ГЛАВА 5

СОРТИРОВКА

*Нет дела, коего устройство было бы труднее,
ведение опаснее, а успех сомнительнее,
нежели замена старых порядков новыми.*

— НИККОЛО МАКИАВЕЛЛИ, *Государь* (1513)

*"Но мы не успеем просмотреть все номера автомобилей",
— возразил Дрейк.
"А нам и не нужно этого делать, Пол. Мы просто
расположим их по порядку и поищем одинаковые."*

— ПЕРРИ МЕЙСОН, Из *The Case of the Angry Mourner* (1951)

*Компьютер "Treesort": при новом "компьютерном подходе"
к изучению природы вы получите возможность быстро распознавать
более 260 видов деревьев США, Аляски и Канады, включая пальмы,
растительность пустынь и прочую "экзотику". Чтобы определить
породу дерева, достаточно просто вставить спицу.*

— Каталог *Edmund Scientific Company* (1964)

В ЭТОЙ ГЛАВЕ мы изучим вопрос, который часто возникает в программировании: переразмещение элементов в порядке возрастания или убывания. Представьте, насколько трудно было бы пользоваться словарем, если бы слова в нем не располагались в алфавитном порядке. Точно так же от порядка, в котором хранятся элементы в памяти компьютера, во многом зависит скорость выполнения и простота алгоритмов, предназначенных для их обработки.

Хотя в словарях слово "сортировка" (sorting) определяется как процесс разделения объектов по виду или сорту, программисты традиционно используют его в гораздо более узком смысле, обозначая им такую перестановку предметов, при которой они располагаются в порядке возрастания или убывания. Такой процесс, пожалуй, следовало бы назвать не сортировкой, а *упорядочением* (ordering), но использование этого слова привело бы к путанице из-за перегруженности значениями слова "порядок". Рассмотрим, например, следующее предложение: "Так как только два из имеющихся у нас лентопротяжных механизмов в порядке, меня призвали к порядку и обязали в срочном порядке заказать еще несколько устройств, чтобы можно было упорядочивать данные разного порядка на несколько порядков быстрее". В математической терминологии это слово также изобилует значениями (порядок группы, порядок перестановки, порядок точки ветвления, отношение порядка и т. п.). Итак, слово "порядок" приводит к хаосу.

В качестве обозначения для процесса упорядочения предлагалось также слово “ранжирование” (sequencing), но оно во многих случаях, по-видимому, не вполне отражает суть дела, особенно если присутствуют равные элементы, и, кроме того, иногда не согласуется с другими терминами. Конечно, слово “сортировка” и само имеет довольно много значений, но оно прочно вошло в программистский жаргон. Поэтому мы без дальнейших извинений будем использовать слово “сортировка” в узком смысле: “размещение по порядку”. Вот некоторые из наиболее важных областей применения сортировки.

a) *Решение задачи группирования*, когда нужно собрать вместе все элементы с одинаковыми значениями некоторого признака. Допустим, имеется 10 000 элементов, расположенных в случайном порядке, причем значения многих из них равны и нужно переупорядочить массив так, чтобы элементы с равными значениями занимали соседние позиции в массиве. Это, по существу, тоже задача “сортировки”, но в более широком смысле, и она легко может быть решена путем сортировки массива в указанном выше узком смысле, а именно — в результате расположения элементов в порядке неубывания $v_1 \leq v_2 \leq \cdots \leq v_{10000}$. Эффект, который может быть достигнут после выполнения этой процедуры, и объясняет изменение первоначального смысла слова “сортировка”.

b) *Поиск общих элементов в двух или более массивах.* Если два или более массивов рассортировать в одном и том же порядке, то можно отыскать в них все общие элементы за один последовательный просмотр всех массивов без возвратов. Именно этим принципом и воспользовался Перри Мейсон, чтобы раскрыть дело об убийстве (см. эпиграфы к этой главе). Оказывается, что, как правило, гораздо удобнее просматривать список последовательно, а не перескакивая с места на место случайным образом, если только список не настолько мал, что он целиком помещается в оперативной памяти. Сортировка позволяет использовать последовательный доступ к большим массивам в качестве приемлемой замены прямой адресации.

c) *Поиск информации по значениям ключей.* Как мы узнаем из главы 6, сортировка используется и при поиске; с ее помощью можно сделать результаты обработки данных более удобными для восприятия человеком. В самом деле, подготовленный компьютером список, рассортированный в алфавитном порядке, зачастую выглядит весьма внушительно, даже если содержащиеся в нем числовые данные были рассчитаны неверно.

Хотя сортировка традиционно и большей частью использовалась для обработки коммерческих данных, в действительности она является инструментом, полезным в самых разных ситуациях, и поэтому о ней не следует забывать. В упр. 2.3.2–17 мы обсудили ее применение для упрощения алгебраических формул. Упражнения, приведенные ниже, иллюстрируют разнообразие типичных применений сортировки.

Одной из первых мощных программных систем, продемонстрировавших богатые возможности сортировки, был компилятор LARC Scientific Compiler, разработанный Дж. Эрдвином (J. Erdwinn) и Д. Е. Фергюсоном (D. E. Ferguson) в фирме Computer Sciences Corporation в 1960 году. В этом оптимизирующем компиляторе для расширенного языка FORTRAN сортировка использовалась весьма интенсивно, так что различные алгоритмы компиляции работали с относящимися к ним фрагментами исходного текста программы, расположенными в удобной последовательности. На первом проходе осуществлялся лексический анализ, т. е. выделение в исходной программе лексических единиц (лексем), каждая из которых соответствует либо идентификатору (имени переменной), либо константе, либо оператору и т. д. Каждая лексема получала несколько порядковых номеров. В результате сортировки по именам и соответствующим порядковым номерам все фрагменты текста, в которых использовался данный идентификатор, оказывались собранными вместе. "Определяющие вхождения", специфицирующие идентификатор как имя функции, простую (параметр) или многомерную (массив) переменную, получали меньшие номера, поэтому они оказывались первыми в последовательности лексем, которые соответствовали этому идентификатору. Тем самым облегчалась проверка правильности употребления идентификаторов, распределение памяти с учетом деклараций `EQUIVALENCE` и т. д. Собранная таким образом информация о каждом идентификаторе присоединялась к соответствующей лексеме. Поэтому не было необходимости хранить в оперативной памяти "таблицу символов", содержащую сведения об идентификаторах. После такой обработки лексемы снова сортировались по другому порядковому номеру; в результате в программе, по существу, восстанавливался первоначальный порядок, если не считать того, что арифметические выражения оказывались записанными в более удобной "польской префиксной" форме. Сортировка использовалась и на последующих фазах компиляции — для упрощения оптимизации циклов, включения в листинг сообщений об ошибках и т. д. Короче говоря, компилятор был спроектирован так, что всю обработку файлов (а для их хранения использовались весьма распространенные в те времена устройства внешней памяти на магнитных барабанах) можно было выполнять последовательно. Поэтому-то данные и снабжались такими порядковыми номерами, которые позволяли упорядочивать эти данные различными удобными способами.

По оценкам производителей компьютеров в 60-х годах в среднем более четверти машинного времени тратилось на сортировку. Во многих вычислительных системах на нее уходит больше половины машинного времени. Исходя из этих статистических данных можно заключить, что либо (i) сортировка имеет много важных применений, либо (ii) ею часто пользуются без нужды, либо (iii) применяются в основном неэффективные алгоритмы сортировки. По-видимому, каждое из приведенных предположений содержит долю истины.

Во всяком случае ясно, что сортировка заслуживает серьезного изучения с точки зрения ее практического использования. Но даже если бы сортировка была почти бесполезна, нашлась бы масса других причин заняться ею! Появление изощренных алгоритмов сортировки говорит о том, что она и сама по себе интересна как объект исследования. В этой области существует множество увлекательных нерешенных задач наряду с весьма немногими уже решенными.

Рассматривая вопрос в более широком плане, мы обнаружим, что алгоритмы сортировки представляют собой интересный *частный пример* того, как следует подходить к решению проблем программирования вообще. Мы познакомимся со многими важными принципами манипулирования структурами данных и проследим за эволюцией различных методов сортировки, причем читателю часто будет предоставлена возможность самостоятельно "изобрести велосипед", как будто бы до него никто с подобными задачами не сталкивался. Обобщение этих частных методов позволит нам в значительной степени овладеть теми подходами, которые помогут создавать качественные алгоритмы для решения других проблем, связанных с использованием компьютеров.

Методы сортировки служат великолепной иллюстрацией базовых концепций *анализа алгоритмов*, т. е. оценки качества алгоритмов, что, в свою очередь, позволяет разумно делать выбор среди, казалось бы, равноценных методов. Читатели, имеющие склонность к математике, найдут в этой главе немало поучительных способов оценки скорости работы алгоритмов и методов решения сложных рекуррентных соотношений. С другой стороны, изложение построено так, что читатели, не имеющие такой склонности, могут безболезненно пропускать выкладки.

Прежде чем двигаться дальше, необходимо более четко сформулировать задачу и ввести соответствующую терминологию. Пусть надо упорядочить N элементов

$$R_1, R_2, \ldots, R_N.$$

Назовем их *записями*, а всю совокупность N записей назовем *файлом*. Каждая запись R_j имеет *ключ*, K_j, который и управляет процессом сортировки. Помимо ключа, запись может содержать дополнительную "сопутствующую информацию", которая не влияет на сортировку, но всегда остается в этой записи.

Отношение порядка "$<$" на множестве ключей вводится таким образом, чтобы для любых трех значений ключей a, b, c выполнялись следующие условия:

i) справедливо одно и только одно из соотношений $a < b$, $a = b$, $b < a$ (закон трихотомии);

ii) если $a < b$ и $b < c$, то $a < c$ (закон транзитивности).

Эти два свойства определяют математическое понятие *линейного упорядочения*, называемого также *совершенным упорядочением*. Любое множество с отношением "$<$", удовлетворяющим обоим этим свойствам, поддается сортировке большинством методов, описанных в этой главе, хотя некоторые из методов годятся только для числовых и буквенных ключей с общепринятым отношением порядка.

Задача сортировки — найти такую перестановку записей $p(1)\,p(2)\ldots p(N)$ с индексами $\{1, 2, \ldots, N\}$, после которой ключи расположились бы в порядке неубывания:

$$K_{p(1)} \le K_{p(2)} \le \cdots \le K_{p(N)}. \tag{1}$$

Сортировка называется *устойчивой*, если она удовлетворяет такому дополнительному условию, что записи с одинаковыми ключами остаются в прежнем порядке, т. е., другими словами,

$$p(i) < p(j) \qquad \text{для любых} \quad K_{p(i)} = K_{p(j)} \quad \text{и} \quad i < j. \tag{2}$$

В одних случаях придется физически перемещать записи в памяти так, чтобы их ключи были упорядочены; в других случаях достаточно создать вспомогательную таблицу, которая некоторым образом описывает перестановку и обеспечивает доступ к записям в соответствии с порядком их ключей.

Некоторые методы сортировки предполагают существование величин "∞" и "$-\infty$" или одной из них. Величина "∞" считается больше, а величина "$-\infty$" меньше любого ключа:

$$-\infty < K_j < \infty \qquad \text{для } 1 \le j \le N. \tag{3}$$

Эти величины используются в качестве искусственных ключей, а также граничных признаков. Равенство в (3), вообще говоря, исключено. Если же оно, тем не менее, допускается, алгоритмы можно модифицировать так, чтобы они все-таки работали, хотя нередко при этом их изящество и эффективность отчасти утрачиваются.

Обычно методы сортировки подразделяют на два класса: внутренние, когда все записи хранятся в быстрой оперативной памяти, и внешние, когда все записи в ней не помещаются. Методы внутренней сортировки обеспечивают большую гибкость при построении структур данных и доступа к ним, внешние же методы обеспечивают достижение нужного результата в "спартанских" условиях ограниченных ресурсов.

Достаточно хороший общий алгоритм затрачивает на сортировку N записей время пропорционально $N \log N$; при этом требуется около $\log N$ "проходов" по данным. Как мы увидим в разделе 5.3.1, это минимальное время, если записи расположены в произвольном порядке и сортировка выполняется попарным сравнением ключей. Так, если удвоить число записей, то и время при прочих равных условиях возрастет немногим более чем вдвое. (На самом деле, когда N неограниченно возрастает, время сортировки растет как $N(\log N)^2$, если все ключи различны, поскольку и размеры ключей увеличиваются, как минимум, пропорционально $\log N$ с ростом N; но практически N всегда остается ограниченным.)

С другой стороны, если известно, что ключи являются случайными величинами с некоторым непрерывным распределением, то, как мы увидим ниже, сортировка может быть выполнена в среднем за $O(N)$ шагов.

УПРАЖНЕНИЯ (часть 1)

1. [*M20*] Докажите, что из законов трихотомии и транзитивности вытекает *единственность* перестановки $p(1)\,p(2)\ldots p(N)$, если сортировка устойчива.

2. [*21*] Пусть каждая запись R_j некоторого файла имеет *два* ключа: "большой ключ" K_j и "малый ключ" k_j, причем оба множества ключей линейно упорядочены. Тогда можно обычным способом ввести *лексикографический порядок* на множестве пар ключей (K, k):

$$(K_i, k_i) < (K_j, k_j), \quad \text{если} \quad K_i < K_j \quad \text{или} \quad K_i = K_j \quad \text{и} \quad k_i < k_j.$$

Алиса рассортировала этот файл сначала по большим ключам, получив n групп записей с одинаковыми большими ключами в каждой группе:

$$K_{p(1)} = \cdots = K_{p(i_1)} < K_{p(i_1+1)} = \cdots = K_{p(i_2)} < \cdots < K_{p(i_{n-1}+1)} = \cdots = K_{p(i_n)},$$

где $i_n = N$. Затем она рассортировала каждую из n групп $R_{p(i_{j-1}+1)}, \ldots, R_{p(i_j)}$ по собственным малым ключам.

Билл взял тот же исходный файл и сначала рассортировал его по малым ключам, а затем получившийся файл рассортировал по большим ключам.

Взяв тот же исходный файл, Крис рассортировал его один раз в лексикографическом порядке, пользуясь парами ключей (K_j, k_j).

Получилось ли у всех троих одно и то же?

3. [*M25*] Пусть на множестве $K_1, \ldots, K_N$ определено отношение "$<$", для которого закон трихотомии выполняется, а закон транзитивности — нет. Докажите, что и в этом случае возможна устойчивая сортировка записей, т. е. сортировка, при которой выполняются условия (1) и (2). (На самом деле существует, по крайней мере, три расположения записей, удовлетворяющих этим условиям!)

▶ **4.** [*21*] Составители словарей фактически не следуют жестко лексикографическому порядку, так как прописные и строчные буквы у них перемежаются. В частности, используется такой порядок:

$$\text{a} < \text{A¡aa} < \text{AA} < \text{AAA} < \text{Aachen} < \text{aah} < \cdots < \text{zzz} < \text{ZZZ}.$$

Поясните, как реализовать подобный словарный порядок сортировки.

▶ **5.** [*M28*] Разработайте двоичный код для всех неотрицательных целых чисел, такой, что, если n закодировано в виде строки $\rho(n)$, то $m < n$ тогда и только тогда, когда $\rho(m)$ меньше в лексикографическом смысле, чем $\rho(n)$. Более того, $\rho(m)$ не должно быть префиксом $\rho(n)$ для любого $m \neq n$. По возможности длина $\rho(n)$ должна быть по крайней мере $\lg n + O(\log\log n)$ для всех больших n. (Такой способ кодирования очень удобен, если приходится сортировать текст, состоящий из чисел и слов, или если желательно отобразить довольно большие текстовые последовательности на двоичные коды.)

6. [*15*] Программисту на `MIX` Б. С. Даллу потребовалось выяснить, находится ли в ячейке `A` число, большее числа из ячейки `B`, меньшее или же равное ему. Он написал в программе "`LDA A; SUB B`", а потом проверил, какой результат получился в регистре `A`: положительный, отрицательный или нуль. Какую серьезную ошибку он допустил и как должен был поступить?

7. [*17*] Напишите подпрограмму для компьютера `MIX` для сравнения ключей с увеличенной точностью, исходя из следующих условий.

Вызов:	`JMP COMPARE`
Состояние при входе:	$\mathrm{rI1} = n$; $\mathtt{CONTENTS(A} + k\mathtt{)} = a_k$ и $\mathtt{CONTENTS(B} + k\mathtt{)} = b_k$ для $1 \leq k \leq n$; полагается, что $n \geq 1$.
Состояние при выходе:	$\mathrm{CI} = \mathtt{GREATER}$, если $(a_n, \ldots, a_1) > (b_n, \ldots, b_1)$; $\mathrm{CI} = \mathtt{EQUAL}$, если $(a_n, \ldots, a_1) = (b_n, \ldots, b_1)$; $\mathrm{CI} = \mathtt{LESS}$, если $(a_n, \ldots, a_1) < (b_n, \ldots, b_1)$; rX и rI1, возможно, изменились.

Здесь отношение $(a_n, \ldots, a_1) < (b_n, \ldots, b_1)$ обозначает лексикографическое упорядочение слева направо, т. е. существует индекс j, такой, что $a_k = b_k$ для $n \geq k > j$, но $a_j < b_j$.

▶ **8.** [*30*] В ячейках `A` и `B` содержатся соответственно числа a и b. Покажите, что можно написать программу для `MIX`, которая вычисляла бы $\min(a, b)$ и записывала результат в ячейку `C`, не пользуясь командами перехода. (*Предостережение.* Поскольку арифметическое переполнение невозможно обнаружить без операторов перехода, разумно так построить программу, чтобы переполнение не могло возникнуть ни при каких значениях a и b.)

9. [*M27*] Какова вероятность того, что после сортировки в порядке неубывания n независимых равномерно распределенных на отрезке [0, 1] случайных величин r-е от начала число окажется $\leq x$?

УПРАЖНЕНИЯ (часть 2)

В каждом из этих упражнений поставлена задача, с которой может столкнуться программист. Предложите хорошее решение задачи, *предполагая, что вы имеете дело с "музейным" компьютером, у которого имеется сравнительно небольшая оперативная память, порядка нескольких тысяч слов* и около полудюжины накопителей на магнитной ленте (НМЛ) — этого количества вполне достаточно для выполнения сортировки. Алгоритм, который сможет эффективно работать в таких "спартанских" условиях, тем более будет прекрасно выполнять задачу на современных компьютерах.

10. [*15*] Имеется лента, на которой записан миллион слов данных. Как определить, сколько на этой ленте различных слов?

11. [*18*] Вообразите себя в роли Управления внутренних доходов Министерства финансов США. Вы получаете миллионы информационных карточек от организаций о том, сколько денег они выплатили различным лицам, и миллионы налоговых деклараций (карточек) о доходах от налогоплательщиков. Как бы вы стали отыскивать людей, которые сообщили не обо всех своих доходах?

12. [*M25*] (*Транспонирование матрицы.*) Имеется магнитная лента, содержащая миллион слов, которые представляют собой элементы матрицы 1000×1000, записанные по строкам: $a_{1,1}\,a_{1,2}\ldots a_{1,1000}\,a_{2,1}\ldots a_{2,1000}\ldots a_{1000,1000}$. Ваша задача — получить ленту, на которой элементы этой матрицы были бы записаны по столбцам: $a_{1,1}\,a_{2,1}\ldots a_{1000,1}\,a_{1,2}\ldots a_{1000,2}\ldots a_{1000,1000}$. (Постарайтесь сделать не более десяти просмотров данных.)

13. [*M26*] В вашем распоряжении есть довольно большой файл из N слов. Как бы вы его "перетасовали" случайным образом?

14. [*20*] Вы работаете с двумя вычислительными системами, в которых по-разному упорядочены литеры (буквы и цифры). Как заставить первую систему сортировать файлы с буквенно-цифровой информацией, предназначенные для использования во второй системе?

15. [*18*] Имеется довольно большой список людей, родившихся в США, с указанием штата, в котором они родились. Как подсчитать тех, кто родился в каждом штате? (Предполагается, что ни один человек не указан в списке более одного раза.)

16. [*20*] Чтобы облегчить внесение изменений в большие программы, написанные на языке FORTRAN, желательно написать программу, которая формирует таблицу *перекрестных ссылок*. Входными данными для нее служит программа на FORTRAN, а в результате получается листинг исходной программы, снабженный указателем всех случаев употребления каждого идентификатора (т. е. имени) в программе. Как написать такую программу?

▶ **17.** [*33*] (*Сортировка библиографических карточек каталога.*) До появления компьютерных баз данных в каждой библиотеке существовал каталог библиографических карточек, с помощью которого читатели могли отыскать интересующие их издания. Но сортировка карточек в порядке, удобном для читателей, усложняется по мере увеличения библиотечного фонда. В следующем "алфавитном" списке содержатся рекомендации, взятые из правил регистрации и хранения каталожных карточек Американской библиотечной ассоциации (Чикаго, 1942).

Текст карточки	*Замечания*
R. Accademia nazionale dei Lincei, Rome	В названиях иностранных (кроме британских) учреждений слово "royalty" (королевский) игнорируется
1812; ein historischer Roman	Achtzehnhundertzwölf (числительное 1812 на немецком языке)
Bibliothèque d'histoire révolutionnaire	В французском тексте апостроф рассматривается как пробел
Bibliothèque des curiosités	Диатонические знаки игнорируются
Brown, Mrs. J. Crosby	Указание положения (Mrs.) игнорируется
Brown, John	Фамилии с датами следуют за фамилиями без дат
Brown, John, mathematician	..., которые упорядочиваются
Brown, John, of Boston	по описательным словам
Brown, John, 1715–1766	Одинаковые фамилии упорядочиваются по датам рождения
BROWN, JOHN, 1715–1766	Работы о нем идут после его работ
Brown, John, d. 1811	Иногда год рождения определяется приблизительно

Текст карточки	*Замечания*
Brown, Dr. John, 1810–1882	Указание положения (Dr.) игнорируется
Brown-Williams, Reginald Makepeace	Дефис рассматривается как пробел
Brown America	Названия книг указываются после составных фамилий
Brown & Dallison’s Nevada directory	& в английском тексте превращается в “and”
Brownjohn, Alan	
Den’, Vladimir Éduardovich, 1867–	Апостроф в именах игнорируется
The den	Артикль в начале текста игнорируется
Den lieben langen Tag	. . . , если существительное стоит в именительном падеже
Dix, Morgan, 1827–1908	Фамилии идут раньше других слов
1812 ouverture	Dix-huit cent douze (числительное 1812 на французском языке)
Le XIXe siècle français	Dix-neuvième (числительное XIX-й на французском языке)
The 1847 issue of U. S. stamps	Eighteen forty-seven (числительное 1847 на английском языке)
1812 overture	Eighteen twelve (числительное 1812 на английском языке)
I am a mathematician	(a book by Norbert Wiener) (книга Норберта Винера)
IBM journal of research and development	Аббревиатуры рассматриваются как ряд однобуквенных слов
ha-I ha-ehad	Артикль в начале текста игнорируется
Ia; a love story	Знаки препинания в названиях игнорируются
International Business Machines Corporation	
al-Khuwārizmī, Muḥammad ibn Mūsā, *fl.* 813–846	Начальное “al-” в арабских именах игнорируется
Labour. A magazine for all workers	Заменяется словом “Labor”
Labor research association	
Labour, *see* Labor	Ссылка на другую карточку в картотеке
McCall’s cookbook	Апостроф в английском тексте игнорируется
McCarthy, John, 1927–	Mc = Mac
Machine-independent computer programming.	Дефис рассматривается как пробел
MacMahon, Maj. Percy Alexander, 1854–1929	Указание положения (Maj.) игнорируется
Mrs. Dalloway	“Mrs.” заменяется словом “Mistress”
Mistress of mistresses	
Royal society of London	В названиях британских учреждений слово “royalty” (королевский) учитывается
St. Petersburger Zeitung	“St.” заменяется словом “Saint”, даже в немецком тексте
Saint-Saëns, Camille, 1835–1921	Дефис рассматривается как пробел
Ste-Marie, Gaston P	Sainte
Seminumerical algorithms	(a book by Donald Ervin Knuth)
Uncle Tom’s cabin	(a book by Harriet Beecher Stowe)
U. S. bureau of the census	“U. S.” заменяется словами “United States”

Текст карточки	*Замечания*
Vandermonde, Alexandre Théophile, 1735–1796	
Van Valkenburg, Mac Elwyn, 1921–	Пробел после префикса в фамилиях игнорируется
Von Neumann, John, 1903–1957	
The whole art of legerdemain	Артикль в начале текста игнорируется
Who's afraid of Virginia Woolf?	Апостроф в текстах на английском языке игнорируется
Wijngaarden, Adriaan van, 1916–	Фамилия никогда не начинается со строчной литеры

(У большинства из этих правил есть исключения; кроме того, существует много других правил, которые здесь не упомянуты.)

Предположим, вам поручено рассортировать большое количество таких карточек с помощью компьютера, а затем обслуживать огромную картотеку, причем у вас нет возможности изменить уже сложившийся порядок заполнения карточек. Как бы вы организовали информацию, чтобы упростить операции сортировки и включения новых карточек?

18. [*M25*] (Э. Т. Паркер (E. T. Parker).) Леонард Эйлер высказал предположение [*Nova Acta Acad. Sci. Petropolitanæ* **13** (1795), 45–63, §3; написана в 1778], что уравнение

$$u^6 + v^6 + w^6 + x^6 + y^6 = z^6$$

не имеет нетривиальных решений среди целых неотрицательных чисел u, v, w, x, y, z. Одновременно он предположил, что уравнение

$$x_1^n + \cdots + x_{n-1}^n = x_n^n$$

не имеет решения в положительных целых числах при $n \geq 3$, но это предположение было опровергнуто уже в наше время, когда с помощью компьютера было найдено тождество $27^5 + 84^5 + 110^5 + 133^5 = 144^5$ [см. L. J. Lander, T. R. Parkin, and J. L. Selfridge, *Math. Comp.* **21** (1967), 446–459]. Множество аналогичных примеров было обнаружено и при $n = 4$ Н. Д. Элкисом (N. D. Elkies) [*Math. Comp.* **51** (1988), 825–835]. Подумайте, как можно было бы использовать сортировку для поиска примеров, опровергающих предположение Эйлера при $n = 6$.

▶ **19.** [*24*] Файл содержит большое количество 30-разрядных двоичных слов: $x_1, \ldots, x_N$. Придумайте хороший способ нахождения в нем всех *пар с взаимно дополняющими элементами* $\{x_i, x_j\}$. (Два слова называются взаимно дополняющими, если второе содержит нули во всех разрядах, в которых были единицы в первом слове, и наоборот; таким образом, они взаимно дополняющие тогда и только тогда, когда их сумма равна $(11\ldots1)_2$, если они рассматриваются как двоичные числа.)

▶ **20.** [*25*] Имеется файл, содержащий тысячу 30-разрядных двоичных слов $x_1, \ldots, x_{1000}$. Как бы вы стали составлять список всех пар (x_i, x_j), таких, что x_i отличается от x_j не более чем в двух разрядах?

21. [*22*] Как бы вы поступили, если бы вам нужно было найти все пятибуквенные анаграммы, такие как `CARET`, `CARTE`, `CATER`, `CRATE`, `REACT`, `RECTA`, `TRACE`; `CRUEL`, `LUCRE`, `ULCER`; `DOWRY`, `ROWDY`, `WORDY`? [Или если бы вы, допустим, захотели узнать, существуют ли в английском языке наборы из десяти или более анаграмм, кроме замечательной серии

`APERS`, `ASPER`, `PARES`, `PARSE`, `PEARS`, `PRASE`, `PRESA`, `RAPES`, `REAPS`, `SPAER`, `SPARE`, `SPEAR`,

к которой можно еще добавить французское слово `APRÈS`.]

22. [*M28*] Пусть даны описания весьма большого числа ориентированных графов. Как можно сгруппировать *изоморфные* графы? (Два ориентированных графа называются изоморфными, если существует взаимно однозначное соответствие между их вершинами и взаимно однозначное соответствие между их дугами, причем эти соответствия сохраняют инцидентность вершин и дуг.)

23. [*30*] В некоторой группе из 4 096 человек каждый имеет около 100 знакомых. Был составлен список всех пар людей, знакомых друг с другом. (Это отношение симметрично, т. е. если x знаком с y, то и y знаком с x. Поэтому в списке содержится примерно 200 000 пар.) Придумайте алгоритм, который по заданному k выдавал бы все *клики* из k человек. (*Клика* — это группа людей, в которой все знают друг друга.) Предполагается, что не бывает слишком больших клик (размером более 25).

▸ **24.** [*30*] Три миллиона человек с различными именами были уложены рядом непрерывной цепочкой от Нью-Йорка до Калифорнии. Каждому из них дали листок бумаги, на котором он написал свое имя и имя своего ближайшего западного соседа. Человек, находившийся в крайней западной точке цепи, не понял, что ему делать, и выбросил свой листок. Остальные 2 999 999 листков собрали в большую корзину и отправили в Национальный архив, в Вашингтон, округ Колумбия. Там содержимое корзины тщательно перетасовали и записали на магнитные ленты.

Специалист по теории информации определил, что имеется достаточно сведений для восстановления списка людей в исходном порядке. Программист нашел способ сделать это менее чем за 1 000 просмотров лент с данными, используя лишь последовательный доступ к файлам на лентах и небольшой объем оперативной памяти. Как ему это удалось?

[Другими словами, как, имея расположенные произвольным образом пары (x_i, x_{i+1}), $1 \le i < N$, где все x_i различны, получить последовательность $x_1 x_2 \ldots x_N$, применяя лишь методы последовательной обработки данных, которые пригодны для работы с магнитными лентами? Это сортировка в случае, когда трудно определить, какой из двух ключей предшествует другому; мы уже поднимали этот вопрос в упр. 2.2.3–25.]

25. [*M21*] (*Дискретные логарифмы.*) Пусть известно, что p — простое число (довольно большое), а a — первообразный корень по модулю p. Следовательно, для любого b в диапазоне $1 \le b < p$ существует единственное n, такое, что $a^n \bmod p = b$, $1 \le n < p$. (Это n называется индексом b по модулю p по отношению к a.) Как по заданному b найти n менее чем за $\Omega(n)$ шагов. [*Указание.* Пусть $m = \lceil \sqrt{p}\, \rceil$. Попытайтесь решить уравнение $a^{mn_1} \equiv ba^{-n_2}$ (по модулю p) при $0 \le n_1, n_2 < m$.]

*5.1. КОМБИНАТОРНЫЕ СВОЙСТВА ПЕРЕСТАНОВОК

Перестановкой конечного множества называется некоторое расположение его элементов в ряд. Перестановки особенно важны при изучении алгоритмов сортировки, так как они служат для представления неупорядоченных исходных данных. Чтобы исследовать эффективность различных методов сортировки, нужно уметь подсчитывать количество перестановок, которые вынуждают повторять некоторый шаг алгоритма определенное число раз.

Мы уже не раз встречались с перестановками в предыдущих главах. Например, в разделе 1.2.5 обсуждались два основных теоретических метода построения $n!$ перестановок n объектов; в разделе 1.3.3 были проанализированы некоторые алгоритмы, связанные с циклической структурой и мультипликативными свойствами перестановок; в разделе 3.3.2 изучались их серии монотонности. Цель настоящего параграфа — описать другие свойства перестановок и рассмотреть общий случай, когда допускается наличие одинаковых элементов. Попутно мы многое узнаем о комбинаторной математике.

Свойства перестановок настолько красивы, что представляют и самостоятельный интерес. Удобно будет дать их систематическое изложение в одном месте, а не разбрасывать материал по всей главе. Читателям, не имеющим склонности к математике, а также тем, кто жаждет поскорее добраться до самих методов сортировки, рекомендуется перейти сразу к разделу 5.2, потому что настоящий раздел *непосредственного* отношения к сортировке почти не имеет.

*5.1.1. Инверсии

Пусть $a_1\,a_2\ldots a_n$ — перестановка множества $\{1,2,\ldots,n\}$. Если $i<j$ и $a_i>a_j$, то пара (a_i,a_j) называется *инверсией* перестановки; например, перестановка 3 1 4 2 имеет три инверсии: (3,1), (3,2) и (4,2). Каждая инверсия — это пара элементов, "нарушающих порядок"; следовательно, единственная перестановка, не содержащая инверсий, — это рассортированная перестановка $1\,2\ldots n$. Такая связь с сортировкой и является главной причиной нашего интереса к инверсиям, хотя это понятие уже использовалось, когда мы анализировали алгоритм динамического распределения памяти (см. упр. 2.2.2–9).

Понятие инверсии ввел Г. Крамер в 1750 году в связи со своим замечательным правилом решения линейных уравнений [*Intr. à l'Analyse des Lignes Courbes Algébriques* (Geneva, 1750), 657–659; см. также Thomas Muir, *Theory of Determinants* **1** (1906), 11–14]. В сущности, он определил детерминант $n\times n$-матрицы следующим образом:

$$\det\begin{pmatrix} x_{11} & x_{12} & \ldots & x_{1n}\\ \vdots & \vdots & & \vdots\\ x_{n1} & x_{n2} & \ldots & x_{nn}\end{pmatrix} = \sum(-1)^{\operatorname{inv}(a_1a_2\ldots a_n)}x_{1a_1}x_{2a_2}\ldots x_{na_n},$$

где сумма берется по всем перестановкам $a_1\,a_2\ldots a_n$ из $\{1,2,\ldots,n\}$, а $\operatorname{inv}(a_1\,a_2\ldots a_n)$ — число инверсий в перестановке.

Таблица инверсий $b_1\,b_2\ldots b_n$ перестановки $a_1\,a_2\ldots a_n$ образуется, если определить b_j как число элементов слева от j, которые больше, чем j. Другими словами, b_j — число инверсий, второй элемент которых равен j. Отсюда, например, следует, что таблицей инверсий перестановки

$$5\ 9\ 1\ 8\ 2\ 6\ 4\ 7\ 3 \qquad (1)$$

будет

$$2\ 3\ 6\ 4\ 0\ 2\ 2\ 1\ 0, \qquad (2)$$

поскольку 5 и 9 расположены левее 1; 5, 9, 8 — левее 2 и т. д. Всего эта перестановка имеет 20 инверсий. По определению числа b_j всегда удовлетворяют неравенствам

$$0 \le b_1 \le n-1, \quad 0 \le b_2 \le n-2, \quad \ldots, \quad 0 \le b_{n-1} \le 1, \quad b_n = 0. \qquad (3)$$

Пожалуй, наиболее важный факт, касающийся перестановок и установленный Маршаллом Холлом (Marshall Hall), состоит в том, что *таблица инверсий единственным образом определяет соответствующую перестановку.* [См. *Proc. Symp. Applied Math.* **6** (American Math. Society, 1956), 203.] Из любой таблицы инверсии $b_1\, b_2 \ldots b_n$, удовлетворяющей условиям (3), можно однозначно восстановить перестановку, которая ее породила, путем последовательного определения относительного расположения элементов $n, n-1, \ldots, 1$ (в этом порядке). Например, перестановку, соответствующую (2), можно построить следующим образом: выпишем число 9, затем разместим 8 после 9, поскольку $b_8 = 1$. Аналогично установим 7 после и 8, и 9, поскольку $b_7 = 2$. Так как $b_6 = 2$, то 6 должно следовать за двумя уже выписанными нами числами; таким образом, имеем промежуточный результат

$$9\ 8\ 6\ 7.$$

Продолжим, приписав 5 левее, поскольку $b_5 = 0$; поместим 4 вслед за четырьмя из уже записанных чисел, а 3 — после шести выписанных чисел (т. е. в правый конец) и получим

$$5\ 9\ 8\ 6\ 4\ 7\ 3.$$

Вставив аналогичным образом 2 и 1, придем к (1).

Такое соответствие важно, потому что часто можно заменить задачу, сформулированную в терминах перестановок, эквивалентной ей задачей, сформулированной в терминах таблиц инверсий, которая, возможно, решается проще. Рассмотрим, например, самый простой вопрос: сколько существует перестановок множества $\{1, 2, \ldots, n\}$? Ответ должен быть равен числу всевозможных таблиц инверсий, а их легко пересчитать, так как b_1 можно выбрать n способами, b_2 независимо от b_1 — $n-1$ способами, …, а b_n — единственным способом; итого получаем $n(n-1)\ldots 1 = n!$ различных таблиц инверсий. Таблицы инверсий пересчитать легче, потому что значения b_k полностью не зависят друг от друга, в то время как a_k должны быть все различны.

В разделе 1.2.10 мы рассматривали задачу о числе локальных максимумов перестановки, если читать ее справа налево. Иными словами, требовалось подсчитать количество элементов, каждый из которых больше любого из следующих после него. (Например, правосторонние максимумы в (1) — это 3, 7, 8 и 9.) Оно равно количеству индексов j, таких, что b_j имеет максимальное значение $n-j$. Так как b_1 будет равно $n-1$ с вероятностью $1/n$ и (независимо) b_2 будет равно $n-2$ с вероятностью $1/(n-1)$ и т. д., из рассмотрения инверсий ясно, что среднее число правосторонних максимумов равно

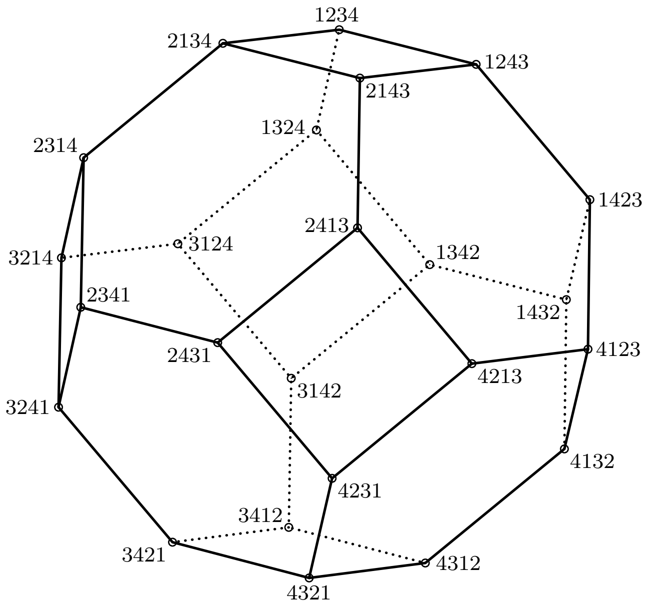

Рис. 1. Усеченный октаэдр, на котором показано изменение числа инверсий, когда меняются местами два соседних элемента перестановки.

$$\frac{1}{n} + \frac{1}{n-1} + \cdots + \frac{1}{1} = H_n.$$

Аналогичным способом легко получить и соответствующую производящую функцию.

Ясно, что если поменять местами *соседние* элементы перестановки, то общее число инверсий увеличится или уменьшится на единицу. На рис. 1 показаны 24 перестановки множества $\{1, 2, 3, 4\}$; линиями соединены перестановки, отличающиеся одна от другой положением двух соседних элементов; двигаясь вдоль линии вниз, мы увеличиваем число инверсий на единицу. Следовательно, число инверсий в перестановке π равно длине нисходящего пути из 1234 в π на рис. 1; все такие пути должны иметь одинаковую длину.

Заметим, что эту диаграмму можно рассматривать как трехмерное твердое тело — "усеченный октаэдр", имеющий 8 шестиугольных и 6 квадратных граней. Это один из классических правильных многогранников, которые исследовал еще Архимед (см. упр. 10).

Не следует путать "инверсии" перестановок (inversions of a permutation) с *обратными* перестановками (*inverse* of a permutation). Вспомним, что перестановку можно записывать в виде двух строк:

$$\begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ a_1 & a_2 & a_3 & \ldots & a_n \end{pmatrix}. \tag{4}$$

Обратной называется перестановка $a'_1\, a'_2\, a'_3 \ldots a'_n$, которая получается, если в (4) поменять местами строки, а затем упорядочить столбцы в порядке возрастания по верхним элементам:

$$\begin{pmatrix} a_1 & a_2 & a_3 & \ldots & a_n \\ 1 & 2 & 3 & \ldots & n \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ a'_1 & a'_2 & a'_3 & \ldots & a'_n \end{pmatrix}. \tag{5}$$

Например, обратной к перестановке $5\,9\,1\,8\,2\,6\,4\,7\,3$ будет перестановка $3\,5\,9\,7\,1\,6\,8\,4\,2$, так как

$$\begin{pmatrix} 5\,9\,1\,8\,2\,6\,4\,7\,3 \\ 1\,2\,3\,4\,5\,6\,7\,8\,9 \end{pmatrix} = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8\,9 \\ 3\,5\,9\,7\,1\,6\,8\,4\,2 \end{pmatrix}.$$

Можно дать другое определение обратной перестановки: $a'_j = k$ тогда и только тогда, когда $a_k = j$.

Понятие обратной перестановки впервые ввел Х. А. Роте (H. A. Rothe) [в *Sammlung combinatorisch-analytischer Abhandlungen*, edited by K. F. Hindenburg, **2** (Leipzig, 1800), 263–305]. Он заметил интересную связь между обратными перестановками и инверсиями: *обратная перестановка содержит ровно столько инверсий, сколько исходная*. Роте дал не самое простое доказательство этого факта, но оно поучительно и притом довольно красиво. Построим таблицу размером $n \times n$, наподобие шахматной доски, в которой точки стоят в j-й клетке i-й строки, если $a_i = j$. После этого расставим крестики во всех клетках, снизу от которых (в том же столбце) и справа (в той же строке) есть точки. Например, для $5\,9\,1\,8\,2\,6\,4\,7\,3$ диаграмма будет выглядеть следующим образом:

×	×	×	×	•				
×	×	×	×		×	×	×	•
•								
	×	×	×		×	×	•	
	•							
		×	×		•			
		×	•					
		×				•		
		•						

Количество крестиков равно числу инверсий, так как нетрудно видеть, что b_j равно числу крестиков в j-м столбце. Если мы теперь транспонируем диаграмму (поменяв ролями строки и столбцы), то получим диаграмму для обратной по отношению к исходной перестановки; значит, число крестиков (число инверсий) одинаково в обоих случаях. Роте использовал данный факт для доказательства того, что детерминант матрицы не меняется при транспонировании.

Для анализа некоторых алгоритмов сортировки необходимо знать число перестановок n элементов, содержащих ровно k инверсий. Обозначим это число через $I_n(k)$; в табл. 1 приведено несколько первых значений данной функции.

Из таблицы инверсий $b_1\,b_2 \ldots b_n$ ясно, что $I_n(0) = 1$, $I_n(1) = n - 1$ и что выполняется свойство симметрии:

$$I_n\left(\binom{n}{2} - k\right) = I_n(k). \tag{6}$$

Далее, так как значения b_k можно выбирать независимо одно от другого, нетрудно видеть, что производящая функция

$$G_n(z) = I_n(0) + I_n(1)\,z + I_n(2)\,z^2 + \cdots \tag{7}$$

Таблица 1

ПЕРЕСТАНОВКА С k ИНВЕРСИЯМИ

n	$I_n(0)$	$I_n(1)$	$I_n(2)$	$I_n(3)$	$I_n(4)$	$I_n(5)$	$I_n(6)$	$I_n(7)$	$I_n(8)$	$I_n(9)$	$I_n(10)$	$I_n(11)$
1	1	0	0	0	0	0	0	0	0	0	0	0
2	1	1	0	0	0	0	0	0	0	0	0	0
3	1	2	2	1	0	0	0	0	0	0	0	0
4	1	3	5	6	5	3	1	0	0	0	0	0
5	1	4	9	15	20	22	20	15	9	4	1	0
6	1	5	14	29	49	71	90	101	101	90	71	49

удовлетворяет соотношению $G_n(z) = (1 + z + \cdots + z^{n-1})G_{n-1}(z)$; следовательно, она имеет довольно простой вид, как показано О. Родригесом (O. Rodrigues) [*J. de Math.* **4** (1839), 236–240]:

$$(1 + z + \cdots + z^{n-1}) \ldots (1 + z)(1) = (1 - z^n) \ldots (1 - z^2)(1 - z)/(1 - z)^n. \tag{8}$$

С помощью этой производящей функции можно легко продолжить табл. 1 и убедиться, что числа, расположенные под ступенчатой линией в таблице, удовлетворяют соотношению

$$I_n(k) = I_n(k-1) + I_{n-1}(k), \quad \text{где} \quad k < n. \tag{9}$$

(Для чисел, находящихся *над* ступенчатой линией, это соотношение *не* выполняется.) Более сложные рассуждения (см. упр. 14) показывают, что на самом деле справедливы формулы

$$\begin{aligned}
I_n(2) &= \binom{n}{2} - 1, && n \ge 2;\\
I_n(3) &= \binom{n+1}{3} - \binom{n}{1}, && n \ge 3;\\
I_n(4) &= \binom{n+2}{4} - \binom{n+1}{2}, && n \ge 4;\\
I_n(5) &= \binom{n+3}{5} - \binom{n+2}{3} + 1, && n \ge 5.
\end{aligned}$$

Общая формула для $I_n(k)$ содержит около $1.6\sqrt{k}$ слагаемых:

$$\begin{aligned}
I_n(k) = \binom{n+k-2}{k} - \binom{n+k-3}{k-2} + \binom{n+k-6}{k-5} + \binom{n+k-8}{k-7} - \cdots\\
+ (-1)^j\left(\binom{n+k-u_j-1}{k-u_j} + \binom{n+k-u_j-j-1}{k-u_j-j}\right) + \cdots, \quad n \ge k,
\end{aligned} \tag{10}$$

где $u_j = (3j^2 - j)/2$ — так называемое "пентагональное число".

Разделив $G_n(z)$ на $n!$, получим производящую функцию $g_n(z)$ распределения вероятностей числа инверсий в случайной перестановке n элементов. Она равна произведению

$$g_n(z) = h_1(z)h_2(z) \ldots h_n(z), \tag{11}$$

где $h_k(z) = (1 + z + \cdots + z^{k-1})/k$ — производящая функция равномерного распределения случайной величины, принимающей целые неотрицательные значения, меньшие k. Отсюда*

$$\begin{aligned}\operatorname{mean}(g_n) &= \operatorname{mean}(h_1) + \operatorname{mean}(h_2) + \cdots + \operatorname{mean}(h_n)\\ &= 0 + \frac{1}{2} + \cdots + \frac{n-1}{2} = \frac{n(n-1)}{4};\end{aligned} \tag{12}$$

$$\begin{aligned}\operatorname{var}(g_n) &= \operatorname{var}(h_1) + \operatorname{var}(h_2) + \cdots + \operatorname{var}(h_n)\\ &= 0 + \frac{1}{4} + \cdots + \frac{n^2-1}{12} = \frac{n(2n+5)(n-1)}{72}.\end{aligned} \tag{13}$$

Таким образом, среднее число инверсий довольно велико — около $\frac{1}{4}n^2$; стандартное отклонение также весьма велико — около $\frac{1}{6}n^{3/2}$.

В качестве интересного завершения данной темы рассмотрим одно замечательное открытие, принадлежащее П. А. Мак-Магону (P. A. MacMahon) [*Amer. J. Math.* **35** (1913), 281–322]. Определим *индекс* перестановки $a_1\,a_2\ldots a_n$ как сумму всех j, таких, что $a_j > a_{j+1}$, $1 \le j < n$. Например, индекс перестановки 5 9 1 8 2 6 4 7 3 равен $2 + 4 + 6 + 8 = 20$. Индекс случайно совпал с числом инверсий. Если составить список всех приведенных ниже 24 перестановок множества $\{1, 2, 3, 4\}$, то получится, что *число перестановок, имеющих данный индекс k, равно числу перестановок, имеющих k инверсий*.

Перестановка	Индекс	Количество инверсий	Перестановка	Индекс	Количество инверсий
1 2 3 4	0	0	3|1 2 4	1	2
1 2 4|3	3	1	3|1 4|2	4	3
1 3|2 4	2	1	3|2|1 4	3	3
1 3 4|2	3	2	3|2 4|1	4	4
1 4|2 3	2	2	3 4|1 2	2	4
1 4|3|2	5	3	3 4|2|1	5	5
2|1 3 4	1	1	4|1 2 3	1	3
2|1 4|3	4	2	4|1 3|2	4	4
2 3|1 4	2	2	4|2|1 3	3	4
2 3 4|1	3	3	4|2 3|1	4	5
2 4|1 3	2	3	4|3|1 2	3	5
2 4|3|1	5	4	4|3|2|1	6	6

На первый взгляд, этот факт может показаться почти очевидным, однако после некоторых размышлений он начинает казаться чуть ли не мистическим, и не видно никакого простого прямого его доказательства. Мак-Магон нашел следующее остроумное косвенное доказательство. Пусть $\operatorname{ind}(a_1\,a_2\ldots a_n)$ — индекс перестановки $a_1\,a_2\ldots a_n$ и соответствующая производящая функция есть

$$H_n(z) = \sum z^{\operatorname{ind}(a_1\,a_2\ldots a_n)}, \tag{14}$$

* Здесь и далее $\operatorname{mean}(g)$ означает среднее значение случайной величины g, а $\operatorname{var}(g)$ — дисперсию величины g. — *Прим. перев.*

где сумма в (14) берется по всем перестановкам множества $\{1, 2, \ldots, n\}$. Требуется доказать, что $H_n(z) = G_n(z)$. Для этого определим взаимно однозначное соответствие между n-мерными строками $(q_1, q_2, \ldots, q_n)$ неотрицательных целых чисел, с одной стороны, и упорядоченными парами n-мерных строк

$$\bigl((a_1, a_2, \ldots, a_n),\ (p_1, p_2, \ldots, p_n)\bigr),$$

с другой стороны, где $a_1\, a_2 \ldots a_n$ — суть перестановка множества индексов $\{1, 2, \ldots, n\}$ и $p_1 \geq p_2 \geq \cdots \geq p_n \geq 0$. Это соответствие будет удовлетворять условию

$$q_1 + q_2 + \cdots + q_n = \operatorname{ind}(a_1\, a_2 \ldots a_n) + (p_1 + p_2 + \cdots + p_n). \tag{15}$$

Производящая функция $\sum z^{q_1+q_2+\cdots+q_n}$, где сумма берется по всем n-мерным строкам неотрицательных целых чисел $(q_1, q_2, \ldots, q_n)$, равна $Q_n(z) = 1/(1-z)^n$; а производящая функция $\sum z^{p_1+p_2+\cdots+p_n}$, где сумма берется по всем n-мерным строкам целых чисел $(p_1, p_2, \ldots, p_n)$, таких, что $p_1 \geq p_2 \geq \cdots \geq p_n \geq 0$, равна

$$P_n(z) = 1/(1-z)(1-z^2)\ldots(1-z^n), \tag{16}$$

как показано в упр. 15. Существование взаимно однозначного соответствия, которое удовлетворяет условию (15) и которое мы собираемся установить, доказывает равенство $Q_n(z) = H_n(z)P_n(z)$, т. е.

$$H_n(z) = Q_n(z)/P_n(z). \tag{17}$$

Но $Q_n(z)/P_n(z)$ и есть $G_n(z)$, как следует из (8).

Требуемое соответствие определяется с помощью простой процедуры сортировки. Любая n-мерная строка $(q_1, q_2, \ldots, q_n)$ может быть устойчиво реорганизована в порядке невозрастания $q_{a_1} \geq q_{a_2} \geq \cdots \geq q_{a_n}$, где $a_1\, a_2 \ldots a_n$ — перестановка, такая, что $q_{a_j} = q_{a_{j+1}}$ и подразумевает $a_j < a_{j+1}$. Установим $(p_1, p_2, \ldots, p_n) = (q_{a_1}, q_{a_2}, \ldots, q_{a_n})$ и затем для $1 \leq j < n$ вычтем 1 из каждого $p_1, \ldots, p_j$ для таких j, которые соответствуют $a_j > a_{j+1}$. По-прежнему $p_1 \geq p_2 \geq \cdots \geq p_n$, поскольку p_j обязательно превышает p_{j+1}, если только $a_j > a_{j+1}$. Полученная в результате пара $\bigl((a_1, a_2, \ldots, a_n), (p_1, p_2, \ldots, p_n)\bigr)$ удовлетворяет условию (15), поскольку суммарное уменьшение элементов p равно $\operatorname{ind}(a_1\, a_2 \ldots a_n)$. Например, если $n = 9$ и $(q_1, \ldots, q_9) = (3, 1, 4, 1, 5, 9, 2, 6, 5)$, то получим $a_1 \ldots a_9 = 6\,8\,5\,9\,3\,1\,7\,2\,4$ и $(p_1, \ldots, p_9) = (5, 2, 2, 2, 2, 2, 1, 1, 1)$.

Несложно вернуться к $(q_1, q_2, \ldots, q_n)$, когда заданы $a_1\, a_2 \ldots a_n$ и $(p_1, p_2, \ldots, p_n)$ (см. упр. 17). Итак, желаемое соответствие установлено, теорема Мак-Магона об индексах доказана.

Д. Фоата (D. Foata) и М. П. Шуценберже (M. P. Schützenberger) отыскали неожиданное расширение теоремы Мак-Магона через 65 лет после его первой публикации. *Число перестановок n элементов, которые имеют k инверсий и индекс l, равно числу перестановок, которые имеют l инверсий и индекс k.* Фактически Фоата и Шуценберже нашли простое однозначное соответствие между перестановками первого и второго типов (см. упр. 25).

УПРАЖНЕНИЯ

1. [*10*] Какова таблица инверсий для перестановки 2 7 1 8 4 5 9 3 6? Какой перестановке соответствует таблица инверсий 5 0 1 2 1 2 0 0?

2. [*M20*] Классическая задача Иосифа формулируется следующим образом (см. также упр. 1.3.2–22): n рабов вначале стоят по кругу; после того как m-го раба казнят, круг смыкается, затем опять казнят m-го раба и так до тех пор, пока всех рабов не постигнет эта печальная участь. Таким образом, порядок, в котором рабы подвергаются наказанию, представляет собой перестановку множества $\{1, 2, \ldots, n\}$. Например, если $n = 8$ и $m = 4$, порядок будет иметь вид 5 4 6 1 3 8 7 2 (первым казнили 5-го раба и т. д.); таблица инверсий для этой перестановки имеет вид 3 6 3 1 0 0 1 0.

Найдите простое рекуррентное соотношение для элементов $b_1\, b_2 \ldots b_n$ таблицы инверсий в общей задаче Иосифа для n рабов, если каждого m-го раба казнят.

3. [*18*] Пусть перестановке $a_1\, a_2 \ldots a_n$ соответствует таблица инверсий $b_1\, b_2 \ldots b_n$. Какой перестановке $\overline{a}_1\, \overline{a}_2 \ldots \overline{a}_n$ соответствует таблица инверсий

$$(n - 1 - b_1)(n - 2 - b_2) \ldots (0 - b_n)\,?$$

▸ **4.** [*20*] Придумайте пригодный для компьютерной реализации алгоритм, который по данной таблице инверсий $b_1\, b_2 \ldots b_n$, удовлетворяющей условиям (3), строил бы соответствующую перестановку $a_1\, a_2 \ldots a_n$. [*Указание.* Вспомните методы работы со связями в памяти.]

5. [*35*] Для выполнения алгоритма из упр. 4 на типичном компьютере потребуется время, приблизительно пропорциональное $n + b_1 + \cdots + b_n$, а это в среднем равно $\Theta(n^2)$. Можно ли создать алгоритм, порядок времени выполнения которого был бы существенно меньше, чем n^2?

▸ **6.** [*26*] Придумайте алгоритм вычисления таблицы инверсий $b_1\, b_2 \ldots b_n$, соответствующей данной перестановке $a_1\, a_2 \ldots a_n$ множества $\{1, 2, \ldots, n\}$, время работы которого на типичном компьютере было бы порядка $n \log n$.

7. [*20*] Помимо таблицы $b_1\, b_2 \ldots b_n$, определенной в этом упражнении, можно определить некоторые типы таблиц инверсий, соответствующих данной перестановке $a_1\, a_2 \ldots a_n$ множества $\{1, 2, \ldots, n\}$. В этом упражнении мы рассмотрим три других типа таблиц инверсий, которые возникают в приложениях.

Пусть c_j — число инверсий, *первая* компонента которых равна j, т. е. число элементов, меньших j и расположенных *правее* j. [Перестановке (1) соответствует таблица 0 0 0 1 4 2 1 5 7; ясно, что $0 \le c_j < j$.] Пусть $B_j = b_{a_j}$ и $C_j = c_{a_j}$.

Покажите, что при $1 \le j \le n$ справедливы неравенства $0 \le B_j < j$ и $0 \le C_j \le n - j$; покажите также, что перестановку $a_1\, a_2 \ldots a_n$ можно однозначно определить, если задана таблица $c_1\, c_2 \ldots c_n$ или $B_1\, B_2 \ldots B_n$, или $C_1\, C_2 \ldots C_n$.

8. [*M24*] Сохраним обозначения, принятые в упр. 7. Пусть $a'_1\, a'_2 \ldots a'_n$ — перестановка, обратная к $a_1\, a_2 \ldots a_n$, и пусть соответствующие ей таблицы инверсий — $b'_1\, b'_2 \ldots b'_n$, $c'_1\, c'_2 \ldots c'_n$, $B'_1\, B'_2 \ldots B'_n$ и $C'_1\, C'_2 \ldots C'_n$. Найдите как можно больше интересных соотношений между числами a_j, b_j, c_j, B_j, C_j, a'_j, b'_j, c'_j, B'_j, C'_j.

▸ **9.** [*M21*] Докажите, что в обозначениях, принятых в упр. 7, перестановка $a_1\, a_2 \ldots a_n$ представляет собой инволюцию (т. е. обратна самой себе) тогда и только тогда, когда $b_j = C_j$ при $1 \le j \le n$.

10. [*HM20*] Рассмотрите представленный на рис. 1 октаэдр как многогранник в трехмерном пространстве. Чему равен диаметр усеченного октаэдра (расстояние между вершинами 1234 и 4321), если все ребра имеют единичную длину?

11. [*M25*] Если $\pi = a_1\, a_2 \ldots a_n$ представляет собой перестановку множества $\{1, 2, \ldots, n\}$, то обозначим как

$$E(\pi) = \{(a_i, a_j) \mid i < j,\ a_i > a_j\}$$

множество ее инверсий, а как

$$\overline{E}(\pi) = \{(a_i, a_j) \mid i > j,\, a_i > a_j\}$$

множество ее "неинверсий".

a) Докажите, что $E(\pi)$ и $\overline{E}(\pi)$ транзитивны. (Множество S упорядоченных пар называется *транзитивным*, если для любых (a, b) и (b, c), принадлежащих S, пара (a, c) также принадлежит S.)

b) Обратно, пусть E — любое транзитивное подмножество множества $T = \{(x, y) \mid 1 \le y < x \le n\}$, дополнение которого $\overline{E} = T \setminus E$ также транзитивно. Докажите, что существует перестановка π, такая, что $E(\pi) = E$.

12. [*M28*] Используя обозначения, принятые в предыдущем упражнении, докажите, что если π_1 и π_2 — перестановки, а E — минимальное транзитивное множество, содержащее $E(\pi_1) \cup E(\pi_2)$, то $\overline{E}$ — также транзитивное множество. [Следовательно, если мы говорим, что π_1 находится "над" π_2, когда $E(\pi_1) \subseteq E(\pi_2)$, то определена *решетка* перестановок; существует единственная "самая низкая" перестановка, находящаяся "над" двумя данными перестановками. Диаграмма решетки при $n = 4$ представлена на рис. 1.]

13. [*M23*] Известно, что в разложении определителя половина членов выписывается со знаком "+", а половина — со знаком "−". Другими словами, при $n \ge 2$ перестановок с *четным* числом инверсий ровно столько же, сколько с *нечетным*. Покажите, что вообще при $n \ge m$ количество перестановок с числом инверсий, конгруэнтным t по модулю m, равно $n!/m$, независимо от того, каково целое число t.

14. [*M24*] (Ф. Франклин (F. Franklin).) Разбиение числа n на k различных частей — это представление n в виде суммы $n = p_1 + p_2 + \cdots + p_k$, где $p_1 > p_2 > \cdots > p_k > 0$. Например, разбиения числа 7 на различные части таковы: 7, $6+1$, $5+2$, $4+3$, $4+2+1$. Пусть $f_k(n)$ — число разбиений n на k различных частей. Докажите, что $\sum_k (-1)^k f_k(n) = 0$, если только n не представляется в виде $(3j^2 \pm j)/2$ при некотором неотрицательном целом j; в этом случае сумма равна $(-1)^j$. Например, для $n = 7$ сумма равна $-1 + 3 - 1 = 1$, потому что $7 = (3 \cdot 2^2 + 2)/2$. [*Указание*. Представьте разбиения в виде массива точек, в i-й строке которого имеется p_i точек, $1 \le i \le k$. Найдите наименьшее j, такое, что $p_{j+1} < p_j - 1$, и обведите крайние справа точки первых j строк. Если $j < p_k$, то эти j точек можно, как правило, изъять из массива, повернуть на 45° и поместить в новую, $(k+1)$-ю, строку. С другой стороны, если $j \ge p_k$, то обычно можно изъять из массива k-ю строку точек, повернуть ее на 45° и поместить справа от обведенных точек (рис. 2). В результате в большинстве случаев разбиения с четным числом строк и разбиения с нечетным числом строк группируются в пары; таким образом, в сумме следует учитывать только непарные разбиения.]

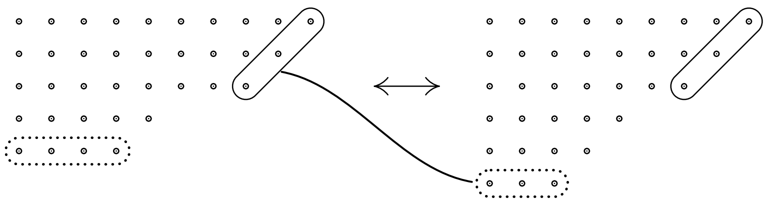

Рис. 2. Соответствие Франклина между разбиениями на различные части.

Замечание. Как следствие получаем формулу Эйлера:

$$(1-z)(1-z^2)(1-z^3)\ldots = 1 - z - z^2 + z^5 + z^7 - z^{12} - z^{15} + \cdots$$
$$= \sum_{-\infty<j<\infty} (-1)^j z^{(3j^2+j)/2}.$$

Поскольку производящая функция для обычных разбиений (не обязательно на различные части) равна $\sum p(n)z^n = 1/(1-z)(1-z^2)(1-z^3)\ldots$, получаем неочевидное рекуррентное соотношение для числа разбиений:

$$p(n) = p(n-1) + p(n-2) - p(n-5) - p(n-7) + p(n-12) + p(n-15) - \cdots.$$

15. [*M23*] Докажите, что соотношение (16) — это производящая функция для числа разбиений не более чем на n частей, т. е. докажите, что коэффициент при z^m в $1/(1-z)(1-z^2)\ldots(1-z^n)$ равен числу способов представления m в виде суммы $m = p_1 + p_2 + \cdots + p_n$, где $p_1 \geq p_2 \geq \cdots \geq p_n \geq 0$. [*Указание.* Нарисуйте точки, как в упр. 14, и покажите, что существует взаимно однозначное соответствие между n-мерными строками чисел $(p_1, p_2, \ldots, p_n)$, такими, что $p_1 \geq p_2 \geq \cdots \geq p_n \geq 0$, и последовательностями $(P_1, P_2, P_3, \ldots)$, такими, что $n \geq P_1 \geq P_2 \geq P_3 \geq \cdots \geq 0$, обладающее тем свойством, что $p_1 + p_2 + \cdots + p_n = P_1 + P_2 + P_3 + \cdots$. Иными словами, покажите, что разбиениям не более чем на n частей соответствуют разбиения на части, не превосходящие n.]

16. [*M25*] (Л. Эйлер.) Докажите следующие тождества, интерпретируя обе части соотношений в терминах разбиений:

$$\begin{aligned}\prod_{k\geq 0}\frac{1}{(1-q^k z)} &= \frac{1}{(1-z)(1-qz)(1-q^2z)\ldots}\\ &= 1 + \frac{z}{1-q} + \frac{z^2}{(1-q)(1-q^2)} + \cdots = \sum_{n\geq 0} z^n \Big/ \prod_{1\leq k\leq n}(1-q^k);\end{aligned}$$

$$\begin{aligned}\prod_{k\geq 0}(1+q^k z) &= (1+z)(1+qz)(1+q^2z)\ldots\\ &= 1 + \frac{z}{1-q} + \frac{z^2 q}{(1-q)(1-q^2)} + \cdots = \sum_{n\geq 0} z^n q^{n(n-1)/2} \Big/ \prod_{1\leq k\leq n}(1-q^k).\end{aligned}$$

17. [*20*] Каковы 24 тетрады (q_1, q_2, q_3, q_4), для которых в соответствии Мак-Магона, определенном в конце этого раздела, $(p_1, p_2, p_3, p_4) = (0,0,0,0)$?

18. [*M30*] (T. Hibbard, *CACM* **6** (1963), 210.)

Пусть $n > 0$ и последовательность 2^n n-разрядных целых чисел $X_0, \ldots, X_{2^n-1}$ получена случайным образом, причем каждый разряд каждого числа независимо от других разрядов принимает значение 1 с вероятностью p. Рассмотрим последовательность $X_0 \oplus 0$, $X_1 \oplus 1$, $\ldots$, $X_{2^n-1} \oplus (2^n - 1)$, где $\oplus$ — операция "исключающее или" над двоичными представлениями. Так, если $p = 0$, то последовательность будет такой: $0, 1, \ldots, 2^n-1$; если $p = 1$, то она будет такой: $2^n-1, \ldots, 1, 0$; если же $p = \frac{1}{2}$, то каждый элемент последовательности — случайное число между 0 и $2^n - 1$. Вообще же, при разных p это хороший способ получения последовательности случайных целых чисел со смещенным числом инверсий, в то время как распределение элементов последовательности, рассматриваемой как единое целое, равномерно (uniform) в том смысле, что все n-разрядные целые двоичные числа будут иметь одинаковые распределения. Определите среднее число инверсий в такой последовательности как функцию от вероятности p.

19. [*M28*] (К. Мейер (C. Meyer).) Если m и n — взаимно простые числа, то известно, что последовательность $(m \bmod n)(2m \bmod n)\ldots((n-1)m \bmod n)$ представляет собой перестановку множества $\{1, 2, \ldots, n-1\}$. Покажите, что число инверсий этой перестановки может быть выражено в терминах сумм Дедекинда (см. п. 3.3.3).

20. [*M43*] Следующее знаменитое тождество, принадлежащее Якоби [*Fundamenta Nova Theoriæ Functionum Ellipticarum* (1829), §64], лежит в основе многих замечательных соотношений, содержащих эллиптические функции:

$$\begin{aligned}\prod_{k\geq 1}(1-u^kv^{k-1})(1-u^{k-1}v^k)(1-u^kv^k)&\\ &=(1-u)(1-v)(1-uv)(1-u^2v)(1-uv^2)(1-u^2v^2)\dots\\ &=1-(u+v)+(u^3v+uv^3)-(u^6v^3+u^3v^6)+\cdots\\ &=\sum_{-\infty<j<+\infty}(-1)^j u^{\binom{j}{2}}v^{\binom{j+1}{2}}.\end{aligned}$$

Если, например, положить $u=z$, $v=z^2$, то получится формула Эйлера из упр. 14. Если положить $z=\sqrt{u/v}$, $q=\sqrt{uv}$, то получим

$$\prod_{k\geq 1}(1-q^{2k-1}z)(1-q^{2k-1}z^{-1})(1-q^{2k})=\sum_{-\infty<n<\infty}(-1)^n z^n q^{n^2}.$$

Существует ли комбинаторное доказательство тождества Якоби, аналогичное доказательству Франклина для частного случая из упр. 14? (Таким образом, нужно рассмотреть "комплексные разбиения"

$$m+ni=(p_1+q_1i)+(p_2+q_2i)+\cdots+(p_k+q_ki),$$

где p_j+q_ji — различные ненулевые комплексные числа; p_j, q_j, — неотрицательные целые числа, причем $|p_j-q_j|\leq 1$. Согласно тождеству Якоби число таких представлений с четными k равно числу представлений с нечетными k, если только m и n не являются соседними треугольными числами!) Какими еще замечательными свойствами обладают комплексные разбиения?

▸ **21.** [*M25*] (Г. Д. Кнотт (G. D. Knott).) Покажите, что перестановку $a_1\dots a_n$ можно получить с помощью стека (см. упр. 2.2.1–5 или 2.3.1–6) тогда и только тогда, когда $C_j\leq C_{j+1}+1$ при $1\leq j<n$ (см. обозначения в упр. 7).

22. [*M26*] Задана перестановка $a_1\,a_2\dots a_n$ множества $\{1,2,\dots,n\}$. Пусть h_j — число индексов $i<j$, таких, что $a_i\in\{a_j{+}1,a_j{+}2,\dots,a_{j+1}\}$. (Если $a_{j+1}<a_j$, элементы этого множества "оборачиваются" от n к 1. Когда $j=n$, используется множество $\{a_n{+}1,a_n{+}2,\dots,n\}$.) Например, перестановка 5 9 1 8 2 6 4 7 3 приводит к $h_1\dots h_9=0\,0\,1\,2\,1\,4\,2\,4\,6$.

a) Докажите, что $a_1\,a_2\dots a_n$ можно восстановить по числам $h_1\,h_2\dots h_n$.

b) Докажите, что $h_1+h_2+\cdots+h_n$ — суть индексы $a_1\,a_2\dots a_n$.

▸ **23.** [*M27*] (*Русская рулетка.*) Группа из n человек, приговоренных к смерти, которые отдают предпочтение теории вероятности перед теорией чисел, могла бы, рассевшись по кругу и несколько модифицировав метод Иосифа (упр. 2), попробовать такой способ самоубийства. Первый приговоренный нажимает спусковой крючок револьвера, направив его себе в висок; с вероятностью p произойдет роковой выстрел, и он покинет круг. Затем револьвер переходит ко второму приговоренному и он делает то же самое. Далее сюжет повторяется по кругу с постоянной вероятностью $p>0$ до тех пор, пока будет кому его продолжать.

Пусть $a_j=k$, если k-му приговоренному выпал j-й роковой выстрел. Докажите, что порядок "выбывания" $a_1\,a_2\dots a_n$ появится с вероятностью, которая является функцией только n, p и индекса дуальной перестановки $(n+1-a_n)\dots(n+1-a_2)\,(n+1-a_1)$. Какой порядок "выбывания" наименее вероятен?

24. [*M26*] Для заданного множество целых чисел $t(1)\,t(2)\dots t(n)$, где $t(j)\geq j$, *обобщенный индекс* перестановки $a_1\,a_2\dots a_n$ равен сумме всех нижних индексов j, таких, что $a_j>t(a_{j+1})$, плюс общее число инверсий, таких, что $i<j$ и $t(a_j)\geq a_i>a_j$. Значит, если $t(j)=j$ для всех j, обобщенный индекс совпадает с обычным индексом, но при $t(j)\geq n$ для всех j это будет число инверсий. Докажите, что число инверсий, для которых обобщенный индекс равен k, — то же самое, что и число перестановок, которые имеют k инверсий. [*Указание.* Покажите, что, если взять любую перестановку $a_1 \ldots a_{n-1}$ множества $\{1, \ldots, n-1\}$ и поместить число n на все возможные места, обобщенный индекс увеличится на $\{0, 1, \ldots, n-1\}$ в некотором порядке.]

▸ **25.** [*M30*] (Фоата и Шуценберже.) Пусть существует перестановка $\alpha = a_1 \ldots a_n$; обозначим через $\operatorname{ind}(\alpha)$ ее индекс, а через $\operatorname{inv}(\alpha)$ — число ее инверсий.

a) Определите взаимно однозначное соответствие, которое преобразует перестановку α множества $\{1, \ldots, n\}$ в перестановку $f(\alpha)$, имеющую такие два свойства: (i) $\operatorname{ind}(f(\alpha)) = \operatorname{inv}(\alpha)$; (ii) для $1 \le j < n$ число j появляется слева от $j+1$ в $f(\alpha)$ тогда и только тогда, когда оно появляется слева от $j+1$ в α. Какая перестановка при этом соответствует $f(\alpha)$, если $\alpha = 1\,9\,8\,2\,6\,3\,7\,4\,5$? Для какой перестановки $f(\alpha) = 1\,9\,8\,2\,6\,3\,7\,4\,5$? [*Указание.* Если $n > 1$, напишите $\alpha = x_1\alpha_1x_2\alpha_2 \ldots x_k\alpha_k a_n$, где $x_1, \ldots, x_k$ — все элементы, меньшие, чем a_n, если $a_1 < a_n$; в противном случае $x_1, \ldots, x_k$ — все элементы, большие, чем a_n; другие элементы появятся в цепочках (возможно, пустых) $\alpha_1, \ldots, \alpha_k$. Сравните число инверсий $h(\alpha) = \alpha_1x_1\alpha_2x_2 \ldots \alpha_kx_k$ с $\operatorname{inv}(\alpha)$; в этом выражении число a_n отсутствует в $h(\alpha)$.]

b) Обозначьте через f другое однозначное соответствие g, которое имеет два следующих свойства: (i) $\operatorname{ind}(g(\alpha)) = \operatorname{inv}(\alpha)$; (ii) $\operatorname{inv}(g(\alpha)) = \operatorname{ind}(\alpha)$. [*Указание.* Примите во внимание обратные перестановки.]

26. [*M25*] Чему равен статистический коэффициент корреляции между числом инверсий и индексом случайной перестановки? (См. упр. 3.3.2–(24).)

27. [*M37*] Докажите, что в дополнение к (15) существует простое соотношение между $\operatorname{inv}(a_1\,a_2 \ldots a_n)$ и n-мерной строкой $(q_1, q_2, \ldots, q_n)$. Используйте это соотношение для получения производной соотношения (17) в общем случае и формирования алгебраического выражения в виде производящей функции двух переменных

$$H_n(w, z) = \sum w^{\operatorname{inv}(a_1\,a_2 \ldots a_n)} z^{\operatorname{ind}(a_1\,a_2 \ldots a_n)},$$

где суммирование выполняется по всем $n!$ перестановкам $a_1\,a_2 \ldots a_n$.

▸ **28.** [*25*] (Р. В. Флойд (R. W. Floyd), 1983.) Если $a_1\,a_2 \ldots\, a_n$ — перестановка множества $\{1, 2, \ldots, n\}$, то его *суммарное смещение* определяется как $\sum_{j=1}^{n} |a_j - j|$. Найдите верхнюю и нижнюю границы суммарного смещения в терминах количества инверсий.

29. [*28*] Если $\pi = a_1\,a_2 \ldots\, a_n$ и $\pi' = a_1'\,a_2' \ldots\, a_n'$ суть перестановки множества $\{1, 2, \ldots, n\}$, то обозначим их произведение $\pi\pi'$ как $a_{a_1}'\,a_{a_2}' \ldots\, a_{a_n}'$. Пусть $\operatorname{inv}(\pi)$ обозначает количество инверсий, как и в упр. 25. Покажите, что $\operatorname{inv}(\pi\pi') \le \operatorname{inv}(\pi) + \operatorname{inv}(\pi')$ и что равенство соблюдается тогда и только тогда, когда $\pi\pi'$ расположено “ниже” π' (как введено в упр. 12).

*5.1.2. Перестановки мультимножества

До сих пор мы рассматривали перестановки *множества* элементов, но это частный случай перестановок *мультимножества*. (Мультимножество — это то же самое, что и множество, но в нем могут содержаться одинаковые элементы. Некоторые основные свойства мультимножеств обсуждались в разделе 4.6.3–19.)

Рассмотрим, например, мультимножество

$$M = \{a, a, a, b, b, c, d, d, d, d\}, \tag{1}$$

в котором содержится 3 элемента a, 2 элемента b, 1 элемент c и 4 элемента d. Повторения элементов в мультимножестве можно записать и другим способом:

$$M = \{3 \cdot a,\ 2 \cdot b,\ c,\ 4 \cdot d\}. \tag{2}$$

Перестановка мультимножества* M — это некоторое расположение его элементов в ряд, например

$$c\ a\ b\ d\ d\ a\ b\ d\ a\ d.$$

С другой стороны, такую последовательность можно назвать буквенной строкой, содержащей 3 буквы a, 2 буквы b, 1 букву c и 4 буквы d. Сколько существует перестановок мультимножества M? Если бы мы рассматривали все элементы M как различные, обозначив их как a_1, a_2, a_3, b_1, b_2, c_1, d_1, d_2, d_3, d_4, то получили бы $10! = 3{,}628{,}800$ перестановок, но после отбрасывания индексов многие из них оказались бы одинаковыми. Фактически каждая перестановка M встретилась бы ровно $3!\,2!\,1!\,4! = 288$ раз, поскольку в любой из них индексы при буквах a_k можно расставить $3!$ способами, при b_k (независимо) — $2!$ способами, при c_k — одним способом, при d_k — $4!$ способами соответственно. Поэтому число перестановок M равно

$$\frac{10!}{3!\,2!\,1!\,4!} = 12{,}600.$$

В применении к общему случаю те же рассуждения показывают, что число перестановок любого мультимножества равно полиномиальному коэффициенту

$$\binom{n}{n_1, n_2, \ldots} = \frac{n!}{n_1!\,n_2!\ldots}\,, \qquad (3)$$

где n_1 — число элементов первого типа, n_2 — число элементов второго типа и т. д., а $n = n_1 + n_2 + \cdots$ — общее число элементов. Количество перестановок множества было известно еще в древние времена. В древнееврейской Книге Творения (ок. 100 г. н. э.), наиболее раннем литературном произведении иудейского философского мистицизма, даны верные значения первых семи факториалов, после чего говорится: "Продолжай, и получишь числа, которые уста не могут произнести, а ухо не может воспринять". [*Сефер Этзирах*, конец части 4. См. Solomon Gandz, *Studies in Hebrew Astronomy and Mathematics* (New York: Ktav, 1970), 494–496; Aryeh Kaplan, *Sefer Yetzirah* (York Beach, Maine: Samuel Weiser, 1993).] Это первый известный в истории подсчет числа перестановок. Второй встречается в индийском классическом произведении *Ануйогадвара-сутра* (ок. 500 г. н. э.), правило 97, в котором приводится формула числа перестановок шести элементов, которые не расположены ни в порядке возрастания, ни в порядке убывания:

$$6 \times 5 \times 4 \times 3 \times 2 \times 1 - 2.$$

[См. G. Chakravarti, *Bull. Calcutta Math. Soc.* **24** (1932), 79–88. "Ануйогадварасутра" — одна из книг канонов джайнизма, религиозной секты, распространенной в Индии.] Соответствующее правило для мультимножеств впервые, по-видимому, встречается в книге "Лилавати", написанной Бхаскарой Ахарьей (ок. 1150 г.) (разд. 270–271). У Бхаскары это правило сформулировано весьма сжато и проиллюстрировано лишь двумя простыми примерами: $\{2,2,1,1\}$ и $\{4,8,5,5,5\}$. В результате в английском переводе это правило не сформулировано корректно, впрочем, имеются некоторые сомнения относительно того, понимал ли сам Бхаскара, о чем говорил.

* В англоязычной литературе такие перестановки иногда называют "permatution" в отличие от "permutation".

Вслед за этим правилом Бхаскара приводит интересную формулу

$$\frac{(4+8+5+5+5)\times 120\times 11111}{5\times 6}$$

для суммы 20 чисел $48555 + 45855 + \cdots$. Верное правило для нахождения числа перестановок в случае, когда только один элемент может повторяться, найдено независимо немецким ученым иезуитом Атанасиусом Кирхером (Athanasius Kircher) в его многотомном труде о музыке [*Musurgia Universalis* **2** (Rome: 1650), 5–7]. Кирхера интересовал вопрос о количестве мелодий, которые можно создать из данного набора нот; для этого он придумал то, что называл "музарифметикой". На стр. 18–21 своего труда он дает верное значение числа перестановок мультимножества $\{m\cdot C,\, n\cdot D\}$ при нескольких значениях m и n, хотя описал он свой метод вычислений лишь для случая $n=1$. Общее правило (3) появилось позже в книге Жана Престэ (J. Prestet) *Elémens de Mathématiques* (Paris: 1675, 351–352), в которой содержится одно из первых изложений комбинаторной математики, написанных в Западной Европе. Престэ верно сформулировал правило для произвольного мультимножества, но проиллюстрировал его лишь простым примером $\{a,a,b,b,c,c\}$. Он особо отметил, что деление на *сумму* факториалов, которое он считал естественным обобщением правила Кирхера, было бы ошибкой. Несколько лет спустя Джон Валлис (John Wallis) в своей книге *Discourse of Combinations* (Oxford: 1685, Chapter 2), опубликованной вместе с его же *Treatise of Algebra*, рассмотрел это правило более подробно.

В 1965 году Доминик Фоата (Dominique Foata) ввел одно интересное понятие, так называемое "соединительное произведение" (intercalation product), которое позволило распространить многие известные результаты, касающиеся обычных перестановок, на общий случай перестановок мультимножества. [См. *Publ. Inst. Statistique*, Univ. Paris, **14** (1965), 81–241; а также *Lecture Notes in Math.* **85** (Springer, 1969).] Предполагая, что элементы мультимножества каким-то способом линейно упорядочены, можно рассмотреть *двухстрочную нотацию*, например

$$\begin{pmatrix} a & a & a & b & b & c & d & d & d & d \\ c & a & b & d & d & a & b & d & a & d \end{pmatrix}. \tag{4}$$

Здесь верхняя строка содержит элементы M в порядке неубывания и нижняя — это сама перестановка. *Соединительное произведение* $\alpha \intercal \beta$ двух перестановок мультимножеств α и β — это перестановка, которая получается, если (a) взять двухстрочные обозначения для α и β, (b) записать соответствующие строки в одну и (c) рассортировать столбцы так, чтобы элементы верхней строки расположились в порядке неубывания. Сортировка должна быть устойчивой в том смысле, что взаимное расположение элементов нижней строки сохраняется, если соответствующие элементы верхней строки равны. Например, $c\ a\ d\ a\ b \intercal b\ d\ d\ a\ d = c\ a\ b\ d\ d\ a\ b\ d\ a\ d$, так как

$$\begin{pmatrix} a & a & b & c & d \\ c & a & d & a & b \end{pmatrix} \intercal \begin{pmatrix} a & b & d & d & d \\ b & d & d & a & d \end{pmatrix} = \begin{pmatrix} a & a & a & b & b & c & d & d & d & d \\ c & a & b & d & d & a & b & d & a & d \end{pmatrix}. \tag{5}$$

Нетрудно видеть, что операция соединительного произведения ассоциативна, т. е.

$$(\alpha \intercal \beta) \intercal \gamma = \alpha \intercal (\beta \intercal \gamma), \tag{6}$$

и что она подчиняется законам сокращения

$$\begin{aligned} \pi \intercal \alpha = \pi \intercal \beta \quad &\text{влечет за собой} \quad \alpha = \beta, \\ \alpha \intercal \pi = \beta \intercal \pi \quad &\text{влечет за собой} \quad \alpha = \beta. \end{aligned} \tag{7}$$

Существует "единичный элемент"

$$\alpha \intercal \epsilon = \epsilon \intercal \alpha = \alpha, \tag{8}$$

где ϵ — нуль-перестановка, "расположение в ряд" элементов пустого множества. Закон коммутативности, вообще говоря, не выполняется (см. упр. 2), тем не менее

$$\alpha \intercal \beta = \beta \intercal \alpha, \qquad \text{если } \alpha \text{ и } \beta \text{ не содержат общих букв.} \tag{9}$$

Аналогичным способом понятие *цикла* можно распространить на случай, когда элементы могут повторяться. Будем записывать в виде

$$(x_1 \quad x_2 \quad \ldots \quad x_n) \tag{10}$$

перестановку, двухстрочное представление которой получается путем устойчивой сортировки столбцов

$$\begin{pmatrix} x_1 & x_2 & \ldots & x_n \\ x_2 & x_3 & \ldots & x_1 \end{pmatrix} \tag{11}$$

по верхним элементам. Например,

$$(d\ b\ d\ d\ a\ c\ a\ a\ b\ d) = \begin{pmatrix} d & b & d & d & a & c & a & a & b & d \\ b & d & d & a & c & a & a & b & d & d \end{pmatrix} = \begin{pmatrix} a & a & a & b & b & c & d & d & d & d \\ c & a & b & d & d & a & b & d & a & d \end{pmatrix},$$

так что перестановка (4) фактически является циклом. Мы могли бы описать этот цикл словесно, сказав что-нибудь наподобие "d переходит в b, переходит в d, переходит в d, переходит в ... переходит в d и возвращается обратно". Заметим, что эти обобщенные циклы не обладают всеми свойствами обычных циклов: $(x_1\, x_2 \ldots x_n)$ — необязательно то же самое, что и $(x_2 \ldots x_n\, x_1)$. В разделе 1.3.3 мы выяснили, что каждую перестановку множества можно единственным с точностью до порядка сомножителей образом представить в виде произведения непересекающихся циклов, где "произведение" перестановок определяется законом композиции. Легко видеть, что *произведение непересекающихся циклов — то же самое, что их соединительное произведение*; это наводит на мысль о том, что можно будет обобщить полученные ранее результаты, если найти единственное (в каком-то смысле) представление и для произвольной перестановки мультимножества в виде соединительного произведения циклов. В действительности существует, по крайней мере, два естественных способа сделать это, и каждый из них имеет важные приложения. Равенство (5) дает один способ представления $c\ a\ b\ d\ d\ a\ b\ d\ a\ d$ в виде соединительного произведения более коротких перестановок. Рассмотрим общую задачу о нахождении всех разложений $\pi = \alpha \intercal \beta$ данной перестановки π. Для этого полезно проанализировать конкретную перестановку, например

$$\pi = \begin{pmatrix} a & a & b & b & b & b & b & c & c & c & d & d & d & d & d \\ d & b & c & b & c & a & c & d & a & d & d & b & b & b & d \end{pmatrix}. \tag{12}$$

Если можно записать π в виде $\alpha \intercal \beta$, где α содержит, по крайней мере, одну букву a, то крайнее слева a в верхней строке двухстрочного представления α должно оказаться над d; значит, перестановка α должна содержать хотя бы одну букву d. Если взглянуть теперь на крайнее слева d в верхней строке α, то можно точно так же увидеть, что оно должно оказаться над d; значит, в α должны содержаться, по меньшей мере, *две* буквы d. Посмотрев на второе d, видим, что α содержит также b. Единственное предположение о том, что α есть левый сомножитель π, содержащий букву a, приводит к такому промежуточному результату:

$$\alpha = \begin{pmatrix} a & \ldots & b & \ldots & d & d & \ldots \\ d & & & & d & b & \end{pmatrix}. \qquad (13)$$

Продолжая рассуждать точно так же, обнаружим, что буква b в верхней строке (13) должна оказаться над c, и т. д. В конце концов, этот процесс вновь приведет нас к букве a, и мы сможем, если захотим, отождествить ее с первой буквой a. Такое рассуждение, по существу, доказывает, что любой левый сомножитель α в разложении перестановки (12), содержащий a, имеет вид $(d\ d\ b\ c\ d\ b\ b\ c\ a) \top \alpha'$, где α' — некоторая перестановка. (Удобно записывать a не в начале, а в конце цикла; это допустимо, поскольку буква a только одна.) Аналогично, если бы мы предположили, что α содержит букву b, то вывели бы, что $\alpha = (c\ d\ d\ b) \top \alpha''$, где α'' — некоторая перестановка. В общем случае эти рассуждения показывают, что *если есть какое-нибудь разложение $\alpha \top \beta = \pi$, где α содержит данную букву y, то существует единственный цикл вида*

$$(x_1\ \ldots\ x_n\ y), \qquad n \geq 0, \qquad x_1, \ldots, x_n \neq y, \qquad (14)$$

который является левым сомножителем в разложении перестановки α. Такой цикл легко отыскать, зная π и y; это самый короткий левый сомножитель в разложении перестановки π, содержащий букву y. Из сказанного следует теорема.

Теорема A. *Пусть элементы мультимножества M линейно упорядочены отношением "$<$". Каждая перестановка π мультимножества M имеет единственное представление в виде соединительного произведения*

$$\pi = (x_{11} \ldots x_{1n_1} y_1) \top (x_{21} \ldots x_{2n_2} y_2) \top \cdots \top (x_{t1} \ldots x_{tn_t} y_t), \quad t \geq 0, \qquad (15)$$

удовлетворяющее следующим двум условиям:

$$y_1 \leq y_2 \leq \cdots \leq y_t \qquad \text{и} \qquad y_i < x_{ij} \quad \text{при } 1 \leq j \leq n_i,\ 1 \leq i \leq t. \qquad (16)$$

(Иными словами, в каждом цикле последний элемент меньше любого другого и последние элементы циклов образуют неубывающую последовательность.)

Доказательство. При $\pi = \epsilon$ получим требуемое разложение, положив $t = 0$. В противном случае пусть y_1 — минимальный элемент в π; определим $(x_{11} \ldots x_{1n_1} y_1)$ — самый короткий левый сомножитель разложения π, содержащий y_1, как в рассмотренном примере. Теперь $\pi = (x_{11}\ \ldots\ x_{1n_1}\ y_1) \top \rho$, где ρ — некоторая перестановка; применив индукцию по длине перестановки, можем написать

$$\rho = (x_{21}\ \ldots\ x_{2n_2}\ y_2) \top \cdots \top (x_{t1}\ \ldots\ x_{tn_t}\ y_t), \quad t \geq 1,$$

где условия (16) выполнены. Тем самым доказано существование такого разложения.

Докажем единственность разложения (15), удовлетворяющего условиям (16). Ясно, что $t = 0$ тогда и только тогда, когда π — нуль-перестановка ϵ. При $t > 0$ из (16) следует, что y_1 — минимальный элемент перестановки и что $(x_{11} \ldots x_{1n_1}\, y_1)$ — самый короткий левый сомножитель, содержащий y_1. Поэтому $(x_{11} \ldots x_{1n_1}\, y_1)$ определяется однозначно; доказательство единственности такого представления завершается применением индукции и законов сокращения (7). ▌

Например, "каноническое" разложение перестановки (12), удовлетворяющее данным условиям, таково:

$$(d\ d\ b\ c\ d\ b\ b\ c\ a) \intercal (b\ a) \intercal (c\ d\ b) \intercal (d), \tag{17}$$

если $a < b < c < d$.

Важно отметить, что на самом деле в этом определении можно отбросить скобки и знаки операции $\intercal$ и это не приведет к неоднозначности! В конце каждого цикла появляется наименьший из оставшихся элементов. Таким образом, наше построение связывает с исходной перестановкой

$$\pi = d\ b\ c\ b\ c\ a\ c\ d\ a\ d\ d\ b\ b\ b\ d$$

перестановку

$$\pi' = d\ d\ b\ c\ d\ b\ b\ c\ a\ b\ a\ c\ d\ b\ d.$$

Если в двухстрочном представлении π содержится столбец вида $\substack{y\\x}$, где $x < y$, то в связанной с π' перестановке присутствует соответствующая пара соседних элементов $\ldots y\,x \ldots$. Так, в нашем примере π содержит три столбца вида $\substack{d\\b}$, трижды встречается пара $d\,b$. Вообще, из этого построения вытекает замечательная теорема.

Теорема B. *Пусть M — мультимножество. Существует взаимно однозначное соответствие между перестановками M, такое, что если π соответствует π', то выполняются следующие условия:*

a) *крайний слева элемент π' равен крайнему слева элементу π;*

b) *для всех пар участвующих в перестановке элементов (x, y), таких, что $x < y$, число вхождений столбца $\substack{y\\x}$ в двухстрочное представление перестановки π равно числу случаев, когда в перестановке π' элемент x следует непосредственно за y.* ▌

Если M — множество, то это, по существу, "нестандартное соответствие", которое обсуждалось в конце раздела 1.3.3, с незначительными изменениями. Более общий результат теоремы B полезен при подсчете числа перестановок специальных типов, поскольку часто проще решить задачу с ограничениями, наложенными на двухстрочное представление, чем эквивалентную задачу с ограничениями на пары соседних элементов.

П. А. Мак-Магон (P. A. MacMahon) рассмотрел задачи этого типа в своей выдающейся книге *Combinatory Analysis* **1** (Cambridge Univ. Press, 1915), 168–186. Он дал конструктивное доказательство теоремы B в частном случае, когда M содержит элементы лишь двух различных типов, скажем a и b; его построение для этого случая, по существу, совпадает с приведенным здесь, но представлено в совершенно ином виде. Для случая трех различных элементов a, b, c Мак-Магон дал сложное неконструктивное доказательство теоремы B; общий случай впервые доказал Фоата (Foata) [см. *Comptes Rendus Acad. Sci. Paris* **258** (1964), 1672–1675].

В качестве нетривиального примера применения теоремы B найдем число строк букв a, b, c, содержащих ровно

$$\begin{array}{ll} A & \text{вхождений буквы } a; \\ B & \text{вхождений буквы } b; \\ C & \text{вхождений буквы } c; \\ k & \text{вхождений пары стоящих рядом букв } ca; \\ l & \text{вхождений пары стоящих рядом букв } cb; \\ m & \text{вхождений пары стоящих рядом букв } ba. \end{array} \tag{18}$$

Из теоремы следует, что это то же самое, что найти число двухстрочных массивов вида

$$\begin{pmatrix} \overbrace{a\ \ \dots\ \ a}^{A}\ \ \overbrace{b\ \ \dots\ \ b}^{B}\ \ \overbrace{c\ \ \dots\ \ c}^{C} \\ \underbrace{\underbrace{\underbrace{\sqcup\ \ \dots\ \ \sqcup}_{A-k-m\,a\text{'s}}\ \ \underbrace{\sqcup\ \ \dots\ \ \sqcup}_{m\ a\text{'s}}}_{B-l\ b\text{'s}}\ \ \underbrace{\underbrace{\sqcup\ \ \dots\ \ \sqcup}_{k\ a\text{'s}}}_{l\ b\text{'s}}}_{Cc\text{'s}} \end{pmatrix} \tag{19}$$

Буквы a можно расположить во второй строке

$$\binom{A}{A-k-m}\binom{B}{m}\binom{C}{k} \qquad \text{способами;}$$

после этого буквы b можно разместить в оставшихся позициях

$$\binom{B+k}{B-l}\binom{C-k}{l} \qquad \text{способами.}$$

Остальные свободные места нужно заполнить буквами c; следовательно, искомое число равно

$$\binom{A}{A-k-m}\binom{B}{m}\binom{C}{k}\binom{B+k}{B-l}\binom{C-k}{l}. \tag{20}$$

Вернемся к вопросу о нахождении всех разложений данной перестановки. Существует ли такой объект, как "простая" перестановка, которая не разлагается на множители, отличные от нее самой и ϵ? Обсуждение, предшествующее теореме A, немедленно приводит к выводу о том, что *перестановка будет простой тогда и только тогда, когда она является циклом без повторяющихся элементов*. В случае, если перестановка является таким циклом, наше рассуждение доказывает, что не существует левых множителей, кроме ϵ и самого цикла. Если же перестановка содержит повторяющийся элемент y, то всегда можно выделить нетривиальный цикл в качестве левого сомножителя, в котором элемент y встречается всего лишь однажды.

Если перестановка непростая, то ее можно разлагать на все меньшие и меньшие части, пока не будет получено произведение простых перестановок. Можно даже показать, что такое разложение является единственным с точностью до порядка записи коммутирующих сомножителей.

Теорема С. *Каждую перестановку мультимножества можно записать в виде произведения*

$$\sigma_1 \top \sigma_2 \top \cdots \top \sigma_t, \qquad t \geq 0, \tag{21}$$

где σ_j — циклы, не содержащие повторяющихся элементов. Это представление единственное в том смысле, что два любых таких представления одной и той же перестановки можно преобразовать одно в другое, последовательно меняя местами соседние непересекающиеся циклы.

Термин "непересекающиеся циклы" относится к циклам, не имеющим общих элементов. В качестве примера можно проверить, что перестановка

$$\begin{pmatrix} a & a & b & b & c & c & d \\ b & a & a & c & d & b & c \end{pmatrix}$$

разлагается на множители ровно пятью способами:

$$\begin{aligned}(a\ b) \top (a) \top (c\ d) \top (b\ c) &= (a\ b) \top (c\ d) \top (a) \top (b\ c) \\ &= (a\ b) \top (c\ d) \top (b\ c) \top (a) \\ &= (c\ d) \top (a\ b) \top (b\ c) \top (a) \\ &= (c\ d) \top (a\ b) \top (a) \top (b\ c).\end{aligned} \tag{22}$$

Доказательство. Нужно установить, что выполняется сформулированное в теореме свойство единственности. Применим индукцию по длине перестановки; тогда достаточно доказать, что если ρ и σ — два различных цикла, не содержащих повторяющихся элементов, и

$$\rho \top \alpha = \sigma \top \beta,$$

то ρ и σ — непересекающиеся циклы и

$$\alpha = \sigma \top \theta, \qquad \beta = \rho \top \theta,$$

где θ — некоторая перестановка. Пусть y — произвольный элемент цикла ρ, тогда у любого левого сомножителя в разложении $\sigma \top \beta$, содержащего этот элемент y, будет левый сомножитель ρ. Значит, если ρ и σ имеют общий элемент, цикл σ должен быть кратен ρ; тогда $\sigma = \rho$ (так как они простые), что противоречит нашему предположению. Следовательно, цикл, содержащий y и не имеющий общих элементов с σ, должен быть левым сомножителем в разложении β. Применив законы сокращения (7), завершим доказательство. ▮

В качестве иллюстрации теоремы С рассмотрим перестановки мультимножества $M = \{A \cdot a,\ B \cdot b,\ C \cdot c\}$, состоящего из A элементов a, B элементов b и C элементов c. Пусть $N(A, B, C, m)$ — число перестановок мультимножества M, двухстрочное представление которых *не содержит* столбцов вида $\genfrac{}{}{0pt}{}{a}{a}$, $\genfrac{}{}{0pt}{}{b}{b}$, $\genfrac{}{}{0pt}{}{c}{c}$ и содержит ровно m столбцов вида $\genfrac{}{}{0pt}{}{a}{b}$. Отсюда следует, что имеется ровно $A - m$ столбцов вида $\genfrac{}{}{0pt}{}{a}{c}$, $B - m$ столбцов вида $\genfrac{}{}{0pt}{}{c}{b}$, $C - B + m$ столбцов вида $\genfrac{}{}{0pt}{}{c}{a}$, $C - A + m$ столбцов вида $\genfrac{}{}{0pt}{}{b}{c}$ и $A + B - C - m$ столбцов вида $\genfrac{}{}{0pt}{}{b}{a}$; следовательно,

$$N(A, B, C, m) = \binom{A}{m} \binom{B}{C - A + m} \binom{C}{B - m}. \tag{23}$$

Теорема C предлагает другой способ подсчета этих перестановок: коль скоро столбцы $\begin{smallmatrix}a\\a\end{smallmatrix}$, $\begin{smallmatrix}b\\b\end{smallmatrix}$, $\begin{smallmatrix}c\\c\end{smallmatrix}$ исключены, в разложении перестановки единственно возможны такие простые множители:

$$(a\ b),\qquad (a\ c),\qquad (b\ c),\qquad (a\ b\ c),\qquad (a\ c\ b). \tag{24}$$

Каждая пара этих циклов имеет хотя бы одну общую букву, значит, разложение единственно. Если цикл $(a\ b\ c)$ встречается в разложении k раз, то из нашего предыдущего предположения следует, что $(a\ b)$ встречается $m-k$ раз, $(b\ c)$ встречается $C-A+m-k$ раз, $(a\ c)$ встречается $C-B+m-k$ раз и $(a\ c\ b)$ встречается $A+B-C-2m+k$ раз. Следовательно, $N(A,B,C,m)$ равно числу перестановок этих циклов (полиномиальному коэффициенту), просуммированному по всем значениям k:

$$\begin{aligned} &N(A,B,C,m)\\ &\quad=\sum_k \frac{(C+m-k)!}{(m-k)!\,(C-A+m-k)!\,(C-B+m-k)!\,k!\,(A+B-C-2m+k)!}\\ &\quad=\sum_k \binom{m}{k}\binom{A}{m}\binom{A-m}{C-B+m-k}\binom{C+m-k}{A}. \end{aligned} \tag{25}$$

Сравнивая (25) с (23), обнаруживаем, что должно выполняться тождество

$$\sum_k \binom{m}{k}\binom{A-m}{C-B+m-k}\binom{C+m-k}{A} = \binom{B}{C-A+m}\binom{C}{B-m}. \tag{26}$$

Оказывается, с этим тождеством мы встречались в упр. 1.2.6–31:

$$\sum_j \binom{M-R+S}{j}\binom{N+R-S}{N-j}\binom{R+j}{M+N} = \binom{R}{M}\binom{S}{N}, \tag{27}$$

где $M=A+B-C-m$, $N=C-B+m$, $R=B$, $S=C$, а $j=C-B+m-k$.

Аналогично можно подсчитать число перестановок мультимножества $\{A\cdot a, B\cdot b, C\cdot c, D\cdot d\}$, если количество столбцов различных типов в них задано следующим образом.

Тип столбца:	$\begin{smallmatrix}a\\d\end{smallmatrix}$	$\begin{smallmatrix}a\\b\end{smallmatrix}$	$\begin{smallmatrix}b\\a\end{smallmatrix}$	$\begin{smallmatrix}b\\c\end{smallmatrix}$	$\begin{smallmatrix}c\\b\end{smallmatrix}$	$\begin{smallmatrix}c\\d\end{smallmatrix}$	$\begin{smallmatrix}d\\a\end{smallmatrix}$	$\begin{smallmatrix}d\\c\end{smallmatrix}$	(28)
Частота:	r	$A-r$	q	$B-q$	$B-A+r$	$D-r$	$A-q$	$D-A+q$	

(Здесь $A+C=B+D$.) Возможными циклами в разложении такой перестановки на простые множители будут

Цикл:	$(a\ b)$	$(b\ c)$	$(c\ d)$	$(d\ a)$	$(a\ b\ c\ d)$	$(d\ c\ b\ a)$	(29)
Частота:	$A-r-s$	$B-q-s$	$D-r-s$	$A-q-s$	s	$q-A+r+s$	

при некотором s (см. упр. 12). В этом случае циклы $(a\ b)$ и $(c\ d)$ заменяют друг друга так же, как циклы $(b\ c)$ и $(d\ a)$, поэтому необходимо подсчитать число различных разложений на простые множители. Оказывается (см. упр. 10), всегда существует единственное разложение, такое, что цикл $(a\ b)$ никогда не следует непосредственно за $(c\ d)$, а $(b\ c)$ не встречается сразу после $(d\ a)$. Отсюда, используя результат упр. 13, получаем тождество

$$\sum_{s,t}\binom{B}{t}\binom{A-q-s}{A-r-s-t}\binom{B+D-r-s-t}{B-q-s}$$
$$\times\frac{D!}{(D-r-s)!\,(A-q-s)!\,s!\,(q-A+r+s)!}$$
$$=\binom{A}{r}\binom{B+D-A}{D-r}\binom{B}{q}\binom{D}{A-q}.$$

Вынося из обеих частей множитель $\binom{D}{A-q}$ и несколько упрощая факториалы, приходим к сложному на вид пятипараметрическому тождеству биномиальных коэффициентов:

$$\sum_{s,t}\binom{B}{t}\binom{A-r-t}{s}\binom{B+D-r-s-t}{D+q-r-t}\binom{D-A+q}{D-r-s}\binom{A-q}{r+t-q}$$
$$=\binom{A}{r}\binom{B+D-A}{D-r}\binom{B}{q}. \qquad (30)$$

Используя тождество (27), можно выполнить суммирование по s, а затем легко вычислить получившуюся сумму по t. Таким образом, выполнив всю работу, мы не смогли обнаружить какое-либо тождество, которое мы бы еще не умели выводить. Но мы, по крайней мере, научились подсчитывать число перестановок определенного вида двумя различными способами, а эти методы подсчета — хорошая подготовка к решению задач, которые еще ждут нас впереди.

УПРАЖНЕНИЯ

1. [*M05*] *Да или нет?* Пусть M_1 и M_2 — мультимножества. Если α — перестановка M_1, а β — перестановка M_2, то $\alpha \top \beta$ — перестановка $M_1 \cup M_2$.

2. [*10*] Соединительное произведение перестановок $c\ a\ d\ a\ b$ и $b\ d\ d\ a\ d$ представлено в (5); найдите соединительное произведение $b\ d\ d\ a\ d\ \top\ c\ a\ d\ a\ b$, которое получается, если сомножители поменять местами.

3. [*M13*] Верно ли утверждение, обратное (9)? Иначе говоря, если перестановки α и β коммутативны относительно операции соединительного произведения, то следует ли из этого, что они не содержат общих букв?

4. [*M11*] Каноническое разложение перестановки (12) в соответствии с теоремой A при $a < b < c < d$ задается формулой (17). Найдите каноническое разложение в случае, когда $d < c < b < a$.

5. [*M23*] В условии (b) теоремы B требуется, чтобы x было меньше y. Что будет, если ослабить это требование, заменив его требованием $x \le y$?

6. [*M15*] Сколько существует цепочек, состоящих ровно из m букв a и n букв b, таких, что ровно k букв b стоят непосредственно перед буквами a и нет никаких других букв, кроме a и b?

7. [*M21*] Сколько строк из букв a, b, c, удовлетворяющих условиям (18), начинаются с буквы a, с буквы b, с буквы c?

▶ **8.** [*20*] Найдите все разложения перестановки (12) на два множителя $\alpha \top \beta$.

9. [*33*] Напишите программы, которые формировали бы разложения заданной перестановки мультимножества, описанные в теоремах A и C.

▶ **10.** [*M30*] *Да или нет?* Согласно теореме C разложение на простые множители не вполне однозначно, тем не менее можно следующим образом обеспечить единственность. "Существует линейное упорядочение $\prec$ на множестве простых перестановок, такое, что каждая перестановка мультимножества имеет единственное разложение $\sigma_1 \intercal \sigma_2 \intercal \cdots \intercal \sigma_n$ на простые множители, удовлетворяющее условию $\sigma_i \preceq \sigma_{i+1}$, если σ_i коммутирует с σ_{i+1} при $1 \le i < n$".

▶ **11.** [*M26*] Пусть $\sigma_1, \sigma_2, \ldots, \sigma_t$ — циклы без повторяющихся элементов. Определим частичное упорядочение $\prec$ на множестве t элементов $\{x_1, \ldots, x_t\}$, полагая $x_i \prec x_j$, если $i < j$ и σ_i имеет, по крайней мере, одну общую букву с σ_j. Докажите следующую связь между теоремой C и понятием "топологическая сортировка" (раздел 2.2.3): *число различных разложений перестановки $\sigma_1 \intercal \sigma_2 \intercal \cdots \intercal \sigma_t$ на простые множители равно количеству способов топологической сортировки данного частичного упорядочения*. (Например, в соответствии с (22) существует пять способов топологической сортировки упорядочения $x_1 \prec x_2$, $x_3 \prec x_4$, $x_1 \prec x_4$.) Обратно, если на множестве из t элементов задано какое-либо частичное упорядочение, то существует множество циклов $\{\sigma_1, \sigma_2, \ldots, \sigma_t\}$, которое определяет это частичное упорядочение указанным способом.

12. [*M16*] Покажите, что (29) есть следствие, вытекающее из предположения (28).

13. [*M21*] Докажите, что число перестановок мультимножества

$$\{A \cdot a,\, B \cdot b,\, C \cdot c,\, D \cdot d,\, E \cdot e,\, F \cdot f\},$$

не содержащих пар стоящих рядом букв *ca* и *db*, равно

$$\sum_t \binom{D}{A-t}\binom{A+B+E+F}{t}\binom{A+B+C+E+F-t}{B}\binom{C+D+E+F}{C, D, E, F}.$$

14. [*M30*] Один из способов определить перестановку π^-, обратную перестановке π, который подсказан нам в других определениях этого раздела, — поменять местами строки двухстрочного представления π и так выполнить устойчивую сортировку столбцов, чтобы элементы верхней строки расположились в порядке неубывания. Например, если $a < b < c < d$, то из этого определения следует, что обратной перестановкой к $c\ a\ b\ d\ d\ a\ b\ d\ a\ d$ будет $a\ c\ d\ a\ d\ a\ b\ b\ d\ d$.

Исследуйте свойства этой операции обращения; имеется ли, например, какая-нибудь простая связь между данной операцией и соединительным произведением? Можно ли подсчитать число перестановок, таких, что $\pi = \pi^-$?

▶ **15.** [*M25*] Докажите, что перестановка $a_1 \ldots a_n$ мультимножества

$$\{n_1 \cdot x_1,\, n_2 \cdot x_2, \ldots, n_m \cdot x_m\},$$

где $x_1 < x_2 < \cdots < x_m$ и $n_1 + n_2 + \cdots + n_m = m$, является циклом тогда и только тогда, когда ориентированный граф с вершинами $\{x_1, x_2, \ldots, x_m\}$ и дугами из x_j в $a_{n_1+\cdots+n_j}$ содержит ровно один ориентированный цикл. В таком случае число способов представления перестановки в виде цикла равно длине этого ориентированного цикла. Например, ориентированным графом, соответствующим перестановке

$$\begin{pmatrix} a & a & a & b & b & c & c & c & d & d \\ d & c & b & a & c & a & a & b & d & c \end{pmatrix}, \qquad \text{будет} \qquad \begin{tikzcd} a \arrow[r] & b \arrow[d, bend left] \\ d \arrow[r] & c \arrow[u, bend left] \end{tikzcd},$$

а два способа представления перестановки в виде цикла имеют вид $(b\ a\ d\ d\ c\ a\ c\ a\ b\ c)$ и $(c\ a\ d\ d\ c\ a\ c\ b\ a\ b)$.

16. [*M35*] В предыдущем разделе, формула 5.1.1–(8), мы нашли производящую функцию для *инверсий* перестановок в частном случае, когда в перестановке участвуют элементы множества. Покажите, что в общем случае перестановок *мультимножества* производящая функция для инверсий $\{n_1 \cdot x_1, n_2 \cdot x_2, \dots\}$ равна "z-полиномиальному коэффициенту"

$$\binom{n}{n_1, n_2, \dots}_z = \frac{n!_z}{n_1!_z\, n_2!_z \dots}, \qquad \text{где} \quad m!_z = \prod_{k=1}^{m} (1 + z + \dots + z^{k-1}).$$

[Ср. с (3) и с определением z-номиальных коэффициентов в формуле 1.2.6–(40).]

17. [*M24*] С помощью производящей функции, найденной в упр. 16, вычислите среднее значение и дисперсию для числа инверсий в случайной перестановке мультимножества.

18. [*M30*] (П. А. Мак-Магон.) *Индекс* перестановки $a_1\, a_2 \dots a_n$ был определен в предыдущем упражнении; мы доказали, что число перестановок этого множества, имеющих данный индекс k, равно числу перестановок, имеющих k инверсий. Верно ли это для перестановок заданного мультимножества?

19. [*HM28*] Определим *функцию Мёбиуса* $\mu(\pi)$ перестановки π: она равна O, если π содержит повторяющиеся элементы, и $(-1)^k$ в противном случае, если π — произведение k простых перестановок. (Ср. с определением обычной функции Мёбиуса; упр. 4.5.2–10.)

a) Докажите, что если $\pi \neq \epsilon$, то

$$\sum \mu(\lambda) = 0,$$

где сумма берется по всем перестановкам λ, являющимся левыми сомножителями в разложении π (т. е. по всем λ, таким, что $\pi = \lambda \intercal \rho$, где ρ — некоторая перестановка).

b) Докажите, что если $x_1 < x_2 < \dots < x_m$ и $\pi = x_{j_1}\, x_{j_2} \dots x_{j_n}$, где $1 \le j_k \le m$ при $1 \le k \le n$, то

$$\mu(\pi) = (-1)^n \epsilon(i_1\, i_2 \dots i_n), \qquad \text{где} \quad \epsilon(i_1\, i_2 \dots i_n) = \operatorname{sign} \prod_{1 \le j < k \le n} (i_k - i_j).$$

▸ **20.** [*HM33*] (Д. Фоата.) Пусть (a_{ij}) — произвольная матрица действительных чисел. Пользуясь обозначениями из упр. 19, (b), определим $\nu(\pi) = a_{i_1 j_1} \dots a_{i_n j_n}$, где двухстрочное представление перестановки π таково:

$$\begin{pmatrix} x_{i_1} & x_{i_2} & \dots & x_{i_n} \\ x_{j_1} & x_{j_2} & \dots & x_{j_n} \end{pmatrix}.$$

Эта функция полезна при вычислении производящих функций для перестановок мультимножества, потому что $\sum \nu(\pi)$, где сумма берется по всем перестановкам π мультимножества

$$\{n_1 \cdot x_1, \dots, n_m \cdot x_m\},$$

будет производящей функцией для числа перестановок, удовлетворяющих некоторым ограничениям. Например, если положить $a_{ij} = z$ при $i = j$ и $a_{ij} = 1$ при $i \neq j$, то $\sum \nu(\pi)$ — производящая функция для числа "неподвижных точек" (столбцов, в которых верхний и нижний элементы равны). Чтобы можно было исследовать $\sum \nu(\pi)$ для всех мультимножеств одновременно, рассмотрим функцию

$$G = \sum \pi \nu(\pi),$$

где сумма берется по всем π из множества $\{x_1, \dots, x_m\}^*$ всех перестановок мультимножеств, содержащих элементы $x_1, \dots, x_m$, и посмотрим на коэффициенты при $x_1^{n_1} \dots x_m^{n_m}$ в G.

В этой формуле для G будем рассматривать π как произведение переменных x. Например, при $m = 2$ имеем

$$G = 1+x_1\nu(x_1)+x_2\nu(x_2)+x_1x_1\nu(x_1x_1)+x_1x_2\nu(x_1x_2)+x_2x_1\nu(x_2x_1)+x_2x_2\nu(x_2x_2)+\cdots$$
$$= 1+x_1a_{11}+x_2a_{22}+x_1^2a_{11}^2+x_1x_2a_{11}a_{22}+x_1x_2a_{21}a_{12}+x_2^2a_{22}^2+\cdots.$$

Таким образом, коэффициент при $x_1^{n_1}\ldots x_m^{n_m}$ в G равен сумме $\sum\nu(\pi)$ по всем перестановкам π мультимножества $\{n_1\cdot x_1,\ldots,n_m\cdot x_m\}$. Нетрудно видеть, что этот коэффициент равен также коэффициенту при $x_1^{n_1}\ldots x_m^{n_m}$ в выражении

$$(a_{11}x_1+\cdots+a_{1m}x_m)^{n_1}(a_{21}x_1+\cdots+a_{2m}x_m)^{n_2}\ldots(a_{m1}x_1+\cdots+a_{mm}x_m)^{n_m}.$$

Цель данного упражнения — доказать формулу

$$G = 1/D, \quad \text{где} \quad D = \det\begin{pmatrix} 1-a_{11}x_1 & -a_{12}x_2 & \ldots & -a_{1m}x_m \\ -a_{21}x_1 & 1-a_{22}x_2 & & -a_{2m}x_m \\ \vdots & & & \vdots \\ -a_{m1}x_1 & -a_{m2}x_2 & \ldots & 1-a_{mm}x_m \end{pmatrix},$$

которую П. А. Мак-Магон (P. A. MacMahon) в своей книге *Combinatory Analysis* **1** (1915), разд. 3, назвал "основной теоремой". Например, если $a_{ij} = 1$ при всех i и j, то эта формула дает

$$G = 1/(1-(x_1+x_2+\cdots+x_m))$$

и коэффициент при $x_1^{n_1}\ldots x_m^{n_m}$ оказывается равным $(n_1+\cdots+n_m)!/n_1!\ldots n_m!$, как и должно быть. Для доказательства основной теоремы Мак-Магона покажите, что

a) $\nu(\pi \mathbin{\top} \rho) = \nu(\pi)\nu(\rho)$;

b) в обозначениях из упр. 19 $D = \sum \pi\mu(\pi)\nu(\pi)$, где сумма берется по всем перестановкам π из множества $\{x_1,\ldots,x_m\}^*$;

c) из (a) и (b) следует $D\cdot G = 1$.

21. [*M21*] Пусть заданы n_1, …, n_m и $d \ge 0$. Сколько перестановок $a_1\,a_2\ldots a_n$ мультимножества $\{n_1\cdot 1,\ldots,n_m\cdot m\}$ удовлетворяют условию $a_{j+1} \ge a_j - d$ при $1 \le j < n = n_1+\cdots+n_m$?

22. [*M30*] Пусть $P(x_1^{n_1}\ldots x_m^{n_m})$ означает множество всех возможных перестановок мультимножества $\{n_1\cdot x_1,\ldots,n_m\cdot x_m\}$ и пусть $P_0(x_0^{n_0}x_1^{n_1}\ldots x_m^{n_m})$ — подмножество $P(x_0^{n_0}x_1^{n_1}\ldots x_m^{n_m})$, в котором первые n_0 элементов не равны x_0.

a) Задав число t, $1 \le t < m$, найдите однозначное соответствие между $P(1^{n_1}\ldots m^{n_m})$ и множеством всех упорядоченных пар перестановок, которые соответственно принадлежат $P_0(0^k1^{n_1}\ldots t^{n_t})$ и $P_0(0^k(t+1)^{n_{t+1}}\ldots m^{n_m})$, для некоторого $k \ge 0$. [*Указание.* Для каждого $\pi = a_1\ldots a_n \in P(1^{n_1}\ldots m^{n_m})$ положите, что $l(\pi)$ — перестановка, полученная путем замены $t+1$, …, m значением 0 и удаления всех 0 на последних $n_{t+1}+\cdots+n_m$ позициях; аналогично положите, что $r(\pi)$ — перестановка, полученная путем замены 1, …, t значением 0 и удаления всех 0 на первых $n_1+\cdots+n_t$ позициях.]

b) Докажите, что число перестановок $P_0(0^{n_0}1^{n_1}\ldots m^{n_m})$, имеющих в двухстрочном представлении p_j столбцов $\genfrac{}{}{0pt}{}{0}{j}$ и q_j столбцов $\genfrac{}{}{0pt}{}{j}{0}$, равно

$$\frac{|P(x_1^{p_1}\ldots x_m^{p_m}y_1^{n_1-p_1}\ldots y_m^{n_m-p_m})|\,|P(x_1^{q_1}\ldots x_m^{q_m}y_1^{n_1-q_1}\ldots y_m^{n_m-q_m})|}{|P_0(0^{n_0}1^{n_1}\ldots m^{n_m})|}.$$

c) Пусть w_1, …, w_m, z_1, …, z_m — комплексные числа на единичной окружности. Определите вес $w(\pi)$ перестановки $\pi \in P(1^{n_1}\ldots m^{n_m})$ как произведение весов ее столбцов в двухстрочном представлении, где вес столбца $\genfrac{}{}{0pt}{}{j}{k}$ равен w_j/w_k, если j и k

оба $\le t$ или оба $> t$, в противном случае вес равен z_j/z_k. Докажите, что сумма $w(\pi)$ по всем $\pi \in P(1^{n_1} \ldots m^{n_m})$ равна

$$\sum_{k\ge 0} \frac{k!^2 (n_{\le t} - k)!\,(n_{>t} - k)!}{n_1! \ldots n_m!} \left| \sum \binom{n_1}{p_1} \ldots \binom{n_m}{p_m} \left(\frac{w_1}{z_1}\right)^{p_1} \ldots \left(\frac{w_m}{z_m}\right)^{p_m} \right|^2,$$

где $n_{\le t}$ означает $n_1 + \cdots + n_t$, $n_{>t}$ означает $n_{t+1} + \cdots + n_m$ и внутреннее суммирование выполняется по всем $(p_1, \ldots, p_m)$, таким, что $p_{\le t} = p_{>t} = k$.

23. [*M23*] Цепочку ДНК можно рассматривать как слово четырехбуквенного алфавита. Предположим, мы скопировали цепочку ДНК и полностью разложили ее на однобуквенные составляющие, а затем случайным образом их вновь объединили. Докажите, что, если поместить полученную таким образом цепочку вслед за исходной, число позиций, в которых эти две цепочки будут отличаться, с большей вероятностью будет четным, чем нечетным. [*Указание.* Примените к этому случаю результат предыдущего упражнения.]

24. [*27*] Рассмотрим некоторое отношение R, которое может существовать между двумя неупорядоченными парами букв; если $\{w, x\}R\{y, z\}$, мы говорим, что $\{w, x\}$ *сохраняет* $\{y, z\}$, в противном случае $\{w, x\}$ *перемещает* $\{y, z\}$.

Операция *транспозиции* $\substack{w\ x\\ y\ z}$ применительно к R меняет $\substack{w\ x\\ y\ z}\ \substack{x\ w\\ y\ z}$ или $\substack{x\ w\\ z\ y}$ в зависимости от того, сохраняет или перемещает пара $\{w, x\}$ пару $\{y, z\}$, полагая, что $w \ne x$ и $y \ne z$; если $w = x$ или $y = z$, то транспозиция всегда формирует $\substack{x\ w\\ z\ y}$.

Операция *сортировки* двухстрочного массива $\binom{x_1\ \cdots\ x_n}{y_1\ \cdots\ y_n}$ применительно к R находит наибольшее x_j, такое, что $x_j > x_{j+1}$, и транспонирует (взаимно переставляет) столбцы j и $j + 1$ до тех пор, пока не установится $x_1 \le \cdots \le x_n$. (Мы не ставим условия, чтобы $y_1 \ldots y_n$ представляло собой перестановку $x_1 \ldots x_n$.)

a) Для данного $\binom{x_1\ \cdots\ x_n}{y_1\ \cdots\ y_n}$ докажите, что для каждого $x \in \{x_1, \ldots, x_n\}$ существует единственное $y \in \{y_1, \ldots, y_n\}$, такое, что $\operatorname{sort}\binom{x_1\ \cdots\ x_n}{y_1\ \cdots\ y_n} = \operatorname{sort}\binom{x\ x'_2\ \cdots\ x'_n}{y\ y'_2\ \cdots\ y'_n}$ для некоторых $x'_2, y'_2, \ldots, x'_n, y'_n$.

b) Обозначим через $\binom{w_1\ \cdots\ w_k}{y_1\ \cdots\ y_k} Ⓡ \binom{x_1\ \cdots\ x_l}{z_1\ \cdots\ z_l}$ результат сортировки $\binom{w_1\ \cdots\ w_k\ \ x_1\ \cdots\ x_l}{y_1\ \cdots\ y_k\ \ z_1\ \cdots\ z_l}$ применительно к R. Например, если R всегда истинно, Ⓡ является просто сопоставлением, если R всегда ложно, Ⓡ представляет собой включающее произведение $\intercal$. Обобщите теорему A — докажите, что любая перестановка π мультимножества M имеет единственное представление вида

$$\pi = (x_{11} \ldots x_{1n_1}\, y_1) Ⓡ \big((x_{21} \ldots x_{2n_2}\, y_2) Ⓡ \cdots Ⓡ (x_{t1} \ldots x_{tn_t}\, y_t)\big),$$

удовлетворяющее (16), если переопределить цикл таким образом: в (11) вместо $(x_1\, x_2 \ldots x_n)$ подставить $(x_2 \ldots x_n\, x_1)$. Например, пусть $\{w, x\}R\{y, z\}$ означает, что w, x, y и z различны. Из этого, в свою очередь, следует, что разложение выражения (12) по аналогии с выражением (17) есть

$$(d\,d\,b\,c\,a) Ⓡ \big((c\,b\,b\,a) Ⓡ \big((c\,d\,b) Ⓡ \big((d\,b) Ⓡ (d)\big)\big)\big).$$

(Операция Ⓡ отнюдь не всегда следует закону ассоциативности; скобки в обобщенном разложении следует раскрывать справа налево.)

*5.1.3. Серии

В главе 3 была проанализирована длина неубывающих серий в перестановке и показано, что этот параметр позволяет проверить случайность последовательности. Если поместить вертикальные черточки до и после перестановки $a_1\, a_2 \ldots a_n$, а также между a_j и a_{j+1}, когда $a_j > a_{j+1}$, то *сериями* будут называться серии, ограниченные парами черточек. Например, в перестановке

$$| \, 3 \;\; 5 \;\; 7 \, | \, 1 \;\; 6 \;\; 8 \;\; 9 \, | \, 4 \, | \, 2 \, |$$

имеется четыре серии. В разделе 3.3.2G были найдены среднее число серий длины k в случайной перестановке множества $\{1, 2, \ldots, n\}$ и ковариация числа серий длины j и длины k. Серии важны при изучении алгоритмов сортировки, так как они представляют упорядоченные серии данных. Поэтому-то мы теперь вновь вернемся к вопросу о сериях.

Обозначим через

$$\left\langle {n \atop k} \right\rangle \tag{1}$$

число перестановок множества $\{1, 2, \ldots, n\}$, имеющих ровно k нисходящих серий $a_j > a_{j+1}$ и $k + 1$ восходящих серий. Такие числа $\left\langle {n \atop k} \right\rangle$ возникают и в других контекстах; их обычно называют *числами Эйлера*, потому что Эйлер проанализировал их в своей знаменитой книге *Institutiones Calculi Differentialis* (St. Petersburg: 1755, 485–487) после того, как впервые использовал несколькими годами ранее [*Comment. Acad. Sci. Imp. Petrop.* **8** (1736), 147–158, §13]; их следует отличать от *чисел Эйлера* E_n, о которых идет речь в упр. 5.1.4–23. Угловые скобки в $\left\langle {n \atop k} \right\rangle$ напоминают символ “>”, который присутствует в определении убывания. Конечно, $\left\langle {n \atop k} \right\rangle$ также равно числу перестановок, в которых имеется k возрастаний $a_j < a_{j+1}$.

Из любой данной перестановки множества $\{1, \ldots, n - 1\}$ можно образовать n новых перестановок, вставляя элемент n во все возможные места. Если в исходной перестановке содержалось k нисходящих серий, то ровно $k + 1$ новых перестановок будут иметь k нисходящих серий; в остальных $n - 1 - k$ перестановках будет по $k + 1$ серий, поскольку всякий раз, когда n вставляется не в конец существующей серии, число нисходящих серий увеличивается на единицу. Например, из перестановки 3 1 2 4 5 можно получить шесть перестановок

$$\begin{array}{ccc} 6\,3\,1\,2\,4\,5, & 3\,6\,1\,2\,4\,5, & 3\,1\,6\,2\,4\,5, \\ 3\,1\,2\,6\,4\,5, & 3\,1\,2\,4\,6\,5, & 3\,1\,2\,4\,5\,6. \end{array}$$

Все эти перестановки, кроме второй и последней, содержат по две нисходящие серии вместо одной исходной. Отсюда имеем рекуррентное соотношение

$$\left\langle {n \atop k} \right\rangle = (k+1) \left\langle {n-1 \atop k} \right\rangle + (n-k) \left\langle {n-1 \atop k-1} \right\rangle, \tag{2}$$

где целое $n > 0$ и k также целое.

Условимся, что

$$\left\langle {0 \atop k} \right\rangle = \delta_{k0}\,, \tag{3}$$

т. е. будем считать, что в нуль-перестановке (пустой перестановке) не содержатся нисходящие серии. Читатель, возможно, найдет небезынтересным сравнение (2) с рекуррентным соотношением для чисел Стирлинга [формулы 1.2.6–(46)]. В табл. 1 приведены числа Эйлера для малых n.

В табл. 1 можно заметить некоторые закономерности. По определению имеем

$$\left\langle {n \atop 0} \right\rangle + \left\langle {n \atop 1} \right\rangle + \cdots + \left\langle {n \atop n} \right\rangle = n!\,; \tag{4}$$

$$\left\langle {n \atop 0} \right\rangle = 1\,; \tag{5}$$

Таблица 1

ЧИСЛА ЭЙЛЕРА

n	$\left\langle{n \atop 0}\right\rangle$	$\left\langle{n \atop 1}\right\rangle$	$\left\langle{n \atop 2}\right\rangle$	$\left\langle{n \atop 3}\right\rangle$	$\left\langle{n \atop 4}\right\rangle$	$\left\langle{n \atop 5}\right\rangle$	$\left\langle{n \atop 6}\right\rangle$	$\left\langle{n \atop 7}\right\rangle$	$\left\langle{n \atop 8}\right\rangle$
0	1	0	0	0	0	0	0	0	0
1	1	0	0	0	0	0	0	0	0
2	1	1	0	0	0	0	0	0	0
3	1	4	1	0	0	0	0	0	0
4	1	11	11	1	0	0	0	0	0
5	1	26	66	26	1	0	0	0	0
6	1	57	302	302	57	1	0	0	0
7	1	120	1191	2416	1191	120	1	0	0
8	1	247	4293	15619	15619	4293	247	1	0
9	1	502	14608	88234	156190	88234	14608	502	1

$$\left\langle{n \atop n-1}\right\rangle = 1\,, \qquad \left\langle{n \atop n}\right\rangle = 0\,, \qquad \text{где } n \geq 1. \tag{6}$$

Соотношение (6) следует из (5) вследствие свойства симметрии

$$\left\langle{n \atop k}\right\rangle = \left\langle{n \atop n-1-k}\right\rangle, \qquad \text{где } n \geq 1, \tag{7}$$

которое вытекает из того факта, что каждая непустая перестановка $a_1\, a_2\, \ldots\, a_n$, содержащая k нисходящих серий, имеет и $n-1-k$ восходящих серий.

Другое важное свойство чисел Эйлера выражается формулой

$$\sum_k \left\langle{n \atop k}\right\rangle \binom{m+k}{n} = m^n\,, \qquad n \geq 0\,, \tag{8}$$

которая была впервые выведена китайским математиком Ли Шан-Ланом и опубликована в 1867 году. [См. J.-C. Martzloff, *A History of Chinese Mathematics* (Berlin: Springer, 1997, 346–348); особый случай, если $n \leq 5$, был независимо рассмотрен японским математиком Йошисуке Мацунага (Matsunaga Yohisuke), который умер в 1744 году.] Тождество Ли Шан-Лана следует из свойств операции сортировки. Рассмотрим m^n последовательностей $a_1\, a_2 \ldots a_n$, где $1 \leq a_i \leq m$. Любую такую последовательность можно устойчиво рассортировать в порядке неубывания и получить:

$$a_{i_1} \leq a_{i_2} \leq \cdots \leq a_{i_n}\,, \tag{9}$$

где $i_1\, i_2 \ldots i_n$ — однозначно определенная перестановка множества $\{1, 2, \ldots, n\}$, такая, что $i_j < i_{j+1}$, если $a_{i_j} = a_{i_{j+1}}$; другими словами, из $i_j > i_{j+1}$ следует $a_{i_j} < a_{i_{j+1}}$. Покажем, что если в перестановке $i_1\, i_2 \ldots i_n$ содержится k серий, то число соответствующих ей последовательностей $a_1\, a_2 \ldots a_n$ равно $\binom{m+n-k}{n}$; тем самым будет доказана формула (8), если заменить k значением $n-k$ и воспользоваться (7), поскольку $\left\langle{n \atop k}\right\rangle$ перестановок имеют $n-k$ серий.

Пусть, например, $n = 9$, $i_1\, i_2 \ldots i_n = 3\,5\,7\,1\,6\,8\,9\,4\,2$ и требуется подсчитать число последовательностей $a_1\, a_2 \ldots a_n$, таких, что

$$1 \leq a_3 \leq a_5 \leq a_7 < a_1 \leq a_6 \leq a_8 \leq a_9 < a_4 < a_2 \leq m\,. \tag{10}$$

Оно равно числу последовательностей $b_1\,b_2\ldots b_9$, таких, что

$$1 \le b_1 < b_2 < b_3 < b_4 < b_5 < b_6 < b_7 < b_8 < b_9 \le m+5\,,$$

поскольку можно положить $b_1 = a_3$, $b_2 = a_5 + 1$, $b_3 = a_7 + 2$, $b_4 = a_1 + 2$, $b_5 = a_6 + 3$ и т. д. Число способов, которыми можно выбрать элементы b, равно просто-напросто числу способов выбора 9 предметов из $m+5$, т. е. $\binom{m+5}{9}$; аналогичное доказательство годится для произвольных n и k и любой перестановки $i_1\,i_2\ldots i_n$ с k сериями.

Так как в обеих частях равенства (8) стоят полиномы от m, вместо m можно подставить любое действительное число, получив интересное выражение степеней через последовательные биномиальные коэффициенты:

$$x^n = \left\langle {n \atop 0} \right\rangle \binom{x}{n} + \left\langle {n \atop 1} \right\rangle \binom{x+1}{n} + \cdots + \left\langle {n \atop n-1} \right\rangle \binom{x+n-1}{n}, \quad n \ge 1. \tag{11}$$

Например,

$$x^3 = \binom{x}{3} + 4\binom{x+1}{3} + \binom{x+2}{3}.$$

В основном, благодаря именно этому свойству числа Эйлера весьма широко применяются в дискретной математике. Положив в (11) $x = 1$, докажем еще раз, что $\left\langle {n \atop n-1} \right\rangle = 1$, поскольку биномиальные коэффициенты обращаются в 0 во всех слагаемых, кроме последнего. Положив $x = 2$, получим

$$\left\langle {n \atop n-2} \right\rangle = \left\langle {n \atop 1} \right\rangle = 2^n - n - 1\,, \qquad n \ge 1. \tag{12}$$

Подставив $x = 3$, 4, $\ldots$, убедимся, что все числа $\left\langle {n \atop k} \right\rangle$ полностью определяются соотношением (11), и придем к формуле, впервые найденной Эйлером:

$$\begin{aligned}\left\langle {n \atop k} \right\rangle &= (k+1)^n - k^n\binom{n+1}{1} + (k-1)^n\binom{n+1}{2} - \cdots + (-1)^k 1^n \binom{n+1}{k}\\ &= \sum_{j=0}^{k} (-1)^j \binom{n+1}{j} (k+1-j)^n, \qquad n \ge 0,\ k \ge 0.\end{aligned} \tag{13}$$

Рассмотрим теперь производящую функцию для серий. Если положить

$$g_n(z) = \sum_k \left\langle {n \atop k-1} \right\rangle \frac{z^k}{n!}\,, \tag{14}$$

то коэффициент при z^k будет равен вероятности того, что случайная перестановка множества $\{1, 2, \ldots, n\}$ содержит ровно k серий. Поскольку k серий в перестановке столь же вероятны, как и $n+1-k$, среднее число серий должно равняться $\frac{1}{2}(n+1)$ и, следовательно, $g_n'(1) = \frac{1}{2}(n+1)$. В упр. 2, (b) показано, что имеет место простая формула для *всех* производных функции $g_n(z)$ в точке $z = 1$:

$$g_n^{(m)}(1) = \left\{ {n+1 \atop n+1-m} \right\} \Big/ \binom{n}{m}, \qquad n \ge m. \tag{15}$$

Так, в частности, дисперсия $g_n''(1) + g_n'(1) - g_n'(1)^2$ равна $(n+1)/12$ при $n \ge 2$, что указывает на довольно устойчивое распределение около среднего значения. (Эта же величина была найдена в упр. 3.3.2–(18); в нем она называлась $\operatorname{covar}(R_1', R_1')$.)

Функция $g_n(z)$ — полином, поэтому с помощью формулы (15) и формулы Тейлора ее можно представить в виде

$$g_n(z) = \frac{1}{n!}\sum_{k=0}^{n}(z-1)^{n-k}k!\left\{{n+1 \atop k+1}\right\} = \frac{1}{n!}\sum_{k=0}^{n} z^{k+1}(1-z)^{n-k}k!\left\{{n+1 \atop k+1}\right\}. \qquad (16)$$

Второе равенство следует из первого, поскольку вследствие условия симметрии (7)

$$g_n(z) = z^{n+1}g_n(1/z), \qquad n \geq 1. \qquad (17)$$

Из рекуррентного соотношения для чисел Стирлинга

$$\left\{{n+1 \atop k+1}\right\} = (k+1)\left\{{n \atop k+1}\right\} + \left\{{n \atop k}\right\}$$

при $n \geq 1$ получаются два более простых представления:

$$g_n(z) = \frac{1}{n!}\sum_{k=0}^{n} z(z-1)^{n-k}k!\left\{{n \atop k}\right\} = \frac{1}{n!}\sum_{k=0}^{n} z^{k}(1-z)^{n-k}k!\left\{{n \atop k}\right\}. \qquad (18)$$

Производящая функция от двух переменных*

$$g(z,x) = \sum_{n\geq 0}\frac{g_n(z)x^n}{z} = \sum_{k,n\geq 0}\left\langle{n \atop k}\right\rangle\frac{z^k x^n}{n!} \qquad (19)$$

равна, следовательно,

$$\sum_{k,n\geq 0}\frac{\big((z-1)x\big)^n}{(z-1)^k}\left\{{n \atop k}\right\}\frac{k!}{n!} = \sum_{k\geq 0}\left(\frac{e^{(z-1)x}-1}{z-1}\right)^k = \frac{(1-z)}{e^{(z-1)x}-z}. \qquad (20)$$

Это еще одно соотношение, проанализированное Эйлером.

Другие свойства чисел Эйлера можно найти в обзорной статье L. Carlitz, *Math. Magazine* **33** (1959), 247–260. (См. также работы J. Riordan, *Introduction to Combinatorial Analysis* (New York: Wiley, 1958, 38–39), 214–219, 234–237**; D. Foata, M. P. Schützenberger, *Lecture Notes in Math.* **138** (Berlin: Springer, 1970).)

Рассмотрим теперь длину серий; какова в среднем длина серии? В разделе 3.3.2 уже было проанализировано математическое ожидание числа серий данной длины; средняя длина серии равна примерно 2. Это согласуется с тем фактом, что в случайной перестановке длины n содержится около $\frac{1}{2}(n+1)$ серий. Применительно к алгоритмам сортировки полезна несколько отличная точка зрения; рассмотрим длину k-й слева серии перестановки при $k = 1, 2, \ldots$.

Какова, например, длина первой (крайней слева) серии случайной перестановки $a_1\, a_2 \ldots a_n$? Ее длина всегда ≥ 1; она ≥ 2 ровно в половине случаев (а именно, если $a_1 < a_2$). Ее длина ≥ 3 ровно для $1/6$ случаев (если $a_1 < a_2 < a_3$). Вообще, ее длина $\geq m$ с вероятностью $q_m = 1/m!$ для $1 \leq m \leq n$. Следовательно, вероятность того, что длина этой серии равна в точности m, есть

$$\begin{aligned} p_m &= q_m - q_{m+1} = 1/m! - 1/(m+1)!\,, \qquad \text{где } 1 \leq m < n\,; \\ p_n &= 1/n!\,. \end{aligned} \qquad (21)$$

* В оригинале — “super generating function”. — *Прим. перев.*

** Имеется русский перевод: Риордан Дж. Введение в комбинаторный анализ. — М.: Изд-во иностр. лит., 1963. — *Прим. перев.*

Средняя длина первой серии равна, таким образом,

$$\begin{aligned} p_1 + 2p_2 + \cdots + np_n &= (q_1 - q_2) + 2(q_2 - q_3) + \cdots + (n-1)(q_{n-1} - q_n) + nq_n \\ &= q_1 + q_2 + \cdots + q_n = \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{n!}. \end{aligned} \tag{22}$$

Предел при $n \to \infty$ равен $e - 1 = 1.71828\ldots$, а для конечных n это значение равно $e - 1 - \delta_n$, где δ_n довольно мало (для больших n. — *Прим. ред.*):

$$\delta_n = \frac{1}{(n+1)!}\left(1 + \frac{1}{n+2} + \frac{1}{(n+2)(n+3)} + \cdots\right) \le \frac{e-1}{(n+1)!}.$$

Поэтому для практических целей удобно рассмотреть серии *случайной бесконечной* последовательности различных чисел

$$a_1, a_2, a_3, \ldots;$$

под "случайностью" последовательности здесь подразумевается то, что все $n!$ возможных взаимных расположений первых n элементов последовательности равновероятны (при любом n. — *Прим. ред.*). Так что средняя длина первой серии случайной бесконечной последовательности в точности равна $e - 1$.

Несколько усовершенствовав этот метод, можно установить среднюю длину k-й серии случайной последовательности. Пусть q_{km} — вероятность того, что общая длина первых k серий $\ge m$; тогда q_{km} равно величине $1/m!$, умноженной на число перестановок множества $\{1, 2, \ldots, m\}$, которые содержат не более k серий:

$$q_{km} = \left(\left\langle {m \atop 0} \right\rangle + \cdots + \left\langle {m \atop k-1} \right\rangle\right) \Big/ m!. \tag{23}$$

Вероятность того, что общая длина первых k серий равна m, есть $q_{km} - q_{k(m+1)}$. Следовательно, обозначив через L_k среднюю длину k-й серии, находим, что

$$\begin{aligned} L_1 + \cdots + L_k &= \text{средняя общая длина первых } k \text{ серий} \\ &= (q_{k1} - q_{k2}) + 2(q_{k2} - q_{k3}) + 3(q_{k3} - q_{k4}) + \cdots \\ &= q_{k1} + q_{k2} + q_{k3} + \cdots. \end{aligned}$$

Вычитая $L_1 + \cdots + L_{k-1}$ и используя значения q_{km}, из (23) получаем нужную нам формулу:

$$L_k = \frac{1}{1!}\left\langle {1 \atop k-1} \right\rangle + \frac{1}{2!}\left\langle {2 \atop k-1} \right\rangle + \frac{1}{3!}\left\langle {3 \atop k-1} \right\rangle + \cdots = \sum_{m \ge 1} \left\langle {m \atop k-1} \right\rangle \frac{1}{m!}. \tag{24}$$

Поскольку $\left\langle {0 \atop k-1} \right\rangle = 0$, кроме случая $k = 1$, значение L_k оказывается равным коэффициенту при z^{k-1} в производящей функции $g(z, 1) - 1$ (см. (19)); таким образом, имеем

$$L(z) = \sum_{k \ge 0} L_k z^k = \frac{z(1-z)}{e^{z-1} - z} - z. \tag{25}$$

Из формулы Эйлера (13) получим представление L_k в виде полинома от e:

$$\begin{aligned}L_k &= \sum_{m\geq 0}\sum_{j=0}^{k}(-1)^{k-j}\binom{m+1}{k-j}\frac{j^m}{m!}\\ &= \sum_{j=0}^{k}(-1)^{k-j}\sum_{m\geq 0}\binom{m}{k-j}\frac{j^m}{m!}+\sum_{j=0}^{k}(-1)^{k-j}\sum_{m\geq 0}\binom{m}{k-j-1}\frac{j^m}{m!}\\ &= \sum_{j=0}^{k}\frac{(-1)^{k-j}j^{k-j}}{(k-j)!}\sum_{n\geq 0}\frac{j^n}{n!}+\sum_{j=0}^{k}\frac{(-1)^{k-j}j^{k-j-1}}{(k-j-1)!}\sum_{n\geq 0}\frac{j^n}{n!}\\ &= k\sum_{j=0}^{k}\frac{(-1)^{k-j}j^{k-j-1}}{(k-j)!}e^j. \end{aligned}\tag{26}$$

Эту формулу для L_k впервые получила Б. Дж. Гэсснер (B. J. Gassner) [см. *CACM* **10** (1967), 89–93]. Имеем, в частности,

$$\begin{aligned} L_1 &= e-1 &&\approx 1.71828\ldots;\\ L_2 &= e^2-2e &&\approx 1.95249\ldots;\\ L_3 &= e^3-3e^2+\tfrac{3}{2}e &&\approx 1.99579\ldots. \end{aligned}$$

Итак, следует ожидать, что вторая серия будет длиннее первой, а третья серия будет в среднем еще длиннее! На первый взгляд, это может показаться странным, но после минутного размышления становится ясно, что, поскольку первый элемент второй серии будет, скорее всего, малым числом (именно это служит причиной окончания первой серии), у второй серии больше шансов оказаться длиннее, чем у первой. Тенденция такова, что первый элемент третьей серии будет даже меньше, чем первый элемент второй серии. Числа L_k важны в теории сортировки посредством выбора с замещением (раздел 5.4.1), поэтому интересно подробно проанализировать их значения. В табл. 2 приведены первые 18 значений L_k с точностью до 15 десятичных знаков. Рассуждения, приведенные в предыдущем абзаце, могут поначалу вызвать подозрение, что $L_{k+1} > L_k$, на самом же деле значения колеблются, то возрастая, то убывая. Заметим, что L_k быстро приближаются к предельному значению 2. Весьма примечательно то, что эти нормированные полиномы от трансцендентного числа e так быстро сходятся к рациональному числу 2! Полиномы (26) представляют некоторый интерес и с точки зрения численного анализа, поскольку являются прекрасным примером потери значащих цифр при вычитании почти равных чисел; используя арифметику с плавающей точкой и представление с точностью до 19 значащих разрядов, Гэсснер пришла к неверному заключению о том, что $L_{12} > 2$, а Джон У. Ренч (мл.) (John W. Wrench, Jr.) отметил, что выполнение арифметических операций с точностью до 42 значащих разрядов дает значения L_{28} с точностью только до 29 значащих цифр.

Асимптотическое поведение L_k можно определить, исходя из простых положений теории функций комплексного переменного. Знаменатель в (25) обращается в нуль лишь при $e^{z-1} = z$, т. е. когда

$$e^{x-1}\cos y = x \qquad \text{и} \qquad e^{x-1}\sin y = y, \tag{27}$$

Таблица 2

СРЕДНЯЯ ДЛИНА k-Й СЕРИИ

k	L_k	k	L_k
1	1.71828 18284 59045+	10	2.00000 00012 05997+
2	1.95249 24420 12560−	11	2.00000 00001 93672+
3	1.99579 13690 84285−	12	1.99999 99999 99909+
4	2.00003 88504 76806−	13	1.99999 99999 97022−
5	2.00005 75785 89716+	14	1.99999 99999 99719+
6	2.00000 50727 55710−	15	2.00000 00000 00019+
7	1.99999 96401 44022+	16	2.00000 00000 00006+
8	1.99999 98889 04744+	17	2.00000 00000 00000+
9	1.99999 99948 43434−	18	2.00000 00000 00000−

полагая $z = x + iy$. На рис. 3, на котором нанесены оба графика этих уравнений, видно, что они пересекаются в точках $z = z_0, z_1, \bar{z}_1, z_2, \bar{z}_2, \ldots$, где $z_0 = 1$,

$$z_1 = (3.08884\ 30156\ 13044-) + (7.46148\ 92856\ 54255-)\, i, \tag{28}$$

и при больших k мнимая часть $\Im(z_{k+1})$ равна приблизительно $\Im(z_k) + 2\pi$.

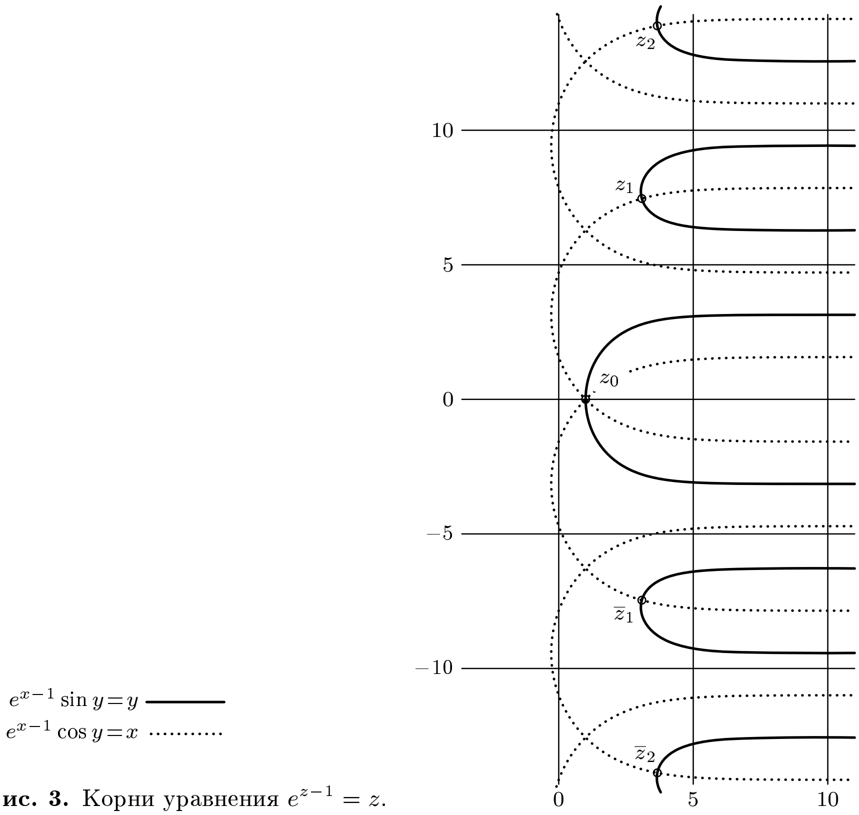

Рис. 3. Корни уравнения $e^{z-1} = z$.

Так как

$$\lim_{z\to z_k}\left(\frac{1-z}{e^{z-1}-z}\right)(z-z_k)=-1 \qquad \text{при } k>0$$

и этот предел равен -2 при $k=0$, функция

$$R_m(z)=L(z)+\frac{2}{z-z_0}+\frac{z_1}{z-z_1}+\frac{\bar z_1}{z-\bar z_1}+\frac{z_2}{z-z_2}+\frac{\bar z_2}{z-\bar z_2}+\cdots+\frac{z_m}{z-z_m}+\frac{\bar z_m}{z-\bar z_m}$$

не имеет особых точек на комплексной плоскости при $|z|<|z_{m+1}|$. Значит, $R_m(z)$ можно разложить в степенной ряд $\sum_k \rho_k z^k$, который сходится абсолютно при $|z|<|z_{m+1}|$; отсюда следует, что $\rho_k M^k\to 0$ при $k\to\infty$, где $M=|z_{m+1}|-\epsilon$. Коэффициентами для $L(z)$ служат коэффициенты разложения функции

$$\frac{2}{1-z}+\frac{1}{1-z/z_1}+\frac{1}{1-z/\bar z_1}+\cdots+\frac{1}{1-z/z_m}+\frac{1}{1-z/\bar z_m}+R_m(z),$$

а именно

$$L_n=2+2r_1^{-n}\cos n\theta_1+2r_2^{-n}\cos n\theta_2+\cdots+2r_m^{-n}\cos n\theta_m+O(r_{m+1}^{-n}), \tag{29}$$

если положить

$$z_k=r_ke^{i\theta_k}. \tag{30}$$

Отсюда можно проследить асимптотическое поведение L_n. Имеем

$$\begin{aligned}
r_1 &= 8.07556\,64528\,89526-, &\qquad \theta_1 &= 1.17830\,39784\,74668+;\\
r_2 &= 14.35456\,68997\,62106-, & \theta_2 &= 1.31268\,53883\,87636+;\\
r_3 &= 20.62073\,15381\,80628-, & \theta_3 &= 1.37427\,90757\,91688-;\\
r_4 &= 26.88795\,29424\,54546-, & \theta_4 &= 1.41049\,72786\,51865-;
\end{aligned} \tag{31}$$

таким образом, главный вклад в L_n-2 дают r_1 и θ_1, а ряд (29) сходится очень быстро. Дальнейший анализ [W. W. Hooker, *CACM* **12** (1969), 411–413] показывает, что $R_m(z)\to -z$ при $m\to\infty$; следовательно, ряд $2\sum_{k\ge 0} r_k^{-n}\cos n\theta_k$ действительно *сходится* к L_n при $n>1$.

Можно провести более тщательный анализ и полностью определить распределение вероятностей для длины k-й серии и для общей длины первых k серий (см. упр. 9–11). Оказывается, сумма $L_1+\cdots+L_k$ асимптотически приближается к $2k-\frac{1}{3}+O(8^{-k})$.

В заключение этого раздела рассмотрим свойства серий в случае, когда в перестановке допускаются одинаковые элементы. Бесчисленные пасьянсы, которым посвящал свой досуг знаменитый американский астроном 19 в. Саймон Ньюкомб (Simon Newcomb), имеют непосредственное отношение к интересующему нас вопросу. Он брал колоду карт и складывал их в одну стопку до тех пор, пока они шли в порядке неубывания по старшинству; как только следующая карта оказывалась младше предыдущей, он начинал новую стопку. Он хотел найти такую вероятность, при которой вся колода окажется разложенной на заданное количество стопок. Задача Саймона Ньюкомба состоит, следовательно, в нахождении распределения вероятностей для серий случайной перестановки мультимножества. В общем случае ответ довольно сложен (см. упр. 12), хотя мы уже видели, как решать задачу в частном случае, когда все карты различны по старшинству. Мы удовлетворимся здесь выводом формулы для *среднего* числа стопок в этом пасьянсе.

Пусть имеется m различных типов карт и каждая встречается ровно p раз. Например, в обычной колоде для бриджа $m = 13$, а $p = 4$, если пренебрегать различием масти. Замечательную симметрию обнаружил в этом случае П. А. Мак-Магон [см. *Combinatory Analysis* **1** (Cambridge, 1915, 212–213)]: число перестановок с $k+1$ сериями равно числу перестановок с $mp-p-k+1$ сериями. Это соотношение легко проверить при $p = 1$ (формула (7)), однако при $p > 1$ оно кажется довольно неожиданным.

Можно доказать свойство симметрии, установив взаимно однозначное соответствие между перестановками, такое, что каждой перестановке с $k + 1$ сериями соответствует перестановка с $mp - p - k + 1$ сериями. Мы настойчиво рекомендуем читателю постараться самостоятельно найти такое соответствие, прежде чем двигаться дальше.

Какое-нибудь очень простое соответствие на ум не приходит; доказательство Мак-Магона основано на производящих функциях, а не на комбинаторном построении. Однако установленное Фоатой соответствие (теорема 5.1.2B) позволяет упростить задачу, так как в нем утверждается существование взаимно однозначного соответствия между перестановками с $k+1$ сериями и перестановками, в двухстрочном представлении которых содержится ровно k столбцов $\frac{y}{x}$, таких, что $x < y$.

Пусть дано мультимножество $\{p\cdot 1, p\cdot 2, \ldots, p\cdot m\}$. Рассмотрим перестановку в двухстрочном представлении

$$\begin{pmatrix} 1 & \ldots & 1 & 2 & \ldots & 2 & \ldots & m & \ldots & m \\ x_{11} & \ldots & x_{1p} & x_{21} & \ldots & x_{2p} & \ldots & x_{m1} & \ldots & x_{mp} \end{pmatrix}. \tag{32}$$

Сопоставим с ней другую перестановку того же мультимножества:

$$\begin{pmatrix} 1 & \ldots & 1 & 2 & \ldots & 2 & \ldots & m & \ldots & m \\ x'_{11} & \ldots & x'_{1p} & x'_{m1} & \ldots & x'_{mp} & \ldots & x'_{21} & \ldots & x'_{2p} \end{pmatrix}, \tag{33}$$

где $x' = m + 1 - x$. Если перестановка (32) содержит k столбцов вида $\frac{y}{x}$, таких, что $x < y$, то (33) содержит $(m - 1)p - k$ таких столбцов, потому что необходимо рассмотреть лишь случай $y > 1$, а неравенство $x < y$ эквивалентно $x' \geq m + 2 - y$. Поскольку (32) соответствует перестановке с $k + 1$ сериями, а (33) — перестановке с $mp - p - k + 1$ сериями и преобразование, переводящее (32) в (33), обратимо (оно же переводит (33) в (32)), то тем самым доказано условие симметрии Мак-Магона. Пример этого построения содержится в упр. 14.

В силу свойства симметрии среднее число серий в случайной перестановке должно равняться $\frac{1}{2}\big((k+1)+(mp-p-k+1)\big) = 1+\frac{1}{2}p(m-1)$. Например, для стандартной колоды среднее число стопок в пасьянсе Ньюкомба равно 25 (так что раскладывание этого пасьянса вряд ли покажется столь уж увлекательным занятием).

На самом деле после несложных рассуждений можно определить среднее число серий в общем случае для *любого* данного мультимножества $\{n_1\cdot x_1, n_2\cdot x_2, \ldots, n_m\cdot x_m\}$, где все x_k различны. Пусть $n = n_1 + n_2 + \cdots + n_m$ и все перестановки $a_1\, a_2 \ldots a_n$ этого мультимножества выписаны в явном виде. Посмотрим, как часто a_i оказывается больше a_{i+1} при каждом фиксированном значении i, $1 \leq i < n$. Число случаев, когда $a_i > a_{i+1}$, равно в точности половине числа случаев, когда $a_i \neq a_{i+1}$, и нетрудно видеть, что $a_i = a_{i+1} = x_j$ ровно в $Nn_j(n_j - 1)/n(n - 1)$ случаях, где N — общее число перестановок. Следовательно, $a_i = a_{i+1}$ ровно в

$$\frac{N}{n(n-1)}\big(n_1(n_1-1)+\cdots+n_m(n_m-1)\big)=\frac{N}{n(n-1)}(n_1^2+\cdots+n_m^2-n)$$

случаях, а $a_i > a_{i+1}$ в

$$\frac{N}{2n(n-1)}\big(n^2-(n_1^2+\cdots+n_m^2)\big)$$

случаях. Суммируя по i и прибавляя N, потому что в каждой перестановке одна серия заканчивается элементом a_n, получим общее число серий во всех N перестановках:

$$N\Big(\frac{n}{2}-\frac{1}{2n}(n_1^2+\cdots+n_m^2)+1\Big). \tag{34}$$

Выполнив деление на N, получим искомое среднее число серий.

Поскольку серии играют весьма важную роль в изучении "порядковых статистик", имеется весьма обширный список работ, посвященных этой теме, включая некоторые типы серий, не рассмотренные здесь. Дополнительную информацию можно найти в книге F. N. David, D. E. Barton, Combinatorial Chance (London: Griffin 1962, гл. 10) и в обзорной статье C. L. Mallows, *Annals of Math. Statistics* **36** (1965), 236–260.

УПРАЖНЕНИЯ

1. [*M26*] Выведите формулу Эйлера (13).

▶ **2.** [*M22*] (a) Попытайтесь развить идею, использованную в тексте при доказательстве тождества (8). Рассмотрите последовательности $a_1\,a_2\ldots a_n$, содержащие ровно q различных элементов, и докажите, что

$$\sum_k \left\langle {n \atop k} \right\rangle \binom{k}{n-q} = \left\{ {n \atop q} \right\} q!.$$

(b) Используя это тождество, докажите, что

$$\sum_k \left\langle {n \atop k} \right\rangle \binom{k+1}{m} = \left\{ {n+1 \atop n+1-m} \right\} (n-m)! \qquad \text{при } n \ge m.$$

3. [*HM25*] Вычислите сумму $\sum_k \left\langle {n \atop k} \right\rangle (-1)^k$.

4. [*M21*] Чему равна сумма $\sum_k (-1)^k \left\{ {n \atop k} \right\} k! \binom{n-k}{m}$?

5. [*M20*] Найдите значение $\left\langle {p \atop k} \right\rangle \bmod p$, если p — простое число.

▶ **6.** [*M21*] Мистер Далл заметил, что из формул (4) и (13) можно получить

$$n! = \sum_{k\ge 0} \left\langle {n \atop k} \right\rangle = \sum_{k\ge 0} \sum_{j\ge 0} (-1)^{k-j} \binom{n+1}{k-j} (j+1)^n.$$

Он обнаружил, что $\sum_{k\ge 0}(-1)^{k-j}\binom{n+1}{k-j} = 0$ при всех $j \ge 0$, выполнив суммирование сначала по k, а затем по $j \ge 0$; отсюда $n! = 0$ при любом $n \ge 0$. Не допустил ли он какой-нибудь ошибки?

7. [*HM40*] Является ли распределение вероятностей для серий, задаваемое формулой (14), асимптотически нормальным? (Ср. с упр. 1.2.10–13.)

8. [*M24*] (П. А. Мак-Магон.) Покажите, что вероятность того, что длина первой серии достаточно длинной перестановки есть l_1, длина второй есть l_2, ..., а длина k-й серии $\ge l_k$ равна

$$\det\begin{pmatrix} 1/l_1! & 1/(l_1+l_2)! & 1/(l_1+l_2+l_3)! & \ldots & 1/(l_1+l_2+l_3+\cdots+l_k)! \\ 1 & 1/l_2! & 1/(l_2+l_3)! & \ldots & 1/(l_2+l_3+\cdots+l_k)! \\ 0 & 1 & 1/l_3! & \ldots & 1/(l_3+\cdots+l_k)! \\ \vdots & & & & \vdots \\ 0 & 0 & \ldots & 1 & 1/l_k! \end{pmatrix}.$$

9. [*M30*] Пусть $h_k(z)=\sum p_{km}z^m$, где p_{km} — вероятность того, что общая длина первых k серий случайной последовательности (бесконечной) равна m. Найдите "простые" выражения для $h_1(z)$, $h_2(z)$ и для производящей функции $h(z,x)=\sum_k h_k(z)x^k$ двух переменных.

10. [*HM30*] Определите асимптотическое поведение математического ожидания и дисперсии распределения $h_k(z)$ из предыдущего упражнения при больших k.

11. [*M40*] Пусть $H_k(z)=\sum P_{km}z^m$, где P_{km} — вероятность того, что длина k-й серии в случайной (бесконечной) последовательности равна m. Выразите $H_1(z)$, $H_2(z)$ и производящую функцию $H(z,x)=\sum_k H_k(z)x^k$ от двух переменных через известные функции.

12. [*M33*] (П. А. Мак-Магон.) Обобщите формулу (13) на случай перестановок мультимножества, доказав, что число перестановок мультимножества $\{n_1\cdot 1,\, n_2\cdot 2,\ldots,\, n_m\cdot m\}$, имеющих ровно k серий, равно

$$\sum_{j=0}^{k}(-1)^j\binom{n+1}{j}\binom{n_1-1+k-j}{n_1}\binom{n_2-1+k-j}{n_2}\ldots\binom{n_m-1+k-j}{n_m},$$

где $n=n_1+n_2+\cdots+n_m$.

13. [*05*] Каким будет среднее число стопок в пасьянсе Ньюкомба, если пользоваться обычной колодой для бриджа (из 52 карт), игнорируя старшинство карт, но считая, что трефы < бубны < черви < пики?

14. [*M18*] Перестановка 3 1 1 1 2 3 1 4 2 3 3 4 2 2 4 4 содержит 5 серий; найдите соответствующую перестановку с 9-ю сериями с помощью построения для условия симметрии Мак-Магона, приведенного в тексте раздела.

▶ **15.** [*M21*] (*Перемежающиеся серии.*) В классической литературе 19 в. по комбинаторному анализу рассматриваемый нами вопрос о сериях в перестановках не изучался, но некоторые авторы изучали попеременно восходящие и нисходящие серии. Так, считалось, что перестановка 5 3 2 4 7 6 1 8 содержит 4 серии: 5 3 2, 2 4 7, 7 6 1 и 1 8. (Первая серия будет восходящей или нисходящей в зависимости от того, $a_1<a_2$ или $a_1>a_2$; таким образом, перестановки $a_1\,a_2\ldots a_n$, $a_n\ldots a_2\,a_1$ и $(n+1-a_1)(n+1-a_2)\ldots(n+1-a_n)$ содержат одинаковое число перемежающихся серий.) Максимальное число серий этого типа в перестановке n элементов равно $n-1$.

Найдите среднее число перемежающихся серий в случайной перестановке множества $\{1,2,\ldots,n\}$. [*Указание.* Разберите вывод формулы (34).]

16. [*M30*] Продолжим предыдущее упражнение. Пусть $\left|{n \atop k}\right|$ — число перестановок множества $\{1,2,\ldots,n\}$, которые имеют ровно k перемежающихся серий. Найдите рекуррентное соотношение, с помощью которого можно вычислить таблицу значений $\left|{n \atop k}\right|$; найдите также соответствующее рекуррентное соотношение для производящей функции $G_n(z)=\sum_k\left|{n \atop k}\right|z^k/n!$. Используя это последнее соотношение, найдите простую формулу для *дисперсии* числа перемежающихся серий в случайной перестановке множества $\{1,2,\ldots,n\}$.

17. [*M25*] Существует всего 2^n последовательностей $a_1\,a_2\ldots a_n$, где каждый элемент a_j — либо 0, либо 1. Сколько среди них последовательностей, содержащих ровно k серий (т. е. содержащих ровно $k-1$ элементов a_j, таких, что $a_j>a_{j+1}$)?

18. [*M28*] Существует всего $n!$ последовательностей $b_1 b_2 \ldots b_n$, в которых каждый элемент b_j — целое число, лежащее в диапазоне $0 \le b_j \le n - j$. Сколько среди них последовательностей, содержащих (a) ровно k нисходящих серий (т. е. содержащих ровно k соотношений элементов, таких, что $b_j > b_{j+1}$) и (b) ровно k отличающихся элементов?

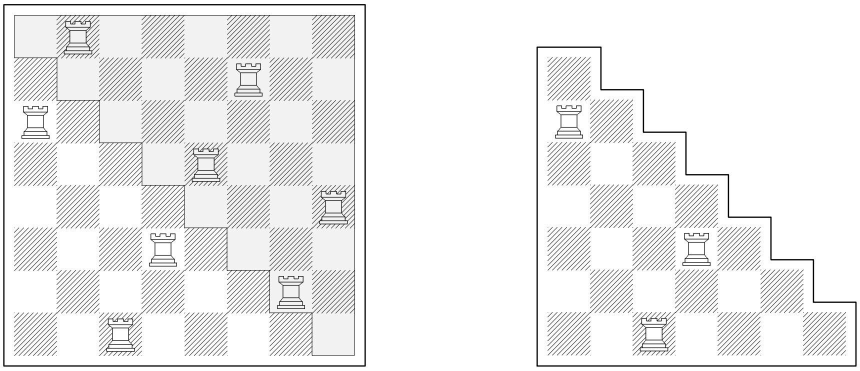

Рис. 4. Неатакующие ладьи на шахматной доске при заданном числе $k = 3$ ладей ниже главной диагонали.

▸ **19.** [*M26*] (Дж. Риордан (J. Riordan).) (a) Сколькими способами можно расположить n неатакующих ладей (т. е. никакие две ладьи не должны находиться на одной вертикали или горизонтали) на шахматной доске размером $n \times n$ так, чтобы ровно k из них находились на заданной стороне от главной диагонали? (b) Сколькими способами можно расположить k неатакующих ладей на заданной стороне от главной диагонали шахматной доски размером $n \times n$? Например, на рис. 4 показан один из 15 619 способов расположения восьми неатакующих ладей на обычной шахматной доске с тремя ладьями на незаштрихованном участке ниже главной диагонали, а также один из 1 050 способов расположения трех неатакующих ладей на треугольной доске.

▸ **20.** [*M21*] Говорят, что перестановка требует k *чтений*, если ее нужно просмотреть k раз слева направо, чтобы прочитать все элементы в порядке неубывания. Например, перестановка 4 9 1 8 2 5 3 6 7 требует четырех чтений: при первом чтении получаем 1, 2, 3, при втором — 4, 5, 6, 7; затем — 8 и 9. Найдите связь между сериями и чтениями.

21. [*M22*] Если перестановка $a_1 a_2 \ldots a_n$ множества $\{1, 2, \ldots, n\}$ содержит k серий и требует j чтений в соответствии с упр. 20, то что можно сказать о перестановке $a_n \ldots a_2 a_1$?

22. [*M26*] (Л. Карлиц, Д. П. Розель и Р. А. Скоувилл.) Покажите, что не существует перестановки множества $\{1, 2, \ldots, n\}$ с $n+1-r$ сериями, требующей s чтений, если $rs < n$; однако такая перестановка существует, если $n \ge n + 1 - r \ge s \ge 1$, $rs \ge n$.

23. [*HM42*] (Вальтер Вейссблюм (Walter Weissblum).) "Удлиненные серии" перестановки $a_1 a_2 \ldots a_n$ получаются, если вставлять вертикальные черточки в тех местах, где нарушается установившаяся монотонность; удлиненные серии бывают как возрастающими, так и убывающими в зависимости от того, в каком порядке расположены первые два элемента, так что длина каждой удлиненной серии (кроме, возможно, последней) ≥ 2. Например, перестановка 7 5 | 6 2 | 3 8 9 | 1 4 содержит четыре удлиненные серии. Найдите средние длины первых двух удлиненных серий бесконечной перестановки и докажите, что в пределе длина удлиненной серии равна

$$(1 + \cot \tfrac{1}{2})/(3 - \cot \tfrac{1}{2}) \approx 2.4202.$$

24. [*M30*] Выразите в виде функции от p среднее число серий в последовательностях, полученных методом, который описан в упр. 5.1.1–18.

25. [*M25*] Пусть $U_1, \ldots, U_n$ — независимые равномерно распределенные числа на интервале $[0\,..\,1)$. Какова вероятность выполнения равенства $\lfloor U_1 + \cdots + U_n \rfloor = k$?

26. [*M20*] Обозначим через ϑ операцию $z\frac{d}{dz}$, которая умножает на n коэффициент при z^n в производящей функции. Покажите, что результат многократного (m раз) применения ϑ к $1/(1-z)$ может быть представлен в терминах чисел Эйлера.

▸ **27.** [*M21*] *Разрастающийся лес* — это лес, в котором узлы пронумерованы $\{1, 2, \ldots, n\}$ таким образом, что родители всегда имеют меньшие номера, чем их потомки. Покажите, что $\left\langle {n \atop k} \right\rangle$ — число n-узловых разрастающихся лесов, в которых имеется $k+1$ лист.

*5.1.4. Диаграммы и инволюции

В заключение нашего обзора комбинаторных свойств перестановок обсудим некоторые замечательные отношения, связывающие их с массивами целых чисел, называемыми диаграммами. *Диаграмма Юнга формы* $(n_1, n_2, \ldots, n_m)$, где $n_1 \geq n_2 \geq \cdots \geq n_m > 0$, — это расположение $n_1 + n_2 + \cdots + n_m$ различных целых чисел в массиве строк, выровненных по левому краю, где в i-й строке содержится n_i элементов; при этом в каждой строке элементы возрастают слева направо, а элементы каждого столбца возрастают сверху вниз. Например, диаграмма Юнга формы (6, 4, 4, 1) имеет вид

$$\begin{array}{|c|c|c|c|c|c|}\hline 1 & 2 & 5 & 9 & 10 & 15 \\ \hline 3 & 6 & 7 & 13 \\ \cline{1-4} 4 & 8 & 12 & 14 \\ \cline{1-4} 11 \\ \cline{1-1} \end{array}\ . \qquad (1)$$

Диаграммы такой формы ввел Альфред Юнг (Alfred Young) в 1900 году в качестве вспомогательного средства при изучении матричного представления перестановок. [См. *Proc. London Math. Soc.* (2) **28** (1928), 255–292; Bruce E. Sagan, *The Symmetric Group* (Pacific Grove, Calif.: Wadsworth & Brooks/Cole, 1991).] Для краткости вместо "диаграмма Юнга" мы будем говорить просто "диаграмма". *Инволюция* — это перестановка, обратная самой себе. Например, существует 10 инволюций множества {1, 2, 3, 4}:

$$\begin{matrix} \begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix} & \begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix} & \begin{pmatrix}1&2&3&4\\3&2&1&4\end{pmatrix} & \begin{pmatrix}1&2&3&4\\4&2&3&1\end{pmatrix} & \begin{pmatrix}1&2&3&4\\1&3&2&4\end{pmatrix} \\ \begin{pmatrix}1&2&3&4\\1&4&3&2\end{pmatrix} & \begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix} & \begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix} & \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix} & \begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix} \end{matrix}. \qquad (2)$$

Термин "инволюция" первоначально использовался в классических задачах геометрии; инволюции в общем смысле, рассматриваемые здесь, были впервые изучены Х. А. Роте (H. A. Rothe), когда он ввел понятие обратной перестановки (см. раздел 5.1.1).

Может показаться странным, что мы рассматриваем диаграммы и инволюции вместе, но существует удивительная связь между этими понятиями, не имеющими, казалось бы, друг к другу никакого отношения: *число инволюций множества*