s$ как представителями множества. В случае 1 $b_i = b_{i_1}$ $(i_1 > t)$ входит в множество S_{j_1}, представителем которого является b_{i_2}, причем $i_2 < i_1$. Если $i_2 > t$, то b_{i_2} входит в множество S_{j_2}, представителем которого является b_{i_3}, причем $i_3 < i_2$, и т. д. Таким образом, мы получаем последовательность $b_{i_1}, b_{i_2}, \ldots, b_{i_m}$ с убывающими индексами $(i_m \leqslant t)$, такую, что каждый ее член является элементом множества, представителем которого является следующий элемент. Но теперь мы можем заменить представителей, беря b_{i_1} в качестве представителя S_{j_1}, b_{i_2} — в качестве представителя $S_{j_2}, \ldots, b_{i_{m-1}}$ — в качестве представителя $S_{j_{m-1}}$, освобождая b_{i_m} от выбора в качестве представителя S_r. В результате этого процесса $S_1, \ldots, S_{r-1}$ так же, как и S_r, имеют различных представителей, и мы можем тем же путем найти представителя S_{r+1}. Таким образом, если случай 2 никогда не наступает, мы можем найти различных представителей для всех множеств $S_1, S_2, \ldots, S_n$. Когда имеет место случай 2 и последовательность $b_1, \ldots, b_s$ исчерпывает элементы, могущие выступить в качестве представителей, то эти элементы являются представителями s множеств и по построению каждый элемент этих s множеств содержится в последовательности. Но тогда эти s множеств, а также множество S_r образуют $s+1$ множеств, которые содержат только s различных элементов; таким образом, мы находим множества, нарушающие условие С.

Исходя из этого доказательства теоремы Ф. Холла для конечного числа множеств, можно различными путями получить доказательство для случая, когда число множеств бесконечно. Способ доказательства, которого мы здесь придер-

живаемся, имеет то преимущество, что дает дополнительные сведения для конечного случая. Назовем конечное число r множеств $S_{i_1}, \ldots, S_{i_r}$ блоком $B_{r,s}$, где s — число различных элементов в r множествах. Тогда, согласно условию С, для каждого блока $B_{r,s}$ имеем $s \geqslant r$. Более того, в доказательстве для конечного случая показано, что если условие С удовлетворено, можно найти различных представителей для любого конечного числа множеств, т. е. для множеств любого блока. Назовем вычеркиванием D вычеркивание некоторых элементов из некоторых множеств S_i. Вычеркивания могут быть частично упорядочены естественным способом: будем говорить, что $D_1 \subseteq D_2$, если каждый элемент, вычеркнутый из множества посредством D_1, оказывается также вычеркнутым посредством D_2. Сосредоточим внимание на вычеркиваниях, при которых сохраняется условие С. Тогда, если $D_1 \subseteq D_2 \subseteq \ldots$ — возрастающая цепочка вычеркиваний, сохраняющих условие С, то верхний предел этой цепочки есть тоже вычеркивание D, сохраняющее условие С, так как для всякого блока $B_{r,s}$ имеется только конечное число вычеркиваний D_i и, следовательно, существует последнее вычеркивание, так что D сохраняет условие С для каждого блока и, следовательно, для всех блоков. В силу леммы Цорна, должно существовать максимальное вычеркивание D, сохраняющее условие С.

Покажем, что вычеркиванием D каждое множество S_i будет сведено к единственному элементу a_i (где a_i — различные представители множеств). Блок $B_{r,s}$, в котором $s=r$, назовем критическим блоком $B_{r,r}$. Если $B_{r,r} \subseteq B_{t,u}$, то элементы $B_{r,r}$ не могут быть использованы как представители множеств блока $B_{t,u}$, не входящих в $B_{r,r}$. Следовательно, допустимое вычеркивание состоит в удалении элементов критического блока из множеств, не входящих в этот блок, и мы можем предположить, что это проделано посредством D. Затем в критическом блоке $B_{r,r}$ выберем различных представителей, сводящих каждое множество к единственному элементу. Можно также предположить, что это проделано посредством D. Наконец, если множество S_i не принадлежит ни к какому критическому блоку и если a_i есть элемент множества S_i, построим вычеркивание, которое сводит S_i к единственному элементу a_i и вычеркивает a_i из всякого другого множества. Теперь a_i не

принадлежит ни к какому критическому блоку, так как в противном случае он был бы исключен из S_i. Таким образом, для блока $B_{r,s}$, содержащего a_i, но не содержащего S_i, первоначально имеем $s \geqslant r+1$; после вычеркивания он становится блоком $B_{r,s-1}$, где $s-1 \geqslant r$. Если $B_{r,s}$ содержит S_i, то $r-1$ других множеств должны содержать до вычеркивания по меньшей мере $r-1$ элементов, отличных от a_i; следовательно, после вычеркивания $B_{r,s}$ содержит по меньшей мере r элементов. Таким образом, условие С сохраняется. Мы видим, что в случае максимального вычеркивания D каждое множество S_i сводится к единственному элементу a_i и, таким образом, элементы a_i являются различными представителями.

Последнее рассуждение можно сделать более изящным, применив следующую теорему.

Теорема. *Если условие* С *соблюдается, то существует некоторое множество* S_i, *такое, что всякий элемент* S_i *может быть выбран в качестве его представителя в системе различных представителей.*

Следствие. *Если наименьшее множество имеет* t *элементов, то существует по меньшей мере* $t(t-1)\ldots(t-n+1)$ *различных представителей, если* $t \geqslant n$, *и по меньшей мере* $t!$ *различных представителей, если* $t < n$.

Если имеются критические блоки, то и среди них есть минимальный критический блок $B_{r,r}$. Всякая система различных представителей для $B_{r,r}$ может быть распространена на представителей всех множеств. Что касается множества S_i из $B_{r,r}$, то его представителем может быть любой элемент, так как внутри $B_{r,r}$ блоки не являются критическими и, следовательно, применимо рассуждение, проведенное выше. Если же критических блоков не существует, то применимость этого рассуждения очевидна.

Рассмотрим теперь теорему Кёнига о матрицах. Пусть A — $n \times t$-матрица, составленная из нулей и единиц. Предположим, что m — минимальное число линий, содержащих все единицы, а M — максимальное число единиц, никакие две из которых не расположены на одной линии. Тогда очевидно, что $m \geqslant M$, так как ни одна линия не может пройти через две из M единиц. Мы можем, использовав теорему Ф. Холла, доказать неравенство $M \geqslant m$. Пусть $m = r+s$, где r — число строк, а s — число столбцов

Расположим эти r строк так, чтобы они были первыми, и назовем их $R_1, \ldots, R_r$. Для каждой из строк R_i соответственно образуем множества $S_1, \ldots, S_r$, где S_i состоит из номеров j столбцов, для которых $a_{ij}=1$, исключая номера s столбцов, входящих в указанное выше минимальное число. Теперь, если k из этих множеств содержат меньше, чем k элементов (скажем, v элементов), то соответствующие $v<k$ столбцов могут быть использованы, чтобы заменить k строк, и в таком случае все единицы будут включены в меньшее число линий. Поскольку это противоречит предположению минимальности m, то условие С удовлетворяется для множеств $S_1, \ldots, S_r$ и мы можем выбрать r единиц из r строк так, чтобы не было двух единиц в одном и том же столбце и ни одной в s столбцах. Теми же самыми рассуждениями мы можем выбрать s единиц из s столбцов, чтобы не было двух единиц в одной и той же строке и ни одной в r строках. Это дает нам всего $r+s=m$ единиц, расположенных не более чем по одной на одной и той же линии. Отсюда $M \geqslant m$, а поскольку мы ранее установили, что $m \geqslant M$, то отсюда следует, что $M=m$, а это доказывает теорему.

В свою очередь, исходя из теоремы Кёнига, нетрудно доказать теорему Ф. Холла. Пусть даны множества $S_1, S_2, \ldots, S_n$ и элементы $a_1, \ldots, a_m$. Образуем матрицу $A=(a_{ij})$, где $a_{ij}=1$, если a_j входит в S_i, и $a_{ij}=0$, если нет. Теперь, если единицы матрицы A могут быть размещены в r строках и s столбцах, причем $r+s<n$, то для $k=n-r$ строк, не совпадающих с r выбранными строками, единицы имеются только в $s<n-r=k$ столбцах и условие С для этих k множеств нарушается. Но если минимальное число линий будет $r+s=n$, то, согласно теореме Кёнига, существуют n единиц, таких, что никакие две из них не лежат на одной линии, а соответствующие n элементов образуют множество различных представителей n множеств.

Теорема Рамсея в случае $r=2$ может быть применена к теории графов следующим образом. Пусть даны N точек. Каждая пара точек ($r=2$) соединена дугой, а каждая дуга окрашена в один из двух цветов (α или β). Тогда, если N достаточно велико, существует или множество p точек, все дуги которого окрашены в цвет α, или множе-

ство q точек, все дуги которого окрашены в цвет β. Задача в этой постановке была исследована Глисоном и Гринвудом [2]; им даже удалось получить результат, являющийся доказательством теоремы Рамсея для любого числа цветов.

Мы, следуя Эрдёшу и Секерешу [13], докажем теорему Рамсея полной индукцией относительно r, p и q, допустив, что результат справедлив для $r-1$ и для любых значений p, q, затем — для r, p, $q-1$ и, наконец, — для r, $p-1$, q. Для $r=1$ значение N равно $p+q-1$. Это следует из того, что мы можем построить множество, содержащее $p-1$ элементов α и $q-1$ элементов β, откуда $N>p+q-2$. Но если для $N\geqslant p+q-1$ не найдется p элементов α, то их не более чем $p-1$ и, следовательно, существует по крайней мере $N-(p-1)\geqslant q$ элементов β. Если при $p=r$ существуют r-множества, то любое из них будет удовлетворять условиям выбора. Если $n\neq r$, то каждое r-множество есть r-множество элементов β, и, следовательно, при $N\geqslant q$ будет существовать q-множество, в котором все r-множества состоят из элементов β. Аналогично, если $q=r$, достаточно иметь $N\geqslant p$. Таким образом, в качестве исходных значений для нашей индукции мы имеем

$$n(p, q, 1)=p+q-1, \quad n(r, q, r)=q, \quad n(p, r, r)=p.$$

Помимо этих начальных значений, условия $p\geqslant r$, $q\geqslant r$, $r\geqslant 1$ также удовлетворяются для p', q', r', где $r'=r-1$, или при $p'=p-1$, $q'=q$, $r'=r$, или при $p'=p$, $q'=q-1$, $r'=r$.

В соответствии с нашей индукцией выберем $p_1=n(p-1, q, r)$, $q_1=n(p, q-1, r)$. Затем предположим, что $n(p, q, r)\leqslant n(p_1, q_1, r-1)+1$. Чтобы доказать это, предположим, что $N\geqslant n(p_1, q_1, r-1)+1$. Выберем фиксированный элемент a_0 из S и определим α' и β' множества из $(r-1)$-множества $S'=S-a_0$ по следующему правилу. Если a_0 и $(r-1)$-множество из $S'=S-a_0$ образуют α-множество из S, то мы назовем это множество α'-множеством из S', если же a_0 и $(r-1)$-множество из S образуют β-множество из S, мы назовем его β'-множеством из S'. Так как S имеет по меньшей мере $n(p_1, q_1, r-1)$ элементов, то S' содержит или p_1-множество, в котором все $(r-1)$-множества суть α-множества, или q_1-множество,

в котором все $(q-1)$-множества суть β-множества. Предположим первое. Пусть T_1 — p_1-множество, в котором все $p-1$-множества будут α'-множествами. Так как $p_1=n(p-1, q, r)$, то T_1 будет или содержать q-множество Q, в котором все r-множества суть β-множества, и в этом случае Q удовлетворяет нашим требованиям. Если же нет, то T_1 содержит $(p-1)$-множество P', в котором все r-множества суть α-множества. Но в таком случае P' и a_0 образуют p-множество P, в котором r-множества те же, что и в P', или состоят из a_0 и $(p-1)$-множества из P'. Но все $(p-1)$-множества из T' суть α'-множества, откуда одно из них, взятое с элементом a_0, есть α-множество из S. Следовательно, все r-множества из P суть α-множества, так что P удовлетворяет нашим условиям. Рассуждение будет аналогичным, если существует q_1-множество T_2, в котором все $(q-1)$-множества суть множества β.

В рекуррентном правиле

$$n(p, q, r)\leqslant n(p_1, q_1, r-1)+1,$$

где

$$p_1=n(p-1, q, r),\ q_1=n(p, q-1, r),$$

равенство сохраняется не всюду. В самом деле, Глисон и Гринвуд [2] доказали, что

$$n(p, q, 2)<n(p_1, q_1, 1)+1=p_1+q_1,$$

где

$$p_1=n(p-1, q, 2),\ q_1=n(p, q-1, 2)$$

для четных p_1 и q_1. Из этого следует, что $n(3, 4, 2)<$ $<4+6=10$, и в самом деле Гринвуд и Глисон доказали, что $n(3, 4, 2)=9$.

2. Приложения теорем

Приложения этих теорем довольно многочисленны. Примером приложения теоремы Рамсея может служить следующая теорема, которую доказали Эрдёш и Секереш [13].

Теорема. *Для любого заданного целого числа n существует целое $N=N(n)$, такое, что среди N точек плоскости, расположенных так, что никакие три из них не лежат на одной прямой, найдутся n точек, образующих выпуклый n-угольник.*

Доказательство состоит из двух частей.

Лемма 1. *Из 5 точек на плоскости, расположенных так, что никакие три из них не лежат на одной прямой, 4 точки оказываются вершинами выпуклого четырехугольника.*

Доказательство. Если выпуклая оболочка 5 точек образует выпуклый четырехугольник или пятиугольник, то это очевидно. Если же выпуклой фигурой является треугольник A, B, C, а другие две точки, D и E, расположены внутри треугольника, тогда две из трех точек A, B, C расположены по одну сторону от прямой DE, скажем B и C, и в этом случае точки B, C, D, E образуют выпуклый четырехугольник.

Лемма 2. *Если каждые четыре точки из n данных точек образуют выпуклый четырехугольник, то эти n точек являются вершинами выпуклого n-угольника.*

Доказательство. Для $n=4$ это очевидно. Перейдем по индукции к случаю n точек. Предположим, что все четырехугольники, образованные из точек A_1, A_2, $\cdots$, A_n, A_{n+1}, являются выпуклыми. Тогда A_1, A_2, $\cdots$, A_n будут, по предположению, вершинами выпуклого n-угольника C_n, и мы можем считать, что они именно в таком порядке расположены вдоль периметра. Если точка A_{n+1} находится внутри C_n, то она должна попасть внутрь одного из треугольников $A_1A_2A_3$, $A_1A_3A_4, \cdots, A_1A_{n-1}A_n$. Но тогда для некоторого i мы имеем точки A_1 $A_iA_{i+1}A_{n+1}$, которые не образуют выпуклого четырехугольника, что противоречит предположению. Это доказывает более общее предположение, что в случае $n+1$ точек выпуклый многоугольник, образованный n из них, не содержит оставшуюся точку внутри себя. Теперь, если мы соединим точку A_{n+1} со всеми точками A_1, $A_2, \cdots$, A_n прямыми, то поскольку A_{n+1} лежит вне выпуклого многоугольника, то среди этих прямых будут две крайние, скажем $A_{n+1}A_i$ и $A_{n+1}A_j$, образующие угол, охватывающий выпуклый n-угольник. Если допустить, что A_i и A_j не являются последовательными вершинами, то A_{n+1} и другие точки должны образовать выпуклый многоугольник, содержащий остальные точки внутри себя. Так как этого не может случиться, то A_i и A_j следуют одна за другой и, помещая A_{n+1} между ними, мы получаем выпуклый $(n+1)$-угольник. Это доказывает вторую лемму.

Доказательство теоремы теперь следует непосредственно из теоремы Рамсея и двух лемм. Пусть 4-множества делятся на выпуклые и невыпуклые четырехугольники. Поскольку нет 5-множества, содержащего только невыпуклые четырехугольники, то если N достаточно велико, будет существовать n-множество, все четырехугольники которого выпуклые.

Из теоремы о различных представителях мы получаем следующую теорему:

Теорема об одновременных представителях. *Пусть множество S разделено на n непересекающихся подмножеств двумя способами: $S=A_1+\cdots+A_n=B_1+\cdots+B_n$. Тогда, если нет k подмножеств A, которые бы содержались в меньшем, чем k, числе подмножеств B, то существуют элементы $x_1, \cdots, x_n$, которые являются одновременно представителями множеств A и множеств B.*

Доказательство. Для каждого подмножества A_i определим множество S_i, состоящее из элементов с такими индексами j, что $A_i \cap B_j$ не пусто. Условие теоремы является условием С для множеств S_i. Но выбор различных представителей для S_i дает для каждого A_i свое особое B_j, с которым оно имеет непустое пересечение. Выбирая в этом пересечении по одному элементу в каждом случае, мы получаем элементы $x_1, x_2, \cdots, x_n$ различных множеств A, а также различных множеств B, как и требовалось. Необходимость условия очевидна, и, рассматривая дополнения, мы видим, что условие симметрично как для множеств A, так и для множеств B. Естественным следствием этой теоремы является

Теорема. *Если H — подгруппа конечной группы G, то мы можем выбрать элементы, которые являются одновременно представителями правого и левого множеств, дополнительных к H.*

Здесь каждое из левых дополнительных множеств A_i и каждое из правых дополнительных множеств B_j содержат то же число элементов, что и H, и теорема доказана. Эта теорема также справедлива, если G бесконечна, а H имеет конечный индекс. Известно, что в G существует нормальная подгруппа K с конечным индексом, которая содержится в H. Отсюда следует справедливость теоремы, так как каждое правое или левое дополнительное к H

множество содержит то же самое число дополнительных множеств K, что и H.

В качестве дальнейшего приложения теоремы о различных представителях мы имеем следующую теорему:

Теорема. *В векторном пространстве конечного или бесконечного числа измерений всякие два базиса имеют одинаковые кардинальные числа.*

Пусть $\mathbf{x}_i$, $i \in I$, а также $\mathbf{y}_j$, $j \in J$, — два базиса векторного пространства $\mathbf{V}$ над полем F. Представляя каждый вектор $\mathbf{x}_i$ как линейную комбинацию векторов $\mathbf{y}$, мы получаем множество S_i векторов $\mathbf{y}$, ассоциированных с векторами $\mathbf{x}_i$, именно тех векторов $\mathbf{y}_j$, которые входят с ненулевыми коэффициентами в выражение для $\mathbf{x}_i$ через векторы $\mathbf{y}_j$. Множества S_i конечны и должны удовлетворять условию C, так как в противном случае векторы $\mathbf{x}$ были бы линейно зависимы. Следовательно, мы можем выбрать различные элементы $\mathbf{y}$ из множеств S_i и кардинальное число элементов $\mathbf{y}$ будет во всяком случае не более числа элементов $\mathbf{x}$. Аналогично кардинальное число элементов $\mathbf{x}$ будет не более кардинального числа элементов $\mathbf{y}$, следовательно, оба кардинальных числа должны быть равны.

В качестве приложения теоремы Кёнига мы рассмотрим задачу о распределении должностей. Предположим, что имеется n должностей, занимаемых n людьми, и что оклады a_{ij} ($i = 1, \ldots, n$; $j = 1, \ldots, n$) для i-го человека в j-й должности. Предполагается, что оклады — неотрицательные целые числа. Требуется найти оптимальное распределение n должностей между n лицами, т. е. такое распределение, при котором сумма соответствующих окладов будет максимальной. Существует, очевидно, $n!$ вариантов, из которых нужно выбрать оптимальный. Задача состоит в том, чтобы найти систематический метод отыскания и исследования решения с помощью сравнительно малого числа попыток. Докажем теорему.

Теорема. *Дана матрица* $A = (a_{ij})$. *Максимум суммы* $a_{1j_1} + a_{2j_2} + \ldots + a_{nj_n}$ *равен минимуму* $\sum_{i=1}^{n} u_i + \sum_{j=1}^{n} v_j$ *для всех чисел* u_i ($i = 1, \ldots, n$), v_j ($j = 1, 2, \ldots, n$), *таких, что* $u_i + v_j \geqslant a_{ij}$ *во всех случаях. Общее значение достигается, когда* $u_i + v_{j_i} = a_{ij_i}$, *и эти значения являются решением задачи о распределении должностей.*

Доказательство. Если задана матрица (a_{ij}), мы всегда можем найти числа u_i, v_j, удовлетворяющие неравенству $u_i+v_j\geqslant a_{ij}$, беря все числа u равными 0 и каждое v_j равным максимуму $a_{ij}(i=1, 2, \ldots, n)$. Поскольку $u_i+v_j\geqslant a_{ij_i}$, то, суммируя, получаем $\sum u_i+\sum v_j\geqslant\sum a_{ij_i}$; следовательно, если m есть минимум $\sum u_i+\sum v_j$, а M — максимум $\sum a_{ij_i}$, тогда $m\geqslant M$. Мы должны доказать, что $m=M$. Для выбора элементов u и v образуем вспомогательную матрицу $B=(b_{ij})$, полагая $b_{ij}=1$, если $u_i+v_j=a_{ij}$, и $b_{ij}=0$, если $u_i+v_j>a_{ij}$. Тогда, если имеется n элементов b и среди них нет двух, лежащих на одной линии, то они дают нам положения n элементов a, т. е. a_{ij_i}, таких, что $\sum u_i+\sum v_j=\sum a_{ij_i}$, откуда $m=M$, и, следовательно, попутно решена задача о распределении должностей. В случае, когда элементы a—целые неотрицательные, при первоначальном выборе элементы u и v были целыми. Если мы не получаем решения сразу и оказывается, что элементов b меньше, чем n, а среди них нет двух, лежащих на одной линии, то, по теореме Кёнига, существует $t<n$ линий, которые включают в себя все единицы. Предположим, что среди этих линий r строк и s столбцов. Тогда мы u и v заменим через u' и v', полагая

$$
\begin{aligned}
u_i' &= u_i+\tfrac{1}{2} && \text{для } r \text{ строк},\\
u_i' &= u_i-\tfrac{1}{2} && \text{для остальных строк},\\
v_j' &= v_j+\tfrac{1}{2} && \text{для } s \text{ столбцов},\\
v_j' &= v_j-\tfrac{1}{2} && \text{для остальных столбцов}.
\end{aligned}
$$

Здесь, если $u_i+v_j=a_{ij}$, то $b_{ij}=1$, а в сумме $u_i'+v_j'$ или $u_i'=u_i+\frac{1}{2}$, или $v_j'=v_j+\frac{1}{2}$, или $u_i'=u_i+\frac{1}{2}$ и $v_j'=v_j+\frac{1}{2}$ одновременно, откуда $u_i'+v_j'=u_i+v_j$, или u_i+v_j+1, и мы все еще имеем $u_i+v_j\geqslant a_{ij}$. Но, если $u_i+v_j>a_{ij}$, то $u_i'+v_j'\geqslant u_i+v_j-1>a_{ij}$. В то же время

$$
\sum u_i'+\sum v_j=\sum u_i+\sum v_j+\tfrac{1}{2}(r+s)-\tfrac{1}{2}(2n-r-s)=
$$
$$
=\sum u_i+\sum v_j+t-n<\sum u_i+\sum v_j.
$$

Следовательно, сумма $\sum u_i + \sum v_j$ уменьшилась на целое число. Мы продолжаем таким образом изменять элементы u и v на $1/2$ до тех пор, пока далее уменьшать $\sum u_i + \sum v_j$ станет невозможно. Когда же это произойдет, то, применив теорему Кёнига, мы получим решение задачи о распределении должностей. Теорема, однако, справедлива и без ограничения, что a_{ij} должны быть целыми неотрицательными числами. В самом деле, если a_{ij} — произвольные числа, мы можем всюду добавить постоянную, чтобы заменить числа a неотрицательными числами. Более того, результат не изменится, если мы умножим каждое a_{ij} на положительную константу. Отсюда, так как теорема справедлива, когда a_{ij} — целые, то она будет также верна и для случая, когда a_{ij} являются рациональными. Если мы с помощью сложения и умножения нормируем числа a, так чтобы $0 \leqslant a_{ij} \leqslant 1$, где a_{ij} — рациональные числа со знаменателем N, то после умножения на N числа a будут находиться в интервале $0 \leqslant a_{ij} \leqslant N$ и будем иметь $0 \leqslant \sum_i u_i + \sum_j v_j \leqslant nN$. Так как сумма уменьшается на целое число на каждом этапе, то существует самое большее nN этапов, на каждом из которых u и v изменяются не более чем на $1/2$. Отсюда получаем

$$-\frac{nN}{2} \leqslant u_i \leqslant +\frac{nN}{2} \quad \text{и} \quad -\frac{nN}{2} \leqslant v_j \leqslant \frac{3nN}{2}.$$

Теперь, деля на N, чтобы вернуться к рациональному решению, получаем для рациональных решений

$$-\frac{n}{2} \leqslant u_i \leqslant +\frac{n}{2} \quad \text{и} \quad -\frac{n}{2} \leqslant v_j \leqslant \frac{3n}{2}.$$

Из компактности области значений u и v следует, что если мы аппроксимируем иррациональные числа a_{ij} рациональными, то в пределе найдется такой набор элементов u и v, который даст равенство для теоремы и оптимальное распределение должностей.

Заметим, что в задаче о распределении должностей определение вспомогательных переменных u и v имеет большое значение не только для нахождения решения, но и для исследования его. Дело в том, что если нам задано некоторое распределение должностей, то соответствующая

сумма окладов легко вычисляется, но без знания u и v невозможно исследовать само распределение, чтобы решить, будет оно оптимальным или нет.

Существует тесная связь между комбинаторным анализом и теорией линейных неравенств и, более общо, с теорией выпуклых пространств; эта связь еще не изучена полностью. Рассмотрим так называемые двойные стохастические матрицы. Двойная стохастическая матрица $X=(x_{ij})$— это квадратная матрица из действительных, неотрицательных чисел, суммы которых по строкам и по столбцам равны единице. Формально

$$X=(x_{ij}),\quad x_{ij}\geqslant 0,\quad i,\ j=1,\ \ldots,\ n,$$
$$\sum_i x_{ij}=1,\quad j=1,\ \ldots,\ n,$$
$$\sum_j x_{ij}=1,\quad i=1,\ \ldots,\ n.$$

Термин „двойная стохастическая матрица“ возник в теории вероятностей. Подобную матрицу можно рассматривать как матрицу, дающую вероятность перехода для случая, когда имеется n различных состояний; x_{ij} — вероятность того, что за i-м состоянием последует j-е состояние. В n^2-мерном пространстве всех действительных $n\times n$-матриц двойная стохастическая матрица образует выпуклое и ограниченное подпространство размерности $(n-1)^2$, а переменные x_{ij}, $i,\ j=1,\ \ldots,\ n-1$, определяют все остальное пространство. Здесь мы ассоциируем $X=(x_{ij})$ с точкой $(z_1,\ \ldots,\ z_{n^2})$, где $x_{ij}=z_{i+(j-1)n}$. Мы называем пространство S выпуклым, если вместе с точками $P_1,\ \ldots,\ P_r$ и $a_1+\ldots+a_r=1$ оно содержит точки вида $a_1P_1+a_2P_2+\ldots+a_rP_r$, где $a_i\geqslant 0$ $(i=1,\ \ldots,\ r)$ и $a_1+\ldots+a_r=1$. В частности, когда $a_1\geqslant 0$, $a_2\geqslant 0$ и $a_1+a_2=1$, $a_1P_1+a_2P_2$ с переменными a дает отрезок, соединяющий P_1 и P_2. Точка P выпуклого пространства называется экстремальной, если она не может быть выражена в вышеуказанной форме как линейная комбинация любых точек пространства. Легко видеть, что в пространстве двойных стохастических матриц матрицы перестановок, которые имеют по единственной единице в каждой строке и в каждом столбце, образуют экстремальные точки.

Теорема. *Всякая $(n \times n)$-матрица из неотрицательных чисел, все строки и столбцы которой имеют одну и ту же сумму, может быть записана как сумма матриц перестановок с положительными коэффициентами.*

Доказательство. Пусть $M=(m_{ij})$ $(i, j=1, \ldots, n)$ — матрица, в которой сумма элементов каждой строки и каждого столбца равна t. Допустим, далее, что число ненулевых элементов m_{ij} равно w. Если M не есть тождественный нуль, то $w \geqslant n$, а если $w=n$, то M есть t-кратная матрица перестановок. Пусть S_i $(i=1, 2, \ldots, n)$ — множества тех j, для которых $m_{ij} \neq 0$. Мы утверждаем, что условие С справедливо для S_i. В самом деле, если условие С не удовлетворяется, то все ненулевые элементы k строк окажутся расположенными менее чем в k столбцах. Отсюда, суммируя эти элементы по строкам, получим kt, а суммируя по столбцам, получим самое большее $(k-1)t$, что противоречит условию теоремы. Следовательно, условие С выполняется и множества S_i имеют различные представители $j_1, \ldots, j_n$, которые образуют перестановку $1, \ldots, n$. Тогда $P=(p_{ij})$ — матрица перестановок, если $p_{ij_i}=1$, а все остальные $p_{ij}=0$. Более того, если выбрать в качестве u наименьшее из m_{ij_i}, то $M-uP$ будет состоять из неотрицательных элементов, суммы которых по строкам и столбцам равны $t-u$, а ненулевых членов будет меньше, чем в M. По индукции, $M-uP=u_2P_2+\ldots+u_rP_r$ и $M=uP+u_2P_2+\ldots+u_rP_r$, что и требовалось доказать.

Отсюда непосредственно следует, что всякая двойная стохастическая матрица может быть выражена через матрицы перестановок и что только эти последние являются единственными экстремальными матрицами. Так как линейная функция, заданная на отрезке, достигает максимума (или минимума) на концах этого отрезка, то отсюда следует, что всякая линейная функция, которая достигает максимума (или минимума) в выпуклом пространстве, будет достигать его в экстремальной точке.

Таким образом, мы установили важную связь между выпуклым пространством двойных стохастических матриц и дискретным пространством матриц перестановок, которые являются экстремальными точками. Так, если $A=(a_{ij})$ —

оклады в задаче о распределении должностей, мы можем, если желаем, рассматривать эту задачу как задачу отыскания максимума линейной формы $\sum_{i,j} a_{ij}x_{ij}$, так как $X=(x_{ij})$ представляет все пространство двойных стохастических матриц. Мы знаем, что этот максимум будет достигаться, когда X — матрица перестановок. Обратно, континуальная задача отыскания максимума линейной формы на пространстве двойных стохастических матриц может быть сведена к комбинаторной задаче отыскания максимизирующей матрицы перестановок.

Метод решения задачи о распределении должностей с употреблением вспомогательных чисел u_i и v_j есть частный случай общей теоремы двойственности из теории линейного программирования. Приложение этого общего метода к комбинаторным задачам было недавно осуществлено А. Гофманом и Г. Куном. Мы приводим основные задачи и теоремы в формулировке М. Флуда [8].

Во-первых, обозначим буквой M прямоугольную $(m \times n)$-матрицу. Буквы **a**, **b**, **x**, **y** обозначают векторы-столбцы. M, **a**, **b** — заданы, **x**, **y**, а также число d — искомые. Мы будем употреблять верхний индекс T, чтобы обозначить транспозицию вектора или матрицы. Векторное неравенство означает, что это неравенство справедливо для каждой из соответствующих компонент.

Задача I. Удовлетворить ограничениям $M\mathbf{x} \leqslant \mathbf{a}$, $\mathbf{x} \geqslant 0$ и выполнить $\mathbf{b}^T\mathbf{x} = d$ для d максимального в том смысле, что не существует **x**, удовлетворяющего ограничениям и приводящего к неравенству $\mathbf{b}^T\mathbf{x} > d$.

Задача II. Удовлетворить ограничениям $M^T\mathbf{y} \geqslant \mathbf{b}$, $\mathbf{y} \geqslant 0$ и выполнить $\mathbf{a}^T\mathbf{y} = d$ для d минимального в том смысле, что не существует **y**, удовлетворяющего ограничениям и приводящего к неравенству $\mathbf{a}^T\mathbf{y} < d$.

Задачи I и II называются двойственными.

Основная теорема выполнимости. *Ограничения в задаче выполнимы* (*т. е. удовлетворяются некоторыми значениями* **x** *или* **y**) *тогда и только тогда, когда двойственная задача в однородной форме* (*т. е. при* $\mathbf{b}=0$ *или* $\mathbf{a}=0$) *имеет нулевое решение.*

Основная теорема существования. 1) *Векторы* **x** *и* **y** *являются решениями задач* I *и* II *тогда и*

только тогда, когда они удовлетворяют поставленным в этих двух задачах ограничениям и осуществляют $\mathbf{a}^T\mathbf{y} = \mathbf{b}^T\mathbf{x}$. *Такие* $\mathbf{x}$ *и* $\mathbf{y}$ *существуют, если ограничения в обеих задачах выполнимы.* 2) *Задача имеет решение тогда и только тогда, когда ее ограничения выполнимы и однородная форма задачи имеет нулевое решение.*

Основная теорема двойственности. *Задача имеет решение (для единственного* d*) тогда и только тогда, когда двойственная ей задача имеет решение (для того же самого* d*).*

Доказательства этих теорем даны Гейлом, Куном и Таккером [1].

В случае задачи о распределении должностей вместо переменных x_{ij} возьмем n^2 переменных с одним индексом. Положим $x_{i+(n-1)j} = x_{ij}$, $i = 1, \ldots, n$, $j = 1, \ldots, n$; аналогично введем обозначения для окладов $b_{i+(n-1)j} = a_{ij}$. Затем возьмем $(n^2 \times 4n)$-матрицу M:

$$M = \begin{vmatrix} J_1, & J_2, & \ldots, & J_n \\ -J_1, & -J_2, & \ldots, & -J_n \\ I_n, & I_n, & \ldots, & I_n \\ -I_n, & -I_n, & \ldots, & -I_n \end{vmatrix} \qquad a = \begin{vmatrix} i_n \\ -i_n \\ i_n \\ -i_n \end{vmatrix},$$

где I_n — единичная $(n \times n)$-матрица и J_i — $(n \times n)$-матрица с единицами в i-й строке и нулями в остальных, а i_n — вектор-столбец из n единиц. Неравенство $M\mathbf{x} \leqslant \mathbf{a}$ выражает через первоначальные x_{ij} тот факт, что суммы элементов строк (и аналогично столбцов) будут самое большее равны $+1$, а суммы их отрицательных значений — самое большее -1, откуда вытекает, что суммы элементов в строках и столбцах равны единице. Следовательно, неравенство $M\mathbf{x} \leqslant \mathbf{a}$ $(\mathbf{x} \geqslant 0)$ показывает, что мы имеем дело с двойными стохастическими матрицами. В частности, при $\mathbf{b}^T = (b_1, \ldots, b_n)$ мы получаем

$$\mathbf{b}^T\mathbf{x} = \sum_{i=1}^{n} b_i x_i = \sum a_{ij} x_{ij}.$$

Максимум последней суммы дает решение задачи о распределении должностей.

В двойственной задаче мы стремимся удовлетворить условиям $M^T\mathbf{y} \geqslant \mathbf{b}$, $\mathbf{y} \geqslant 0$ и добиться, чтобы $\mathbf{a}^T\mathbf{y}$ было минимальным. Здесь $\mathbf{y}$ является $4n$-компонентным вектором.

Если мы положим $u_i = y_i - y_{n+i}$ для $i = 1, \ldots, n$ и $v_j = y_{2n+j} - y_{3n+j}$ для $j = 1, \ldots, n$, то условие $M^T\mathbf{y} \geqslant \mathbf{b}$ принимает вид $u_i + v_j \geqslant a_{ij}$. Положительность y не накладывает никакого условия на значения u и v. Таким образом, двойственная задача дает вспомогательные числа u и v, а из основной теоремы двойственности следует, что минимум суммы $\sum u_i + \sum v_j$, который равен $\mathbf{a}^T\mathbf{y}$, является максимумом $\sum a_{ij}x_{ij}$. Этот максимум дает решение задачи о распределении должностей, так как мы показали, что перестановки суть экстремальные точки двойных стохастических матриц. Практически значение теоремы двойственности состоит не в том, что решение одной задачи достигается посредством решения другой однотипной, но в установлении того, что одно и то же d входит в решения обеих задач и что на практике лучше всего решать их одновременно. Существенно, наконец, что, получив решение, мы можем исследовать его.

Манн и Райзер [7] обобщили задачу отыскания системы различных представителей. Они поставили вопрос: когда заданное множество элементов $e_1, \ldots, e_t$, которые они назвали маргинальными, может встретиться в некоторой системе различных представителей. При этом они доказали, что если каждый из элементов $e_1, \ldots, e_t$ встречается по меньшей мере t раз в множествах S_i, тогда существует некоторая система различных представителей, содержащая $e_1, \ldots, e_t$. Это условие, однако, слишком сильное. Гофман и Кун [3] нашли более подходящее условие и доказали его с помощью теоремы двойственности. Естественно, что условие C должно быть соблюдено. Так что условием для маргинальных элементов будет следующее.

Условие C*. *Для всякого* $p = 1, \ldots, t$ *и для всякого выбора* $E' = e_{i_1}, \ldots, e_{i_p}$ p *маргинальных элементов число множеств* S_j, *в которых встречаются* E', *будет по меньшей мере* p.

Здесь будет дана только схема доказательства.

Пусть $C = (c_{ij})$, $(i = 1, \ldots, m, \ j = 1, \ldots, n)$ — матрица инцидентности, где $c_{ij} = 1$, если i-й объект находится в j-м множестве, и $c_{ij} = 0$ во всех других случаях. Естественно, что $m \geqslant n$. Итак, $i = 1, 2, \ldots, t$ будет соответствовать данным t маргинальным элементам $e_1, \ldots, e_t$. Теперь определим (t, m, n)-матрицу перестановок как

матрицу из нулей и единиц, причем: 1) имеется в точности одна единица в каждой из первых t строк; 2) в каждой строке имеется не более одной единицы; 3) в каждом из n столбцов встречается в точности одна единица.

Далее рассмотрим полиэдральное выпуклое множество K всех $(m \times n)$-матриц $X=(x_{ij})$, таких, что

$$x_{ij} \geqslant 0, \quad i=1, \ldots, m, \ j=1, \ldots, n,$$
$$\sum_j x_{ij}=1, \quad i=1, \ldots, t,$$
$$\sum_j x_{ij} \leqslant 1, \quad i=t+1, \ldots m,$$
$$\sum_i x_{ij}=1, \quad j=1, \ldots, n.$$

Рассмотрим максимум r суммы $\sum_{i,j} c_{ij}x_{ij}$ на выпуклом множестве K. В этом случае, согласно теореме двойственности, r есть также минимум для $\sum_{i=1}^{m} u_i + \sum_{j=1}^{n} v_j$, где $u_i + v_j \geqslant c_{ij}$, $i=1, \ldots, m$, $j=1, \ldots, n$, а $u_i \geqslant 0$, $i=t+1, \ldots, m$. Доказывается лемма, утверждающая, что экстремальные точки множества K суть (t, m, n)-матрицы перестановок. Это нетрудно увидеть, так как всякая матрица X может быть дополнена до двойной стохастической $(m \times m)$-матрицы X, если дополнить первые t строк нулями. Таким образом, X есть комбинация $(m \times m)$-матриц перестановок, в которых элементы, лежащие на пересечении первых t строк и последних $m-n$ столбцов, суть нули. Следовательно, экстремум X соответствует экстремуму той матрицы X, которая является (t, m, n)-матрицей перестановок в ее первых n столбцах.

Таким образом, максимум r для $\sum c_{ij}x_{ij}$ на K достигается для (t, m, n)-матрицы перестановок, следовательно, r есть целое число. Так как минимум для $\sum_{i=1}^{m} u_i + \sum_{j=1}^{n} v_j$, где $u_i + v_j \geqslant c_{ij}$, также равен r, то следующий шаг состоит в том, чтобы показать, что для получения минимума r могут быть взяты целые значения u и v.

Наконец, при строгом соблюдении условий C и C* показывается, что в качестве чисел u и v могут быть выбраны нули и единицы, и из этого следует, что $r=n$ и, таким образом, существует система различных представителей, включающая маргинальные элементы.

Этот результат может также быть получен из вышеуказанного алгоритма для нахождения систем различных представителей. Если мы вычеркнем все элементы, за исключением маргинальных, то, согласно условию C*, существует t различных множеств, для которых $e_1, \ldots, e_t$ могут быть взяты как представители. Если выбрать их в качестве $S_1, \ldots, S_t$ и восстановить оставшиеся элементы, то алгоритм завершается системой различных представителей, где эти элементы вводятся в качестве различных представителей для некоторых t множеств, хотя и не обязательно множеств $S_1, \ldots, S_t$. Алгоритм никогда не отбрасывает элемента как представитель, но может перенести представитель из одного множества в другое.

Задача распределения, или транспортная, возникла из исследования наиболее экономичного способа распределения продукции из нескольких источников снабжения в многочисленные участки потребления. Математическая формулировка этой задачи весьма сходна с формулировкой задачи о распределении должностей. Мы задаем $(m \times n)$-матрицу $D = (d_{ij})$ и ищем матрицу $X = (x_{ij})$, удовлетворяющую условиям:

$$x_{ij} \geqslant 0, \quad i = 1, \ldots, m, \quad j = 1, \ldots, n,$$
$$\sum_j x_{ij} = r_i, \quad j = 1, \ldots, n,$$
$$\sum_i x_{ij} = c_j, \quad i = 1, \ldots, m,$$

и ищем способ минимизировать $\sum d_{ij} x_{ij}$. Флуд [8] рассмотрел вычислительные аспекты решения этой задачи. Двойственная задача включает в себя числа u_i, $i = 1, \ldots, m$, v_j, $j = 1, \ldots, n$ (Флуд употребляет символ $-u_i$), такие, что

$$d_{ij} \geqslant u_i + v_j, \quad i = 1, \ldots, m, \quad j = 1, 2, \ldots, n.$$

Затем разыскивается минимум $\sum c_j v_j + \sum r_i u_i$. В качестве решения мы получаем $x_{ij}(d_{ij} - u_i - v_j) = 0$. Таким образом, решение включает в себя нахождение значений x_{ij} в подходящих строках и столбцах, суммы которых равны нулю, за исключением тех случаев, когда имеют место равенства $d_{ij} = u_i + v_j$. Это приводит к несколько сложным комбинаторным исследованиям графов, ассоциированных с положениями (i, j), для которых $d_{ij} = u_i + v_j$.

Задачу о странствующем коммивояжере также можно сравнить с задачей о распределении должностей, но она имеет дополнительные усложнения. В этой задаче мы задаем $(n \times n)$-матрицу $M = (d_{ij})$, где d_{ij} выражает в общем виде обобщенное расстояние от i-го города до j-го. Требуется найти маршрут, проходящий один и только один раз через каждый город и имеющий минимальную протяженность. Расстояния d_{ij} могут быть совершенно произвольными и не предполагаются симметричными или удовлетворяющими неравенству треугольника.

Здесь нам нужно найти матрицу перестановок $X = (x_{ij})$, такую, чтобы $\sum d_{ij}x_{ij}$ была минимальной. Это — то же самое условие, что и в задаче о распределении должностей (где слово „максимум“ изменено на „минимум“), с той разницей, что перестановка должна быть n-циклом. Мы можем увеличить диагональные элементы d_{ii} и таким образом быть уверенными, что минимум $\sum d_{ij}x_{ij}$ не включает ни одного из них. Тогда перестановка, найденная так же, как в задаче о распределении должностей, будет перестановкой, не имеющей фиксированных элементов. Но эта перестановка не дает решения задачи о странствующем коммивояжере, пока не доказано, что она является n-циклом.

Тем не менее этот подход является первым шагом к решению задачи о странствующем коммивояжере. Исходя из этого, Флуд [9] и Данциг [4] пытались различными способами получить решение для некоторых частных случаев. Мы можем присоединить к пространству области двойных стохастических матриц еще ряд неравенств. Так, если положить $x_{12} + x_{23} + x_{31} \leqslant 2$, то исключили бы 3 цикла (1, 2, 3). Общее число таких неравенств, необходимых для исключения циклов, более коротких, нежели n-циклы, фантастически велико. Однако применение некоторых из них оказывается эффективным в частных случаях. Все же нельзя сказать, что общее решение уже известно, даже приблизительно.

ЛИТЕРАТУРА

1. Гейл, Кун и Таккер (Gale D., Kuhn H. W. and Tucker A. W.), Linear programing and the theory of games, in *Activity Analysis of Production and Allocation*, 317—329, New York, 1951.

2. Глисон и Гринвуд (Gleason A. M. and Greenwood R.), Combinatorial relations and chromatic graphs, *Can. J. Math.*, **7**, 1—7 (1955).
3. Гофман и Кун (Hoffman A. and Kuhn H. J.), Systems of distinct representative and linear programing (готовится к печати в *Amer.* Math. Monthly).
4. Данциг, Фулкерсон и Джонсон (Dantzig G., Fulkerson R. and Johnson S.), Solution of a large scale traveling-salesman problem, *J. Oper. Res. Soc. Amer.*, **2**, 393—410 (1954).
5. Кёниг (König D.), Theorie der endlichen und unendlichen Graphen, Chelsea, New York, 1950.
6. Купманс (Koopmans T. C.), Optimum utilization of the transportation system, *Econometric*, **17**, 136—146, Supplement (1949).
7. Манн и Райзер (Mann H. B. and Ryser H.), Systems of distinct representatives, *Amer. Math. Monthly*, **60**, 397—401 (1953).
8. Флуд (Flood M.), On the Hitchcock distribution problem, *Pacific J. Math.*, **3**, 369—386 (1953).
9. Флуд (Flood M.), The traveling-salesman problem, Seminar in Operations Research, paper No 13, 1955.
10. Хичкок (Hitchcock F. L.), The distribution of a product from several sources to numerous localities, *J. Math. Phys.*, **20**, 224—230 (1941).
11. Холл М. (Hall M., Jr.), Distinct representatives of subsets, *Bull. Amer. Math. Soc.*, **54**, 922—926 (1948).
12. Холл Ф. (Hall Ph.), On representatives of subsets, *J. London Math. Soc.*, **10**, 26—30 (1935).
13. Эрдёш и Секереш (Frdös P. and Szekeres G.), A combinatorial problem in geometry, *Compositio Math.*, **2**, 463—470 (1935).

ГЛАВА IV

СУЩЕСТВОВАНИЕ И ПОСТРОЕНИЕ СХЕМ

1. Предварительные замечания

Отбор материала для этой главы оказался особенно затруднительным. В число невключенных вопросов входят матрицы Адамара, впервые исследованные Пэли, многие до сих пор не решенные задачи, самые недавние исследования Брауера. В настоящей главе внимание сконцентрировано на сбалансированных неполных блок-схемах, преимущественно на симметричных схемах, включающих конечные проективные плоскости.

Современные знания в области блок-схем не только неполны, но и в некоторых отношениях беспорядочны. В блок-схеме мы имеем v элементов (в статистических приложениях — совокупностей), размещенных в b блоках по k отдельных объектов в каждом. Каждый элемент встречается r раз, а всякая неупорядоченная пара встречается λ раз. Элементарные условия для параметров будут

$$bk = vr, \quad r(k-1) = \lambda(v-1).$$

Если $b = v$, $r = k$, получаем симметрическую схему. Первое из условий делается очевидным, тогда как второе сводится к $k(k-1) = \lambda(v-1)$.

В некоторых случаях необходимые условия, налагаемые на параметры, являются достаточными для существования схем. Это справедливо для систем, в которых $k = 3$, а $\lambda = 1$ или 2. Но в других случаях существуют арифметические условия; так, для симметричных схем наиболее важными будут, по-видимому, арифметические свойства разности $k - \lambda$, которую мы обозначим через n. С другой стороны, многие схемы зависят от арифметических свойств v или r. Существование определенного класса схем оказалось невозможным, что выяснилось главным образом благодаря результатам Брука и Райзера [6], а также Човла

и Райзера [32]. Однако построена лишь чрезвычайно малая часть возможных схем; трудности в исследовании других случаев в настоящее время оказались непреодолимыми.

2. Латинские квадраты

Латинским квадратом называется квадратная таблица из n элементов (чисел или букв), такая, что каждый из них встречается в точности один раз в каждой строке и в каждом столбце. Так, для $n = 5$ имеем 2 латинских квадрата:

1 2 3 4 5	1 2 3 4 5
2 3 4 5 1	2 1 4 5 3
3 4 5 1 2	3 4 5 1 2
4 5 1 2 3	4 5 2 3 1
5 1 2 3 4	5 3 1 2 4

Из заданного латинского квадрата мы можем образовать другой, переставляя строки или столбцы, производя перестановку букв или же комбинируя эти операции. Квадраты, получаемые друг из друга подобным образом, называют эквивалентными. Легко установить, что всякий латинский квадрат вида 5×5 эквивалентен одному из двух приведенных выше квадратов. При преобразованиях, сохраняющих эквивалентность, будут сохраняться типы разложения на циклы перестановок, определяемых какими-либо двумя строками, скажем

$$\begin{pmatrix} 2 & 1 & 4 & 5 & 3 \\ 4 & 5 & 2 & 3 & 1 \end{pmatrix} = (1\ 5\ 3)\ (2\ 4),$$

хотя этот тип разложения на циклы может относиться к другим двум строкам, если строки переставлены. Таким образом, множество всех типов разложений на циклы остается инвариантным при преобразованиях эквивалентности. Для первого из приведенных выше квадратов все 10 типов разложений на циклы (мы считаем каждую пару строк лишь в одном порядке) суть 5-циклы. Для второго квадрата имеется 6 типов, являющихся 5-циклами, и четыре типа, состоящих из 3-циклов и 2-циклов, причем вторую группу составляют разложения перестановок, в которых участвует вторая строка.

Таблица Кэли для умножения в группе является, разумеется, латинским квадратом, а первый из приведенных выше квадратов представляет собой таблицу Кэли для

циклической группы пятого порядка. Это замечание убеждает нас в существовании латинских квадратов всех порядков.

Существует геометрическая интерпретация латинских квадратов. Будем рассматривать каждое из n^2 мест как точку и проведем через эти точки линии, образующие 3 семейства: 1) строки квадрата; 2) столбцы квадрата; 3) линии, связанные с каждым элементом квадрата, так что они проходят через те ячейки, в которые вписан этот элемент. Эти линии образуют 3-сеть с n^2 узлами. Такая сеть состоит из трех семейств линий, каждая из которых содержит n точек. Линии каждого множества не пересекаются, и через каждую точку проходит в точности одна линия каждого множества. Наоборот, 3-сеть может быть интерпретирована как латинский квадрат. Эквивалентность латинских квадратов можно рассматривать как переименование линий каждого семейства при сохранении всей 3-сети неизменной. Существует $3! = 6$ различных способов рассматривать эти три „параллельных“ пучка, соответствующих строкам, столбцам и линиям одинаковых элементов. Вообще говоря, 6 латинских квадратов, получаемых из одной и той же сети, не будут эквивалентны в ранее принятом смысле. При желании можно рассматривать эту взаимную замену „связей“ (это общее название для строк, столбцов и линий, соединяющих одинаковые элементы) как эквивалентность в более широком смысле. Эта расширенная эквивалентность не будет вообще сохранять типы разложений на цикле, но, как читатель сам может показать в качестве упражнения, оставит неизменным общее число 2-циклов.

Сходство связей вновь делается очевидным, если представить латинский квадрат посредством n^2 троек, выбирая тройку (i, j, k) для случая, когда в ячейке i-й строки и j-го столбца мы найдем элемент k. Условие, при котором n троек представляют латинский квадрат, таково: для всяких двух данных координат заданная пара однозначных чисел u, v должна встречаться в тройке в точности один раз. Это свойство, очевидно, сохраняется при перестановке координат.

Теорема о различных представителях может быть применена к построению латинских квадратов следующим образом.

Теорема. *Пусть задан латинский прямоугольник R с r строками и $n > r$ столбцами. Тогда мы можем по меньшей мере $(n-r)!$ способами добавить к R новую строку, чтобы построить латинский прямоугольник вида $(r+1) \times n$.*

Здесь под латинским прямоугольником вида $r \times n$ подразумевается прямоугольная вида $r \times n$ таблица из n букв, где каждая буква встречается один раз в каждой строке и самое большее один раз в каждом столбце. Для каждого столбца j образуем множество S_j из $n-r$ букв, которые не встречались в j-м столбце. Если мы сможем выбрать различные представители из $S_1, S_2, \ldots, S_n$, то в множество различных представителей каждая буква должна входить в точности один раз, что может быть использовано для построения $(r+1)$-й строки. Разумеется и обратно, всякая $(r+1)$-я строка содержит различные представители для $S_1, S_2, \ldots, S_n$. Мы должны теперь проверить условие С. Поскольку каждая буква встречается r раз в R, то она встречается в точности $n-r$ раз в множествах $S_1, \ldots, S_n$. Но тогда k множеств S_i содержат $k(n-r)$ букв, считая и повторяющиеся; а так как каждая буква встречается в этих k множествах самое большее $n-r$ раз, то они должны содержать по меньшей мере k различных букв и тогда условие С удовлетворяется. Из следствия этой теоремы вытекает, что существует по меньшей мере $(n-r)!$ различных представителей и таким образом самое меньшее $(n-r)!$ возможностей для образования $(r+1)$-й строки. Мы заключаем отсюда, что число латинских квадратов вида $n \times n$ будет по меньшей мере $n!(n-1)!\ldots 2!\,1!$ В самом деле, существует $n!$ возможных первых строк и только одна возможная последняя строка. При добавлении последних двух строк определяются типы разложения их на циклы по отношению ко всяким другим строкам. Если существует c циклов, то мы можем добавлять последние две строки $2^c \times 1$ способами. Следовательно, если $c=1$, то последние два множителя $2!\,1!$ будут верными. Но все остальные множители будут меньшими. В самом деле, второй множитель, как мы уже показали, должен быть $n!/e$, а в работе Эрдёша и Капланского [36] доказано, что k-й множитель приблизительно равен $n!/e^k$, если k мало по сравнению с n. По-видимому, это прибли-

жение не проходит, если $k > \sqrt[3]{n}$. Но даже приведенное выше грубо приблизительное значение показывает, что число квадратов огромно, даже если допустить расширенную эквивалентность; именно, в случае расширенной эквивалентности существует по крайней мере $6(n!)^3$ различных квадратов. Квадраты всех порядков вплоть до семи были перечислены. Те из них, порядок которых не превосходит 6, перечислены Фишером и Иейтсом [25], а Нортон [17] перечислил (7×7)-квадраты. В работе Нортона была допущена ошибка, которую обнаружил Сад [20], произведя независимую проверку числа (7×7)-квадратов Число неэквивалентных квадратов дано в следующей таблице:

n	2	3	4	5	6	7
	1	1	2	2	17	563

Таблица Нортона составлена с учетом расширенной эквивалентности, благодаря чему число типов (7×7)-квадратов свелось к 147, 24 из которых при перестановке связей дают 1 класс эквивалентности каждый, 4 — 2 класса, 61—3 класса и 58 — 6 классов каждый. В соответствии с числом автоморфизмов различные классы эквивалентности могут давать разное число различных квадратов. Если при подсчете общего числа всех различных квадратов T_n, мы произведем нормирование упорядочением первой строки и первого столбца, то получим число приведенных квадратов I_n и $T_n = n!(n-1)!\, I_n$. Здесь

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

Говорят, что два латинских квадрата ортогональны, если при наложении одного квадрата на другой каждая пара одинаковых чисел встречается один и только один раз. Вот, например, ортогональная пара квадратов вида 8×8, наложенных друг на друга

11	22	33	44	55	66	77	88
28	31	46	13	64	75	82	57
37	48	15	26	73	84	51	62
42	17	24	35	86	53	68	71
54	63	72	81	18	27	36	45
65	74	87	52	21	38	43	16
76	85	58	67	32	41	14	23
83	56	61	78	47	12	25	34

Ортогональная пара латинских квадратов эквивалентна 4-сети, проходящей через n^2 точек, где точками будут являться n^2 ячеек, первое семейство „параллелей" задается строками, второе — столбцами, третье — одинаковыми числами первого квадрата, а четвертое — одинаковыми числами второго квадрата. Связи взаимозаменяемы. Мы можем представить ортогональную пару посредством множества n^2 четверок. Например, одна из таких четверок (6, 7, 4, 3) будет четверкой, отнесенной к точке в 6-й строке, 7-м столбце, 4-й линии третьего „параллельного" пучка и 3-й линии четвертого „параллельного" пучка. Эта конкретная ортогональная пара имеет то интересное свойство, что четыре латинских квадрата, получаемых вычеркиванием каждой координаты поочередно, суть латинские квадраты групп. Для первых трех координат (первые однозначные числа, указанные выше) это есть абелева группа типа (4, 2). Для первой, второй и четвертой координат (вторые однозначные числа, упоминаемые выше) это будет диэдральная группа. Для первой, третьей и четвертой получаем квадрат

1	2	3	4	5	6	7	8
3	8	1	6	7	4	5	2
5	6	7	8	1	2	3	4
7	4	5	2	3	8	1	6
8	7	6	5	4	3	2	1
6	1	8	3	2	5	4	7
4	3	2	1	8	7	6	5
2	5	4	7	6	1	8	3

который является групповой таблицей для диэдральной группы. Для второй, третьей и четвертой координат имеем квадрат

1	8	7	2	4	5	6	3
7	2	1	8	6	3	4	5
5	4	3	6	8	1	2	7
3	6	5	4	2	7	8	1
8	1	2	7	5	4	3	6
2	7	8	1	3	6	5	4
4	5	6	3	1	8	7	2
6	3	4	5	7	2	1	8

который является групповой таблицей для элементарной абелевой группы.

Возможно также построить множество квадратов, которые попарно взаимно ортогональны. Множество m пар ортогональных латинских квадратов эквивалентно $m+2$ параллельным пучкам, проходящим через n^2 точек. Максимумом для m будет $n-1$, и такое множество называется полностью ортогональным. Стивенс [22] заметил, что полное множество ортогональных квадратов дает конечную евклидову плоскость; справедливо и обратное.

Эйлер [35] первый исследовал латинские квадраты, предложив в 1779 г. задачу о 36 офицерах. Он поставил вопрос, возможно ли выбрать 36 офицеров 6 рангов из 6 полков по одному офицеру каждого ранга от каждого полка и расположить их в каре так, чтобы в каждом ряду и в каждой шеренге было бы по одному офицеру каждого ранга и по одному от каждого полка. Задача эквивалентна построению парных ортогональных 6×6 квадратов. Терри [23] систематическими попытками показал, что это невозможно.

Была высказана гипотеза, что для $n = 4k+2$ не существует пар ортогональных квадратов: она подтвердилась пока только для случаев $n=2$ и $n=6$. В результате обширных исследований с помощью СВАК (Калифорнийский университет) не удалось построить ортогональную пару (10×10) квадратов. После 100 часов работы быстродействующей машины доля исследованных возможных случаев оказалась настолько малой, что никаких заключений нельзя было сделать. Впрочем, некоторые выводы можно сделать на том основании, что аналогичные поиски ортогональных пар (8×8)-квадратов дали свыше 200 пар менее чем за 15 минут.

Наши познания об ортогональных квадратах весьма отрывочны. Манн [12] нашел метод построения взаимно ортогональных квадратов, являющийся лучшим из известных методов. Пусть $n = p_1^{e_1} p_2^{e_2} \ldots p_r^{e_r}$ будет разложением n в произведение простых чисел; здесь $p_1, p_2, \ldots, p_r$ — различные простые числа. Манн строит m взаимно ортогональных $(n \times n)$-квадратов, где m — наименьшее из чисел $p_1^{e_1}-1, \ldots, p_r^{e_r}-1$. Он берет конечное кольцо R, которое является прямой суммой $R = F_1 \oplus F_2 \oplus \ldots \oplus F_r$, где F_i есть конечное поле порядка $p_i^{e_i}$. Возьмем $x_0 = 0$, $x_1 = 1, \ldots, x_n$ в качестве элементов R. Возьмем также элемент

$u = u_1 + u_2 + \ldots + u_r$, где мультипликативный порядок u_i в F_i не меньше чем m (если каждый u_i есть простой корень, это будет верно). Тогда в r-м квадрате ($r = 0, \ldots, m-1$) на (i, j) месте будет стоять элемент $u^r x_i + x_j$. Почти очевидно, что r-й квадрат есть латинский квадрат. И чтобы показать, что при наложении r-го и s-го квадратов появляется каждая пара, нам нужно прежде всего установить, что разность $u^r - u^s$ имеет инверсию. Этот результат дает, например, три взаимно ортогональных квадрата порядка 20. Никто не нашел большего числа ортогональных квадратов, чем гарантирует результат Манна. Для полноты множества ортогональных квадратов требуется существование аффинной и, следовательно, проективной конечной плоскости. Это будет рассмотрено позже.

3. Системы троек Штейнера.

В 1852 г. Штейнер [34] поставил следующую задачу. Для какого целого числа n возможно разделить n букв на тройки таким образом, чтобы каждая пара букв встречалась в одной и только одной тройке? Здесь мы имеем в виду неупорядоченные пары и неупорядоченные тройки. Необходимые условия для n легко отыскать. Каждая буква встречается в тройке с двумя другими буквами. Так как буква встречается в точности один раз с каждой другой буквой, то $n-1$ должно быть четным, и, следовательно, $n \equiv 1 \pmod 2$. Так как каждая тройка содержит три пары, а каждая пара встречается точно один раз, то общее число пар $n(n-1)/2$ должно быть кратным трем. Комбинируя эти условия, получаем, что n имеет вид $n = 6k+1$ или $6k+3$.

В 1859 г. Рисс [19] конструктивным методом показал, что необходимые условия являются также достаточными и что система троек существует для каждого $n = 6k+1$ или $n = 6k+3$. Для $n = 3, 7, 9$ мы получаем решения

$n = 3$:	$n = 7$:	$n = 9$:
123	123	123
	145	145 249 348
	167	168 256 357 467
	246	179 278 369 589
	257	
	347	
	356	

Эти решения являются единственными в пределах эквивалентности. Два решения будут называться эквивалентными, если одно может быть получено из другого подстановкой букв и перестановкой троек. Для $n = 13$ существуют в точности два неизоморфных решения.

В оба решения мы можем включить тройки

1, 2, 3
1, 4, 5 2, 4, 6
1, 6, 7 2, 5, 7 4, 3, 8
1, 8, 9 2, 8, 10 4, 7, 9 7, 3, 11
1, 10, 11 2, 9, 12 4, 10, 13 7, 8, 13 8, 5, 11 6, 9, 11
1, 12, 13 2, 11, 13 4, 11, 12 7, 10, 12 8, 6, 12 3, 5, 12

Для первого решения мы также берем тройки

3, 6, 10, 3, 9, 13 5, 6, 13 5, 9, 10

Для второго решения мы берем

3, 6, 13 3, 9, 10 5, 6, 10 5, 9, 13

Системы троек Штейнера из 15 букв изучили Кол, Уайт и Каммингс [9], которые нашли 80 различных систем. Позднее Фишер [24] перечислил системы из 15 букв, отыскав 79 систем и пропустив одну из таблицы Кола. Недавно автор и Свифт произвели систематическое исследование систем из 15 букв, используя СВАК. Это оказалось проверкой результата, найденного Колом, который не был нам заранее известен.

Задавая 2 системы штейнеровых троек порядков t_1 и t_2, мы можем построить другую систему порядка t_1t_2 следующим образом: пусть (a_i, a_j, a_k) — какая-либо тройка системы A порядка t_1, а (b_r, b_s, b_u) — какая-либо тройка системы B порядка t_2. Образуем новую систему C с t_1t_2 элементами c_{ij}, $i = 1, \ldots, t_1$, $j = 1, \ldots, t_2$. Тогда (c_{ir}, c_{js}, c_{ku}) будет тройкой системы C, если: 1) $r = s = u$ и (a_i, a_j, a_k) является тройкой из A; или 2) $i = j = k$ и (b_r, b_s, b_u) является тройкой из B; или 3) как (a_i, a_j, a_k) является тройкой из A, так и (b_r, b_s, b_u) является тройкой из B. Легко проверить, что эти правила образуют C-систему

троек Штейнера. Те тройки, в которых $r=s=u=1$, образуют подсистему C, изоморфную A, а те, в которых $i=j=k=1$, образуют систему, изоморфную B.

Построение систем троек Штейнера всех порядков $n=6k+1$ или $6k+3$, которое здесь будет дано, нашел Мур [15].

Теорема. *Если существует система троек Штейнера порядка t_2, содержащая подсистему порядка t_3, и если существует также система троек Штейнера порядка $t_1>1$, то мы можем построить систему порядка $t=t_3+t_1(t_2-t_3)$, содержащую t_1 подсистем порядка t_2 и одну подсистему порядка t_1.*

Доказательство. В этом доказательстве мы считаем, что единственный элемент образует систему троек порядка 1, где при $t_3=1$, требование, чтобы система порядка t_2 содержала одну систему порядка t_3, удовлетворяется для любой системы порядка $t_2>1$. Мы строим множество элементов $t=t_3+t_1(t_2-t_3)$, использованных в (t_1+1)-множествах:

$$
\begin{array}{lll}
S_0\colon & a_1,\ a_2,\ \ldots,\ a_{t_3}, & \\
S_1\colon & b_{11},\ \ldots,\ b_{1s}, & \\
S_2\colon & b_{21},\ \ldots,\ b_{2s}, & s=t_2-t_3.\\
\ldots\ldots\ldots\ldots & & \\
S_{t_1}\colon & b_{t_1 1},\ \ldots,\ b_{t_1 s}. &
\end{array}
$$

Мы образуем тройки этих t элементов по трем правилам: 1. Ассоциируем элементы S_0 с системой порядка t_3 и берем тройку (a_i, a_j, a_k), если эти элементы соответствуют тройкам в этой системе. 2. Приводим S_0 и всякое S_i $(i=1,\ldots,t_1)$ в соответствие с системой порядка t_2, а S_0 — в соответствие с подсистемой порядка t_3. Тройки элементов a уже определены правилом 1. Другие тройки содержат самое большее один элемент a. Образуем тройки (a_m, b_{ij}, b_{ik}) или (b_{ij}, b_{ik}, b_{ir}), согласно соответствию с системой порядка t_2. 3. Если (j, k, r) есть тройка системы порядка t_1, образуем все тройки (b_{jx}, b_{ky}, b_{rz}), где вторые индексы удовлетворяют условию $x+y+z\equiv 0 (\mathrm{mod}\, s)$.

Эти три правила, взятые вместе, дают тройки для системы порядка t, и мы устанавливаем, что S_0 и S_i $(i=1,\ldots,t_1)$ образуют t_1 систем порядка t_2. Первое правило дает тройки

в S_0, и мы замечаем, что тройка, содержащая два элемента a, будет иметь в качестве третьего элемента также a. Второе правило дает тройки с одним элементом a и вторым b, а третий элемент будет также b из той же самой строки, что и второй. Это правило дает также тройки для элементов b из одной и той же строки. Здесь в случае двух элементов b из S_i третьим элементом в тройке будет или a, или b из той же строки. Третье правило охватывает тройки из трех различных строк. Если выбирать элементы из двух строк, то третий ряд определяется системой порядка t_1. Условие $x+y+z\equiv 0 \pmod{s}$ для вторых индексов убеждает нас в том, что всякие два элемента могут быть выбраны произвольно, и определяет единственным образом третий элемент тройки. Мы также замечаем, что в соответствии с этим условием, поскольку $s\equiv 0 \pmod{s}$, элементы $b_{1s}, \ldots, b_{t_1 s}$ образуют подсистему порядка t_1.

Мы можем доказать существование систем всех порядков $n=6k+1$ и $n=6k+3$, используя несколько частных случаев этого правила:

(A)	$t_1=t'$,	$t_2=3$,	$t_3=1$,	$t=2t'+1$,	$t'\geqslant 3$,
(B)	$t_1=3$,	$t_2=t'$,	$t_3=1$,	$t=3t'-2$,	$t'\geqslant 3$,
(C)	$t_1=3$,	$t_2=t'$,	$t_3=3$,	$t=3t'-6$,	$t'\geqslant 7$,
(D)	$t_1=t'$,	$t_2=9$,	$t_3=3$,	$t=6t'+3$,	$t'\geqslant 3$,
(E)	$t_1=3$,	$t_2=t'$,	$t_3=7$,	$t=3t'-14$,	$t'\geqslant 15$.

Мы можем применить правила рекуррентно, чтобы построить системы для всех значений n по модулю 36. Начинаем с систем порядков 1, 3, 7, 9, 13. Заметим, что для применения правила (E) мы должны иметь подсистему порядка 7 в системе порядка t'. В самом деле, для всякого допустимого порядка, не превосходящего 15, существует система с подсистемой порядка 7. Так как система порядка $t=t_3+t_1(t_2-t_3)$ имеет подсистемы порядков t_1, t_2 и t_3, то свойство иметь подсистему порядка 7 сохраняется при построении. Нам нужен метод более быстрого построения, обеспечивающий достаточно начальных систем с подсистемами порядка 7. Для некоторых начальных порядков должны быть использованы специальные случаи, вроде $85=1+7(13-1)$.

Вид $n\ (=t)$	Правило	Значение для t'
$36k+1$	(B)	$12k+1$
$36k+3$	(A)	$18k+1$
$36k+7$	(A)	$18k+3$
$36k+9$	(D)	$6k+1$
$36k+13$	(E)	$12k+9$
$36k+15$	(A)	$18k+7$
$36k+19$	(B)	$12k+7$
$36k+21$	(D)	$6k+3$
$36k+25$	(B)	$12k+9$
$36k+27$	(A)	$18k+13$
$36k+31$	(A)	$18k+15$
$36k+33$	(C)	$12k+13$

4. Построение блок-схем

Системы троек Штейнера являются частными случаями общего класса размещений, которые мы называем блок-схемами. Предположим, что мы имеем v элементов, размещенных в b блоках, так что каждый блок содержит k различных элементов, каждый элемент появляется в r блоках и каждая (неупорядоченная) пара элементов встречается всего λ раз. Существуют два элементарных условия, которым эти пять параметров должны удовлетворять

$$bk = vr, \quad r(k-1) = \lambda(v-1).$$

Первое выражает равенство общего числа появлений всех элементов при подсчете двумя способами. С одной стороны, каждый из b блоков содержит k элементов, а с другой стороны, каждый из v элементов встречается r раз. Второе условие вытекает из рассмотрения пар, в которых встречается данный элемент x_1. Он встречается r раз и всякий раз в паре с одним из $k-1$ других элементов, но он также должен встречаться с каждым из остающихся $v-1$ элементов λ раз. Системы троек Штейнера являются частным случаем, в котором $k=3$, $\lambda=1$. Следовательно, в этом случае

$$3b = vr, \quad 2r = v-1,$$

откуда

$$v = 2r+1, \quad b = \frac{r(2r+1)}{3}.$$

Таким образом, оказывается, что $r \equiv 0, 1 \pmod 3$, а $v = 6m + 1$ или $v = 6m + 3$, т. е. получаются те самые необходимые условия, которые мы рассматривали в предыдущей главе. В случае систем троек Штейнера мы видели, что эти необходимые условия являются также достаточными для существования решения. Но вообще эти условия не являются достаточными; необходимо найти условия более глубокого характера. Те условия, которые известны, имеют арифметическую природу, причем совершенно неясно, каковы же должны быть истинные условия.

Если $v = b$, то $k = r$ и $k(k-1) = \lambda(v-1)$. В этом случае мы называем схему симметричной блок-схемой. Частным случаем симметричной блок-схемы при $\lambda = 1$ является конечная проективная плоскость. Эти схемы подверглись наиболее интенсивному изучению. Для симметричных схем самым важным числом, связанным с существованием схемы, оказывается число $n = k - \lambda$. В самом деле, в случае проективных плоскостей плоскость существует, когда n — простое число или степень простого числа. Неизвестны никакие другие значения, которые давали бы конечные плоскости. Но мы очень еще далеки от какого-либо категорического утверждения.

В статистике называют блок-схемы сбалансированными неполными блок-схемами. Более общим видом схем является частично сбалансированная неполная блок-схема, которая отличается от сбалансированных схем тем, что число появлений пар не постоянно. Всякий элемент x_i может иметь t видов связей, а x_i встречается в j-й связи λ_j раз: $j = 1, 2, \ldots, t$. Если возможно разделить все элементы на группы таким образом, чтобы соответствующее соотношение между двумя элементами зависело только от группы, к которой они принадлежат, то схема называется схемой с групповой делимостью. Латинские квадраты и, более общо, ортогональные множества латинских квадратов могут быть рассматриваемы как схемы с групповой делимостью. Рассмотрим mn элементов, разделенных на m групп из n элементов. Будем говорить, что элементы в одной и той же группе первично связаны, и положим $\lambda_1 = 0$. Будем также утверждать, что элементы в разных группах вторично связаны, и положим $\lambda_2 = 1$. Тогда в случае n^2 блоков по m элементов в каждом мы получим мно-

жество элементов, которые определяют $m-2$ взаимно ортогональных латинских квадрата точно тем же способом, каким они были изображены ранее. Образцом превосходного изложения теории частично сбалансированных схем является исследование Боса, Клэтуорти и Шрикхенда [4]. В нем освещены как статистическая, так и комбинаторная стороны вопроса. Эта работа содержит также весьма обширную библиографию.

В блок-схемах элементы размещены в множества одинаковых размеров; требуется также, чтобы единичные элементы, а также пары элементов появлялись одно и то же число раз. Мы можем даже требовать большего и рассматривать так называемые тактические конфигурации, требуя, скажем, чтобы все тройки, четверки или пятерки встречались одинаково часто. Об этом так мало известно, что мы упомянем только 2 случая, которые связаны с любопытными с математической точки зрения группами Мэтью. Дробно-линейная группа (т. е. проективная группа проективных линий) есть множество преобразований

$$x \longrightarrow \frac{ax+b}{cx+d},$$

где $ad-bc \neq 0$, рассматриваемых как перестановки элементов поля F, включающего формальный элемент ∞, такой, что $1/0=\infty$. Если мы положим, что F есть поле из 11 элементов, то дробно-линейная группа преобразует 6 элементов ∞, 1, 3, 4, 5, 9 в 132 множества. Каждая пятерка из 12 элементов ∞, 0, 1, ..., 10 встречается точно в одной из шестерок. Наибольшая группа, включающая в себя систему шестерок, есть пятиричная транзитивная группа Мэтью порядка $12\cdot11\cdot10\cdot9\cdot8$. Аналогично дробно-линейная группа над полем с 23 элементами преобразует 8 элементов ∞, 0, 1, 3, 12, 15, 21, 22 в 768 восьмерок, таких, что каждая пятерка из 24 элементов ∞, 0, 1, ..., 22 встречается в точности в одной восьмерке. Наибольшей группой, содержащей восьмерки, является пятиричная транзитивная группа Мэтью из 24 букв порядка $24\cdot23\cdot22\cdot21\cdot20\cdot48$. Эти две группы суть единственные известные пятиричные транзитивные группы (естественно, за исключением знакопеременных и симметрических групп), а подгруппы с фиксированной буквой являются единственными

известными четверичными транзитивными группами. Эти группы благодаря некоторым свойствам являются единственными в своем роде. Обобщая теорему Жордана, автор [27] показал, что единственная четверичная транзитивная группа конечного или бесконечного числа букв, если подгруппа, фиксирующая 4 буквы, имеет конечный четный порядок, является группой Мэтью из 11 букв (разумеется, вместе с симметрическими группами из 4 и 5 букв и знакопеременными группами из 6 и 7 букв). Группы Мэтью из 23 и 24 букв суть транзитивные расширения группы коллинеаций проективной плоскости с 21 точкой. Цассенхауз [31] показал, что существуют единственные четверичные транзитивные расширения группы коллинеаций любого проективного пространства.

Далее мы будем рассматривать только сбалансированные неполные блок-схемы с параметрами v, b, r, k, λ, удовлетворяющие необходимым условиям $bk = vr$, $r(k-1) = \lambda(v-1)$. О них известно больше, нежели о других классах схем, а все методы, применявшиеся во всех других случаях, были применены и для них.

Существование нескольких классов этих схем было доказано непосредственным построением. Мы уже рассмотрели системы троек Штейнера, которые являются частным видом схем для $k=3$, $\lambda=1$, откуда $2r=v-1$ и $3b=vr=(2r+1)r$. Здесь имели место два случая: $v=6t+1$, $b=t(6t+1)$, $r=3t$, $k=3$, $\lambda=1$ и $v=6t+3$, $b=(2t+1)(3t+1)$, $r=3t+1$, $k=3$, $\lambda=1$. Когда $\lambda=2$ и $k=3$, мы получим $2r=2(v-1)$ и $vr=3b$, откуда $v=r+1$ и $r(r+1)=3b$. Здесь $r\equiv 0,2 \pmod 3$ и $v\equiv 0,1 \pmod 3$. Если v имеет вид $6t+1$ или $6t+3$, то ясно, что две системы троек Штейнера для тех же самых v элементов, взятых вместе, дадут решение. Мы должны, таким образом, найти решение для

$$E_1\colon\quad v=6t+6,\ b=2(t+1)(6t+5),\ r=6t+5,\ k=3,\ \lambda=2,$$

$$E_2\colon\quad v=6t+4,\ b=2(2t+1)(3t+2),\ r=6t+3,\ k=3,\ \lambda=2.$$

Метод построения, предложенный Босом [2], основан на применении разностей некоторой аддитивной группы, обычно вычетов по модулю некоторого целого числа m. Для рядов

E_1 мы берем один элемент b и аддитивные вычеты по модулю $6t+5$. Сначала мы берем $6t+5$ троек $(b, j, j+3t+2)$, $j=0, \ldots, 6t+4 \pmod{6t+5}$. Они дают нам b дважды с каждым другим элементом, а каждую пару один раз, причем они отличаются друг от друга на

$$3t+2 \text{ или } -(3t+2) \equiv 3t+3 \pmod{6t+5}.$$

Теперь мы используем два множества разностей:

1. $(i, 2t+3-2i, 2t+3-i) = (x_i, y_i, z_i)$, где $i=1, 2, \ldots, t+1$. Здесь $z_i = x_i + y_i$.

2. $(2i, 3t+3-i, 3t+2-i) = (x_i, y_i, z_i)$, где $i=1, 2, \ldots, t$. Здесь $x_i + y_i + z_i = 6t+5$.

С помощью первого множества мы строим все тройки $(j, j+x_i, j+z_i)$, $i=1, \ldots, t+1$, $j=0, \ldots, 6t+4 \pmod{6t+5}$, а из второго множества — все тройки $(j, j+x_i, j+x_i+y_i)$, $i=1, \ldots, t$, $j=0, \ldots, 6t+4 \pmod{6t+5}$. Мы утверждаем, что эти тройки приводят к построению схем. Для всяких двух различных вычетов r, $s \pmod{6t+5}$ возьмем одну из двух величин $r-s$ или $s-r$, лежащих в последовательности $1, \ldots, 3t+2$. Назовем ее их меньшей разностью d. Тогда r и s встречаются одновременно один раз в тройке одного из рядов, всякий раз, когда d является одной из меньших разностей множества разностей. Предположим, что $d=y_i$ для некоторого i первого ряда. Тогда $(j+z_i)-(j+x_i) \equiv y_i \equiv d \pmod{6t+5}$. Если положим $r-s \equiv d \pmod{6t+5}$, то, определив j посредством $j+z_i \equiv r \pmod{6t+5}$, получим $j+x_i \equiv j+z_i-d \equiv r-d \equiv s$ и тройка $(j, j+x_i, j+z_i) = (j, s, r)$ будет содержать r и s. В обоих рядах x_i, y_i, z_i — меньшие разности, и мы находим, что каждая меньшая разность $1, 2, \ldots, 3t+1$ встречается в точности дважды, а разность $3t+2$ — однажды, встречаясь второй раз в тройках $(b, j, j+3t+2)$. Следовательно, каждая пара встречается одновременно в точности два раза, и мы построили схему. Для рядов E_2 мы используем элемент b и вычеты по модулю $6t+2$. Берем тройки $(b, j, j+3t+1)$, $j=0, \ldots, 6t+1 \pmod{6t+2}$ и таким образом получаем тройки, чьи меньшие разности заданы посредством

$$(i, 2t+1-2i, 2t+1-i), \quad i=1, \ldots, t,$$
$$(2i, 3t+1-i, 3t+1-i), \quad i=1, \ldots, t.$$

Это использование разностей можно рассматривать как построение схем с заданной группой автоморфизмов. В двух приведенных выше случаях мы имели группу автоморфизмов порядка $v-1$, которая была циклической и, поскольку рассматривались элементы, имела транзитивные составляющие, причем одна из них состояла из единственного элемента b, а другая содержала оставшиеся $v-1$ элементов. Это можно обобщить, если рассматривать автоморфизм с несколькими транзитивными составляющими. В качестве примера возьмем семейство систем троек Штейнера с параметрами $v=6t+3$, $b=(3t+1)(2t+1)$, $r=3t+1$, $k=3$, $\lambda=1$. Если мы возьмем элементы j_1, j_2, j_3, где j в каждом случае пробегает значения от 0 до $2t \pmod{2t+1}$, мы получим всего $6t+3$ элементов. Теперь возьмем $3t$ базисных троек $[i_1, (2t-i)_1, 0_2]$, $[i_2, (2t-i)_2, 0_3]$, $[i_3, (2t-i)_3, 0_1]$, где $i=1, \ldots, t$ во всех трех случаях, и также единственную базисную тройку $(0_1, 0_2, 0_3)$. Если мы возьмем $3t+1$ базисных троек и добавим повсюду $j=0, 1, \ldots, 2t \pmod{2t+1}$, мы получим всего $(3t+1)(2t+1)=b$ троек. Это будут штейнеровские системы троек, поскольку в базисных тройках каждая „смешанная“ разность $r \neq s$, $d_{rs} \equiv 0, 1, \ldots, 2t \pmod{2t+1}$ и каждая „чистая“ разность $d_{rr} \equiv 1, 2, \ldots, 2t \pmod{2t+1}$ появляются в точности один раз, так как $b_r - c_s \equiv (b-c)_{rs} \equiv d_{rs} \pmod{2t+1}$, где b_r и c_s входят в базисную тройку. Здесь $r, s=1, 2, 3$. По-видимому, для систем троек Штейнера в случае $v=6t+1$ требуется не столь простое построение.

Существенная часть этого „метода симметрически повторяющихся разностей“, естественно, состоит в отыскании подходящих разностных чисел. Важно отметить, что в одном случае модуль был $v-1$, а в другом — $v/3$. Но поскольку мы показали, что необходимые условия являются также достаточными, нет оснований предполагать, что эти числа имеют какое-либо конкретное арифметическое значение, относящееся не к постановке задачи, а только к ее частному построению.

При построении схем были использованы разнообразные остроумные применения конечных полей. Приведем доказательство простого случая.

Теорема. *Если $4t-1$ есть степень простого числа*

$q = p^r$, то существует симметрическая схема с параметрами $v = b = 4t - 1$, $k = r = 2t - 1$, $\lambda = t - 1$.

Доказательство. Рассмотрим конечное поле K из q элементов. Используем хорошо известные факты, что в K имеется $(q-1)/2$ ненулевых квадратов и $(q-1)/2$ неквадратов и что произведение двух квадратичных вычетов или двух неквадратов есть квадрат. Итак, поскольку $q \equiv 3 \pmod 4$, то элемент -1 есть невычет. Предположим, что $x^2 - y^2 = 1$ имеет N решений (x^2, y^2) при $x^2 \neq 0$, $y^2 \neq 0$. Мы утверждаем, что $x^2 - y^2 = d$ при $d \neq 0$, $x^2 \neq 0$, $y^2 \neq 0$ тоже имеет N решений (x^2, y^2). Потому что, если $d = u^2$ — квадратные решения $x^2 - y^2 = d$, являющиеся квадратичными вычетами, то они находятся во взаимно однозначном соответствии с такими же решениями $X^2 - Y^2 = 1$, где $X = x/u$, $Y = y/u$. С другой стороны, если d не является квадратом, то $d = -u^2$ и мы получим взаимно однозначное соответствие с $X^2 - Y^2 = 1$, полагая $Y = x/u$, $X = y/u$. Отсюда в каждом случае $x^2 - y^2 = d \neq 0$ имеет N решений при $x^2 \neq 0$, $y^2 \neq 0$. Таким образом, все значения $x^2 - y^2$ при $x^2 \neq 0$, $y^2 \neq 0$, $x^2 \neq y^2$ дают каждую разность $d \neq 0$ одно и то же число раз N. Но всего существует $[(q-1)/2]\,[(q-3)/2]$ разностей $x^2 - y^2$ и всего $q - 1$ значений d. Отсюда $(q-1)N = (q-1)(q-3)/4$ и $N = (q-3)/4$.

Теперь для $q = 4t - 1$ получим $(q-1)/2 = 2t - 1$ и $(q-3)/4 = t - 1$. Следовательно, если мы образуем q множеств $(x_1 + b, x_2 + b, \ldots, x_{2t-1} + b)$, где $x_1, \ldots, x_{2t-1}$ суть ненулевые квадраты в K, а b пробегает q элементов K, то получим $4t - 1$ блоков с $2t - 1$ элементами в каждом блоке. Каждый элемент w встречается один раз для данного i в форме $x_i + b$, так что каждый элемент встречается $2t - 1$ раз. Для некоторой пары w, z, если $w - z = d = x_1 - x_j$, определяя b как $b = w - x_i$, получаем $x_i + b = w$, $x_j + b = z$. Следовательно, пара w, z встречается в блоке так же часто, как d появляется в качестве разности $d = x_i - x_j$. Но это имеет место $N = (q-3)/4$ раз для всякого $d \neq 0$, так что мы имеем симметрическую схему для $\lambda = N = t - 1$. Это полностью исчерпывает доказательство.

Другие построения, зависящие от конечных полей, более сложны. Так, если $4t + 1$ есть степень простого числа, то

существует схема с $v=12t+4$, $b=(3t+1)(4t+1)$, $r=4t+1$, $k=4$, $\lambda=1$. Здесь при $4t+1=q=p^r$ мы снова применяем поле K из q элементов. Построение будет проведено без доказательства. Пусть x будет первообразный корень из K. Тогда для некоторого нечетного b мы получим $(x^b+1)/(x^b-1)=x^s$, где s также нечетное. Наши $v=12t+4$ элементов будут состоять из трех воспроизведений элементов K и дополнительного элемента ∞. Следующие четверки будут являться базисом схемы

$$\begin{array}{llll}(x_1^{2i}, & x_1^{2t+2i}, & x_2^{2i+b}, & x_2^{2t+2i+b}),\\ (x_2^{2i}, & x_2^{2t+2i}, & x_3^{2i+b}, & x_3^{2t+2i+b}),\\ (x_3^{2i}, & x_3^{2t+2i}, & x_1^{2i+b}, & x_1^{2t+2i+b}),\\ (\infty, & 0_1, & 0_2, & 0_3).\end{array} \qquad i=0,\ 1,\ \ldots,\ t-1$$

Мы получим всю схему, добавляя к элементам базисных четверок все элементы K поочередно.

Много блок-схем дают конечные геометрии. Евклидова геометрия s измерений над полем K с p^r элементами, которую мы обозначим $EG(s, p^r)$, имеет точки $P=(x_1, \ldots, x_s)$, $x_i \in K$, $i=1, \ldots, s$ и подпространства всех измерений $1, \ldots, s$. Пространством u измерений будет множество точек

$$a_1P_1+a_2P_2+\ldots+a_uP_u, \quad a_1+a_2+\ldots+a_u=1;$$

u — минимальное для множества. Аналогично проективная геометрия s измерений над полем K, которую мы обозначим $PG(s, p^r)$, имеет точки $(px_0, px_1, \ldots, px_s) \neq (0, \ldots, 0)$, $x_i \in K$ и p пробегает все поле K, исключая 0. В $PG(s, p^r)$ имеются подпространства всех измерений $1, \ldots, s$, а пространство u измерений будет векторным пространством, определяемым u независимыми точками.

В конечной евклидовой или проективной геометрии существует единственная прямая, соединяющая две различные точки. Если исходить из того, что в этих геометриях две несовпадающие точки соединяет единственная прямая и что каждая прямая содержится в одинаковом числе подпространств размерности u, то из этого следует, что если взять точки как элементы, то подпространства размерности u образуют блок-схему.

Теорема. *u-мерное подпространство в* $PG(s, q)$, $q=p^r$, *образует блок-схему с параметрами*

$$v=\frac{q^{s+1}-1}{q-1},$$

$$b=\frac{(q^{s+1}-1)(q^{s+1}-q)\ \dots\ (q^{s+1}-q^u)}{(q^{u+1}-1)(q^{u+1}-q)\ \dots\ (q^{u+1}-q^u)}=b(s, u),$$

$$r=\frac{(q^{s+1}-q)\ \dots\ (q^{s+1}-q^u)}{(q^{u+1}-q)\ \dots\ (q^{u+1}-q^u)}=r(s, u),$$

$$k=\frac{q^{u+1}-1}{q-1},$$

$$\lambda=1, \qquad \text{если } u=1,$$

$$\lambda=\frac{(q^{s+1}-q^2)\ \dots\ (q^{s+1}-q^u)}{(q^{u+1}-q^2)\ \dots\ (q^{u+1}-q^u)}=\lambda(s, u), \qquad \text{если } u>1.$$

Употребляя ту же самую символику, мы получим следующую теорему.

Теорема. *u-мерные подпространства в* $EG(s, q)$, $q=p^r$, *образуют блок-схему с параметрами*:

$$v=q^s,$$
$$b=b(s, u)-b(s, u-1),$$
$$r=r(s, u),$$
$$k=q^u,$$
$$\lambda=\lambda(s, u).$$

Конечные евклидовы или проективные пространства размерности три или выше необходимо являются геометриями с координатами из конечных полей, как было указано выше. Существуют, однако, конечные плоскости, которые не могут быть получены из конечных полей: они называются недезарговыми плоскостями.

Теорема. *Прямые на проективной плоскости с* $n+1$ *точками на прямой линии образуют симметричную блок-схему с параметрами*

$$v=n^2+n+1,$$
$$b=n^2+n+1,$$
$$r=n+1,$$
$$k=n+1,$$
$$\lambda=1.$$

Для всех известных плоскостей число n является степенью простого числа, но, может быть, существуют и другие плоскости, которые еще не построены. Следует сделать

одно существенное замечание. Блок-схема с параметрами проективной или евклидовой плоскости будет определенно плоскостью. Если блок-схема с параметрами для случаев более высокой размерности является геометрией, то она будет определенно дезарговой, но она может и не быть геометрией. Так, $v=b=121$, $r=k=40$, $\lambda=13$ суть параметры для проективных геометрий $PG(3, 3)$, содержащихся в $PG(4, 3)$, но, как мы увидим далее, существуют и другие схемы с этими же параметрами. Различие возникает потому, что в случае плоскостей все плоскости, прямые и точки удовлетворяют комбинаторным требованиям. Но для $PG(3, 3)$, содержащейся в $PG(4, 3)$, комбинаторные требования распространяются на 4-пространства, 3-пространства и 2-пространства как пересечения 3-пространств, но ни в коем случае не прямых. Превосходное описание этих конструктивных методов дано в книге Манна [13].

Свойство симметрических схем, которое будет доказано в следующем разделе, таково, что всякие два блока имеют вместе в точности λ элементов. Так, если мы возьмем фиксированный блок B_0, то пересечениями B_0 с B_1, ..., B_{v+1} будут множества β_1, ..., β_{v+1}, каждое из которых содержит λ элементов. B_0 и множества β содержат все вхождения k элементов B_0. Следовательно, в β_1, ..., β_{v+1} каждый элемент из k встречается $r-1$ раз, а каждая пара встречается $\lambda-1$ раз. Множества β образуют так называемую производную блок-схему. Аналогично, если мы вычеркнем B_0 и все β, то у нас останется так называемая остаточная схема. Так, для симметрической схемы мы имеем $v=v$, $b=v$, $r=k$, $k=k$, $\lambda=\lambda$. Для производной схемы $v'=k$, $b'=v-1$, $r'=k-1$, $k'=\lambda$, $\lambda'=\lambda-1$. Для остаточной схемы $v''=v-k$, $b''=v-1$, $r''=k$, $k''=k-\lambda$, $\lambda''=\lambda$.

Приведем пример из статьи Нанди [16]:

$v=b=15$, $r=k=7$, $\lambda=3$

1	1	1	1	1	1	1	2	2	2	2	3	3	3	9
2	2	2	3	4	4	5	3	4	4	5	4	4	5	10
3	3	6	7	5	6	7	6	5	7	6	5	6	6	11
4	5	7	8	6	8	8	8	8	8	7	7	7	8	12
9	12	9	11	11	10	9	10	9	11	10	10	9	9	13
10	13	13	14	12	13	10	12	14	12	11	13	12	11	14
11	14	15	15	15	14	12	15	15	13	14	15	14	13	15

Для производной схемы получаем $v=7$, $b=14$, $r=6$, $k=3$, $\lambda=2$. Для остаточной схемы получаем $v=8$, $b=14$, $r=7$, $k=4$, $\lambda=3$.

Если отбросить последний блок, то остаточная конфигурация включает элементы 1, ..., 8. Здесь для каждого блока четверок существует другой блок, который имеет три общих с ним элемента. Но для остаточной схемы, полученной отбрасыванием первого блока и еще каких-либо элементов, это не так. Следовательно, одна и та же симметричная схема может давать неизоморфные остаточные схемы.

О применении разностей в построении схем уже говорилось. Мы рассмотрим здесь систематическую попытку построить симметрические схемы, которые даются разностями по модулю v. Как обычно, $k(k-1)=\lambda(v-1)$. Если $a_1, a_2, \ldots, a_k \pmod v$ суть вычеты, такие, что для любого $d \equiv 0 \pmod v$ сравнение

$$a_i - a_j \equiv d \pmod v$$

справедливо в точности для λ выборов (a_i, a_j) из всех a, то мы назовем $a_1, \ldots, a_k$ множеством разностей по модулю v. Если задать множество разностей, то v множеств

$$S_j = \{a_1 + j,\ a_2 + j,\ \ldots,\ a_k + j\} \pmod v$$
$$\text{для } j = 0,\ 1,\ \ldots,\ v-1$$

образуют блоки симметричных схем. Это получается потому, что если $r \neq s$ суть два различных вычета, то существует подходящее m, такое, что $r \equiv a_i + m \pmod v$, $s \equiv a_j + m \pmod v$, когда $a_i - a_j \equiv d \equiv r - s \pmod v$. Таким образом, r и s появляются вместе в точности в λ блоках, а блоки образуют симметричную блок-схему. В схеме, заданной множеством разностей, отображение $r \to r+1 \pmod v$ определяет автоморфизм порядка v схемы, которая является циклической и транзитивной относительно элементов, а также относительно блоков. Нетрудно показать, что, наоборот, симметричная схема с таким автоморфизмом задана множеством разностей по модулю v. Ниже использованы работы автора и Райзера [26, 28].

Может случиться, что для некоторого t взаимно простого с v отображение $r \to rt \pmod v$ является также автоморфизмом схемы, заданной множеством разностей. Такое

число t мы называем *мультипликатором* разностного множества. Очевидно, что мультипликаторы множества разностей образуют мультипликативную группу модуля v. В множестве разностей $a_1, \ldots, a_k \pmod v$ определяющим свойством мультипликатора t является то, что $ta_1, ta_2, \ldots, ta_k \pmod v$ для некоторых s будут соответственно кратными $a_1+s, a_2+s, \ldots, a_k+s \pmod v$. Каждое ранее найденное множество разностей имеет нетривиальные мультипликаторы. Задание мультипликатора t помогает определить, существует или нет множество разностей; если оно существует, то знание t облегчает его построение. Теперь множество разностей $a_1, \ldots, a_k \pmod v$ дает ту же самую схему, что и всякий блок $a_1+u, \ldots, a_k+u$, и для мультипликатора t $t(a_1+u), \ldots, t(a_k+u)$ являются кратными $a_1+s+tu, \ldots, a_k+s+tu$. Следовательно, если мы можем выбрать u так, чтобы $s+tu \equiv u \pmod v$, а это мы определенно можем сделать, если $(t-1, v)=1$, то множество разностей $a_1+u, \ldots, a_k+u$ переводится мультипликатором t само в себя. В свою очередь, для любого известного множества разностей мы можем, выбирая u подходящим образом, найти множество, переводимое само в себя любым мультипликатором. Простое применение теоремы, приводимой ниже, показывает в случае, когда $v=73$, $k=9$, $\lambda=1$, что 2 является мультипликатором. Так как $(2-1, 73)=1$, то существует множество, переходящее в себя, и мы его находим с помощью множества разностей 1, 1, 2, 4, 8, 16, 32, 37, 55, 64 (mod 73). Всякое другое множество отличается от данного некоторым множителем.

Теорема. *Пусть* $a_1, \ldots, a_k$ — *множество разностей по модулю* v. *Предположим что* p *есть простой делитель* $n=k-\lambda$, *что* $(p, v)=1$ *и что* $p>\lambda$. *В таком случае* p *является мультипликатором множества разностей.*

Доказательство. Мы имеем кольцо полиномов с неизвестным x и его обратным значением $x^{-1} \pmod{(x^v-1)}$. Это кольцо обладает тем основным свойством, что, если $i \equiv j \pmod v$, то $x^i \equiv x^j \pmod{(x^v-1)}$. С разностным множеством $a_1, \ldots, a_k \pmod v$ ассоциирован полином $0(x)=x^{a_1}+\ldots+x^{a_k}$. Тогда определяющим свойством множества разностей при $n=k-\lambda$ является

$$0(x)\,0(x^{-1}) \equiv n+\lambda T(x) \pmod{(x^v-1)}, \qquad \text{(A)}$$

где

$$T(x) = 1 + x + \ldots + x^{v-1} = \frac{x^v - 1}{x - 1}.$$

В доказательстве используется, во-первых, прием ослабления модуля в (A) и затем усиления его. Поскольку $p \mid n$, то из (A) следует ослабляющее соответствие $\theta(x)\theta(x^{-1}) \equiv 0 \pmod{p, T(x)}$. Теперь умножим на $\theta(x^{-1})^{p-1}$ и заметим, что $\theta(x^{-1})^p \equiv \theta(x^{-p}) \pmod{p}$, потому что полиномиальные коэффициенты кратны p. Следовательно, $\theta(x)\theta(x^{-p}) \equiv 0 \pmod{p, T(x)}$. Замечая, что $A(x)T(x) \equiv A(1)T(x) \pmod{(x^v - 1)}$, потому что $x^v - 1 = (x-1)T(x)$, мы получаем

$$\theta(x)\theta(x^{-p}) \equiv pM(x) + AT(x) \pmod{(x^v - 1)}. \qquad \text{(B)}$$

Теперь, положив $x = 1$ в этом соотношении, получим $k^2 = pM(1) + Av$. Поскольку $k^2 = n + \lambda v$ и p делится на n, это дает $Av \equiv \lambda v \pmod{p}$; итак, поскольку $(p, v) = 1$, то $A \equiv \lambda \pmod{v}$. Используя это, преобразуем (B) в (C)

$$\theta(x)\theta(x^{-p}) \equiv pR(x) + \lambda T(x) \pmod{(x^v - 1)}. \qquad \text{(C)}$$

Здесь коэффициент b_i любого члена с x^i слева неотрицателен, а справа $b_i \equiv \lambda \pmod{p}$, и так как $p > \lambda$, то $b_i \geqslant \lambda$, откуда коэффициенты $R(x)$ будут также целыми неотрицательными. Полагая в (C) $x = 1$, мы имеем $k^2 = pR(1) + \lambda v$, откуда $pR(1) = n$. Меняя x на x^{-1} в тождестве (C), получаем

$$\theta(x^p)\theta(x^{-1}) \equiv pR(x^{-1}) + \lambda T(x) \pmod{(x^v - 1)}, \qquad \text{(D)}$$

так как $T(x^{-1}) \equiv T(x)$. Замечая также, что $(p, v) = 1$, $T(x^p) \equiv T(x) \pmod{(x^v - 1)}$, и заменяя x на x^p в (A), имеем

$$\theta(x^p)\theta(x^{-p}) \equiv n + \lambda T(x) \pmod{(x^v - 1)}. \qquad \text{(E)}$$

Теперь произведение левых сторон (C) и (D) будет таким же, как произведение левых сторон (A) и (E). Полагая равными произведения правых сторон и замечая, что $pR(x)T(x) \equiv pR(1)T(x) \equiv nT(x) \pmod{(x^v - 1)}$, получаем после упрощений

$$pR(x)\,pR(x^{-1}) \equiv n^2 \pmod{(x^v - 1)}. \qquad \text{(F)}$$

Так как $R(x)$ и $R(x^{-1})$ имеют неотрицательные коэффициенты, то в (F) не может быть более одного неисчезающего члена в $pR(x)$ или в $pR(x^{-1})$. Следовательно, для некоторого s $pR(x)=nx^{-s}$, $pR(x^{-1})=nx^{s}$. Подставляя это в (D), имеем

$$\theta(x^p)\theta(x^{-1})\equiv nx^s+\lambda T(x) \pmod{(x^v-1)}. \qquad \text{(G)}$$

Умножая на $\theta(x)$, применяя (A) и упрощая, находим

$$\theta(xp)\equiv x^s\theta(x) \pmod{(x^v-1)}. \qquad \text{(H)}$$

Но это есть как раз условие того, чтобы p было мультипликатором множества разностей.

Условие $p>\lambda$, разумеется, не имеет геометрического смысла при $\lambda=1$, но это оказывается излишним для всех известных множеств разностей. В самом деле, для каждого из известных множеств разностей $(n, v)=1$, а для всех этих множеств всякий делитель числа n является мультипликатором. Сингер [21] показал, что гиперплоскости проективных дезарговых пространств могут быть представлены множеством разностей. Любое известное планарное ($\lambda=1$) множество разностей дает дезаргову плоскость, и естественно предположить, что это имеет место всегда, так как Манн и Эванс [14] показали, что для всех значений $n\leqslant 1600$ планарное множество разностей не может существовать, если n не является степенью простого числа, и что для значений n, равных степеням простых чисел, существуют дезарговы плоскости, хотя, возможно, для некоторых из этих значений могут также существовать недезарговы множества разностей.

Множества разностей подвергались различным обобщениям. Бос [3] обобщил теорему Сингера, выведя аналогичную теорему для евклидовых пространств, а Гофман [8] доказал соответствующую теорему о мультипликаторах для евклидовых плоскостей. Еще более широкого обобщения достиг Брук [5], который рассматривал симметрические схемы для группы G порядка v автоморфизмов транзитивной и регулярной как относительно элементов, так и относительно блоков. Он перенес соотношение (A) на кольцо Г группы G над рациональным полем. Если группа G — абелева, $p|n$, $(p, v)=1$, а также $p>\lambda$, то p будет муль-

типликатором такого $x \to x^p$, которое является автоморфизмом схемы.

Когда для параметров v, k существует множество разностей, то оно не обязательно единственное. Так, для $v=31$, $k=15$, $\lambda=7$ мы имеем самый первый пример (т. е. наименьшее k), где существуют два неизоморфных решения. Первым решением являются квадратичные вычеты

1, 2, 4, 5, 7, 8, 9, 10, 14, 16, 18, 19, 20, 25, 28 (mod 31)

и вторым решением —

1, 2, 3, 4, 6, 8, 12, 15, 16, 17, 23, 24, 27, 29, 30 (mod 31).

Если мы возьмем 3 в качестве первообразного корня, то существуют вычеты с индексами 0, 1, 3 (mod 6). В самом деле, автор [30] доказал, что существуют два неизоморфных решения для $v=p$, $k=(p-1)/2$, $\lambda=(p-3)/4$ всегда, когда p — простое число вида $p=4x^2+27$. Если существует бесконечное множество простых чисел этого вида, то существует бесконечно много примеров неизоморфных разностных множеств с одними и теми же параметрами. Еще более удивительный случай четырех неизоморфных решений при $v=121$, $k=40$, $\lambda=13$ приведен в указанной выше статье.

5. Теоремы существования

Всякое конечное размещение v объектов в b блоках может быть представлено $(v \times b)$-матрицей $A=(a_{ij})$; $i=1, \ldots, v$, $j=1, \ldots, b$ (объекты и блоки перенумерованы), где $a_{ij}=1$, если i-й объект находится в j-м блоке, и $a_{ij}=0$, если не находится. Обозначим символом A^T транспонированную матрицу A. Тогда

$$AA^T=B=(b_{ij}), \quad i, j=1, \ldots, v, \tag{1}$$

где $r_i=b_{ii}$ — число всех появлений i-го объекта, а $\lambda_{ij}=b_{ij}=b_{ji}$, $j \neq i$ — число совместных появлений в блоке i-го и j-го объектов. Таким образом, для блок-схемы (и, более общо, для частично сбалансированных схем) матрица B включает информацию, определяющую главные требования. То же самое соотношение может быть выражено посредством квадратичных форм от v переменных $x_1, x_2, \ldots, x_v$, связывающих переменную с каждым объ-

ектом. Если теперь мы свяжем блок B_j с линейной формой $L_j = \sum_i a_{ij} x_i$, то

$$L_1^2 + \ldots + L_b^2 = \sum_i r_{ii} x_i^2 + 2 \sum_{i<j} \lambda_{ij} x_i x_j = Q(x_1, \ldots, x_v). \quad (2)$$

Для решения спорных вопросов относительно существования схем весьма полезно рассматривать матрицу B как данную, а (1) как уравнение относительно A с тем ограничением, что A состоит из нулей и единиц, или аналогично рассматривать (2) с заданным Q, из которого должны быть найдены все L.

Имеются две теоремы существования, которые исходят непосредственно из матричных формулировок. Если задана блок-схема, то $r_{ii} = r$ для всех i, и $\lambda_{ij} = \lambda$ для всех $i \neq j$, так что

$$B = \begin{pmatrix} r & \ldots & \lambda \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \lambda & \ldots & r \end{pmatrix}. \quad (3)$$

Мы без труда найдем детерминант от B

$$\det B = (r - \lambda)^{v-1} (v\lambda - \lambda + r). \quad (4)$$

Если $r = \lambda$, то схема тривиальна, так как, если рассматриваются все появления каждого x_i с каждым другим x_j, каждый блок состоит из всех v объектов. Следовательно, нам нужно рассмотреть только $r > \lambda$, а в этом случае $\det B \neq 0$. Отсюда мы можем вывести неравенство Фишера

$$b \geqslant v. \quad (5)$$

В самом деле, если $b < v$, то ранг A будет меньше, чем v, и B будет вырожденной, что противоречит тому, что $\det B \neq 0$. Для симметричных схем легко находится более сильный результат.

Теорема. *Если в симметричной блок-схеме v четное, то $k - \lambda$ является квадратом.*

Доказательство. Когда $b = v$, A является квадратной матрицей, так что $\det B = (\det A)^2$. Но для симмет-

ричной схемы $k^2 - k = v\lambda - \lambda$, и поскольку $r = k$, то $v\lambda - \lambda + r = k^2$. Следовательно, $\det B = k^2 (k - \lambda)^{v-1}$. Но для того, чтобы $\det B$ был квадратом, а v — четным, требуется, чтобы разность $k - \lambda$ была квадратом. Это простое и сильное условие не было найдено вплоть до 1950 г., когда оно было открыто независимо Човла и Райзером [32], а также Шрикхендом [33]. В обоих случаях исследования были стимулированы новым подходом, введенным Бруком и Райзером [6].

В 1949 г. Брук и Райзер обнаружили, что в матрице, или в квадратичной формулировке схем, условие, чтобы a_{ij} были нулями и единицами, означает, что они a fortiori являются элементами рационального поля. Но в этой трактовке соотношение (1) для симметричных схем доказывает рациональную конгруэнтность B и тождественной матрицы, а (2) соответственно доказывает рациональную эквивалентность квадратичной формы Q и суммы v квадратов

$$Q(x_1, \ldots, x_v) = \sum_i kx^2 + 2 \sum_{i<j} \lambda x_i x_j = \sum_j L_j^2. \qquad (6)$$

Для рациональной эквивалентности квадратичных форм пригодился мощный аппарат Хассе — Минковского, где применяется гильбертов символ норменного-вычета. Мы дадим здесь элементарный вывод вытекающих отсюда условий. Обозначим $k - \lambda = n$. Тогда

$$L_1^2 + \ldots + L_v^2 = n(x_1^2 + \ldots + x_v^2) + \lambda (x_1 + \ldots + x_v)^2. \qquad (7)$$

Рассмотрим сначала случай, когда $v \equiv 1 \pmod 4$. По теореме Лагранжа всякое целое число n есть сумма четырех квадратов, а произведение двух сумм четырех квадратов рационально выражается через сумму четырех квадратов. Таким образом, $n(x_i^2 + x_{i+1}^2 + x_{i+2}^2 + x_{i+3}^2)$ в (7) может быть выражено в виде $y_i^2 + y_{i+1}^2 + y_{i+2}^2 + y_{i+3}^2$ при y, рациональных относительно x, и наоборот.

Так, если $v \equiv 1 \pmod 4$, имеем

$$L_1^2 + \ldots + L_v^2 = y_1^2 + \ldots + y_{v-1}^2 + ny_v^2 + \lambda w^2, \qquad (8)$$

где $y_v = x_v$, а все L и $w = x_1 + \ldots + x_v$ выражены рационально через независимые переменные $y_1, \ldots, y_v$. Теперь (8) является тождеством в независимых переменных

$y_1, \ldots, y_v$. Предположим, что $L_1 = b_{11}y_1 + \ldots + b_{1v}y_v$. Если $b_{11} \neq 1$ и мы положим $L_1 = y_1$ или если $b_{11} = 1$ и мы положим $L_1 = -y_1$ то в любом случае мы получим соотношение, которое мы можем рассматривать как требование, чтобы y_1 был некоторой рациональной комбинацией переменных $y_2, \ldots, y_v$, а также дающее $L_1^2 = y_1^2$. Выполнив это требование, получаем

$$L_2^2 + \ldots + L_v^2 = y_2^2 + \ldots + y_{v-1}^2 + ny_v^2 + \lambda w^2. \qquad (9$$

Продолжая этот процесс для $L_2, \ldots, L_{v-1}$, мы окончательно получаем

$$L_v^2 = ny_v^2 + \lambda w^2. \qquad (10)$$

Здесь L_v и w, которые всюду сохраняли свою независимость, рационально зависят от y_v. Это существенно, так как если бы такое соотношение, как (10), выполнялось для любых L_v, y_v и w, тождественно равных нулю, оно не имело бы смысла. Теперь, взяв в качестве y_v целое, которое является произведением знаменателей w и L_v в (10), получаем уравнение

$$z^2 = nx^2 + \lambda y^2, \qquad (11)$$

разрешимое в целых числах при $x \neq 0$, как следствие существования схемы для $v \equiv 1 \pmod 4$. Когда $v \equiv 3 \pmod 4$, мы добавляем к обеим частям (7) по nx_{v+1}^2, где x_{v+1} — новая переменная, и получаем, как выше,

$$nx^2 = y_{v+1}^2 + \lambda w^2 \qquad (12)$$

с независимым y_{v+1}. Это означает, что уравнение

$$z^2 = nx^2 - \lambda y^2 \qquad (13)$$

разрешимо в целых числах. Эти результаты мы объединяем в теореме.

Теорема. *Если существует симметрическая схема с параметрами v, k, λ и мы обозначим $n = k - \lambda$, то:* а) *при v четном n будет квадратом*; б) *при v нечетном выражение $z^2 = nx^2 + (-1)^{(v-1)/2}\lambda y^2$ разрешимо в целых числах, которые не все равны нулю.*

Справедливо и обратное, именно, если эти условия выполняются, то (1) и (2) имеют рациональные решения.

Когда n — квадрат, мы можем положить

$$L_i = \sqrt{n}\, x_i + \frac{k-\sqrt{n}}{v}(x_1 + \ldots + x_v), \quad i = 1, \ldots, v, \qquad (14)$$

чтобы получить рациональное решение (2). Но чтобы доказать противное, вообще говоря, оказывается необходимым более глубокое применение аппарата Хассе — Минковского.

Применяя эту теорему к проективным плоскостям, мы имеем $\lambda = 1$ и $v = n^2 + n + 1$, которое нечетно для любого n. Для $n \equiv 0,3 \pmod 4$ мы получаем $v \equiv 1 \pmod 4$ и разрешимость $z^2 = nx^2 + y^2$ очевидна. Но для $n \equiv 1,2 \pmod 4$ мы получаем $v \equiv 3 \pmod 4$ и в соответствии с хорошо известными результатами теории чисел $z^2 = nx^2 - y^2$, или $z^2 + y^2 = nx^2$ разрешимы в целых числах, не равных нулю, тогда и только тогда, когда n является суммой двух квадратов: $n = a^2 + b^2$. Отсюда мы получаем важное следствие.

Следствие. *Необходимое условие существования проективной геометрии с $n+1$ точками на прямой состоит в том, что если $n \equiv 1,2 \pmod 4$, то n имеет вид: $n = a^2 + b^2$.*

Это следствие было основным результатом оригинальной статьи Брука и Райзера. В ней доказано, что не существует геометрий для $n = 6, 14, 21, 22, \ldots$. Так как геометрия существует всегда, когда n является степенью простого числа, то $n = 10$ — наименьший сомнительный случай. Тэрри еще раньше показал, что для $n = 6$ плоскости не существует. Однако следует подчеркнуть, что из вышеупомянутого результата не вытекает результат Тэрри, так как существование пары ортогональных $(n \times n)$-квадратов может оказаться возможным и в случае, если полное множество взаимно ортогональных квадратов не существует. В самом деле, по построению, осуществленному Манном, существует пара ортогональных (21×21)-квадратов, хотя не существует даже геометрии этого порядка. Другое свойство матрицы — инцидентность — вытекает из того факта, что если S обозначает $(v \times v)$-матрицу, где каждый элемент — единица, то для симметрической схемы

$$AS = SA = kS. \qquad (15)$$

Учитывая, что каждый объект появляется k раз, а каждый блок содержит k объектов, мы можем записать (1) в виде

$$AA^T = B = (k - \lambda) I + \lambda S, \tag{16}$$

где I — есть тождественная $(v \times v)$-матрица. Тогда, применяя (15), запишем

$$A^T A = A^{-1}(AA^T) A = A^{-1}(k - \lambda) IA + \lambda A^{-1} SA = \\ = (k - \lambda) I + \lambda S = B. \tag{17}$$

Отсюда для симметричных схем получим

$$AA^T = A^T A = B = (k - \lambda) I + \lambda S. \tag{18}$$

Это показывает, что матрица инцидентности A симметричной схемы перестановочна со своей транспонированной матрицей. Такие матрицы называются *нормальными;* они имеют много важных свойств. Теперь из (17) мы видим, что в симметричной схеме всякие два различных блока имеют вместе в точности λ элементов. Соотношения (15), (16) и (17) зависимы, и в самом деле Райзер [18] доказал, что соотношение (16) вместе с $AS = kS$ влекут за собой остальные соотношения и даже соотношение $k(k-1) = \lambda(v-1)$.

Другой подход был введен Коннором [10] в 1952 году. Этот подход основан на том, что в (2) формы L_j имеют действительные коэффициенты. Так, если для пробы заданы t начальных блоков и определены $L_1, L_2, \ldots, L_t$, то из (2) следует, что

$$L_{t+1}^2 + \ldots + L_b^2 = Q - L_1^2 - \ldots - L_t^2 = Q^*. \tag{19}$$

Если схему можно дополнить, отыскав $L_{t+1}, \ldots, L_b$, то форма Q^* должна быть полуопределенной. В самом деле, поскольку все L рациональные, если $t = b - v$, то симметрический детерминант, соответствующий Q^*, должен быть квадратом. Если $t > b - v$, то соответствующая Q^* будет вырожденной. Это испытание t начальных блоков Коннор проводит в форме оценки $(t \times t)$-детерминанта. Положим, что $B_1, \ldots, B_t$ — заданные t блоков. Тогда пусть s_{ij} — число элементов в пересечении B_i и B_j (для симметрической схемы мы знаем, что во всех случаях $s_{ij} = \lambda$). Образуем матрицу $C_t = (c_{ij})$, $i, j = 1 \ldots, t$, где

$c_{ii} = (r-k)(r-\lambda)$, $c_{ij} = \lambda k - rs_{ij}$. Тогда теорема Коннора выглядит следующим образом:

Теорема. *Если возможно дополнить t заданных блоков $B_1, \ldots, B_t$ до блок-схемы, тогда необходимо, чтобы:*

a) $\det C_t \geqslant 0$, *если* $t < b - v$,
b) $\det C_t = 0$, *если* $t > b - v$,
c) *если* $t = b - v$, *то* $k\,(r)^{-b+v+1}(r-\lambda)^{2v-b-1} \det C_t$ *является полным целым квадратом.*

Заметим, что если мы имеем дело с симметричной схемой, то C_t тождественно равна нулю и не содержит никакой информации. На практике эта теорема дает наиболее полную информацию для почти симметрических схем, т. е. когда v и b почти равны. В предыдущем разделе было доказано, что существование симметрической схемы влечет за собой существование производной схемы и остаточной схемы. Обратное, вообще говоря, не имеет места. Для симметричной схемы с параметрами $v = b = 25$, $r = k = 9$, $\lambda = 3$ остаточная схема имеет параметры $v = 16$, $b = 24$, $r = 9$, $k = 6$, $\lambda = 3$. Бхаттачария [7] дает следующий пример:

1	2	7	8	14	15	1	4	7	8	11	16
3	5	7	8	11	13	2	4	8	10	12	14
2	3	8	9	13	16	5	6	8	10	15	16
3	5	8	9	12	14	1	6	8	10	12	13
1	6	7	9	12	13	1	2	3	11	12	15
2	5	7	10	13	15	2	6	7	9	14	16
3	4	7	10	12	16	1	4	5	13	14	16
3	4	6	13	14	15	2	5	6	11	12	16
4	5	7	9	12	15	1	3	9	10	15	16
2	4	9	10	11	13	4	6	8	9	11	15
3	6	7	10	11	14	1	5	9	10	11	14
1	2	3	4	5	6	11	12	13	14	15	16

Поскольку 5-й и 16-й из этих блоков имеют 4 общих элемента: 1, 6, 12, 13, то ясно, что эта схема не может быть расширена до симметрической, в которой любые два блока имели бы в точности 3 общих элемента. Однако существует симметрическая схема для $v = 25$, $k = 9$, $\lambda = 3$, хотя существование вышеуказанной схемы не доказывает этого. Симметрической схемой с $\lambda = 1$ является проективная

плоскость. Остаточная схема является евклидовой плоскостью, а хорошо известно, что всякая евклидова плоскость может быть расширена до проективной плоскости. Коннор и автор [11] использовали аппарат из первой работы Коннора, чтобы показать, что при $\lambda=2$ всякая схема с параметрами остаточной схемы может быть расширена единственным образом до симметричной схемы. Пример Бхаттачария показывает, что соответствующий результат для $\lambda=3$ неверен. Разница, видимо, состоит в том, что для симметричных схем при $\lambda=1$ или $\lambda=2$ производные схемы тривиальны, в то время как для $\lambda=3$ это не так. Коннор и другие применили этот аппарат к частично упорядоченным блок-схемам.

Пытаясь выяснить, почему аппарат Коннора не может дать никакой информации о симметрических схемах, Холл и Райзер [29] получили результат противоположного характера. Если для симметрической схемы, параметры которой удовлетворяют условиям Човла — Райзера, выбраны начальные блоки $B_1, \ldots, B_t$ и если, поскольку это, очевидно, необходимо, любые два различных B имеют λ общих элементов, то, выбирая $B_1, \ldots, B_t$, чтобы определить первые t столбцов, мы можем отыскать матрицу A с такими t столбцами, которые не только действительны, но даже рациональны и нормальны, удовлетворяющую уравнениям инцидентности: $AA^T=A^TA=B=(k-\lambda)I+\lambda S$. Этот результат также был обобщен в ранних результатах Алберта [1].

Дальнейшее применение этого метода к теоремам существования пока не осуществлено, но очевидно, что этот метод гораздо более сильный, нежели метод Коннора. Мы замечаем, что в (2) линейные формы $L_1, \ldots, L_b$ не только действительны, но также неотрицательны. Таким образом, если мы испробуем начальные опытные блоки, задавая $L_1, \ldots, L_t$, то получим

$$L_{t+1}^2+\ldots+L_b^2=Q(x_1, \ldots, x_v)-L_1^2-\ldots-L_t^2=Q^*.$$

Отсюда, если начальные блоки можно дополнить до полной схемы, форма Q^* должна быть суммой $b-t$ квадратов неотрицательных линейных форм. Условия, которые могут быть наложены на Q^*, будут тем строже, чем больше мы имеем ограничений в выборе начальных блоков и чем

большую информацию относительно существования и построения схем мы получаем. Теперь Коннор использует только то условие, что Q^* будет полуопределенной. Автор поставил общий вопрос, могут ли полуопределенные формы с неотрицательными коэффициентами всегда быть представлены в виде суммы квадратов неотрицательных линейных форм. Профессор А. Горн доказал существование форм, которые не имели этого свойства, а автору удалось построить следующий пример:

$$Q = x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 + x_1x_4 + x_1x_5 + x_2x_5 + x_3x_4 + \frac{3}{2}x_2x_3 =$$

$$= \left(x_5 + \frac{x_1}{2} + \frac{x_2}{2}\right)^2 + \left(x_4 + \frac{x_1}{2} + \frac{x_3}{2}\right)^2 + \frac{1}{2}\left(x_1 - \frac{x_2}{2} - \frac{x_3}{2}\right)^2 + \frac{5}{8}(x_2 + x_3)^2.$$

Ясно, что Q полуопределенна и имеет положительные коэффициенты. Мы покажем, что предположение о представимости Q как суммы квадратов неотрицательных форм ведет к противоречию. Если $Q = \sum L_j^2$, а некоторое $L_j = (\ldots ax_i + bx_k \ldots)$, то смешанное произведение $2abx_ix_k$ не может взаимно уничтожиться с членами из других L поскольку не существует отрицательных смешанных произведений. Отсюда L, в котором как члены с x_2, так и члены с x_3 имеют положительные коэффициенты, не содержит других x, поскольку Q не имеет членов x_1x_2, x_2x_4, x_3x_5. Следовательно,

$$Q = \sum_i (a_ix_2 + b_ix_3)^2 + \sum_j L_j^2 = Ax_2^2 + \frac{3}{2}x_2x_3 + Bx_3 + Q_1.$$

Если теперь в Q мы положим

$$x_1 = 2x_2 + 2x_3, \quad x_4 = -\frac{x_1}{2} - \frac{x_3}{2}, \quad x_5 = -\frac{x_1}{2} - \frac{x_2}{2},$$

то Q сведется к $\frac{5}{8}(x_2 + x_3)^2$ и Q_1 должно быть полуопределенным. Тогда

$$\frac{5}{8}(x_2 + x_3)^2 = Ax_2^2 + \frac{3}{2}x_2x_3 + Bx_3^2 + Q_1.$$

Следовательно,

$$Q_1 = \left(\frac{5}{8} - A\right) x_2^2 - \frac{1}{4} x_2 x_3 + \left(\frac{5}{8} - B\right) x_3^2.$$

Но мы сразу видим, что при $0 \leqslant A \leqslant \frac{5}{8}$, $0 \leqslant B \leqslant \frac{5}{8}$ форма $Ax_2^2 + \frac{3}{2} x_2 x_3 + Bx_3^2$ неопределенна, следовательно, мы пришли к противоречию. Профессор Горн установил, что формы Q, имеющие то свойство, что $(P) - Q$ есть сумма квадратов неотрицательных линейных форм, составляют выпуклый конус K в пространстве, заданном коэффициентами Q. Присоединенное пространство K^* соответствует формам, которые неотрицательны для неотрицательных аргументов. Таким образом, подсчет экстремальных точек в K^* дал бы критерии, определяющие, будет форма Q иметь свойство (P) или же нет.

Во многих случаях может быть показано, что если квадратичная форма Q, связанная со схемой, может быть представлена как сумма самое большее b квадратов неотрицательных линейных форм, то эти формы дают решение схемы. Таким образом, оказывается, что число слагаемых, пожалуй, самое решающее из всех условий. Возможно, что теория выпуклых поверхностей даст существенно новые вклады в комбинаторный анализ.

ЛИТЕРАТУРА

1. Альберт (Albert A. A.), Rational normal matrices satisfying the incidence equation, *Proc. Amer. Math. Soc.*, **4**, 554—559 (1953).
2. Бос (Bose R. C.), On the construction of balanced incomplete block designs, *Ann. Eugenics*, **9**, 353—399 (1939).
3. Бос (Bose R. C.), An affine analogue of Singer's theorem, *J. Indian Math. Soc.* (NS), **6**, 1—15 (1942).
4. Бос, Клэтуорти и Шрикхенд (Bose R. C., Clatworthy W. H. and Shrikhande S. S.), Tables of partially balanced designs with two associate classes, *Tech. Bull.* No 107, North Carolina Agricultural Experiment Station (1954)
5. Брук (Bruck R. H.), Difference sets in a finite group, *Trans. Amer. Math. Soc.*, **78**, 464—481 (1955).
6. Брук и Райзер (Bruck R. H. and Ryser H. J.), The nonexistence of certain finite projective planes, *Can. J. Math*, **1**, 88—93 (1949).

7. Бхаттачарья (Bhattacharya K. N.), A new balanced incomplete block design, *Science and Culture*, **9**, 508 (1944).
8. Гофман (Hoffman A. J.), Cyclic affine planes, *Can J. Math.*, **4**, 295—301 (1952).
9. Кол, Уайт и Камминге (Cole F. N., White A. S. and Cummings L. D.), Complete classification of triad systems on fifteen elements, *Mem. Nat. Acad. Sci.*, **XIV**, second memoir, 89 pp. (1925).
10. Коннор (Connor W. S.), On the structure of balanced incomplete block designs, *Ann. Math. Stat.*, **23**, 57—71 (1952).
11. Коннор и Холл М. (Connor W. S. and Hall M., Jr), An embedding theorem for balanced incomplete block designs, *Can. J. Math.*, **6**, 35—41 (1953).
12. Манн (Mann H. B.), On the construction of sets of orthogonal Latin squares, *Ann. Math. Stat.*, **14**, 401—414 (1943).
13. Манн (Mann H. B.), Analysis and Design of Experiments, Dover Publications, Inc., New York, 1949.
14. Манн и Эванс (Mann H. B. and Evans T. A.), On simple difference sets, *Sankhya*, **11**, 357—364 (1951).
15. Мур (Moore E. H.), Concerning triple systems, *Math. Ann.*, **43**, 271—285 (1893).
16. Нанди (Nandi H. K.), A further note on non-isomorphic solutions of incomplete block designs, *Sankhya*, **7**, 313—316 (1946).
17. Нортон (Norton H. W.), The 7×7 squares, *Ann. Eugenics*, **2**, 269—307 (1939).
18. Райзер (Ryser H. J.), A note on a combinatorial problem, *Proc. Amer. Math. Soc.*, **1**, 422—424 (1950).
19. Рисс (Riess M.), Über eine Steinersche combinatorische Aufgabe welche in 45-sten Bande dieses Journals, Seite 181, gestellt worden ist, *Crelle's J.*, **56**, 326—344 (1859).
20. Сад (Sade A.), An omission in Norton's list of 7×7 squares, *Ann. Math. Stat.*, **22**, 306—307 (1951).
21. Сингер (Singer J.), A theorem in finite projective geometry and some applications to number theory, *Trans. Amer. Math. Soc.*, **43**, 377—385 (1938).
22. Стивенс (Stevens W. L.), The completely orthogonalized Latin square, *Ann. Eugenics*, **9**, 82—93 (1939).
23. Терри (Tarry G.), Le problème des 36 officiers, *C. R. Ass. Franc. Av. Sci.*, **1**, 122—123 (1900); **2**, 170—203 (1901).
24. Фишер (Fischer R. A.), An examination of the different possible solutions of a problem in incomplete blocks, *Ann. Eugenics*, **10**, 52—75 (1940).
25. Фишер и Иейтс (Fisher R. A. and Yates F.), Statistical Tables for Biological, Agricultural, and Medical Research, 2nd ed., Oliver and Boyd Ltd., London, 1943.
26. Холл М. (Hall M., Jr.), Cyclic projective planes, *Duke* Math. J., **14**, 1079—1090 (1947).

27. Холл М. (Hall M., Jr.) On a theorem of Jordan, *Pacific Math. J.*, **4**, 219—226 (1954).
28. Холл М. и Райзер (Hall M., Jr. and Ryser H. J.), Cyclic incidence matrices, *Can. J. Math.*, **3**, 495—502 (1951).
29. Холл М. и Райзер (Hall M., Jr. and Ryser H. J.), Normal completions of incidence matrices, *Amer. J. Math.*, **76**, 581—589 (1954).
30. Холл М. и Райзер (Hall M., Jr. and Ryser H. J.), A survey of difference sets, *Proc. Amer. Math. Soc.*, **7**, 975—986 (1956).
31. Цассенхаус (Zassenhaus H.), Über transitive Erwerterung gewisser Gruppen aus Automorphismen endlicher mehrdimensionaler Geometrien, *Math. Ann.*, **111**, 748—759 (1935).
32. Човла и Райзер (Chowla S. and Ryser H. J.), Combinatorial problems, *Can. J. Math.*, **2**, 93—99 (1950).
33. Шрикхенд (Shrikhande S. S.), The impossibility of certain symmetrical balanced incomplete block designs. *Ann. Math. Stat.*, **21**, 106—111 (1950).
34. Штейнер (Steiner J.), Combinatorische Aufgabe, *Crelle's J.*, **45**, 181—182 (1953).
35. Эйлер (Euler L.), Commentationes Arithmeticae, II, 302—361, Петербург, 1849.
36. Эрдёш и Капланский (Erdös P. and Kaplansky I.), The asymptotic number of Latin rectangles, *Amer. J. Math.*, **68**, 230—236 (1946).

ОГЛАВЛЕНИЕ

Предисловие к русскому изданию 5
Глава I. **Введение и резюме** 7
1. Введение 7
2. Общие направления и итоги 10

Глава II. **Методы перечисления** 13
1. Общие замечания 13
2. Перестановки и сочетания 13
*3. Рекуррентные формулы и производящие функции 19
4. Разбиения 26
Литература 37

Глава III. **Теоремы выбора** 38
1. Основные теоремы 38
2. Приложения теорем 45
Литература 58

Глава IV. **Существование и построение схем** . . 60
1. Предварительные замечания 60
2. Латинские квадраты 61
3. Системы троек Штейнера 67
4. Построение блок-схем 71
5. Теоремы существования 85
Литература 94

М. Холл

КОМБИНАТОРНЫЙ АНАЛИЗ

Редакторы *И. Л. Никольская, А. А. Бряндинская*
Художник *Н. А. Липин*
Художественный редактор *В. И. Шаповалов*
Технические редакторы
Е. И. Шилина и Л. М. Харьковская
Корректор *Р. Я. Новик*

Сдано в производство 28/VIII—1962 г.
Подписано к печати 14/XII—1962 г.
Бумага 84 × $108^{1}/_{32}$ =1,6 бум. л.
5,1 печ. л..
Уч.-изд. л. 4,6. Изд. № 1/1258
Цена 32 коп. Зак. № 3329

ИЗДАТЕЛЬСТВО
ИНОСТРАННОЙ ЛИТЕРАТУРЫ
Москва, 1-й Рижский пер., д. 2.

Первая Образцовая типография
имени А. А. Жданова
Московского городского совнархоза
Москва, Ж-54, Валовая, 28.

Отпечатано в Производственно-издательском
комбинате ВИНИТИ
Люберцы, Октябрьский просп., д. 403, Зак. 260

ИЗДАТЕЛЬСТВО ИНОСТРАННОЙ ЛИТЕРАТУРЫ

Выпускает серию брошюр под общим названием

«БИБЛИОТЕКА СБОРНИКА „МАТЕМАТИКА“»

Вышли из печати

В 1959 г.

Микусинский Я., Сикорский Р., **Элементарная теория обобщенных функций.** Вып. I. Варшава, 1957, *перевод с английского*, 3,5 изд. л.

Хёрмандер Л., **К теории общих дифференциальных операторов в частных производных.** Уппсала, 1959, *перевод с английского*, 6 изд. л.

Халмош П. Р., **Лекции по эргодической теории.** Токио, 1956, *перевод с английского*, 7 изд. л.

Капланский И., **Введение в дифференциальную алгебру.** Париж, 1957, *перевод с английского*, 4 изд. л.

В 1960 г.

Карлеман Т., **Математические задачи кинетической теории газов.** Уппсала, 1957, *перевод с французского*, 5,7 изд. л.

Хейман В. К., **Многолистные функции.** Кембридж, 1958, *перевод с английского*, 8,4 изд. л.

Номидзу К., **Группы Ли и дифференциальная геометрия.** Токио, 1956, *перевод с английского*, 6 изд. л.

Судзуки М., **Строение группы и строение структуры ее подгрупп.** Берлин—Геттинген—Гейдельберг, 1956, *перевод с английского*, 7 изд. л.

Рутисхаузер Г., **Алгоритм частных и разностей.** Базель — Штутгарт, 1957, *перевод с немецкого*, 4 изд. л.

Ито К., **Вероятностные процессы.** Вып. I, Токио, 1957, *перевод с японского*, 6,1 изд. л.

В 1961 и 1962 гг.

Гренандер У., **Случайные процессы и статистические выводы.** Стокгольм, 1960, *перевод с английского*, 8 изд. л.

Гординг Л., **Задача Коши для гиперболических уравнений.** Чикаго, 1957, *перевод с английского*, 5,3 изд. л.

Гудстейн Р. Л., **Математическая логика.** Лейчестер, 1957, *перевод с английского*, 7,9 изд. л.