

Московский государственный технический университет
имени Н.Э. Баумана

А.Е. Жуков, Д.А. Жуков

Элементы комбинаторики

*Рекомендовано Научно-методическим советом
МГТУ им. Н.Э. Баумана в качестве учебного пособия*

Москва
Издательство МГТУ им. Н.Э. Баумана
2014

УДК 519.1
ББК 22.141
Ж85

Рецензенты: *А.В. Чашкин, П.Г. Ключарев*

Жуков А. Е.

Ж85 Элементы комбинаторики: учеб. пособие / А. Е. Жуков, Д. А. Жуков. — М.: Изд-во МГТУ им. Н. Э. Баумана, 2014. — 99, [5] с.: ил.

ISBN 978-5-7038-3752-8

Изложены основные идеи и понятия, нашедшие применение в области компьютерной криптографии. Приведены разные конструкции и методы работы с комбинаторными объектами, большое количество примеров и задач.

Для студентов, изучающих курсы «Информатика», «Дискретная математика», «Основы теории информации» и «Комбинаторика». Может быть полезно студентам и аспирантам для самостоятельного изучения.

УДК 519.1
ББК 22.141

ПРЕДИСЛОВИЕ

О значении математики для защиты информации в компьютерах и сетях связи сказано и написано довольно много. Знание разработанных математических теорий, идей и методов позволяет находить новые оригинальные технические решения, в свою очередь, практические задачи защиты информации ставят перед математиками новые интересные проблемы. Важнейшими математическими объектами, используемыми в процессе разработки и проектирования систем информационной безопасности и в информатике в целом, являются комбинаторные схемы и конфигурации. Комбинаторика — раздел математики, посвященный решению задач выбора и расположения элементов некоторого, обычно конечного, множества в соответствии с установленными правилами. Каждое такое правило определяет способ построения некоторой конструкции из элементов исходного множества, называемой комбинаторной конфигурацией. Поэтому можно сказать, что целью комбинаторного анализа является изучение комбинаторных схем и конфигураций.

Работая над книгой, авторы ставили своей целью создание руководства по перечислительной комбинаторике, ориентированного на прикладное применение. В основу пособия положено содержание курсов и семинаров, которые авторы на протяжении ряда лет проводили в МГУ, МГТУ, МИФИ, ИКСИ.

В приложении содержатся строгие математические доказательства некоторых утверждений, включение которых в основной текст сделало бы его чрезмерно громоздким и сложным для восприятия. Кроме того, приведено интересное комбинаторное понятие — числа Каталана, имеющие разнообразное применение.

Все разделы содержат примеры и задачи, полезные для самостоятельного изучения студентами и аспирантами. Освоение материала даст читателю необходимый инструментарий для теоретической и практической работы в области информационной безопасности.

Глава 1. ОСНОВНЫЕ КОМБИНАТОРНЫЕ ПОНЯТИЯ И СХЕМЫ

Цель комбинаторного анализа — решение задач выбора и расположения элементов некоторого, обычно конечного, множества в соответствии с установленными правилами (схемами). Каждое такое правило определяет способ построения из элементов исходного множества некоторой конструкции, называемой комбинаторной конфигурацией. Задачей комбинаторики является изучение и в первую очередь перечисление комбинаторных схем и конфигураций.

1.1. Основные перечислительные правила

Основные перечислительные правила комбинаторики очень просты, естественны и понятны. При правильном их использовании можно решить очень большое количество самых разнообразных перечислительных задач, появляющихся в дискретной математике.

Правило суммы: если первое событие может произойти n_1 способами, а второе n_2 способами и при этом *они не могут произойти одновременно*, то или первое, или второе событие (*но только одно из них*) может произойти $n_1 + n_2$ способами.

Правило произведения: если первое событие может произойти n_1 способами, а второе *независимо от исхода первого события*, может произойти n_2 способами, то совместная реализация двух событий может произойти $n_1 \times n_2$ способами.

Пример 1.1. В группе из 20 студентов и 15 студенток:

— выбор старосты возможен $20 + 15 = 35$ способами (правило суммы);

— выбор пары «студент — студентка» $20 \times 15 = 300$ способами (правило произведения).

Пример 1.2. По правилу произведения выбирают:

- семизначные телефонные номера (10^7 вариантов);
- семизначные телефонные номера с неповторяющимися цифрами $10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4$ вариантов;
- число перестановок из n элементов равно $n(n-1)(n-2) \cdot \dots \cdot 3 \cdot 2 \cdot 1 = n!$;
- число двоичных наборов длины n равно 2^n ;
- число булевых функций от n переменных равно 2^{2^n} .

1.2. Основные комбинаторные схемы

Важнейшими математическими объектами, используемыми не только в дискретной математике, но и в информатике в целом, являются различные комбинаторные схемы и конфигурации. Из них более всего распространены схемы выборок, с которыми связаны, пожалуй, наиболее употребимые в математике (причем не только дискретной) понятия размещения и сочетания. Доказательства в этом разделе даются по большей части схематично, так как рассматриваемые величины, как правило, уже определялись и изучались в других математических дисциплинах.

1.2.1. Схемы выборок. Пусть имеется конечное множество M , его мощность $|M| = n$. Рассмотрим *выборки* объема k , которые извлекаются из множества M . Существуют следующие типы выборок.

I. *Размещения (упорядоченные выборки без возвращения).* Число размещений находят по правилу произведения:

$$A_n^k = n(n-1) \dots (n-k+1) = (n)_k = \frac{n!}{(n-k)!}.$$

Размещение называется *перестановкой*, если $k = n$, их число $A_n^n = n!$.

II. *Размещения с повторениями (упорядоченные выборки с возвращением).* По правилу произведения число размещений с повторениями

$$\bar{A}_n^k = n^k.$$

III. *Сочетания (неупорядоченные выборки без возвращения).* Число сочетаний C_n^k получается группировкой различных размещений, состоящих из одних и тех же элементов, т. е. образующих одно и то же сочетание:

$$C_n^k = \frac{A_n^k}{A_k^k} = \frac{n!}{(n-k)! k!}.$$

IV. *Сочетания с повторениями (неупорядоченные выборки с возвращением).* Число сочетаний с повторениями $\bar{C}_n^k$ соответствует числу способов деления $n+k$ элементов, выстроенных в линию, на n непустых зон:

$$\bar{C}_n^k = C_{n+k-1}^{m-1} = C_{n+k-1}^k.$$

Пример 1.3. Интерпретация числа сочетаний C_n^k :

— коэффициенты в формуле *бинома Ньютона* $(x+y)^n = \sum_{k=0}^n C_n^k x^k y^{n-k}$. Величины C_n^k называют также *биномиальными коэффициентами* поскольку они появляются в формуле бинома Ньютона.

— число разных подмножеств мощности k в множестве из n элементов. Число всех подмножеств такого множества равно 2^n ;

— число последовательностей длины n , содержащих ровно k единиц;

— число неубывающих путей длины n , соединяющих точки $(0,0)$ и $(k, n-k)$ на прямоугольной решетке;

1.2.2. Свойства биномиальных коэффициентов. Большая часть свойств биномиальных коэффициентов может быть получена по меньшей мере двумя способами — из алгебраического выражения для величины C_n^k и из комбинаторных соображений, вытекающих из определения сочетания. Другие свойства могут быть легко получены из формулы бинома Ньютона.

Свойство симметрии $C_n^k = C_n^{n-k}$. Алгебраическое доказательство свойства симметрии очевидно из формулы для C_n^k . Комбинаторное доказательство состоит в том, что выбор подмножества мощности k в множестве мощности n эквивалентен выбору в том же множестве подмножества мощности $n-k$.

Рекуррентное соотношение $C_n^k = C_{n-1}^{k-1} + C_{n-1}^k$. Написав выражения для биномиальных коэффициентов и проделав очевидные

преобразования, получаем алгебраическое доказательство приведенного тождества. Для комбинаторного доказательства рассмотрим множество $\mathcal{M}$, состоящее из n элементов. Пусть один из элементов этого множества отмечен. Тогда отмеченный элемент либо входит в подмножество мощности k (таких подмножеств будет C_{n-1}^{k-1}) либо не входит (таких подмножеств будет C_{n-1}^k). Отсюда и следует указанное рекуррентное соотношение с очевидными граничными условиями: $C_n^0 = C_n^n = 1$.

Сумма биномиальных коэффициентов: $\sum_{k=0}^n C_n^k = 2^n$. Тождество

легко получаем из формулы бинома Ньютона, если в ней положить $x = y = 1$.

$$\sum_{k=0}^n (-1)^k C_n^k = 0 \Rightarrow C_n^0 + C_n^2 + \dots = C_n^1 + C_n^3 + \dots = 2^{n-1}. \text{ Тождество}$$

следует из формулы бинома Ньютона, если в ней положить $x = -1$; $y = 1$.

$$\sum_{k=1}^n k(-1)^k C_n^k = 0. \text{ Это и следующее тождество получаем из}$$

формулы бинома Ньютона после ее однократного или соответственно r -кратного дифференцирования.

$$\sum_{k=r}^n (-1)^k C_k^r C_n^k = 0.$$

$$C_n^{k-1} = \frac{(n)_{k-1}}{(k-1)!} \leq \frac{(n)_k}{k!} = C_n^k \text{ при } k \leq n - k + 1 \Leftrightarrow k \leq \frac{n+1}{2}.$$

Неравенство непосредственно выводят из алгебраической формулы для биномиальных коэффициентов.

$$\text{Свертка Вандермонда } \sum_{j=0}^n C_n^j C_m^{k-j} = C_{n+m}^k.$$

Для доказательства можно воспользоваться алгебраическим тождеством

$$(x+1)^n (x+1)^m = (x+1)^{n+m}$$

или комбинаторными соображениями (рис. 1.1).

Биномиальные коэффициенты C_n^k , рас-

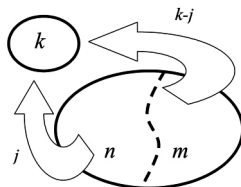


Рис. 1.1

положенные в виде прямоугольной таблицы (табл. 1.1), образуют так называемый *треугольник Паскаля*, наглядно показывающий свойство симметрии $C_n^k = C_n^{n-k}$, рекуррентное соотношение $C_n^k = C_{n-1}^{k-1} + C_{n-1}^k$ и неравенство

$$C_n^{k-1} = \frac{(n)_{k-1}}{(k-1)!} \leq \frac{(n)_k}{k!} = C_n^k \text{ при } k \leq \frac{n+1}{2}.$$

Таблица 1.1

n	k							
	0	1	2	3	4	5	6	...
0	1							
1	1	1						
2	1	2	1					
3	1	3	3	1				
4	1	4	6	4	1			
5	1	5	10	10	5	1		
6	1	6	15	20	15	6	1	
...								

1.2.3. Полиномиальные коэффициенты. Рассмотрим схему, состоящую в «раскрашивании» k красками элементов множества M , $|M| = n$. Обозначим через n_i количество элементов, раскрашенных i -м цветом, причем $n_i \geq 0$, $n_1 + n_2 + \dots + n_k = n$. Найдем число способов раскраски n элементов, при которой n_i элементов раскрашено i -й краской:

$$\begin{aligned} C(n; n_1, \dots, n_k) &= C_n^{n_1} C_{n-n_1}^{n_2} C_{n-n_1-n_2}^{n_3} \cdot \dots \cdot C_{n-n_1-\dots-n_{k-1}}^{n_k} = \\ &= \frac{n!}{n_1! (n-n_1)!} \frac{(n-n_1)!}{n_2! (n-n_1-n_2)!} \cdot \dots \cdot \frac{(n-n_1-n_2-\dots-n_{k-1})!}{n_k! 0!} \end{aligned}$$

или после сокращения $C(n; n_1, n_2, \dots, n_k) = \frac{n!}{n_1! n_2! \cdot \dots \cdot n_k!}$.
Полученное выражение называется *полиномиальным коэффициентом*.

Теоретико-множественный смысл полиномиального коэффициента заключается в количестве способов разбиения n -элементного множества на k различных подмножеств (может быть и пустых). Иными словами, полиномиальный коэффициент — число выборов, для которых n_i элементам присваивается метка i , причем $n = n_1 + n_2 + \dots + n_k$.

Полиномиальный коэффициент появляется как коэффициент при соответствующем слагаемом в полиномиальном представлении выражения $(x_1 + x_2 + \dots + x_k)^n$:

$$(x_1 + x_2 + \dots + x_k)^n = \sum_{n_1+n_2+\dots+n_k=n} C(n; n_1, n_2, \dots, n_k) x_1^{n_1} x_2^{n_2} \dots x_k^{n_k}.$$

Заметим, что при $k = 2$ получаем уже известные биномиальные коэффициенты: $C(n; n_1, n - n_1) = \frac{n!}{n_1!(n - n_1)!} = C_n^{n_1}$.

1.2.4. Разбиения чисел. Разбиением натурального числа n называют его представление в виде суммы натуральных слагаемых:

$$n_1 + n_2 + \dots + n_k = n.$$

Если порядок слагаемых значения не имеет, то такое разбиение называется *неупорядоченным*. Если не оговорено противное, то в дальнейшем под *разбиением* будем понимать неупорядоченное разбиение натурального числа n . Разбиение обычно представляется в стандартной форме, в которой слагаемые выписывают в невозрастающем порядке:

$$n_1 \geq n_2 \geq \dots \geq n_k.$$

Например, $9 = 3 + 2 + 2 + 1 + 1$. Числа n_i , образующие разбиение, называют его *частями*. Обозначим через $P_k(n)$ число разбиений n на k частей.

Пример 1.4. $P_3(7) = 4$, так как

$$7 = 5 + 1 + 1 = 4 + 2 + 1 = 3 + 3 + 1 = 3 + 2 + 2.$$

Иными словами $P_k(n)$ — это число натуральных решений уравнения

$$x_1 + x_2 + \dots + x_k = n; \quad x_1 \geq x_2 \geq \dots \geq x_k \geq 1.$$

Это уравнение можно преобразовать к виду

$$(x_1 - 1) + (x_2 - 1) + \dots + (x_k - 1) = n - k;$$

$$x_1 \geq x_2 \geq \dots \geq x_k \geq 1.$$

Отсюда, сделав замену $y_i = x_i - 1$, $i = 1, \dots, k$, получим

$$y_1 + y_2 + \dots + y_k = n - k; \quad y_1 \geq y_2 \geq \dots \geq y_k \geq 0.$$

Однако если $y_s > 0$, $y_{s+1} = \dots = y_k = 0$, то предыдущая формула дает разбиение $n - k$ на s частей. Таким образом, число решений этого уравнения равно числу разбиений $n - k$ не более чем на k частей, отсюда следует рекуррентное соотношение для числа разбиений

$$P_k(n) = P_k(n - k) + P_{k-1}(n - k) + \dots + P_1(n - k)$$

с очевидными граничными условиями $P_1(n) = P_n(n) = 1$ и $P_k(n) = 0$ при $n < k$.

Применяя рекуррентное соотношение, получаем, в частности,

$$\begin{aligned} P_2(n) &= P_2(n - 2) + P_1(n - 2) = P_2(n - 2) + 1 = \\ &= P_2(n - 4) + 2 = \dots \\ &= \begin{cases} \frac{n}{2} & \text{при } n = 2k; \\ \frac{n-1}{2} & \text{при } n = 2k + 1. \end{cases} \end{aligned}$$

Если теперь через $P(n)$ обозначить количество всех неупорядоченных разбиений числа n , то ясно, что

$$P(n) = P_n(n) + P_{n-1}(n) + \dots + P_2(n) + P_1(n).$$

В то же время $P(n)$ можно рассматривать как число неотрицательных целочисленных решений уравнения

$$x_1 + x_2 + \dots + x_n = n; \quad x_1 \geq x_2 \geq \dots \geq x_n \geq 0.$$

Любое фиксированное разбиение числа n содержит λ_1 слагаемых, равных 1; λ_2 слагаемых, равных 2 и т. д. Таким образом, разбиение числа n можно однозначно описать набором $\lambda_1, \lambda_2, \dots, \lambda_n$.

Тогда величину $P(n)$ можно рассматривать как число неотрицательных целочисленных решений уравнения

$$\lambda_1 + 2\lambda_2 + 3\lambda_3 + \dots + n\lambda_n = n; \quad \lambda_i \geq 0, \quad i = 1, \dots, n.$$

Некоторые другие подходы, связанные с разными схемами разбиений, используют метод производящих функций (гл. 4).

1.3. Числа Стирлинга второго рода

Числа Стирлинга обычно вводят как коэффициенты, которые появляются при разложении по степеням x обобщенной степени $(x)_n = x(x-1)(x-2)\dots(x-n+1)$ (числа Стирлинга первого рода) или при разложении обычной степени x^n по обобщенным степеням x (числа Стирлинга второго рода). Другим, более комбинаторным подходом является определение чисел Стирлинга второго рода через разбиение конечного множества на непустые подмножества. Именно этой интерпретации мы и отдадим предпочтение.

1.3.1. Разбиение множества. Разбиением множества M , $|M| = n$ называют набор непустых подмножеств $\mathcal{M} = \{M_1, \dots, M_k\}$, удовлетворяющих следующим свойствам:

$$M_i \subseteq M; \quad M = \bigcup_{i=1}^k M_i;$$

$$\forall i \neq j \Rightarrow M_i \cap M_j = \emptyset.$$

1.3.2. Тип разбиения. Будем говорить, что разбиение имеет тип $1^{\lambda_1} 2^{\lambda_2} \dots n^{\lambda_n}$, если оно содержит λ_1 подмножеств мощности 1, λ_2 подмножеств мощности 2 и т.д. Очевидно, что $\lambda_1 + 2\lambda_2 + 3\lambda_3 + \dots + n\lambda_n = n = |M|$.

Найдем число разбиений типа $1^{\lambda_1} 2^{\lambda_2} \dots n^{\lambda_n}$. Для этого рассмотрим следующую конструкцию:

$$\underbrace{\{\circ\} \{\circ\} \dots \{\circ\}}_{\lambda_1} \quad \underbrace{\{\circ\circ\} \{\circ\circ\} \dots \{\circ\circ\}}_{\lambda_2} \quad \underbrace{\{\circ\circ\circ\} \{\circ\circ\circ\} \dots \{\circ\circ\circ\}}_{\lambda_3} \dots$$

Если на месте кружочков расставить все элементы множества M , то мы получим некоторое разбиение множества M , имеющее заданный тип $1^{\lambda_1} 2^{\lambda_2} 3^{\lambda_3} \dots n^{\lambda_n}$. Всего существует $n!$ способов размещения элементов в такой конструкции. При этом разные размещения могут давать одно и то же разбиение. Так, элементы, находящиеся внутри одного подмножества, могут быть переставлены произвольным образом. Количество таких перестановок внутри одного подмножества мощности k равно $k!$, для всех подмножеств мощности k оно равно $(k!)^{\lambda_k}$, а для всех подмножеств разбиения —

$\prod_{k=1}^n (k!)^{\lambda_k}$. Все полученные при этом разбиения будут одинаковы-

ми. Также могут быть переставлены между собой подмножества одной мощности — все полученные при этом разбиения также будут одинаковыми. Число перестановок λ_k подмножеств мощности

k равно $\lambda_k!$, для всего разбиения — $\prod_{k=1}^n \lambda_k!$. На основании ска-

занного получим формулу для числа разбиений заданного типа $1^{\lambda_1} 2^{\lambda_2} 3^{\lambda_3} \dots n^{\lambda_n}$:

$$\frac{n!}{(2!)^{\lambda_2} \cdot (3!)^{\lambda_3} \cdot \dots \cdot (n!)^{\lambda_n} \cdot (\lambda_1!) \cdot (\lambda_2!) \cdot \dots \cdot (\lambda_n!)}.$$

Числом Стирлинга второго рода S_n^m называют количество способов разбиения n -элементного множества на m непустых подмножеств:

$$S_n^m = \sum_{\substack{(\lambda_1 \dots \lambda_n) \\ \lambda_i \geq 0 \\ \sum \lambda_i = m \\ \sum i \lambda_i = n}} \frac{n!}{(2!)^{\lambda_2} \cdot (3!)^{\lambda_3} \cdot \dots \cdot (n!)^{\lambda_n} \cdot (\lambda_1!) \cdot (\lambda_2!) \cdot \dots \cdot (\lambda_n!)}.$$

1.3.3. Рекуррентная формула для чисел Стирлинга второго рода. Очевидно, что $S_n^1 = S_n^n = 1$. Возьмем множество M' , состоящее из $n - 1$ элементов: $|M'| = n - 1$. Его можно разбить на m подмножеств S_{n-1}^m способами. Добавим к множеству M' еще один элемент и рассмотрим теперь количество способов разбиения на m подмножеств нового множества M , состоящего из n элементов. Возможные разбиения нового множества будут состоять из

разбиений, в которых новый элемент образует отдельное подмножество, и разбиений, в которых новый элемент входит в некоторое подмножество вместе с другими элементами. Очевидно, что число разбиений, где новый элемент образует отдельное подмножество, будет равно числу разбиений исходного множества $\mathcal{M}'$ на $m - 1$ подмножеств, т.е. S_{n-1}^{m-1} . Если же новый элемент входит в некоторое подмножество вместе с другими (а всего должно существовать m таких подмножеств), новое разбиение будет однозначно задаваться разбиением множества $\mathcal{M}'$ на m подмножеств и выбором подмножества, в которое добавлен новый элемент. Число таких разбиений составит mS_{n-1}^m . Таким образом, получена рекуррентная формула для чисел Стирлинга второго рода:

$$S_n^m = S_{n-1}^{m-1} + mS_{n-1}^m$$

с граничными условиями $S_0^0 = 1$, $S_n^0 = 0$, $S_n^n = 1$, $n \geq 1$.

В табл. 1.2 приведены значения чисел Стирлинга второго рода для небольших значений параметров n и m .

Таблица 1.2

n	m								
	0	1	2	3	4	5	6	7	...
0	1								
1	0	1							
2	0	1	1						
3	0	1	3	1					
4	0	1	7	6	1				
5	0	1	15	25	10	1			
6	0	1	31	90	65	15	1		
7	0	1	63	301	350	140	21	1	
...									

1.4. Подстановки на конечном множестве

Подстановки на конечном множестве являются фундаментальным математическим понятием, возникшим прежде всего в алгебре, но также широко используемым и в других разделах дискретной математики, в том числе в комбинаторике. Мы не будем касаться алгебраических свойств подстановок, ограничившись только основными понятиями, необходимыми для комбинаторных приложений.

1.4.1. Определение подстановки. Пусть множество $\mathcal{M} = \{1, 2, \dots, n\}$. Подстановкой на множестве $\mathcal{M}$ называется взаимно однозначное отображение множества $\mathcal{M}$ на себя:

$$\pi : \mathcal{M} \rightarrow \mathcal{M}, \quad |\mathcal{M}| = n.$$

Если обозначить $\pi(i) = \pi_i \in \mathcal{M}$, то подстановка π может быть задана двустрочной таблицей

$$\pi : \begin{pmatrix} 1 & 2 & \dots & n \\ \pi_1 & \pi_2 & \dots & \pi_n \end{pmatrix}, \quad \pi_i \neq \pi_j.$$

Нижняя строка таблицы является *перестановкой* элементов множества $\mathcal{M}$.

На множестве подстановок может быть определена операция произведения как композиция соответствующих отображений множества $\mathcal{M}$. Произведение подстановок не является коммутативной операцией: в общем случае $\pi_1 \circ \pi_2 \neq \pi_2 \circ \pi_1$. Множество всех подстановок $S_n = \{\pi | \pi : \mathcal{M} \rightarrow \mathcal{M}\}$ образует группу относительно введенной операции — *симметрическую группу степени n* ; ее порядок $|S_n| = n!$.

1.4.2. Порождение всех подстановок в лексикографическом порядке. Приведем алгоритм генерации подстановок в лексикографическом порядке. Обозначим через $\pi_1, \dots, \pi_n$ элементы, соответствующие элементам $1, \dots, n$ для подстановки π : $\pi(i) = \pi_i$.

Алгоритм, порождающий все подстановки в лексикографическом порядке:

1. Выбираем в качестве текущей подстановки тождественную.
2. Выводим текущую подстановку.
3. Находим такое максимальное i , что $\pi_i < \pi_{i+1}$.

4. Находим π_j — такой наименьший элемент справа от π_i , что $\pi_j > \pi_i$.

5. Меняем местами π_i и π_j .

6. «Переворачиваем» последовательность $\pi_{i+1} \dots \pi_n$.

7. Переходим к п. 2.

На псевдоязыке программирования соответствующая программа будет выглядеть следующим образом:

Input: n ;

Output: *все $n!$ подстановок в лексикографическом порядке.*

for $j=0$ **to** n **do**

$\pi_j \leftarrow j, i \leftarrow 1$

while $i \neq 0$ **do**

вывести $\Pi = (\pi_1, \pi_2, \dots, \pi_n)$

найти самое правое место, где $\pi_i < \pi_{i+1}$:

$i \leftarrow (n - 1)$

while $\pi_i > \pi_{i+1}$ **do**

$i \leftarrow i - 1$

найти π_i , наименьший элемент справа от π_j и больший его:

$i \leftarrow n$

while $\pi_i > \pi_j$ **do**

$j \leftarrow j - 1$

поменять местами π_i и π_j , а затем «перевернуть» $\pi_{i+1}, \dots, \pi_1$:

$\pi_i \leftrightarrow \pi_j$

$r \leftarrow n,$

$s \leftarrow i + 1$

while $r > s$ **do**

$\pi_r \leftrightarrow \pi_s,$

$r \leftarrow r - 1,$

$s \leftarrow s + 1.$

1.5. Числа Стирлинга первого рода

В разд. 1.3 упоминалось, что числа Стирлинга первого рода можно определить как коэффициенты, появляющиеся при разложении обобщенной степени x по обычным степеням x . Однако мы отдадим предпочтение более комбинаторному подходу, определяющему числа Стирлинга первого рода через цикловую структуру подстановок.

1.5.1. Цикловая структура подстановки. Любая подстановка может быть представлена как произведение независимых циклов. Например:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 0 \\ 4 & 3 & 2 & 7 & 0 & 6 & 1 & 5 & 9 & 8 \end{pmatrix} = (1, 4, 7)(2, 3)(5, 0, 8)(6)(9).$$

Цикловая структура подстановки обозначается как $1^{\lambda_1} 2^{\lambda_2} 3^{\lambda_3} \dots n^{\lambda_n}$, если в разложении в произведение независимых циклов она представима в виде произведения λ_1 циклов длиной 1, λ_2 циклов длиной 2 и т. д.

Найдем число подстановок на множестве $\mathcal{M} = \{1, 2, \dots, n\}$ с фиксированной цикловой структурой $1^{\lambda_1} 2^{\lambda_2} 3^{\lambda_3} \dots n^{\lambda_n}$. Для этого рассмотрим следующую конструкцию:

$$\underbrace{\left(\begin{array}{c} \circ \\ \circ \end{array} \right) \left(\begin{array}{c} \circ \\ \circ \end{array} \right) \dots \left(\begin{array}{c} \circ \\ \circ \end{array} \right)}_{\lambda_1} \underbrace{\left(\begin{array}{cc} \circ & \circ \end{array} \right) \left(\begin{array}{cc} \circ & \circ \end{array} \right) \dots \left(\begin{array}{cc} \circ & \circ \end{array} \right)}_{\lambda_2} \underbrace{\left(\begin{array}{ccc} \circ & \circ & \circ \end{array} \right) \left(\begin{array}{ccc} \circ & \circ & \circ \end{array} \right) \dots \left(\begin{array}{ccc} \circ & \circ & \circ \end{array} \right)}_{\lambda_3} \dots$$

По аналогии с числом разбиений рассмотрим все возможные заполнения этой строки элементами из множества $\mathcal{M}$. Всего таких заполнений $n!$. При этом любые перестановки циклов одинаковой длины не изменяют подстановку. Число перестановок циклов длины k равно $\lambda_k!$, для всей подстановки их $\prod_{k=1}^n \lambda_k!$. Любые циклические перемещения элементов внутри одного цикла (например, переход от цикла $(\sigma_1, \sigma_2, \dots, \sigma_{n-1}, \sigma_n)$ к циклу $(\sigma_n, \sigma_1, \sigma_2, \dots, \sigma_{n-1})$) также не приводят к ее изменению, всего возможно k таких перемещений внутри цикла длины k и k^{λ_k} внутри всех циклов длины k нашей подстановки. Таким образом, число различных подстановок из S_n , имеющих заданную цикловую структуру $1^{\lambda_1} 2^{\lambda_2} 3^{\lambda_3} \dots n^{\lambda_n}$, равно

$$\frac{n!}{\lambda_1! \cdot \lambda_2! \cdot \dots \cdot \lambda_n! \cdot 1^{\lambda_1} \cdot 2^{\lambda_2} \cdot \dots \cdot n^{\lambda_n}}.$$

Числа Стирлинга первого рода s_n^m задаются следующим образом:

$$s_n^m = (-1)^{n-m} s(n, m),$$

где $s(n, m)$ — число подстановок из S_n , разлагающихся на m независимых циклов.

В общем виде число Стирлинга первого рода s_n^m задается выражением

$$s_n^m = (-1)^{n-m} \sum_{\substack{(\lambda_1, \dots, \lambda_n) \\ \lambda_i \geq 0 \\ \sum i\lambda_i = n \\ \sum \lambda_i = m}} \frac{n!}{\lambda_1! \lambda_2! \cdot \dots \cdot \lambda_n! \cdot 1^{\lambda_1} 2^{\lambda_2} \cdot \dots \cdot n^{\lambda_n}}.$$

1.5.2. Рекуррентная формула для чисел Стирлинга первого рода. Найдем рекуррентное соотношение для чисел Стирлинга первого рода. Очевидно, что $s_n^0 = 0$ и $s_n^n = 1$. Рассмотрим множество подстановок на множестве $\mathcal{M}'$ из $n - 1$ элементов. Существует $s(n - 1, m)$ подстановок на множестве $\mathcal{M}'$, разлагающихся на m независимых циклов. Добавим еще один элемент к множеству $\mathcal{M}'$. Множество подстановок, разлагающихся на m независимых циклов и определенных на новом множестве $\mathcal{M}$, $|\mathcal{M}| = n$, будет состоять из подстановок, в которых добавленный элемент отображается сам в себя, образуя цикл длины 1 (всего будет $s(n - 1, m - 1)$ таких подстановок), и подстановок, где новый элемент присоединен к одному из существующих циклов подстановки на $\mathcal{M}'$. Элемент может быть помещен в любую позицию любого существующего цикла (т.е. занять место после любого элемента старого множества). Всего существует $s(n - 1, m)$ подстановок на исходном множестве, состоящих из m независимых циклов, и $(n - 1)$ способов «поставить» новый элемент после одного из элементов старого множества. Рекуррентная формула для числа подстановок, таким образом, будет иметь вид

$$s(n, m) = s(n - 1, m - 1) + (n - 1) \cdot s(n - 1, m).$$

Поскольку $s_n^m = (-1)^{n-m} s(n, m)$, очевидно, что s_n^m и s_{n-1}^{m-1} всегда будут иметь одинаковый знак, а s_n^m и s_{n-1}^m — всегда противоположный. В итоге рекуррентная формула для чисел Стирлинга первого рода принимает вид

$$s_n^m = s_{n-1}^{m-1} - (n-1)s_{n-1}^m$$

с граничными условиями $s_0^0 = 1$, $s_n^0 = 0$, $s_n^n = 1$, $n \geq 1$.

В табл. 1.3 приведены числа Стирлинга первого рода для больших значений параметров n и m .

Таблица 1.3

n	m							
		1	2	3	4	5	6	...
0	1							
1	0	1						
2	0	-1	1					
3	0	2	-3	1				
4	0	-6	11	-6	1			
5	0	24	-50	35	-10	1		
6	0	-120	274	-225	85	-15	1	
...	...							...

1.6. Урновые схемы

Урновыми называют схемы распределения объектов данной природы по некоторому множеству классов: шаров по урнам, частиц по ячейкам и т. п. Объекты (шары) могут быть различимыми или неразличимыми и иметься в том или ином количестве; независимо от этого урны могут различаться по виду, вместимости и др. Порядок объектов, помещаемых в одну урну, учитывается или не учитывается. Подобные задачи имеют тесную связь с размещениями и сочетаниями, однако ввиду достаточной специфичности и большой распространенности имеет смысл рассматривать их отдельным образом.

1.6.1. Классификация простейших урновых схем. Пусть имеется k урн и n шаров, размещаемых по урнам. В табл. 1.4 приведено число способов размещения n шаров по k урнам при разных условиях.

Таблица 1.4

№	Различимы ли шары?	Различимы ли урны?	Может ли урна быть пустой? Если нет $\Rightarrow n \geq k$	Число способов размещения n шаров по k урнам
1	Да	Да	Да	k^n
2	Да	Да	Нет	$k!S_n^k$
3	Нет	Да	Да	$\bar{C}_k^n = C_{k+n-1}^n$
4	Нет	Да	Нет	$\bar{C}_k^{n-k} = C_{n-1}^{k-1}$
5	Да	Нет	Да	$S_n^1 + S_n^2 + \dots + S_n^k$
6	Да	Нет	Нет	S_n^k
7	Нет	Нет	Да	$P_1(n) + P_2(n) + \dots + P_k(n)$
8	Нет	Нет	Нет	$P_k(n)$

Задачи, связанные с урновыми схемами при наличии ограничений на число шаров того или иного типа, а также на вместимость той или иной урны, решают более сложными методами, например с помощью теории производящих функций (гл. 4).

1.6.2. Одна задача статистической физики. В этой модели урны различимы и интерпретируются как энергетические уровни некоторой физической системы, шары — элементарные частицы, которые могут находиться на том или ином энергетическом уровне. Состояние физической системы описывается тем, сколько частиц находится на том или ином энергетическом уровне.

Пусть имеется n элементарных частиц и N возможных энергетических уровней. Требуется найти вероятность любого конкретного состояния, в частности, вероятность того, что каждая урна с номером $1 \dots n$ содержит ровно по одному шару. На рис. 1.2 показаны вероятности таких состояний при дополнительных условиях: различимы шары или неразличимы и будет ли урна содержать не более одного шара (принцип исключения Паули) или может содержать неограниченное число шаров. Из рисунка понятно, что при высоких температурах (когда значение N — велико) все стати-

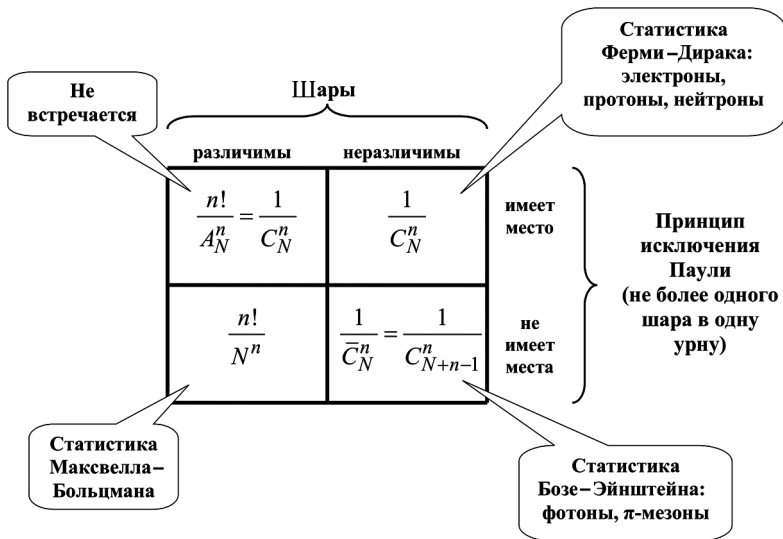


Рис. 1.2

стики сходятся к статистике Максвелла — Больцмана. При низких температурах (при небольших N) статистики неодинаковы, что проявляется в различных физических явлениях, наблюдаемых при сверхнизких температурах.

1.7. Схемы отображений конечных множеств

Рассмотрим еще одну комбинаторную схему: отображение конечного множества $\mathcal{A}$ в конечное множество $\mathcal{B}$, где $|\mathcal{A}| = n$ и $|\mathcal{B}| = m$.

1.7.1. Классификация отображений $\mathcal{A} \rightarrow \mathcal{B}$. Отображение может принадлежать одному из следующих типов:

1) *инъективные*

$$\forall a_i, a_j \in \mathcal{A}, a_i \neq a_j \Rightarrow f(a_i) \neq f(a_j)$$

(в этом случае $|\mathcal{A}| \leq |\mathcal{B}|$);

2) *сюръективные*

$$\forall b \in \mathcal{B} \Rightarrow \exists a \in \mathcal{A}: f(a) = b \text{ (в этом случае } |\mathcal{A}| \geq |\mathcal{B}| \text{)}.$$

3) *биективные*

$$\forall b \in \mathcal{B} \exists! a \in \mathcal{A}: f(a) = b \text{ (в этом случае } |\mathcal{A}| = |\mathcal{B}| \text{)}.$$

Найдем число различных отображений из $\mathcal{A}$ в $\mathcal{B}$.

Число всех отображений из $\mathcal{A}$ в $\mathcal{B}$ равно n^m .

Число инъективных отображений ($n \leq m$) равно

$$m(m-1)(m-2) \cdot \dots \cdot (m-n+1) = \frac{m!}{(m-n)!} = \mathcal{A}_m^n.$$

Число сюръективных отображений ($n \geq m$) равно $S_n^m m!$, так как подобное отображение подразумевает разбиение множества $\mathcal{A}$ на m непустых групп (по соответствию элементам множества $\mathcal{B}$), причем группы различимы между собой (поскольку различимы элементы множества $\mathcal{B}$).

Число биективных отображений ($n = m$) равно $n! = m!$.

1.7.2. Число отображений $\mathcal{A} \rightarrow \mathcal{B}$ для разных типов элементов в множествах и разных типов отображений. В табл. 1.5 приведена классификация отображений конечных множеств $\mathcal{A} \rightarrow \mathcal{B}$, где $|\mathcal{A}| = n$, $|\mathcal{B}| = m$.

Таблица 1.5

№	Элементы $\mathcal{A}$	Элементы $\mathcal{B}$	Число отображений	Число инъекций ($n \leq m$)	Число сюръекций ($n \geq m$)	Число биекций ($n = m$)
1	Различимы	Различимы	m^n	$(m)_n$	$m! S_n^m$	$n!$
2	Не различимы	Различимы	C_{n+m-1}^n	C_m^n	C_{n-1}^{m-1}	1
3	Различимы	Не различимы	$\sum_{k=1}^m S_n^k$	1	S_n^m	1
4	Не различимы	Не различимы	$\sum_{k=1}^m P_k(n)$	1	$P_m(n)$	1

1.8. Задачи

1. Сколькими способами можно разместить n_1 белых, n_2 черных, n_3 красных шаров по m урнам?

2. Найти число упорядоченных разбиений числа n ровно на k частей и число всех упорядоченных разбиений числа n .

3. Показать, что величина $\tilde{P}(n) = P(n) - P(n-1)$, $n \geq 1$ есть число разбиений n на части, большие 1. Вывести отсюда неравенство $P(n+2) - 2P(n+1) + P(n) \geq 0$.

4. Сколько последовательностей длины $n + m$ можно составить из n нулей и m единиц, в записи которых общее число пар 01 и 10 равно: а) $2r - 1$; б) $2r$.

5. Доказать равенства: а) $\sum_{k=m}^n C_k^m = C_{n+1}^{m+1}$; б) $\sum_{k=0}^n (C_n^k)^2 = C_{2n}^n$.

6. Доказать двумя способами равенство $C_n^m C_m^k = C_n^k C_{n-k}^{m-k}$.

7. Доказать равенство $C_n^0 + C_{n+1}^1 + \dots + C_{n+r}^r = C_{n+r+1}^r$.

8. Найти суммы: а) $\sum_{k=0}^n 2^k C_n^k$; б) $\sum_{k=1}^n k C_n^k 2^{n-k}$.

9. Доказать рекуррентное соотношение для чисел Стирлинга второго рода

$$S_{n+1}^k = \sum_{j=k-1}^n C_n^j S_j^{k-1}.$$

10. Число Белла $B(n)$ равно числу всех возможных разбиений n -элементного множества, т. е. $B(n) = S_n^1 + S_n^2 + \dots + S_n^n$. Доказать рекуррентное соотношение

$$B(n+1) = \sum_{i=0}^n C_n^i B(n-i) = \sum_{i=0}^n C_n^i B(i), \quad B(0) = 1.$$

11. Доказать правильность заполнения табл. 1.4—1.5.

Глава 2. ФОРМУЛА ВКЛЮЧЕНИЯ-ИСКЛЮЧЕНИЯ

Формула включения-исключения часто характеризуется как пример использования логических методов в комбинаторике. Этот подход, известный еще со времен Бернулли, получил развитие и в так называемых формулах обращения. В этой главе мы остановимся на классической формулировке принципа включения-исключения и наиболее важных случаях его применения.

2.1. Характеристическая функция множества

При изучении алгебры множеств очень полезным оказывается понятие характеристической функции множества. Определим характеристическую функцию множества $\mathcal{A}$ как

$$\varphi_{\mathcal{A}}(x) = \begin{cases} 1 & \text{при } x \in \mathcal{A}; \\ 0 & \text{при } x \notin \mathcal{A}. \end{cases}$$

Очевидно, что будут справедливы соотношения

$$\varphi_{\mathcal{A} \cap \mathcal{B}} = \varphi_{\mathcal{A}} \varphi_{\mathcal{B}}, \quad \varphi_{\mathcal{A} \cup \mathcal{B}} = \varphi_{\mathcal{A}} + \varphi_{\mathcal{B}} - \varphi_{\mathcal{A}} \varphi_{\mathcal{B}},$$

$$\varphi_{\bar{\mathcal{A}}} = 1 - \varphi_{\mathcal{A}}.$$

Для конечных множеств характеристическая функция позволяет использовать следующее выражение для мощности множества:

$$|\mathcal{A}| = \sum_x \varphi_{\mathcal{A}}(x).$$

Лемма 2.1. *Справедливо равенство*

$$\begin{aligned}
 (1 - a_1)(1 - a_2) \cdot \dots \cdot (1 - a_n) &= \prod_{i=1}^n (1 - a_i) = \\
 &= 1 - \sum_{k=1}^n a_k + \sum_{1 \leq k_1 < k_2 \leq n} a_{k_1} a_{k_2} - \sum_{1 \leq k_1 < k_2 < k_3 \leq n} a_{k_1} a_{k_2} a_{k_3} + \dots \\
 &\quad \dots + (-1)^n \sum_{1 \leq k_1 < \dots < k_n \leq n} a_{k_1} \cdot \dots \cdot a_{k_n}.
 \end{aligned}$$

Доказательство. Докажем лемму, используя метод математической индукции. Для $n = 1$ выражение верно: $(1 - a_1) = 1 - a_1$. Запишем выражение для n , предположив, что и для $n - 1$ оно верно:

$$\begin{aligned}
 \prod_{i=1}^n (1 - a_i) &= \left(\prod_{i=1}^{n-1} (1 - a_i) \right) (1 - a_n) = \\
 &= \left(1 + \sum_{i=1}^{n-1} (-1)^i \left(\sum_{1 \leq k_1 < \dots < k_i \leq n-1} \prod_{m=1}^i a_{k_m} \right) \right) (1 - a_n).
 \end{aligned}$$

Обозначим $S(n) = \sum_{i=1}^n (-1)^i \left(\sum_{1 \leq k_1 < \dots < k_i \leq n} \prod_{m=1}^i a_{k_m} \right)$. В таком случае после раскрытия скобок рассматриваемое выражение примет вид

$$\prod_{i=1}^n (1 - a_i) = 1 + S(n - 1) - a_n - a_n S(n - 1).$$

Произведя почленное суммирование, получим выражение

$$\begin{aligned}
 \prod_{i=1}^n (1 - a_i) &= 1 - \left(a_n + \sum_{1 \leq k_1 \leq n-1} a_{k_1} \right) + \\
 &\quad + \left(\sum_{1 \leq k_1 < k_2 \leq n-1} a_{k_1} a_{k_2} + \sum_{1 \leq k_1 \leq n-1} a_{k_1} a_n \right) -
 \end{aligned}$$

$$- \left(\sum_{1 \leq k_1 < k_2 < k_3 \leq n-1} a_{k_1} a_{k_2} a_{k_3} + \sum_{1 \leq k_1 < k_2 \leq n-1} a_{k_1} a_{k_2} a_n \right) + \dots =$$

$$= 1 + S(n).$$

Лемма доказана. $\square$

Найдем характеристическую функцию для объединения n множеств $\mathcal{A}_1 \cup \mathcal{A}_2 \cup \dots \cup \mathcal{A}_n$. Так как

$$\mathcal{A}_1 \cup \mathcal{A}_2 \cup \dots \cup \mathcal{A}_n = \overline{\overline{\mathcal{A}_1} \cap \overline{\mathcal{A}_2} \cap \dots \cap \overline{\mathcal{A}_n}},$$

то характеристическая функция

$$\varphi_{\mathcal{A}_1 \cup \mathcal{A}_2 \cup \dots \cup \mathcal{A}_n} = 1 - \prod_{i=1}^n (1 - \varphi_{\mathcal{A}_i}).$$

Тогда с помощью доказанной выше леммы может быть получена следующая формула для мощности объединения конечного числа множеств:

$$\begin{aligned} |\mathcal{A}_1 \cup \mathcal{A}_2 \cup \dots \cup \mathcal{A}_n| &= \sum_x \varphi_{\mathcal{A}_1 \cup \dots \cup \mathcal{A}_n}(x) = \\ &= \sum_x \sum_{i=1}^n (-1)^{i-1} \left(\sum_{1 \leq k_1 < \dots < k_i \leq n} \varphi_{\mathcal{A}_{k_1}}(x) \cdot \dots \cdot \varphi_{\mathcal{A}_{k_i}}(x) \right) = \\ &= \sum_x \sum_{i=1}^n (-1)^{i-1} \left(\sum_{1 \leq k_1 < \dots < k_i \leq n} \varphi_{\mathcal{A}_{k_1} \cap \dots \cap \mathcal{A}_{k_i}}(x) \right) = \\ &= \sum_{i=1}^n (-1)^{i-1} \left(\sum_{1 \leq k_1 < \dots < k_i \leq n} \sum_x \varphi_{\mathcal{A}_{k_1} \cap \dots \cap \mathcal{A}_{k_i}}(x) \right) = \\ &= \sum_{i=1}^n (-1)^{i-1} \left(\sum_{1 \leq k_1 < \dots < k_i \leq n} \left| \bigcap_{s=1}^i \mathcal{A}_{k_s} \right| \right). \quad (2.1) \end{aligned}$$

2.2. Число элементов, удовлетворяющих тем или иным свойствам

Ниже дадим классическую формулировку принципа включения-исключения (иначе формулы включения-исключения).

Рассмотрим множество $\mathcal{A}$, $|\mathcal{A}| = N$; пусть задано n свойств, при этом элементы множества $\mathcal{A}$ могут обладать или не обладать свойствами из заданного набора. Обозначим через N_i — число элементов, обладающих свойством i , а через $N_{i_1, \dots, i_k}$ — число элементов, обладающих свойствами $i_1, \dots, i_k$. В таком случае $N(0)$ — число элементов, не обладающих ни одним свойством, будет выражаться формулой, называемой *формулой включения-исключения**

Теорема 2.1. *Рассмотрим множество $\mathcal{A}$, $|\mathcal{A}| = N$, элементы которого могут обладать теми или иными из n свойств. Тогда количество элементов, не обладающих ни одним свойством*

$$N(0) = N - \sum_{1 \leq i \leq n} N_i + \sum_{1 \leq i_1 < i_2 \leq n} N_{i_1 i_2} - \sum_{1 \leq i_1 < i_2 < i_3 \leq n} N_{i_1 i_2 i_3} + \dots + (-1)^n N_{i_1 i_2 \dots i_n}. \quad (2.2)$$

Доказательство. Справедливость теоремы следует из формулы (2.1) и выражения $N(0) = |\mathcal{A}| - |\mathcal{A}_1 \cup \mathcal{A}_2 \cup \dots \cup \mathcal{A}_n|$, где $\mathcal{A}_i$ — множество элементов, обладающих i -м свойством. $\square$

Дадим другое доказательство формулы (2.2). Покажем, что элемент, обладающий $s > 0$ свойствами, не будет учтен в правой части (2.2). Действительно, в первом слагаемом он будет учтен один раз, во 2-м — s раз, в 3-м — C_s^2 раз и т. д. В результате получим, что этот элемент в правой части (2.2) будет учтен 0 раз, так как $1 - s + C_s^2 - C_s^3 + \dots + (-1)^s C_s^s = 0$. Этот подход позволяет найти число элементов, обладающих ровно k свойствами.

Теорема 2.2. *Рассмотрим множество $\mathcal{A}$, $|\mathcal{A}| = N$, элементы которого могут обладать теми или иными из n свойств. Тогда количество элементов, обладающих ровно k свойствами,*

$$N(k) = \sum_{1 \leq i_1 < \dots < i_k \leq n} N_{i_1 \dots i_k} - C_{k+1}^k \times$$

*См. ниже формулу (2.2).

$$\begin{aligned} & \times \sum_{1 \leq i_1 < \dots < i_{k+1} \leq n} N_{i_1 \dots i_{k+1}} + C_{k+2}^k \times \\ & \times \sum_{1 \leq i_1 < \dots < i_{k+2} \leq n} N_{i_1 \dots i_{k+2}} - \dots + (-1)^{n-k} C_n^k N_{i_1 i_2 \dots i_n}. \quad (2.3) \end{aligned}$$

Доказательство. Элемент, обладающий ровно k свойствами, будет учтен в сумме $\sum_{1 \leq i_1 < \dots < i_k \leq n} N_{i_1 \dots i_k}$ ровно один раз и не будет учтен ни в одной из оставшихся сумм правой части (2.3). Элемент, обладающий $t > k$ свойствами, будет учтен в первой сумме C_t^k раз, во второй — $C_{k+1}^k C_t^{k+1}$ раз и т. д. В итоге такой элемент будет учтен 0 раз, так как

$$C_t^k - C_{k+1}^k C_t^{k+1} + C_{k+2}^k C_t^{k+2} - \dots + (-1)^{t-k} C_t^k C_t^t = 0.$$

□

2.3. Приложения формулы включения-исключения

Из всех многочисленных приложений формулы включения-исключения остановимся на ее применении при вычислении значения функции Эйлера и решении классической задачи о беспорядках.

2.3.1. Функция Эйлера $\varphi(n)$. Эта функция широко используется не только в алгебре и теории чисел, но и в таких прикладных науках, как криптография. Значение $\varphi(n)$ определено на множестве $\mathbb{N}$ натуральных чисел и равняется количеству натуральных чисел, не превосходящих n и взаимно простых с n .

Теорема 2.3. Если разложение числа n на простые множители имеет вид $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, $\alpha_i \geq 1$, то значение функции Эйлера $\varphi(n)$ задается формулой

$$\varphi(n) = (p_1^{\alpha_1} - p_1^{\alpha_1-1})(p_2^{\alpha_2} - p_2^{\alpha_2-1}) \dots (p_k^{\alpha_k} - p_k^{\alpha_k-1}).$$

Доказательство. Рассмотрим множество чисел $\mathcal{A} = \{1, \dots, n\}$. На этом множестве зададим i -е свойство как делимость числа на простое число p_i . Тогда искомая величина равняется количеству элементов из $\mathcal{A} = \{1, \dots, n\}$, не обладающих ни одним из k свойств. По формуле включения-исключения

$$N(0) = N - \sum_{1 \leq i \leq k} N_i + \sum_{1 \leq i_1 < i_2 \leq k} N_{i_1 i_2} - \\ - \sum_{1 \leq i_1 < i_2 < i_3 \leq k} N_{i_1 i_2 i_3} + \dots + (-1)^k N_{i_1 i_2 \dots i_k}.$$

Число элементов, обладающих свойством i , очевидным образом равно $N_i = \frac{n}{p_i}$. Аналогично число элементов, обладающих свойствами $i_1, \dots, i_k$ равно $N_{i_1, \dots, i_k} = \frac{n}{p_{i_1} \dots p_{i_k}}$. Таким образом,

$$\varphi(n) = n - \sum_{1 \leq i \leq k} \frac{n}{p_i} + \sum_{1 \leq i_1 < i_2 \leq k} \frac{n}{p_{i_1} p_{i_2}} - \dots + (-1)^k \frac{n}{p_1 p_2 \dots p_k} = \\ = n \left(1 - \sum_{1 \leq i \leq k} \frac{1}{p_i} + \sum_{1 \leq i_1 < i_2 \leq k} \frac{1}{p_{i_1} p_{i_2}} - \dots + (-1)^k \frac{1}{p_1 p_2 \dots p_k} \right) = \\ = n \prod_{i=1}^k \left(1 - \frac{1}{p_i} \right) = (p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}) \prod_{i=1}^k \left(1 - \frac{1}{p_i} \right) = \\ = \prod_{i=1}^k (p_i^{\alpha_i} - p_i^{\alpha_i - 1}).$$

□

2.3.2. Задача о беспорядках *Беспорядком* называют подстановку на множестве $\mathcal{A} = \{1, \dots, n\}$, в которой ни один элемент не переходит в себя, т. е. $\pi(i) \neq i$ для всех i . Определим число беспорядков на n элементах. Общее число подстановок на n элементах равно $n!$. Будем говорить, что подстановка $\pi \in S_n$ обладает «свойством i », если $\pi(i) = i$. Элемент i , для которого $\pi(i) = i$, называют *неподвижным элементом* подстановки π . Тогда $D(n)$ — число беспорядков на n элементах — равно числу подстановок из S_n , не имеющих неподвижных элементов, т. е. не обладающих ни одним из свойств $1, \dots, n$:

$$D(n) = N(0) = N - \sum_{1 \leq i \leq n} N_i + \sum_{1 \leq i_1 < i_2 \leq n} N_{i_1 i_2} - \\ - \sum_{1 \leq i_1 < i_2 < i_3 \leq n} N_{i_1 i_2 i_3} + \dots + (-1)^n N_{i_1 i_2 \dots i_n}.$$

Поскольку существует $(n-k)!$ подстановок из S_n с заданными k неподвижными элементами, то $N_{i_1 i_2 \dots i_k} = (n-k)!$. В результате получаем выражение

$$N(0) = n! - C_n^1(n-1)! + C_n^2(n-2)! - \\ - C_n^3(n-3)! + \dots + (-1)^n C_n^n(n-n)!.$$

Так как $C_n^k(n-k)! = \frac{n!}{k!}$, выражение для $D(n)$ принимает вид

$$D(n) = n! - \frac{n!}{1!} + \frac{n!}{2!} - \frac{n!}{3!} + \dots + (-1)^n \frac{n!}{n!} = \\ = n! \left(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \dots + (-1)^n \frac{1}{n!} \right).$$

Учитывая, что $e^{-1} = \sum_{k=0}^{\infty} \frac{(-1)^k}{k!}$, получим выражение, справедливое для больших n :

$$D(n) \approx \frac{n!}{e}.$$

2.4. Задачи

1. Сколько чисел, не превосходящих 10^4 , не делятся на 5, 9, 15, 18?

2. Сколько чисел, лежащих в интервале $[100, 700]$, взаимно просты с 5, 8, 14, 20?

3. Пусть $n = 210k$. Доказать, что количество чисел, не превосходящих n и не делящихся на 2, 3, 5, 7, равно $48k$.

4. Найти число способов расстановки восьми ладей на шахматной доске таким образом, чтобы они не били друг друга и главная белая диагональ была свободна от фигур.

5. Найти число булевых функций от n переменных, у которых нет фиктивных переменных.

6. Найти число таких размещений n шаров по k урнам, чтобы все урны были заполнены.

7. Решить задачу 1 из гл. 1 при условии, что не должно быть пустых урн.

8. Пользуясь формулой включения-исключения, выразить число сюръекций n -элементного множества на k -элементное без помощи чисел Стирлинга второго рода. Получить отсюда следующее явное выражение для чисел Стирлинга второго рода:

$$S_n^k = \frac{1}{k!} \sum_{j=0}^k (-1)^j C_k^j (k-j)^n.$$

9. Пусть $D(n)$ — число беспорядков на n элементах. Доказать следующие рекуррентные соотношения:

а) $D(n) = nD(n-1) + (-1)^n$;

б) $D(n) = (n-1)(D(n-1) + D(n-2))$.

10. *Задача о встречах.* Найти число подстановок из S_n , каждая из которых имеет ровно k неподвижных элементов.

Глава 3. ЛИНЕЙНЫЕ РЕКУРРЕНТНЫЕ ПОСЛЕДОВАТЕЛЬНОСТИ

В гл. 1 уже рассматривались рекуррентные соотношения для биномиальных коэффициентов, чисел Стирлинга первого и второго рода, чисел Белла — соотношения, выражающие величину, определяемую одним или несколькими параметрами через аналогичные величины с меньшими значениями параметров. Идеальным решением является формула, явно выражающая значение нашей величины через значения определяющих ее параметров. Примером может служить алгебраическое выражение для биномиальных коэффициентов: $C_n^k = \frac{n!}{k!(n-k)!}$. Однако в общем случае, для произвольного рекуррентного соотношения методы получения таких выражений неизвестны. В настоящей главе рассмотрим класс рекуррентных соотношений — линейных рекуррентных соотношений с постоянными коэффициентами, для которых эта задача легко разрешима.

3.1. Основные понятия и определения

Определение 3.1. Рассмотрим бесконечную числовую последовательность $\{a_n\} = a_0, a_1, a_2, \dots$, для членов которой выполняется соотношение

$$a_n + C_1 a_{n-1} + C_2 a_{n-2} + \dots + C_k a_{n-k} = 0. \quad (3.1)$$

Такая последовательность называется *однородной линейной рекуррентной последовательностью порядка k* , а соотношение (3.1) — *однородным линейным рекуррентным соотношением порядка k* .

Пример 3.1. Рассмотрим последовательность Фибоначчи $\{f_n\}$, а именно — однородную линейную рекуррентную последовательностью второго порядка, задаваемую соотношением $f_n - f_{n-1} - f_{n-2} = 0$ и начальными условиями $f_0 = 0, f_1 = 1$. Тогда $\{f_n\} = 0, 1, 1, 2, 3, 5, 8, 13, \dots$

Последовательность $\{a_n\}$, удовлетворяющая соотношению

$$a_n + C_1 a_{n-1} + C_2 a_{n-2} + \dots + C_k a_{n-k} = C, \quad (3.2)$$

где $C \neq 0$, называется *неоднородной линейной рекуррентной последовательностью порядка k* .

Последовательность $\{a_n\}$ является *решением* линейного рекуррентного соотношения порядка k , если *любые* $k + 1$ ее последовательных членов удовлетворяют или соотношению (3.1) или (3.2).

Поставим в соответствие однородному линейному рекуррентному соотношению (3.1) *характеристический многочлен*:

$$P(x) = x^k + C_1 x^{k-1} + \dots + C_{k-1} x + C_k, \quad (3.3)$$

где коэффициенты C_i взяты из соотношения (3.1).

Так, характеристический многочлен для последовательности Фибоначчи $P(x) = x^2 - x - 1$.

3.2. Линейное пространство линейных рекуррентных последовательностей

Напомним, что *линейное пространство* над полем $\mathbb{F}$ — это множество $\mathcal{L} = \{\mathbf{x}\}$, для элементов которого определены две операции:

- 1) операция сложения $\mathbf{x} + \mathbf{y} = \mathbf{z}, \mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathcal{L}$;
- 2) операция умножения на константу $\lambda \mathbf{x} = \mathbf{y}, \mathbf{x}, \mathbf{y} \in \mathcal{L}; \lambda \in \mathbb{F}$.

При этом множество $\mathcal{L}$ образует абелеву группу относительно операции сложения, т. е. операция сложения:

- ассоциативна;
- коммутативна;
- $\exists \mathbf{0} \in \mathcal{L} : \forall \mathbf{x} \in \mathcal{L} : \mathbf{x} + \mathbf{0} = \mathbf{x}$;
- $\forall \mathbf{x} \in \mathcal{L} \exists (-\mathbf{x}) \in \mathcal{L} : \mathbf{x} + (-\mathbf{x}) = \mathbf{0}$.

$$\text{Кроме того, } \forall \alpha, \beta \in \mathbb{F}, \forall \mathbf{x}, \mathbf{y} \in L \Rightarrow \begin{cases} (\alpha + \beta)\mathbf{x} = \alpha\mathbf{x} + \beta\mathbf{x}; \\ \alpha(\mathbf{x} + \mathbf{y}) = \alpha\mathbf{x} + \alpha\mathbf{y}; \\ (\alpha\beta)\mathbf{x} = \alpha(\beta\mathbf{x}); \end{cases}$$

$$\forall \mathbf{x} \in L \Rightarrow 0 \cdot \mathbf{x} = \underline{0}; \quad 1 \cdot \mathbf{x} = \mathbf{x}.$$

Для того чтобы множество $B = \{\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_m\}$ элементов линейного пространства $\mathcal{L}$ являлось *базисом* этого пространства, должны выполняться условия:

1) линейная независимость

$$\alpha_1 \mathbf{x}_1 + \alpha_2 \mathbf{x}_2 + \dots + \alpha_m \mathbf{x}_m = \underline{0} \Leftrightarrow \alpha_1 = \dots = \alpha_m = 0;$$

2) полнота

$$\forall \mathbf{y} \in \mathcal{L} \quad \exists \alpha_1, \dots, \alpha_m : \mathbf{y} = \alpha_1 \mathbf{x}_1 + \alpha_2 \mathbf{x}_2 + \dots + \alpha_m \mathbf{x}_m.$$

Если B — базис, то представление элемента $\mathbf{y} \in \mathcal{L}$ в виде

$$\mathbf{y} = \alpha_1 \cdot \mathbf{x}_1 + \alpha_2 \cdot \mathbf{x}_2 + \dots + \alpha_m \cdot \mathbf{x}_m$$

называется *разложением* по базису B . Любой элемент линейного пространства $\mathcal{L}$ *будет иметь единственное разложение по базису* B . Докажем это. Предположим, что элемент y имеет два разложения:

$$\mathbf{y} = \sum_{i=1}^m \alpha_i \mathbf{x}_i = \sum_{i=1}^m \beta_i \mathbf{x}_i,$$

тогда

$$\sum_{i=1}^m \beta_i \mathbf{x}_i - \sum_{i=1}^m \alpha_i \mathbf{x}_i = \sum_{i=1}^m (\beta_i - \alpha_i) \mathbf{x}_i = \mathbf{y} - \mathbf{y} = \underline{0}.$$

Из линейной независимости базисных векторов следует, что $\beta_i - \alpha_i = 0$ для всех $i = 1, \dots, m$.

Рассмотрим множество *всех* последовательностей над полем $\mathbb{F}$ ($\mathbb{F} = \mathbb{R}$ или $\mathbb{F} = \mathbb{C}$), удовлетворяющих фиксированному соотношению (3.1). Любая такая последовательность будет однозначно определяться своими первыми k членами. Введем на множестве этих рекуррентных последовательностей операции:

1) суммирования $\{a_n\} + \{b_n\} = \{c_n\}$, где $c_n = a_n + b_n$, $n = 0, 1, 2, \dots$;

2) умножения на константу $\lambda \cdot \{a_n\} = \{b_n\}$, где $b_n = \lambda a_n$, $n = 0, 1, 2, \dots$.

Докажем, что множество таких последовательностей представляет собой линейное пространство над полем $\mathbb{F}$ относительно введенных выше операций.

Пусть L — множество всех последовательностей над полем $\mathbb{F}$, удовлетворяющих фиксированному соотношению (3.1). Докажем, что для любых последовательностей $\{a_n\}, \{b_n\} \in L$ их сумма $\{a_n\} + \{b_n\} = \{a_n + b_n\} \in L$. Действительно, пусть $z_n = a_n + b_n$. Подставим члены последовательности $\{z_n\}$ в соотношение (3.1):

$$\begin{aligned} z_n + C_1 z_{n-1} + \dots + C_k z_{n-k} &= \\ &= (a_n + b_n) + C_1(a_{n-1} + b_{n-1}) + \dots + C_k(a_{n-k} + b_{n-k}) = \\ &= (a_n + C_1 a_{n-1} + \dots + C_k a_{n-k}) + \\ &\quad + (b_n + C_1 b_{n-1} + \dots + C_k b_{n-k}) = 0 + 0 = 0. \end{aligned}$$

Аналогично докажем, что для всех $\{a_n\} \in L$, $\alpha \in \mathbb{F}$ последовательность $\alpha \{a_n\} = \{\alpha a_n\} \in L$. Таким образом, доказано, что на множестве L операции сложения и умножения на константу определены корректно. Нулевым элементом является последовательность $\{0\} = 0, 0, \dots, 0, \dots$. Выполнение аксиом линейного пространства — очевидно.

Теорема 3.1. Для того чтобы последовательности $\{a_n^{(1)}\}, \dots, \{a_n^{(k)}\}$ образовывали базис линейного пространства L , необходимо и достаточно выполнения следующего условия:

$$\det \begin{pmatrix} a_0^{(1)} & a_0^{(2)} & \dots & a_0^{(k)} \\ a_1^{(1)} & a_1^{(2)} & \dots & a_1^{(k)} \\ \vdots & \vdots & \ddots & \vdots \\ a_{k-1}^{(1)} & a_{k-1}^{(2)} & \dots & a_{k-1}^{(k)} \end{pmatrix} \neq 0.$$

Доказательство. Докажем достаточность условия. Допустим, что

$$\beta_1 \{a_n^{(1)}\} + \beta_2 \{a_n^{(2)}\} + \dots + \beta_k \{a_n^{(k)}\} = \{0\} = 0, 0, \dots, 0, \dots$$

Тогда для первых k элементов последовательности $\{0\}$ верна система линейных уравнений

$$\begin{cases} a_0^{(1)}\beta_1 + a_0^{(2)}\beta_2 + \dots + a_0^{(k)}\beta_k = 0, \\ a_1^{(1)}\beta_1 + a_1^{(2)}\beta_2 + \dots + a_1^{(k)}\beta_k = 0, \\ \dots \quad \dots \quad \dots \quad \dots \quad \dots \\ a_{k-1}^{(1)}\beta_1 + a_{k-1}^{(2)}\beta_2 + \dots + a_{k-1}^{(k)}\beta_k = 0. \end{cases} \quad (3.4)$$

Так как определитель матрицы этой системы не равен нулю, то единственное решение имеет вид $\beta_1 = \beta_2 = \dots = \beta_k = 0$. Тем самым доказана линейная независимость для множества $\{a_n^{(1)}\}, \dots, \{a_n^{(k)}\}$.

Рассмотрим теперь произвольную последовательность $\{b_n\} \in L$ и попытаемся выразить ее как линейную комбинацию $\{b_n\} = \beta_1\{a_n^{(1)}\} + \beta_2\{a_n^{(2)}\} + \dots + \beta_k\{a_n^{(k)}\}$. Тогда для первых k элементов получаем систему линейных уравнений

$$\begin{cases} a_0^{(1)}\beta_1 + a_0^{(2)}\beta_2 + \dots + a_0^{(k)}\beta_k = b_0, \\ a_1^{(1)}\beta_1 + a_1^{(2)}\beta_2 + \dots + a_1^{(k)}\beta_k = b_1, \\ \dots \quad \dots \quad \dots \quad \dots \quad \dots \\ a_{k-1}^{(1)}\beta_1 + a_{k-1}^{(2)}\beta_2 + \dots + a_{k-1}^{(k)}\beta_k = b_{k-1}. \end{cases} \quad (3.5)$$

Так как определитель матрицы этой системы не равен нулю, получим единственное решение $\beta_1, \beta_2, \dots, \beta_k$. Тогда последовательности $\{b_n\}$ и $\beta_1\{a_n^{(1)}\} + \beta_2\{a_n^{(2)}\} + \dots + \beta_k\{a_n^{(k)}\}$ удовлетворяют соотношению (3.1) и совпадают на первых k элементах. Поскольку первые k элементов однозначно определяют последовательность из пространства L , получаем, что последовательности $\{b_n\}$ и $\beta_1\{a_n^{(1)}\} + \beta_2\{a_n^{(2)}\} + \dots + \beta_k\{a_n^{(k)}\}$ тождественно совпадают. Тем самым доказана полнота множества $\{a_n^{(1)}\}, \dots, \{a_n^{(k)}\}$. Таким образом, $\{a_n^{(1)}\}, \dots, \{a_n^{(k)}\}$ образуют базис линейного пространства L .

Для доказательства необходимости предположим, что последовательности $\{a_n^{(1)}\}, \dots, \{a_n^{(k)}\}$ образуют базис линейного про-

пространства L , при этом определитель

$$\det \begin{pmatrix} a_0^{(1)} & a_0^{(2)} & \dots & a_0^{(k)} \\ a_1^{(1)} & a_1^{(2)} & \dots & a_1^{(k)} \\ \vdots & \vdots & \ddots & \vdots \\ a_{k-1}^{(1)} & a_{k-1}^{(2)} & \dots & a_{k-1}^{(k)} \end{pmatrix} = 0.$$

Тогда система (3.4) имеет нетривиальные решения, что противоречит линейной независимости множества $\{a_n^{(1)}\}, \dots, \{a_n^{(k)}\}$. $\square$

3.3. Решение линейных рекуррентных соотношений

Выражение для произвольного члена линейного однородного рекуррентного соотношения может иметь один из следующих видов.

Задано соотношение вида (3.1). Общее решение будет

$$\{b_n\} = \beta_1 \{a_n^{(1)}\} + \beta_2 \{a_n^{(2)}\} + \dots + \beta_k \{a_n^{(k)}\},$$

где $\{a_n^{(1)}\}, \{a_n^{(2)}\}, \dots, \{a_n^{(k)}\}$ — некоторый базис линейного пространства L ; $\beta_1, \beta_2, \dots, \beta_k$ — произвольные коэффициенты.

Заданы соотношение (3.1) и начальные значения $b_0, b_1, \dots, b_{k-1}$. В таком случае решением будет единственная последовательность вида

$$\{b_n\} = \beta_1 \{a_n^{(1)}\} + \beta_2 \{a_n^{(2)}\} + \dots + \beta_k \{a_n^{(k)}\},$$

где коэффициенты $\beta_1, \beta_2, \dots, \beta_k$ однозначно находят из системы линейных уравнений (3.5).

Задача, таким образом, сводится к нахождению базиса линейного пространства, образованного множеством всех последовательностей, удовлетворяющих фиксированному рекуррентному соотношению (3.1).

3.3.1. Случай простых корней. Будем строить базисные последовательности с помощью корней характеристического многочлена $P(x)$.

Лемма 3.1. Пусть

$$P(x) = C_0 x^k + C_1 x^{k-1} + \dots + C_{k-1} x + C_k, \quad C_0 = 1, \quad C_k \neq 0$$

— характеристический многочлен соотношения (3.1), а $\lambda \neq 0$ — корень этого многочлена. Тогда последовательность $\{\lambda^n\} = 1, \lambda, \lambda^2, \lambda^3, \dots, \lambda^n, \dots$ удовлетворяет соотношению (3.1).

Доказательство. Подставим члены последовательности $\{\lambda^n\}$ в соотношение (3.1). Так как $\lambda \neq 0$, получаем

$$\begin{aligned} C_0 a_n + \dots + C_k a_{n-k} &= \\ &= C_0 \lambda^n + \dots + C_k \lambda^{n-k} = \lambda^{n-k} (C_0 \lambda^k + \dots + C_k) = 0. \end{aligned}$$

□

Будем искать базис пространства L в виде набора последовательностей, образованных степенями корней характеристического многочлена $P(x)$.

Теорема 3.2. Пусть характеристический многочлен $P(x)$ линейного однородного рекуррентного соотношения (3.1) не имеет кратных корней и $\lambda_1, \lambda_2, \dots, \lambda_k$ — его корни. Тогда последовательности $\{\lambda_1^n\}, \dots, \{\lambda_k^n\}$ образуют базис пространства L .

Доказательство. В силу леммы 3.1 все последовательности $\{\lambda_i^n\}$ удовлетворяют соотношению (3.1), т.е. лежат в пространстве L .

Определитель, образованный первыми k элементами последовательностей $\{\lambda_1^n\}, \dots, \{\lambda_k^n\}$, имеет вид

$$\begin{vmatrix} 1 & 1 & \dots & 1 \\ \lambda_1 & \lambda_2 & \dots & \lambda_k \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_1^{k-1} & \lambda_2^{k-1} & \dots & \lambda_k^{k-1} \end{vmatrix}.$$

Определитель такого вида называют *определителем Вандермонда*:

$$\begin{vmatrix} 1 & 1 & \dots & 1 \\ \lambda_1 & \lambda_2 & \dots & \lambda_k \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_1^{k-1} & \lambda_2^{k-1} & \dots & \lambda_k^{k-1} \end{vmatrix} = \prod_{i < j} (\lambda_j - \lambda_i).$$

В нашем случае все корни $\lambda_1, \lambda_2, \dots, \lambda_k$ различны, следовательно, $\prod_{i < j} (\lambda_j - \lambda_i) \neq 0$. Из теоремы, доказанной в предыдущем разделе, следует, что последовательности $\{\lambda_1^n\}, \dots, \{\lambda_k^n\}$ образуют базис пространства L . $\square$

В таком случае общее решение линейного однородного рекуррентного соотношения выглядит следующим образом:

$$\{a_n\} = \beta_1 \{\lambda_1^n\} + \beta_2 \{\lambda_2^n\} + \dots + \beta_k \{\lambda_k^n\},$$

а его n -й член $a_n = \beta_1 \lambda_1^n + \beta_2 \lambda_2^n + \dots + \beta_k \lambda_k^n$.

Замечание. Приведенное выше выражение для определителя Вандермонда можно доказать, используя метод математической индукции:

$$\begin{aligned} & \begin{vmatrix} 1 & 1 \\ \lambda_1 & \lambda_2 \end{vmatrix} = \lambda_2 - \lambda_1; \\ & \begin{vmatrix} 1 & 1 & \dots & 1 \\ \lambda_1 & \lambda_2 & \dots & \lambda_k \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_1^{k-1} & \lambda_2^{k-1} & \dots & \lambda_k^{k-1} \end{vmatrix} = \\ & = \begin{vmatrix} 1 & 1 & \dots & 1 \\ 0 & \lambda_2 - \lambda_1 & \dots & \lambda_k - \lambda_1 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \lambda_2^{k-1} - \lambda_2^{k-2} \lambda_1 & \dots & \lambda_k^{k-1} - \lambda_k^{k-2} \lambda_1 \end{vmatrix} = \\ & = \begin{vmatrix} \lambda_2 - \lambda_1 & \lambda_3 - \lambda_1 & \dots & \lambda_k - \lambda_1 \\ \lambda_2(\lambda_2 - \lambda_1) & \lambda_3(\lambda_3 - \lambda_1) & \dots & \lambda_k(\lambda_k - \lambda_1) \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_2^{k-2}(\lambda_2 - \lambda_1) & \lambda_3^{k-2}(\lambda_3 - \lambda_1) & \dots & \lambda_k^{k-2}(\lambda_k - \lambda_1) \end{vmatrix} = \\ & = \left(\prod_{i=2}^k (\lambda_i - \lambda_1) \right) \cdot \begin{vmatrix} 1 & 1 & \dots & 1 \\ \lambda_2 & \lambda_3 & \dots & \lambda_k \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_2^{k-2} & \lambda_3^{k-2} & \dots & \lambda_k^{k-2} \end{vmatrix}. \end{aligned}$$

Таким образом,

$$\begin{vmatrix} 1 & 1 & \cdots & 1 \\ \lambda_1 & \lambda_2 & \cdots & \lambda_k \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_1^{k-1} & \lambda_2^{k-1} & \cdots & \lambda_k^{k-1} \end{vmatrix} = \prod_{i < j} (\lambda_j - \lambda_i) \neq 0.$$

Далее в приложении будет рассмотрен случай кратных корней у характеристического многочлена $P(x)$. Если некоторый корень λ многочлена $P(x)$ имеет кратность m , ему будут соответствовать следующие базисные последовательности:

$$\{\lambda^n\}, \{n\lambda^n\}, \dots, \{n^{m-1}\lambda^n\}.$$

3.3.2. Случай комплексных корней. Специально выделим случай, когда характеристический многочлен имеет комплексные корни, а все коэффициенты в (3.1) являются действительными числами.

Пусть характеристический многочлен $P(x)$ имеет комплексный корень $\lambda_1 = \rho(\cos \varphi + i \sin \varphi)$. Тогда сопряженное число

$$\lambda_2 = \rho(\cos \varphi - i \sin \varphi) = \rho(\cos(-\varphi) + i \sin(-\varphi))$$

также будет корнем многочлена $P(x)$. Соответствующие базисные последовательности имеют вид

$$\{\lambda_1^n\} = \rho^n(\cos n\varphi + i \sin n\varphi),$$

$$\{\lambda_2^n\} = \rho^n(\cos n(-\varphi) + i \sin n(-\varphi)) = \rho^n(\cos n\varphi - i \sin n\varphi).$$

Очевидно, что если к системе базисных векторов любого линейного пространства применить невырожденное линейное преобразование, то полученная в результате этого система векторов также будет базисной. Применим к системе базисных последовательностей линейного пространства L невырожденное линейное

преобразование

$$\begin{pmatrix} \frac{1}{2} & -\frac{i}{2} & 0 & \cdots & 0 \\ \frac{1}{2} & \frac{i}{2} & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}.$$

Тогда

$$\begin{pmatrix} \lambda_1^0 & \lambda_2^0 & \cdots & \lambda_k^0 \\ \lambda_1^1 & \lambda_2^1 & \cdots & \lambda_k^1 \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_1^{k-1} & \lambda_2^{k-1} & \cdots & \lambda_k^{k-1} \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{2} & -\frac{i}{2} & 0 & \cdots & 0 \\ \frac{1}{2} & \frac{i}{2} & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix} =$$

$$= \begin{pmatrix} \left(\frac{1}{2}\lambda_1^0 + \frac{1}{2}\lambda_2^0\right) & \left(-\frac{i}{2}\lambda_1^0 + \frac{i}{2}\lambda_2^0\right) & \lambda_3^0 & \cdots & \lambda_k^0 \\ \left(\frac{1}{2}\lambda_1^1 + \frac{1}{2}\lambda_2^1\right) & \left(-\frac{i}{2}\lambda_1^1 + \frac{i}{2}\lambda_2^1\right) & \lambda_3^1 & \cdots & \lambda_k^1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \left(\frac{1}{2}\lambda_1^{k-1} + \frac{1}{2}\lambda_2^{k-1}\right) & \left(-\frac{i}{2}\lambda_1^{k-1} + \frac{i}{2}\lambda_2^{k-1}\right) & \lambda_3^{k-1} & \cdots & \lambda_k^{k-1} \end{pmatrix}.$$

В результате получаем систему базисных последовательностей, в которой пара комплексных последовательностей $\{\lambda_1^n\} = \rho^n(\cos n\varphi + i \sin n\varphi)$, $\{\lambda_2^n\} = \rho^n(\cos n\varphi - i \sin n\varphi)$ преобразована в пару действительных последовательностей $\{\rho^n \cos n\varphi\}$, $\{\rho^n \sin n\varphi\}$. То же самое можно проделать и с последовательностями, соответствующими другим парам комплексно сопряженных корней.

3.3.3. Решение неоднородных линейных рекуррентных соотношений. Напомним, что если $C_0 = 1$, $C \neq 0$, то соотношение вида

$$C_0 a_n + C_1 a_{n-1} + \dots + C_k a_{n-k} = C$$

задает линейную неоднородную рекуррентную последовательность.

Теорема 3.3. *Общее решение неоднородного линейного рекуррентного соотношения представляется в виде суммы некоторого его частного решения и общего решения соответствующего однородного соотношения (3.1).*

Доказательство. Пусть $\{a_n\}$ — некоторое фиксированное частное решение неоднородного соотношения, $\{a'_n\}$ — другое его частное решение. Очевидно, что последовательность $\{\tilde{a}_n\} = \{a'_n\} - \{a_n\}$ удовлетворяет соответствующему однородному соотношению. Доказательство того, что любая вышеописанная сумма является решением, проводится аналогично. $\square$

Частное решение неоднородного рекуррентного соотношения

$$C_0 a_n + C_1 a_{n-1} + \dots + C_k a_{n-k} = C$$

можно, например, искать в виде постоянной последовательности $\{a_n = a\}$: так как в этом случае $C_0 a + C_1 a + \dots + C_k a = C$, то

$$a = \frac{C}{C_0 + C_1 + \dots + C_k} \quad (\text{при условии, что } C_0 + C_1 + \dots + C_k \neq 0).$$

Если же $\sum_{i=0}^k C_i = 0$, но $\sum_{i=1}^k i C_i \neq 0$, то существует частное решение вида $\{a_n = an\}$, где константа a находится из уравнения

$$C_0 an + C_1 a(n-1) + \dots + C_k a(n-k) = C,$$

получающегося в результате подстановки величин $\{a_n = an\}$ в соотношение (3.2). Учитывая равенство $\sum_{i=0}^k C_i = 0$, предыдущее уравнение сводится к уравнению

$$a \sum_{i=1}^k i C_i = -C,$$

откуда получаем

$$a = -\frac{C}{\sum_{i=1}^k iC_i}.$$

Таким образом, частное решение неоднородного линейного рекуррентного соотношения в этом случае имеет вид

$$\{a_n = -\frac{Cn}{\sum_{i=1}^k iC_i}\}.$$

Существует стандартный способ сведения неоднородного линейного рекуррентного соотношения порядка k к однородному рекуррентному линейному соотношению порядка $k+1$. Так как члены неоднородной линейной рекуррентной последовательности удовлетворяют равенствам

$$\begin{cases} C_0a_n + C_1a_{n-1} + \dots + C_ka_{n-k} = C, \\ C_0a_{n-1} + C_1a_{n-2} + \dots + C_ka_{n-k-1} = C, \end{cases}$$

то, вычитая из первого равенства второе, получаем, что для членов последовательности $\{a_n\}$ справедливо соотношение

$$C_0a_n + (C_1 - C_0)a_{n-1} + \dots + (C_k - C_{k-1})a_{n-k} - C_ka_{n-k-1} = 0.$$

Характеристический многочлен $P_1(x)$ полученной однородной рекуррентной последовательности получаем из характеристического многочлена $P(x)$ исходной последовательности умножением на $x-1$:

$$P_1(x) = P(x)(x-1).$$

3.4. Задачи

1. Решить однородные рекуррентные соотношения:

а) $a_{n+3} + 3a_{n+2} + 3a_{n+1} + a_n = 0$;

б) $a_{n+3} + 10a_{n+2} + 32a_{n+1} + 32a_n = 0$;

в) $a_{n+3} - 3a_{n+2} + a_{n+1} - 3a_n = 0$, $a_0 = 3$, $a_1 = 7$, $a_2 = 27$;

г) $a_{n+2} - 2\cos \alpha a_{n+1} + a_n = 0$, $a_0 = \cos \alpha$, $a_1 = \cos 2\alpha$.

2. Дана рекуррентная последовательность $\{a_n\}$

$$a_{n+4} + 2a_{n+3} + 3a_{n+2} + 2a_{n+1} + a_n = 0;$$

$$a_0 = a_1 = a_3 = 0, \quad a_2 = -1.$$

Найти a_{100} .

3. Решить неоднородные рекуррентные соотношения:

а) $a_{n+1} - a_n = n, \quad a_0 = 1;$

б) $a_{n+2} + 2a_{n+1} - 8a_n = 27 \cdot 5^n, \quad a_0 = -9, \quad a_1 = 45;$

в) $a_{n+3} - 6a_{n+2} + 11a_{n+1} - 6a_n = 6n^2 - 4n - 17,$
 $a_0 = 3, \quad a_1 = 15, \quad a_2 = 41.$

4. Пусть $\{f_n\}$ последовательность Фибоначчи:

$f_n = f_{n-1} + f_{n-2}$ с начальными условиями $f_0 = 0; f_1 = 1$. Доказать справедливость следующих соотношений:

а) $f_{n+m} = f_{n-1}f_m + f_n f_{m+1};$

б) $\sum_{k=0}^n f_{2k+1} = f_{2n+2};$

в) $\sum_{k=0}^n f_{2k} = f_{2n+1} - 1;$

г) $f_{n+1}^3 + f_n^3 - f_{n-1}^3 = f_{3n}.$

5. Решить следующие нелинейные рекуррентные соотношения, сведя их к однородным линейным:

а) $a_{n+1} = a_n - a_{n+1}a_n, \quad a_0 = 1;$ б) $a_{n+2} = \frac{a_{n+1}^3}{a_n^2}, \quad a_0 = 1, \quad a_1 = e.$

Глава 4. ПРОИЗВОДЯЩИЕ ФУНКЦИИ

Метод производящих функций был и остается наиболее эффективным средством решения перечислительных комбинаторных задач, т.е. задач, в которых речь идет о нахождении числа тех или иных комбинаторных конфигураций. При этом решение соответствующей перечислительной задачи естественным образом оказывается связанным с изучением свойств числовых последовательностей, зависящих от одного или нескольких натуральных параметров. Рассмотрение производящей функции — формального степенного ряда от одного или нескольких переменных — дает возможность представить в свернутом виде наиболее существенную информацию о числовой последовательности, связанной с данной перечислительной задачей.

В основе используемого подхода к перечислительным задачам лежит следующий простой принцип. Вначале с помощью тех или иных комбинаторных соображений устанавливают взаимно однозначные соответствия между множествами различных дискретных структур, откуда затем выводят функциональные соотношения между производящими функциями этих множеств.

4.1. Энумераторы

Энумератором события называется выражение в котором взаимоисключающие исходы соединены операцией суммирования, а происходящие одновременно — операцией произведения. Такой выбор мотивирован тем, что выполнение комбинаторных правил суммы и произведения (см. гл. 1) обеспечивается свойством дистрибутивности указанных арифметических операций.

Действительно, рассмотрим два события: $\mathcal{A}$, имеющее n возможных элементарных исходов $(a_1, a_2, \dots, a_n)$, и $\mathcal{B}$, имеющее m возможных элементарных исходов $(b_1, b_2, \dots, b_m)$. Тогда энумератором события $\mathcal{A}$ является выражение $A = (a_1 + a_2 + \dots + a_n)$ — формальная сумма, где каждое слагаемое соответствует одному из элементарных исходов.

Аналогично энумератором события $\mathcal{B}$ является выражение $B = (b_1 + b_2 + \dots + b_m)$. Тогда энумераторы событий $\mathcal{A} + \mathcal{B}$ и $\mathcal{A} \cdot \mathcal{B}$ можно выразить через энумераторы событий $\mathcal{A}$ и $\mathcal{B}$:

$$A + B = a_1 + \dots + a_n + b_1 + \dots + b_m;$$

$$\begin{aligned} A \cdot B &= (a_1 + a_2 + \dots + a_n) \cdot (b_1 + b_2 + \dots + b_m) = \\ &= a_1 \cdot b_1 + a_1 \cdot b_2 + \dots + a_n \cdot b_m. \end{aligned}$$

При этом каждое слагаемое по-прежнему соответствует одному из возможных взаимоисключающих исходов, а все слагаемые описывают совокупность всех возможных исходов.

Рассмотрим, как используется это понятие при решении различных задач.

4.1.1. Сочетания. Рассмотрим множество всех возможных неупорядоченных выборок без возвращения из множества $X = \{x_1, \dots, x_n\}$. Обозначим через $\mathcal{A}_i$ событие, связанное с включением или невключением элемента x_i в выборку. Учитывая, что исход, соответствующий случаю, когда элемент не попадает в выборку, является нейтральным элементом относительно операции одновременной реализации двух исходов (выбор элемента x_1 и одновременно невыбор x_2 равнозначны просто выбору x_1), обозначим его знаком 1. В таком случае энумератор события $\mathcal{A}_i$ выглядит следующим образом:

$$A_i = x_i^0 + x_i^1 = 1 + x_i.$$

Тогда энумератор события выборки произвольного набора элементов из множества $X = \{x_1, \dots, x_n\}$ имеет вид

$$A = A_1 \cdot A_2 \cdot \dots \cdot A_n = (1 + x_1) \cdot (1 + x_2) \cdot \dots \cdot (1 + x_n).$$

Так, если множество X будет состоять из трех элементов, энумератор для выборки примет вид

$$A = A_1 A_2 A_3 = 1 + x_1 + x_2 + x_3 + x_1 x_2 + x_1 x_3 + x_2 x_3 + x_1 x_2 x_3.$$

Исходя из вышесказанного ответим на вопрос, *сколько существует выборок из X , содержащих k элементов, если $|X| = n$* . Для этого достаточно сосчитать количество слагаемых k -й степени в выражении

$$(1 + x_1)(1 + x_2) \cdot \dots \cdot (1 + x_n).$$

Если положить $x_1 = x_2 = \dots = x_n = x$, задача сводится к нахождению коэффициента при x^k в выражении $(1 + x)^n$. Очевидно, что искомый коэффициент равен C_n^k — уже известный нам результат, но полученный в данном примере из совершенно других соображений, чем в гл. 1.

4.1.2. Сочетания с повторениями. Энумератор события, связанного с включением элемента x_i в выборку с повторениями, выглядит следующим образом:

$$A_i = 1 + x_i + x_i^2 + x_i^3 + \dots$$

Тогда количество выборок, содержащих k элементов, определяется как количество слагаемых k -й степени в выражении

$$\prod_{i=1}^n (1 + x_i + x_i^2 + \dots),$$

которое является энумератором выборки с повторением из множества, содержащего n элементов.

Положив $x_1 = x_2 = \dots = x_n = x$, сведем задачу к определению коэффициента при x^k в выражении

$$(1 + x + x^2 + x^3 + \dots)^n.$$

Поскольку $1 + x + x^2 + \dots = \frac{1}{1 - x}$, задача сводится к разложению в ряд Тэйлора — Маклорена функции

$$f(x) = \frac{1}{(1 - x)^n}.$$

Последовательно производя дифференцирование, получим следующее выражение:

$$f^{(k)}(0) = \frac{(n + k - 1)!}{(n - 1)!}.$$

В таком случае разложение в ряд Тэйлора — Маклорена функции $\frac{1}{(1-x)^n}$ имеет вид

$$\frac{1}{(1-x)^n} = \sum_{k=0}^{\infty} \frac{(n+k-1)!}{(n-1)!k!} x^k$$

и, следовательно, искомым коэффициент

$$\bar{C}_n^k = \frac{(n+k-1)!}{(n-1)!k!} = C_{n+k-1}^k$$

— опять уже известный нам результат, но полученный с помощью функции энумератора.

4.1.3. Задача о размене доллара. Определим, сколькими способами можно разменять один доллар в американской монетной системе, т. е. используя монеты достоинством 1, 5, 10, 25 и 50 центов. Обозначим через $F(x_i)$ — энумератор события выбора монеты достоинством в i центов: $F(x_i) = 1 + x_i + x_i^2 + \dots$. Тогда энумератор события, состоящего в выборе каких-то наборов монет, имеет вид

$$\begin{aligned} E &= F(x_1) \cdot F(x_5) \cdot \dots \cdot F(x_{50}) = \\ &= (1 + x_1 + x_1^2 + \dots) \cdot \dots \cdot (1 + x_{50} + x_{50}^2 + \dots). \end{aligned}$$

Таким образом, задача о размене сводится к определению числа слагаемых в E , дающих сумму в 100 центов. Так как одновременный выбор монет достоинством m и n центов добавляет к получаемой сумме $m + n$ центов, задача сводится к нахождению коэффициента при x^{100} в выражении

$$\begin{aligned} E(x) &= (1 + x + x^2 + \dots)(1 + x^5 + x^{10} + \dots)(1 + x^{10} + x^{20} + \dots) \times \\ &\quad \times (1 + x^{25} + x^{50} + \dots)(1 + x^{50} + x^{100} + \dots) = \\ &= \frac{1}{(1-x)(1-x^5)(1-x^{10})(1-x^{25})(1-x^{50})}, \end{aligned}$$

которое на самом деле является некоторым степенным рядом.

Для нахождения искомого коэффициента применим следующий прием. Введя обозначения

$$\frac{1}{1-x} = A(x) = \sum_{i=0}^{\infty} a_i x^i;$$

$$\frac{1}{(1-x)(1-x^5)} = B(x) = \sum_{i=0}^{\infty} b_i x^i;$$

$$\frac{1}{(1-x)(1-x^5)(1-x^{10})} = C(x) = \sum_{i=0}^{\infty} c_i x^i;$$

$$\frac{1}{(1-x)(1-x^5)(1-x^{10})(1-x^{15})} = D(x) = \sum_{i=0}^{\infty} d_i x^i;$$

$$\frac{1}{(1-x)(1-x^5)(1-x^{10})(1-x^{25})(1-x^{50})} = E(x) = \sum_{i=0}^{\infty} e_i x^i,$$

получим следующие рекуррентные выражения для коэффициентов:

$$\begin{cases} A(x) = B(x)(1-x^5) \\ B(x) = C(x)(1-x^{10}) \\ C(x) = D(x)(1-x^{25}) \\ D(x) = E(x)(1-x^{50}) \end{cases} \Rightarrow \begin{cases} b_n = b_{n-5} + a_n \\ c_n = c_{n-10} + b_n \\ d_n = d_{n-25} + c_n \\ e_n = e_{n-50} + d_n \end{cases}$$

Имея рекуррентные соотношения для b_n, c_n, d_n, e_n и учитывая, что $a_n = 1$ для всех $n \geq 0$, находим e_{100} . Результаты вычисления приведены в табл. 4.1.

Таблица 4.1

n	0	5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100
a_n	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
b_n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
c_n	1	2	4	6	9	12	16	20	25	30	36	42	49	56	64	72	81	90	100	110	121
d_n	1	2	4	6	9	13					49					121					242
e_n	1										50										292

Таким образом, искомая величина $e_{100} = 292$.

4.1.4. Задача о заполнении полосы плитками. Требуется определить количество способов заполнения полосы длиной n и шириной 2 плитками длиной 2 и шириной 1, которые можно класть как вертикально, так и горизонтально. Обозначим через F энумератор события, состоящего в правильном заполнении полосы шириной 2. Каждое слагаемое F соответствует тому или иному заполнению полосы некоторой длины, а весь энумератор F является «суммой» всех возможных заполнений для полос всех возможных длин:

$$F = \emptyset + \boxed{} + \boxed{}\boxed{} + \boxed{}\boxed{} + \boxed{}\boxed{}\boxed{} + \boxed{}\boxed{}\boxed{} + \boxed{}\boxed{}\boxed{} + \dots$$

Интересующая нас величина равна числу слагаемых в F , имеющих длину n .

Если каждую плитку в энумераторе F заменить на x , то укладке длиной n будет соответствовать слагаемое x^n и, следовательно, интересующая нас величина будет равна коэффициенту при x^n в ряде $F(x)$, получаемом из энумератора F с помощью такой замены:

$$\begin{aligned} F(x) &= 1 + x + x^2 + x^2 + x^3 + x^3 + x^3 + \dots = \\ &= 1 + x + 2x^2 + 3x^3 + \dots \end{aligned}$$

Рассмотрим повнимательнее строение энумератора F . Так как первым элементом любой укладки может быть либо один вертикальный блок, либо два горизонтальных, либо пустое множество (если укладка является пустой), слагаемые в F можно перегруппировать следующим образом:

$$\begin{aligned} F &= \emptyset + \boxed{} + \boxed{}\boxed{} + \boxed{}\boxed{} + \boxed{}\boxed{}\boxed{} + \boxed{}\boxed{}\boxed{} + \dots = \\ &= \emptyset + \boxed{} (\emptyset + \boxed{} + \boxed{}\boxed{} + \dots) + \\ &\quad + \boxed{}\boxed{} (\emptyset + \boxed{} + \boxed{}\boxed{} + \dots) . \end{aligned}$$

Следовательно, если α — выбор в качестве элемента для укладки одного вертикально поставленного блока, а β — выбор в качестве элемента для укладки двух горизонтально поставленных друг

на друга блоков, то для энумератора F справедливо следующее выражение:

$$F = \oslash + \alpha F + \beta F. \quad (4.1)$$

Смысл выражения сводится к тому, что множество всех вариантов укладки представимо в виде объединения пустой укладки и результатов конкатенации укладок α и β со всеми возможными укладками. Тогда для интересующего нас ряда $F(x)$ из равенства (4.1) следует соотношение

$$F(x) = 1 + xF(x) + x^2F(x).$$

Выполнив очевидные алгебраические преобразования, получаем

$$F(x) = \frac{1}{1 - x - x^2}.$$

Будем искать коэффициент при x^n в $F(x)$. Представив $F(x)$ в виде ряда с неопределенными коэффициентами $F(x) = \sum_{n=0}^{\infty} a_n x^n$, получим соотношение $(a_0 + a_1 x + a_2 x^2 + \dots)(1 - x - x^2) = 1$. Таким образом, коэффициенты a_n удовлетворяют рекуррентному соотношению

$$\begin{cases} a_n - a_{n-1} - a_{n-2} = 0; \\ a_0 = a_1 = 1. \end{cases}$$

Найдем последовательность $\{a_n\}$. Эта последовательность является сдвинутой последовательностью Фибоначчи. Корнями характеристического многочлена $x^2 - x - 1$ служат

$$\lambda_1 = \frac{1 + \sqrt{5}}{2} \approx 1,62; \quad \lambda_2 = \frac{1 - \sqrt{5}}{2} \approx -0,62.$$

Таким образом, $a_n = C_1 \lambda_1^n + C_2 \lambda_2^n$. С учетом начальных условий получаем

$$\begin{cases} C_1 + C_2 = a_0 = 1 \\ C_1 \lambda_1 + C_2 \lambda_2 = a_1 = 1 \end{cases} \Leftrightarrow \begin{cases} C_2 = 1 - C_1 \\ C_1 \lambda_1 + (1 - C_1) \lambda_2 = 1 \end{cases} \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} C_1 = \frac{\lambda_2}{\lambda_1 - \lambda_2} = \frac{1 + \sqrt{5}}{2\sqrt{5}} \\ C_2 = \frac{\sqrt{5} - 1}{2\sqrt{5}} \end{cases};$$

$$a_n = \frac{1 + \sqrt{5}}{2\sqrt{5}} \left(\frac{1 + \sqrt{5}}{2} \right)^n + \frac{\sqrt{5} - 1}{2\sqrt{5}} \left(\frac{1 - \sqrt{5}}{2} \right)^n.$$

Оценим порядок a_n : $a_n \sim C_1 \cdot 1.62^n$, $C_1 = \frac{1 + \sqrt{5}}{2\sqrt{5}}$. Соответственно

$$a_{1000} \sim 0,72 \cdot 1,62^{1000} \approx 2,36 \cdot 10^{209}.$$

4.2. Формальные степенные ряды

Из рассмотренных в разд. 4.1 примеров видим, что приходится иметь дело с выражениями, аналогичными понятию степенного ряда, изучаемого в курсе математического анализа. Однако в отличие от рядов, рассматриваемых в математическом анализе, нас, как правило, не интересуют вопросы их сходимости. Такие степенные ряды называют формальными.

4.2.1. Определение. *Формальным степенным рядом над $\mathbb{R}$ называют выражение*

$$\sum_{i=0}^{\infty} c_i x^i = c_0 + c_1 x + c_2 x^2 + \dots + c_i x^i + \dots, \quad c_i \in \mathbb{R}.$$

Введем на множестве формальных степенных рядов $\mathbb{R}[[x]] = \left\{ \sum_{i=0}^{\infty} c_i x^i \right\}$ операции сложения и умножения: если $A(x) = a_0 + a_1 x + a_2 x^2 + \dots$, $B(x) = b_0 + b_1 x + b_2 x^2 + \dots$, то их сумма определяется как ряд

$$A(x) + B(x) = S(x) = s_0 + s_1 x + s_2 x^2 + \dots; \quad s_i = a_i + b_i;$$

а произведение — как ряд $A(x)B(x) = U(x) = u_0 + u_1 x +$

$+u_2x_2 + \dots$, где коэффициенты u_k определяются равенствами

$$\begin{aligned} u_0 &= a_0b_0, \\ u_1 &= a_0b_1 + a_1b_0, \\ u_2 &= a_0b_2 + a_1b_1 + a_2b_0, \\ &\dots \quad \dots \quad \dots \quad \dots \quad \dots \quad \dots \\ u_k &= \sum_{i=0}^k a_ib_{k-i}, \\ &\dots \quad \dots \quad \dots \quad \dots \quad \dots \quad \dots \end{aligned}$$

Относительно введенных операций множество формальных степенных рядов образует кольцо, а точнее — коммутативное кольцо с единицей. Кольцо многочленов над $\mathbb{R}$ можно рассматривать как подкольцо кольца формальных степенных рядов: $\mathbb{R}[x] \subset \mathbb{R}[[x]]$.

Формальный степенной ряд от двух переменных определяется следующим образом:

$$f(x, y) \in \mathbb{R}[[x, y]]; \quad f(x, y) = \sum_{n, m \geq 0} a_{n, m} x^n y^m.$$

Аналогичным образом определяется формальный степенной ряд от любого числа переменных.

Вернемся к множеству $\mathbb{R}[[x]]$. Оно естественным образом распадается на два подмножества:

$$\mathbb{R}[[x]]_0 = \{A(x) : a_0 = 0\} \text{ и } \mathbb{R}[[x]]_1 = \{A(x) : a_0 \neq 0\}.$$

Эти подмножества нам понадобятся в дальнейшем.

Дадим еще несколько определений. *Коэффициентным оператором* называют оператор $[x^i]$, действующий следующим образом: если дан ряд $A(x) = \sum_n a_n x^n$, то $[x^i]A(x) = a_i$.

Суммируемым семейством называют такое множество формальных степенных рядов $\mathcal{F} = \{F_i(x) \in \mathbb{R}[[x]]\}$, что для всех k только конечное число рядов имеет ненулевой коэффициент при x^k .

4.2.2. Композиция рядов. Рассмотрим два ряда: $A(x) = \sum a_n x^n$ и $B(x) = \sum b_n x^n$. *Композицией* этих рядов будет называться ряд

$$A(B(x)) = \sum a_n (B(x))^n = \sum c_n x^n.$$

Композиция рядов имеет смысл, если $\{a_0, a_1 B(x), a_2 B^2(x), a_3 B^3(x), \dots\}$ является суммируемым семейством.

Теорема 4.1. Если $B(x) \in \mathbb{R}[[x]]_0$, то композиция $A(B(x))$ имеет смысл.

Доказательство. Если $b_0 = 0$, слагаемые, формирующие композицию, имеют вид $a_n(b_1 x + b_2 x^2 + b_3 x^3 + \dots)^n$. Очевидно, что такое слагаемое, приведенное к виду $\sum \lambda_k x^k$, не будет содержать слагаемых степени $k < n$ и при этом для каждого k будет содержать конечное количество слагаемых степени k . Тогда вся композиция также будет содержать лишь конечное число слагаемых с x^n для каждого n . $\square$

4.2.3. Формальная производная и формальный интеграл.

Операторы *формальной производной* D_x и *формального интеграла* I_x определяют следующим образом: если дан ряд $A(x) = \sum_n a_n x^n$, то

$$D_x A(x) = \sum_{n=0}^{\infty} (n+1) a_{n+1} x^n;$$

$$I_x A(x) = \sum_{n=1}^{\infty} \frac{1}{n} a_{n-1} x^n.$$

Приведем несколько примеров свойств, выполняющихся для формальных рядов и демонстрирующих аналогию с функциями действительного переменного:

1) $D_x (I_x A(x)) = A(x);$

2) $I_x (D_x A(x)) = A(x) - a_0 = A(x) - A(0);$

3) обозначим через $\text{Exp}(x)$ ряд $\text{Exp}(x) = \sum_{n=0}^{\infty} \frac{1}{n!} x^n$, тогда

$$D_x \text{Exp}(x) = \text{Exp}(x);$$

4) пусть ряд от двух переменных $f(x, y) = \sum_{n=0}^{\infty} y(y-1) \cdot \dots \times (y-n+1) \frac{1}{n!} x^n$, обозначим его через $(1+x)^y$, тогда

$$D_x (1+x)^y = y(1+x)^{y-1}.$$

4.2.4. Свойства формальных степенных рядов. Из п. 4.2.2 и 4.2.3 видно, что формальные степенные ряды во многом ведут себя аналогично функциям от действительного переменного. При выполнении определенных условий можно также «делить» на степенной ряд и переходить к «обратному» ряду аналогично переходу к обратной функции.

Теорема о существовании функционально обратного ряда.

Если ряд $f(x) = xg(x)$, $g(x) \in \mathbb{R}[[x]]_1$, то существует однозначно определенный ряд $f^{[-1]}(x) \in \mathbb{R}[[x]]$ такой, что $f(f^{[-1]}(x)) = x$ и $f^{[-1]}(f(x)) = x$.

Доказательство. Пусть ряд $f(x) = a_1x + a_2x^2 + \dots$; $a_1 \neq 0$; ряд $f^{[-1]}(x)$ будем искать в виде $f^{[-1]}(x) = b_1x + b_2x^2 + \dots$. Рассмотрим композицию

$$\begin{aligned} f(f^{[-1]}(x)) &= a_1(b_1x + b_2x^2 + b_3x^3 + \dots) + \\ &\quad + a_2(b_1x + b_2x^2 + b_3x^3 + \dots)^2 + \\ &\quad + a_3(b_1x + b_2x^2 + b_3x^3 + \dots)^3 + \dots, \end{aligned}$$

тогда

$$\begin{aligned} f(f^{[-1]}(x)) &= (a_1b_1)x + \\ &\quad + (a_1b_2 + a_2b_1^2)x^2 + \\ &\quad + (a_1b_3 + 2a_2b_1b_2 + a_3b_1^3)x^3 + \dots \end{aligned}$$

Нам требуется, чтобы композиция этих рядов $f(f^{[-1]}(x)) = x$. Приравняв полученный выше ряд к x , получим систему линейных уравнений, связывающих коэффициенты a_i и b_i , причем при их последовательном решении в каждом следующем уравнении будет присутствовать только одна новая неизвестная.

В свою очередь, для композиции $f^{[-1]}(f(x))$ будет получен ряд

$$\begin{aligned} f^{[-1]}(f(x)) &= (a_1b_1)x + \\ &\quad + (a_2b_1 + a_1^2b_2)x^2 + \\ &\quad + (a_3b_1 + 2a_1a_2b_2 + a_1^3b_3)x^3 + \\ &\quad + \dots \end{aligned}$$

Если аналогично предыдущему случаю полученный ряд приравнять к x , получим также систему линейных уравнений, связывающих коэффициенты a_i и b_i , причем при их последовательном решении в каждом следующем уравнении будет присутствовать

только одна новая неизвестная. Заметим, что выражения для b_i в обоих случаях совпадают. Таким образом, ряд $f^{[-1]}(x)$ существует и определен однозначно. Теорема доказана. $\square$

Ряд $f^{[-1]}(x)$ называется *функционально обратным* ряду $f(x)$.

Теорема о существовании мультипликативно обратного ряда. Пусть ряд $f(x) \in \mathbb{R}[[x]]_1$. Тогда существует однозначно определенный ряд $f^{-1} \in \mathbb{R}[[x]]_1$ такой, что $f(x)f^{-1}(x) = 1$.

Доказательство. Пусть

$$\begin{aligned} f(x) &= a_0 + a_1x + a_2x^2 + \dots; \quad a_0 \neq 0; \\ f^{-1}(x) &= b_0 + b_1x + b_2x^2 + \dots \end{aligned}$$

Тогда $f(x)f^{-1}(x) = (a_0 + a_1x + a_2x^2 + \dots)(b_0 + b_1x + b_2x^2 + \dots)$.

Приравняв полученное произведение к 1, получим систему линейных уравнений

$$\begin{cases} a_0b_0 = 1; \\ a_0b_1 + a_1b_0 = 0; \\ a_0b_2 + a_1b_1 + a_2b_0 = 0; \\ a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0 = 0; \\ \dots \quad \dots \quad \dots \quad \dots \quad \dots \quad \dots \end{cases}$$

Каждое следующее уравнение будет содержать одно новое неизвестное по сравнению с предыдущими, при этом коэффициент при новом неизвестном $a_0 \neq 0$. В таком случае система будет иметь единственное решение. Теорема доказана. $\square$

Ряд $f^{-1}(x)$ называется *мультипликативным обратным* ряду $f(x)$ и часто обозначается как $\frac{1}{f(x)}$.

4.2.5. Определение производящей функции последовательности. Производящей функцией последовательности $\{a_n\} = a_0, a_1, a_2, \dots$ называют формальный степенной ряд вида

$$F(x) = a_0 + a_1x + a_2x^2 + \dots$$

В некоторых случаях этот ряд сходится, тогда производящая функция является некоторой функцией действительного переменного.

Рассмотрим несколько примеров производящих функций:

$$\left\{ \begin{array}{ll} \{a_n\} = 1, 1, 1, 1, \dots & \Rightarrow F_a(x) = \frac{1}{1-x}; \\ \{b_n\} = 1, 0, 1, 0, \dots & \Rightarrow F_b(x) = \frac{1}{1-x^2}; \\ \{c_n\} = 0, 1, 0, 1, \dots & \Rightarrow F_c(x) = \frac{x}{1-x^2}; \\ \{d_n\} = 1, 3, 3, 1, 0, 0, \dots & \Rightarrow F_d(x) = (1+x)^3. \end{array} \right.$$

Когда рассматривается множество элементов $a_{i_1, \dots, i_n}$ с несколькими индексами, соответствующая производящая функция будет иметь вид

$$F(x_1, \dots, x_n) = \sum_{i_1, \dots, i_n} a_{i_1, \dots, i_n} x_1^{i_1} \cdot \dots \cdot x_n^{i_n}.$$

4.3. Получение производящих функций

На примерах разд. 4.1 можно сформулировать следующий подход, описывающий использование метода производящих функций. Пусть нам необходимо определить значение комбинаторной величины a_n , зависящей от целочисленного параметра n . Обычно a_n — число комбинаторных конфигураций, характеризующихся параметром n . Исходя из некоторых, чаще всего комбинаторных, соображений строим производящую функцию — формальный степенной ряд, коэффициенты которого равны искомым величинам a_n . Анализируя этот ряд, находим выражение для коэффициента, стоящего при x^n , т. е. для величины a_n .

4.3.1. Комбинаторные конфигурации и их производящие функции. Определим *множество комбинаторных конфигураций* как множество S тех объектов, среди которых по условию задачи требуется провести отбор и подсчет.

Весовая функция $\omega : S \rightarrow \tilde{\mathbb{N}}$, где $\tilde{\mathbb{N}} = \mathbb{N} \cup \{0\}$.

Выбор весовой функции зависит от решаемой задачи. Например:

— в задаче поиска числа подмножеств мощности n целесообразно взять в качестве S множество всех подмножеств, а в качестве ω — мощность соответствующего подмножества;

— в задаче о заполнении полосы плитками взять в качестве S множество всех правильных заполнений полосы плитками, а в качестве ω — длину полосы, покрытой таким заполнением;

— в задаче о размене доллара взять в качестве S множество всех возможных наборов монет, а в качестве ω — стоимость соответствующего набора.

Задавая надлежащим образом S и ω , любую комбинаторную задачу перечислительного типа можно свести к поиску числа комбинаторных конфигураций заданного веса.

Обыкновенная производящая функция множества S относительно весовой функции ω определяется как сумма вида¹⁾

$$\Phi_S^{(\omega)}(x) = \sum_{\sigma \in S} x^{\omega(\sigma)}.$$

В этом случае **задача поиска числа комбинаторных конфигураций заданного веса сводится к вычислению коэффициента при x^n в производящей функции $\Phi_S^{(\omega)}(x)$:**

$$|\{\sigma \in S : \omega(\sigma) = n\}| = [x^n] \Phi_S^{(\omega)}(x).$$

4.3.2. Представление, сохраняющее вес. Пусть даны два множества комбинаторных конфигураций с заданными на них весовыми функциями: (S, ω) и (T, ω') . *Представление, сохраняющее вес*, — это такое взаимно однозначное отображение $(S, \omega) \rightarrow (T, \omega')$, что $\forall \sigma \leftrightarrow \tau$ выполняется равенство $\omega(\sigma) = \omega'(\tau)$. Непосредственно из определения следует равенство соответствующих производящих функций

$$\Phi_S^{(\omega)}(x) = \Phi_T^{(\omega')}(x).$$

Понятие представления является формальным выражением известного приема взаимно однозначного соответствия между множеством интересующих нас комбинаторных конфигураций и другим множеством, более удобным для перечисления. При этом для нового множества конфигураций могут оказаться применимы следующие леммы, существенно упрощающие построение соответствующей производящей функции.

¹⁾Когда весовая функция ясна из контекста, верхний индекс (ω) в записи производящей функции будет, как правило, опускаться.

Лемма о сумме. Пусть на множестве S задана весовая функция ω и выделены подмножества $A, B \subset S$, $A \cap B = \emptyset$. Тогда

$$\Phi_{A \cup B}^{(\omega)}(x) = \Phi_A^{(\omega)}(x) + \Phi_B^{(\omega)}(x).$$

Доказательство.

$$\begin{aligned} \Phi_{A \cup B}^{(\omega)}(x) &= \sum_{\sigma \in A \cup B} x^{\omega(\sigma)} = \sum_{\sigma \in A} x^{\omega(\sigma)} + \sum_{\sigma \in B} x^{\omega(\sigma)} = \\ &= \Phi_A^{(\omega)}(x) + \Phi_B^{(\omega)}(x). \end{aligned}$$

Лемма о произведении. Пусть на множестве A задана весовая функция α , на множестве B — весовая функция β , а на множестве $A \times B$ — весовая функция ω . При этом весовые функции связаны соотношением $\omega((\sigma, \tau)) = \alpha(\sigma) + \beta(\tau)$. Тогда

$$\Phi_{A \times B}^{(\omega)}(x) = \Phi_A^{(\alpha)}(x) \cdot \Phi_B^{(\beta)}(x).$$

Доказательство.

$$\begin{aligned} \Phi_{A \times B}^{(\omega)}(x) &= \sum_{(\sigma, \tau) \in A \times B} x^{\omega(\sigma, \tau)} = \sum_{\sigma \in A} \sum_{\tau \in B} x^{\omega(\sigma, \tau)} = \\ &= \sum_{\sigma \in A} \sum_{\tau \in B} x^{\alpha(\sigma) + \beta(\tau)} = \sum_{\sigma \in A} x^{\alpha(\sigma)} \sum_{\tau \in B} x^{\beta(\tau)} = \Phi_A^{(\alpha)}(x) \cdot \Phi_B^{(\beta)}(x). \end{aligned}$$

Последняя лемма естественным образом приводит к следующему определению. Пусть на множестве A_1 задана весовая функция ω_1 , на множестве A_2 — весовая функция $\omega_2, \dots$, на множестве A_k — весовая функция ω_k . Представление $(S, \omega) \rightarrow A_1 \times \dots \times A_k$ называется *представлением, аддитивно сохраняющим вес*, если для любого $(a_1, a_2, \dots, a_k) \in A_1 \times \dots \times A_k$, $(a_1, a_2, \dots, a_k) \leftrightarrow \sigma$ выполняется равенство

$$\omega(\sigma) = \omega_1(a_1) + \omega_2(a_2) + \dots + \omega_k(a_k).$$

Лемма о звездочке. Пусть на множестве A задана весовая функция ω и для любого натурального k вес $\tilde{\omega}$ элемента $(a_1, a_2, \dots, a_k) \in A^k = \underbrace{A \times \dots \times A}_k$ определяется как сумма весов

элементов набора:

$$\tilde{\omega}((a_1, a_2, \dots, a_k)) = \omega(a_1) + \omega(a_2) + \dots + \omega(a_k).$$

Тогда производящая функция множества $\mathcal{A}^*$ относительно весовой функции $\tilde{\omega}$ может быть выражена через производящую функцию для множества $\mathcal{A}$:

$$\Phi_{\mathcal{A}^*}^{(\tilde{\omega})}(x) = \frac{1}{1 - \Phi_{\mathcal{A}}(x)}.$$

Доказательство. Рассмотрим конечное множество $\mathcal{A}$ как алфавит: $\mathcal{A} = \{a, b, c, \dots\}$, $|\mathcal{A}| < \infty$. Множество $\mathcal{A}^*$ можно рассматривать как множество всех конечных слов в алфавите $\mathcal{A}$, поэтому оно может быть выражено следующим образом:

$$\mathcal{A}^* = \bigcup_{k=0}^{\infty} \mathcal{A}^k,$$

где $\mathcal{A}^k = \underbrace{\mathcal{A} \times \dots \times \mathcal{A}}_k$; $\mathcal{A}^0 = \emptyset$.

Выразим производящую функцию множества $\mathcal{A}^*$ через производящую функцию $\Phi_{\mathcal{A}}^{(\omega)}(x)$ для множества $\mathcal{A}$. В силу соотношения

$$\tilde{\omega}((a_1, a_2, \dots, a_k)) = \omega(a_1) + \omega(a_2) + \dots + \omega(a_k)$$

и леммы о произведении получаем $\Phi_{\mathcal{A}^k}^{(\tilde{\omega})}(x) = \left(\Phi_{\mathcal{A}}^{(\omega)}(x)\right)^k$. Тогда по лемме о сумме

$$\begin{aligned} \Phi_{\mathcal{A}^*}^{(\omega')} (x) &= \Phi_{\emptyset}(x) + \Phi_{\mathcal{A}}(x) + \Phi_{\mathcal{A}^2}(x) + \dots = \\ &= 1 + \Phi_{\mathcal{A}}(x) + (\Phi_{\mathcal{A}}(x))^2 + \dots = \frac{1}{1 - \Phi_{\mathcal{A}}(x)}. \end{aligned}$$

□

4.3.3. Представления комбинаторных конфигураций. Пусть даны два множества комбинаторных конфигураций с заданными на них весовыми функциями $(\mathcal{A}, \omega)$ и $(\mathcal{B}, \omega')$, для которых существует представление $(\mathcal{A}, \omega) \rightarrow (\mathcal{B}, \omega')$. Пусть множество $\mathcal{B}$ построено из некоторого количества множеств $\mathcal{B}_1, \dots, \mathcal{B}_k$ с заданными на них весовыми функциями $\omega_1, \dots, \omega_k$ с помощью операций непересекающегося объединения и прямого произведения. При этом весо-

вые функции определены таким образом, что справедливы леммы о сумме и произведении. Тогда такое представление называется

- *прямым* для $\mathcal{A}$, если $\forall i : \mathcal{A} \neq \mathcal{B}_i$;
- *косвенным* для $\mathcal{B}_i$, если $\mathcal{A} \neq \mathcal{B}_i$;
- *рекурсивным* для $\mathcal{A}$, если $\exists i : \mathcal{A} = \mathcal{B}_i$.

С помощью доказанных выше лемм можно попытаться выразить производящую функцию для интересующего нас множества через производящие функции для оставшихся множеств.

Так, например, если

$$\mathcal{A} = (\mathcal{B}_1 \times \mathcal{B}_2) \cup \mathcal{B}_3 \quad (4.2)$$

и при этом весовые функции определены соответствующим образом, то это равенство задает прямое представление для множества $\mathcal{A}$. В результате получаем следующее выражение для производящей функции множества $\mathcal{A}$:

$$\Phi_{\mathcal{A}}(x) = \Phi_{\mathcal{B}_1}(x) \cdot \Phi_{\mathcal{B}_2}(x) + \Phi_{\mathcal{B}_3}(x).$$

Выражение (4.2) одновременно является косвенным представлением для множества $\mathcal{B}_1$, откуда получаем следующее выражение для производящей функции множества $\mathcal{B}_1$:

$$\Phi_{\mathcal{B}_1}(x) = \frac{\Phi_{\mathcal{A}}(x) - \Phi_{\mathcal{B}_3}(x)}{\Phi_{\mathcal{B}_2}(x)}.$$

Другие примеры прямых и косвенных представлений можно найти в разд. 4.3.4. Если же в (4.2) множества $\mathcal{A}$ и $\mathcal{B}_1$ равны, т. е. справедливо равенство

$$\mathcal{A} = (\mathcal{A} \times \mathcal{B}_2) \cup \mathcal{B}_3,$$

мы имеем рекурсивное представление для множества $\mathcal{A}$. В результате для производящей функции множества $\mathcal{A}$ получаем выражение

$$\Phi_{\mathcal{A}}(x) = \frac{\Phi_{\mathcal{B}_3}(x)}{1 - \Phi_{\mathcal{B}_2}(x)}.$$

Другим примером рекурсивного представления является представление из разд. 4.1.4.

Пример 4.1. Получим один результат довольно общего характера. Пусть множество $S = \mathcal{A} \setminus \mathcal{B}$, причем $\mathcal{A} \supset \mathcal{B}$ и весовые

функции определены соответствующим образом. Будем обозначать эту ситуацию как $S = \mathcal{A} - \mathcal{B}$. Поставим задачу найти производящую функцию для множества $S^* = (\mathcal{A} - \mathcal{B})^*$. Так как для S мы имеем косвенное представление $\mathcal{A} = S \cup \mathcal{B}$, то по лемме о сумме $\Phi_S(x) = \Phi_{\mathcal{A}}(x) - \Phi_{\mathcal{B}}(x)$. В то же время по лемме о звездочке

$$\begin{aligned}\Phi_{(\mathcal{A}-\mathcal{B})^*}(x) &= \Phi_{S^*}(x) = \frac{1}{1 - \Phi_S(x)} = \frac{1}{1 - (\Phi_{\mathcal{A}}(x) - \Phi_{\mathcal{B}}(x))} = \\ &= \frac{1}{1 - \Phi_{\mathcal{A}}(x) + \Phi_{\mathcal{B}}(x)}.\end{aligned}$$

4.3.4. Примеры перечислительных задач. Рассмотрим несколько примеров использования метода производящих функций для решения комбинаторных перечислительных задач.

Пример 4.2. Задача Терквема. Найти величину $c(n, k)$ — количество последовательностей $\{s_1, s_2, \dots, s_k\}$ длиной k , таких, что $1 \leq s_1 < s_2 < \dots < s_k \leq n$ и при этом $s_i = i \pmod{2}$.

Например, $c(6, 3) = 4$, так как имеется только четыре последовательности указанного вида: $\{1, 2, 3\}$; $\{1, 2, 5\}$; $\{1, 4, 5\}$; $\{3, 4, 5\}$.

Определим множество комбинаторных конфигураций

$$S_k = \{(s_1, s_2, \dots, s_k)_n \mid 1 \leq s_1 < s_2 < \dots < s_k \leq n; s_i = i \pmod{2}\},$$

при этом положим вес $\omega((s_1, s_2, \dots, s_k)_n) = n$. Тогда наша задача сводится к определению числа комбинаторных конфигураций $\sigma \in S_k$, вес которых $\omega(\sigma) = n$, и, следовательно, к определению коэффициента при x^n в производящей функции $\Phi_k^{(\omega)}(x)$.

Пусть $\mathbb{O} = \{1, 3, 5, \dots\}$ — множество нечетных чисел, а $\tilde{\mathbb{N}} = \mathbb{N} \cup 0$, где $\mathbb{N}$ — множество натуральных чисел. Построим представление

$$S_k \leftrightarrow \underbrace{\mathbb{O} \times \dots \times \mathbb{O}}_k \times \tilde{\mathbb{N}} = \mathbb{O}^k \times \tilde{\mathbb{N}}$$

следующим образом. Каждой комбинаторной конфигурации $\sigma \in S_k$ сопоставим элемент множества $\underbrace{\mathbb{O} \times \dots \times \mathbb{O}}_k \times \tilde{\mathbb{N}}$ по следующему

правилу:

$$(s_1, s_2, \dots, s_k)_n \leftrightarrow (\alpha_1, \alpha_2, \dots, \alpha_k; \alpha_{k+1}),$$

где $\alpha_1 = s_1 \in \mathbb{O}$, $\alpha_i = s_i - s_{i-1} \in \mathbb{O}$, $i = 2, \dots, k$, $\alpha_{k+1} = n - s_k \in \tilde{\mathbb{N}}$. Очевидно, что это взаимно однозначное соответствие между указанными множествами определяет прямое представление для множества S_k .

На множествах $\mathbb{O}$ и $\tilde{\mathbb{N}}$ зададим весовые функции ω' и ω'' : $\forall \alpha \in \mathbb{O} \Rightarrow \omega'(\alpha) = \alpha$, $\forall \alpha \in \tilde{\mathbb{N}} \Rightarrow \omega''(\alpha) = \alpha$. Поскольку

$$\begin{aligned} \tilde{\omega}((\alpha_1, \alpha_2, \dots, \alpha_k; \alpha_{k+1})) &= \\ &= \omega'(\alpha_1) + \omega'(\alpha_2) + \dots + \omega'(\alpha_k) + \omega''(\alpha_{k+1}) = \\ &= \alpha_1 + \alpha_2 + \dots + \alpha_k + \alpha_{k+1} = n, \end{aligned}$$

получаем, что указанное представление является сохраняющим вес. Таким образом, $\Phi_{S_k}^{(\omega)}(x) = \Phi_{\mathbb{O}^k \times \tilde{\mathbb{N}}}^{(\tilde{\omega})}(x)$.

Производящая функция для множества $\mathbb{O}^k \times \tilde{\mathbb{N}}$ находится с помощью лемм о сумме и о произведении:

$$\begin{aligned} \Phi_{\mathbb{O}^k \times \tilde{\mathbb{N}}}^{(\tilde{\omega})}(x) &= \underbrace{\Phi_{\mathbb{O}}^{(\omega')}(x) \cdot \dots \cdot \Phi_{\mathbb{O}}^{(\omega')}(x)}_k \cdot \Phi_{\tilde{\mathbb{N}}}^{(\omega'')}(x) = \\ &= (\Phi_{\mathbb{O}}(x))^k \cdot \Phi_{\tilde{\mathbb{N}}}(x) = \left(\frac{x}{1-x^2} \right)^k \frac{1}{1-x} = \frac{x^k(1+x)}{(1-x^2)^{k+1}}. \end{aligned}$$

Нетрудными вычислениями можно установить, что искомая величина

$$c(n, k) = [x^n] \Phi_{\mathbb{O}^k \times \tilde{\mathbb{N}}}^{(\tilde{\omega})}(x) = [x^{n-k}] \frac{(1+x)}{(1-x^2)^{k+1}} = \left(\left\lfloor \frac{n+k}{2} \right\rfloor \right)_k,$$

где $\binom{n}{m}$ — биномиальный коэффициент C_n^m .

Пусть дана последовательность элементов из множества $\mathcal{A} = \{a, b, c, \dots\}$, $|\mathcal{A}| < \infty$. Максимальным блоком будем называть подслово, содержащее элементы только одного типа и ограниченное с двух сторон элементами других типов. На приведенном ниже примере показано разбиение $(0,1)$ -последовательности на максимальные блоки:

$$111001000101111 = (111)(00)(1)(000)(1)(0)(1111).$$

Пример 4.3. Найти количество двоичных последовательностей длины n , в которых вслед за максимальным блоком из нулей, имеющим нечетную длину, не следует максимальный блок из единиц, имеющий нечетную длину.

Множество всех двоичных последовательностей может быть задано регулярным выражением следующим образом:

$$(0 + 1)^* = 1^*(00^*11^*)^*0^*.$$

Подслова, состоящие из максимального блока из нулей и следующего за ним максимального блока из единиц, являются базовыми для данного представления. Исключив под слова, не входящие по условию в искомое множество, получаем следующее представление для множества интересующих нас последовательностей:

$$S = 1^*(00^*11^* - 0(0^2)^*1(1^2)^*)^*0^*.$$

Найдем производящую функцию искомого множества

$$\begin{aligned} \Phi_{1^*(00^*11^*-0(0^2)^*1(1^2)^*)^*0^*}(x) &= \\ &= \Phi_{1^*}(x) \cdot \Phi_{(00^*11^*-0(0^2)^*1(1^2)^*)^*}(x) \cdot \Phi_{0^*}(x) = \\ &= \frac{1}{1-x} \cdot \frac{1}{1 - \Phi_{00^*11^*-0(0^2)^*1(1^2)^*}(x)} \cdot \frac{1}{1-x} = \\ &= \frac{1}{(1-x)^2} \cdot \frac{1}{1 - (\Phi_{00^*}(x) \Phi_{11^*}(x) - \Phi_{0(0^2)^*}(x) \Phi_{1(1^2)^*}(x))} = \\ &= \frac{1}{(1-x)^2} \cdot \frac{1}{1 - \left(\left(\frac{x}{1-x} \right)^2 - \left(\frac{x}{1-x^2} \right)^2 \right)} = \frac{1+2x+x^2}{1-2x^2-2x^3}. \end{aligned}$$

Задача сведена к нахождению коэффициента при x^n в представлении найденной функции в виде степенного ряда.

Пример 4.4. Найти количество способов заполнения полосы длины n и высоты 1 плитками следующих видов:

$$a = \triangleleft; \quad b = \nabla; \quad c = \text{параллелограмм}.$$

Множество комбинаторных конфигураций, которое мы будем рассматривать, состоит из всех правильных укладок, образованных плитками указанного вида, и может быть задано регулярным

выражением $S = (ac^*b)^*$. Определим весовую функцию на плитках следующим образом: $\omega(a) = 1$, $\omega(b) = 1$, $\omega(c) = 4$. Задача сводится к нахождению коэффициента при x^{2n} в представлении в виде степенного ряда производящей функции

$$\begin{aligned}\Phi_{(ac^*b)^*}(x) &= \frac{1}{1 - \Phi_{ac^*b}(x)} = \frac{1}{1 - x \cdot \frac{1}{1 - x^4} \cdot x} = \\ &= \frac{1 - x^4}{1 - x^2 - x^4} = 1 + \frac{x^2}{1 - x^2 - x^4}.\end{aligned}$$

Пример 4.5. Пусть теперь используются плитки a и b из предыдущего примера, а вместо плитки c используется плитка d вида . Весовая функция на плитках: $\omega(a) = 1$, $\omega(b) = 1$, $\omega(d) = 2$.

Пусть, кроме того, использование плиток того или иного вида требует определенных затрат. Например, стоимость использования плитки a $\omega'(a) = 5$, стоимость использования остальных плиток соответственно $\omega'(b) = 1$ и $\omega'(d) = 2$. Найти количество способов заполнения этими плитками полосы размера $n \times 1$, при этом стоимость заполнения должна равняться m .

Множество комбинаторных конфигураций, которое мы будем рассматривать, аналогично множеству из предыдущего примера: $S = (ad^*b)^*$. Однако в этом случае каждой плитке σ приписывается векторный вес:

$$\tilde{\omega}(\sigma) = (\omega(\sigma), \omega'(\sigma)).$$

Производящая функция определяется теперь как формальный степенной ряд от двух переменных:

$$\Phi_S^{(\tilde{\omega})}(x, y) = \sum_{\sigma \in S} x^{\omega(\sigma)} y^{\omega'(\sigma)}.$$

Нетрудно видеть, что доказанные в предыдущих пунктах результаты переносятся на случай производящих функций от нескольких

переменных. Тогда для нашей производящей функции получаем

$$\begin{aligned}\Phi_{(ad^*b)^*}(x, y) &= \frac{1}{1 - \Phi_{ad^*b}(x, y)} = \frac{1}{1 - x^1 y^5 \frac{1}{1 - x^2 y^2} x^1 y^1} = \\ &= \frac{1 - x^2 y^2}{1 - x^2 y^2 - x^2 y^6} = \frac{1 - x^2 y^2}{1 - x^2 y^2 (1 + y^4)}.\end{aligned}$$

Задача сводится к нахождению коэффициента при x^{2n} для ряда

$$\begin{aligned}&(1 - x^2 y^2) \left(1 + x^2 y^2 (1 + y^4) + x^4 y^4 (1 + y^4)^2 + \right. \\ &\left. + x^6 y^6 (1 + y^4)^3 + \dots \right) = \\ &= 1 + x^2 y^6 + x^4 y^8 (1 + y^4) + x^6 y^{10} (1 + y^4)^2 + \dots = \\ &= 1 + \sum_{n=1}^{\infty} x^{2n} y^{2n+4} (1 + y^4)^{n-1}.\end{aligned}$$

4.4. Задачи

1. Найти число способов размена 1 руб. в советской монетной системе.

2. Найти производящие функции следующих последовательностей:

а) $1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, \dots$;

б) $-1, 1, -1, 1, -1, 1, -1, \dots$;

в) $0, 1, 2, 3, 4, 5, 6, 7, 8, \dots$;

г) $0, 0, 0, 0, 1, 0, 0, -4, 0, 0, 9, 0, 0, -16, 0, 0, 25, \dots$

3. Найти производящие функции следующих последовательностей:

а) $a_n = n(n-1)$;

б) $a_n = \begin{cases} (n+1)(n+2), & n = 0, 1, \dots, N-1; \\ 0, & n \geq N. \end{cases}$

4. Выразить производящую функцию для последовательности $\{a_n\}$ через производящую функцию для последовательности $\{b_n\}$, если:

а) $a_n = nb_n$;

б) $b_n = \begin{cases} 0, & n = 0, 1, \dots, k-1; \\ a_{n-k}, & n \geq k. \end{cases}$

в) $b_n = a_{n+1} - a_n$;

г) $b_n = \sum_{i=0}^n a_i$.

5. Найти число $(0,1)$ -последовательностей длиной n , в которых вслед за максимальным блоком из 0, имеющим четную длину, не стоит максимальный блок из 1, имеющий нечетную длину.

6. Найти число $(0,1)$ -последовательностей длиной n , у которых все максимальные блоки из 1 имеют четную длину, а все максимальные блоки из 0 имеют нечетную длину.

П1. РЕШЕНИЕ ЛИНЕЙНЫХ РЕКУРРЕНТНЫХ УРАВНЕНИЙ МЕТОДОМ ПРОИЗВОДЯЩИХ ФУНКЦИЙ

П1.1. Алгебраическое введение

Пусть $\mathbb{F}$ — некоторое поле, т. е. множество с двумя коммутативными алгебраическими операциями «+» и «·», называемыми сложением и умножением, для которых выполняется закон дистрибутивности $a(b + c) = ab + ac$, и множества $(\mathbb{F}, +)$ и $(\mathbb{F} \setminus \{0\}, \cdot)$ являются группами. Через $\mathbb{F}[x]$ будем обозначать множество всевозможных многочленов от переменной x с коэффициентами из поля $\mathbb{F}$, а через $\mathbb{F}[[x]]$ — множество всевозможных формальных степенных рядов с коэффициентами из $\mathbb{F}$. Далее в качестве поля $\mathbb{F}$ нам встретятся только поле действительных чисел $\mathbb{R}$ и поле комплексных чисел $\mathbb{C}$, но следует иметь в виду, что бывают и другие поля, например, конечное поле вычетов $\mathbb{Z}_p$ по простому модулю p .

Многочлен положительной степени $f(x) \in \mathbb{F}[x]$ называется *неприводимым* над полем $\mathbb{F}$, если из равенства $f(x) = g(x)h(x)$, где $g(x), h(x) \in \mathbb{F}$, следует, что степень одного из многочленов (g или h) равна нулю, т. е. он является константой из $\mathbb{F}$. Например, многочлен $x^2 + 1$ неприводим над полем $\mathbb{R}$, но приводим над $\mathbb{C}$: $x^2 + 1 = (x + i)(x - i)$. Под многочленом везде будем понимать многочлен положительной степени (т. е. отличный от константы), если иное не сказано явно или не следует из контекста.

Дальнейшее изложение будет существенно опираться на теорему, доказательство которой можно найти, например, в [9] на стр. 276.

Теорема (основная теорема алгебры). *Любой многочлен из $\mathbb{C}[x]$ обладает в $\mathbb{C}$ хотя бы одним корнем.*

Свойство, состоящее в том, что всякий многочлен с коэффициентами из поля $\mathbb{F}$ имеет в нем корень, называют *алгебраической замкнутостью* поля $\mathbb{F}$. Не всякий многочлен из $\mathbb{R}[x]$ имеет корни в $\mathbb{R}$ (таков, например, многочлен $x^2 + 1$), однако так как $\mathbb{R} \subset \mathbb{C}$, то по основной теореме алгебры каждый многочлен из $\mathbb{R}[x]$ имеет

корни в $\mathbb{C}$. Таким образом, поле $\mathbb{C}$ — алгебраически замкнуто, а поле $\mathbb{R}$ — нет.

Применяя основную теорему алгебры, индукцией по степени многочлена легко доказать следующее следствие.

Следствие П1.1. *Всякий многочлен из $\mathbb{C}[x]$ (и тем более из $\mathbb{R}[x]$) разлагается над полем $\mathbb{C}$ на линейные множители единственным с точностью до их порядка образом.*

Пусть $z = x + iy \in \mathbb{C}$. Будем использовать общепринятое обозначение $\bar{z} = x - iy$ для комплексно сопряженного с z числа.

Лемма П1.1. *Пусть $f(x) \in \mathbb{R}[x]$ — многочлен с действительными коэффициентами. Тогда для всех $z \in \mathbb{C}$ выполняется равенство $f(\bar{z}) = \overline{f(z)}$.*

Доказательство. Нетрудно убедиться, что $\bar{z}^k = \overline{z^k}$ для всех $z \in \mathbb{C}$ и всех $k \in \mathbb{Z}$. Отсюда и из равенства $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$ легко следует, что если $f \in \mathbb{R}[x]$ и $z \in \mathbb{C}$, то $f(\bar{z}) = \overline{f(z)}$. Отметим, что для произвольного многочлена $f(x) \in \mathbb{C}[x]$ это утверждение неверно.

Следствие П1.2. *Пусть $f(x) \in \mathbb{R}[x]$ — многочлен с действительными коэффициентами и $a \in \mathbb{C}$ — его корень кратности α . Тогда сопряженное число $\bar{a} \in \mathbb{C}$ также будет его корнем той же кратности.*

Доказательство. Согласно лемме П.1.1 получаем $f(\bar{a}) = \overline{f(a)} = \overline{0} = 0$. Таким образом, $\bar{a}$ и a одновременно являются или не являются корнями многочлена $f(x)$. Докажем теперь, что корень $\bar{a}$ имеет ту же кратность, что и a . Действительно, так как $\bar{a}$ и a — корни $f(x)$, то многочлен $f(x)$ должен делиться без остатка на многочлен $A(x) = (x - a)(x - \bar{a}) = x^2 - (a + \bar{a})x + a\bar{a}$. Так как все коэффициенты многочлена $A(x)$ действительны, то и все коэффициенты частного $f_1(x) = f(x)/A(x)$ также действительны. Поэтому к многочлену f_1 применимы все предыдущие рассуждения и искомое утверждение, очевидно, следует по индукции.

Следствие П1.3. *Всякий многочлен из $\mathbb{R}[x]$ однозначно разлагается на сомножители из $\mathbb{R}[x]$, степень которых не превосходит двух.*

Таким образом, неприводимыми над $\mathbb{C}$ являются только линейные многочлены, а неприводимыми над $\mathbb{R}$ — только линейные многочлены и квадратные трехчлены с отрицательным дискриминантом, т. е. без корней в поле $\mathbb{R}$.

П1.2. Разложение на простейшие дроби

Этот раздел посвящен классической теореме о разложении правильной (комплексной или действительной) рациональной дроби в сумму простейших дробей. Эту теорему можно найти во всех классических учебниках математического анализа (см. [6]), однако для полноты изложения доказательство приведем здесь полностью.

Напомним общеизвестную классификацию рациональных дробей.

Определение П1.1. Дробь вида $\frac{P(x)}{Q(x)}$, где $P, Q \in \mathbb{F}[x]$ называют правильной (над полем $\mathbb{F}$), если степень ее числителя строго меньше степени знаменателя, т. е. $\deg P < \deg Q$.

Следствия основной теоремы алгебры мотивируют следующие определения простейших дробей как дробей со знаменателями — степенями неприводимых многочленов.

Определение П1.2. Простейшими дробями над полем $\mathbb{C}$ называют дроби вида $\frac{A}{(z-a)^k}$, где $a, A \in \mathbb{C}$, $k \in \mathbb{N}$.

Определение П1.3. Простейшими дробями над полем $\mathbb{R}$ называют дроби вида $\frac{A}{(z-a)^k}$ или $\frac{Ax+B}{(x^2+ax+b)^k}$, где $a, b, A, B \in \mathbb{R}$, $k \in \mathbb{N}$, а многочлен x^2+ax+b неприводим над полем $\mathbb{R}$.

Отметим, что всякая простейшая дробь является правильной.

Лемма П1.2. Пусть $\frac{P(z)}{Q(z)}$ — правильная несократимая дробь над полем $\mathbb{C}$ и $a \in \mathbb{C}$ — корень ее знаменателя кратности α , т. е. $Q(z) = (z-a)^\alpha R(z)$, где $R(a) \neq 0$. Тогда существует единственное представление дроби $\frac{P(z)}{Q(z)}$ в виде

$$\frac{P(z)}{Q(z)} = \frac{P(z)}{(z-a)^\alpha R(z)} = \frac{A}{(z-a)^\alpha} + \frac{T(z)}{(z-a)^\beta R(z)}, \quad (\text{П1.1})$$

где $A \in \mathbb{C}$, $\beta < \alpha \in \mathbb{N}$ (возможно, $\beta = 0$), и дробь $\frac{T(z)}{(z-a)^\beta R(z)}$ является правильной над полем $\mathbb{C}$.

Доказательство. Вычтем из дроби $\frac{P(z)}{Q(z)}$, где $Q(z) = (z - a)^\alpha \times$
 $\times R(z)$, простейшую дробь $\frac{A}{(z - a)^\alpha}$ с некоторым комплексным ко-
 эффициентом A и получим некоторую дробь $\frac{S(z)}{Q(z)}$. Дробь $\frac{S(z)}{Q(z)}$
 будет правильной как разность двух правильных дробей. В полу-
 ченном соотношении

$$\frac{P(z)}{(z - a)^\alpha R(z)} = \frac{A}{(z - a)^\alpha} + \frac{S(z)}{(z - a)^\alpha R(z)}$$

числитель $S(z)$ удовлетворяет равенству

$$S(z) = P(z) - AR(z). \quad (\text{П1.2})$$

Для представимости дроби $\frac{S(z)}{(z - a)^\alpha R(z)}$ в виде $\frac{T(z)}{(z - a)^\beta R(z)}$
 при таком β , что $0 \leq \beta < \alpha$, необходимо и достаточно, чтобы чи-
 сло a было корнем многочлена $S(z)$, т. е. $S(a) = 0$. Отсюда и из
 равенства (П1.2) получаем уравнение $P(a) - AR(a) = 0$, которое
 решается относительно A единственным образом:

$$A = \frac{P(a)}{R(a)}. \quad (\text{П1.3})$$

Отметим, что $A \neq 0$.

Пусть кратность числа a как корня многочлена $S(z)$ равна
 $\gamma > 0$. Тогда по теореме Безу $S(z) = (z - a)^\gamma T(z)$, где $T(z)$ — не-
 который многочлен из $\mathbb{C}[z]$ и $T(a) \neq 0$. Следовательно,

$$\frac{S(z)}{Q(z)} = \frac{(z - a)^\gamma T(z)}{(z - a)^\alpha R(z)} = \frac{T(z)}{(z - a)^{\gamma - \alpha} R(z)}.$$

Теперь в случае $\gamma \leq \alpha$ достаточно взять $\beta = \alpha - \gamma$. Если же
 $\gamma > \alpha$, то возьмем $\beta = 0$, а многочленом $T(z)$ будем считать мно-
 гочлен $(z - a)^{\gamma - \alpha} T(z)$. И в одном и в другом случае получаем
 разложение (П1.1). Лемма полностью доказана. $\square$

Лемму П1.2 можно обобщить на случай дробей над полями,
 отличными от поля $\mathbb{C}$.

Лемма П1.3. Пусть $\frac{p(x)}{q(x)}$ — правильная несократимая дробь
 над полем $\mathbb{F}$, $p(x), q(x) \in \mathbb{F}[x]$ и пусть $q(x) = a^\alpha(x)r(x)$, где

$a(x) \in \mathbb{F}[x]$ — некоторый неприводимый многочлен, α — некоторое натуральное число и многочлены $a(x)$ и $r(x)$ взаимно просты. Тогда существует единственное представление дроби $\frac{p(x)}{q(x)}$ в виде

$$\frac{p(x)}{q(x)} = \frac{p(x)}{a^\alpha(x) \cdot r(x)} = \frac{b(x)}{a^\alpha(x)} + \frac{t(x)}{a^\beta(x) \cdot r(x)}, \quad (\text{П1.4})$$

здесь $b(x) \in \mathbb{F}[x]$ — некоторый многочлен, степень которого строго меньше степени многочлена $a(x)$, β — такое неотрицательное целое число, что $\beta < \alpha$ (возможно, $\beta = 0$), и дробь $\frac{t(x)}{a^\beta(x) \cdot r(x)}$ является правильной несократимой дробью над полем $\mathbb{F}$.

Доказательство. Доказательство леммы П1.3 в целом следует идее доказательства леммы П1.2.

Очевидно, что искомое представление (П1.4) существует при некотором $\beta < \alpha$ тогда и только тогда, когда многочлен $p(x) - b(x)r(x)$ делится без остатка на многочлен $a(x)$, т.е. тогда и только тогда, когда выполнено равенство

$$b(x)r(x) = p(x) \bmod a(x). \quad (\text{П1.5})$$

В силу неприводимости многочлена $a(x)$ и того, что $r(x) \neq 0$, уравнение (П1.5) имеет единственное решение

$$b(x) = p(x)r^{-1}(x) \bmod a(x), \quad (\text{П1.6})$$

которое можно найти, например, применяя алгоритм Евклида к взаимно простым по условию многочленам $a(x)$ и $r(x)$. Отметим, что $\deg b(x) < \deg a(x)$.

В соответствии со сказанным найдется такое число $\gamma > 0$, что $p(x) - b(x)r(x) = a^\gamma(x)s(x)$, многочлены $a(x)$ и $s(x)$ взаимно просты. Тогда дробь

$$\frac{p(x)}{q(x)} - \frac{b(x)}{a^\alpha(x)} = \frac{p(x) - b(x)r(x)}{a^\alpha(x) \cdot r(x)} = \frac{a^\gamma(x) \cdot s(x)}{a^\alpha(x) \cdot r(x)}$$

является сократимой. Обозначим $\beta = \alpha - \gamma$ и $t(x) = s(x)$, если $\alpha \geq \gamma$, и $\beta = 0$, $t(x) = a^{\gamma-\alpha}(x)s(x)$ в противном случае. В обоих случаях справедливость равенства (П1.4) очевидна.

Осталось доказать несократимость дроби $\frac{t(x)}{a^\beta(x)r(x)}$. В силу выбора ее числителя $t(x)$, при $\beta > 0$ взаимно простого с многочленом $a(x)$, достаточно доказать, что несократима дробь $\frac{t(x)}{r(x)}$, т. е. многочлены $t(x)$ и $r(x)$ взаимно просты. Предположим противное: пусть $d(x)$ — наибольший общий делитель $t(x)$ и $r(x)$, $\deg d(x) > 0$. Пусть $t(x) = t'(x)d(x)$ и $r(x) = r'(x)d(x)$. Тогда получаем

$$\frac{p(x)}{a^\alpha(x)r(x)} = \frac{b(x)}{a^\alpha(x)} + \frac{t'(x)}{a^\beta(x)r'(x)} = \frac{p'(x)}{a^\alpha(x)r'(x)},$$

где $p'(x)$ — некоторый многочлен, т. е. исходная дробь — сократима, что противоречит условию. Лемма доказана. $\square$

Замечание. Лемму П1.2 можно получить как следствие леммы П1.3. Действительно, если в условии леммы П1.3 взять $\mathbb{F} = \mathbb{C}$, то, как мы знаем, неприводимыми будут только многочлены первой степени. Кроме того, если $f(z) \in \mathbb{C}[z]$ — произвольный многочлен и $a \in \mathbb{C}[z]$, то по теореме Безу $f(z) = f(a) \bmod (z - a)$. Таким образом, равенство (П1.6) превращается в равенство (П1.3).

Теперь можно сформулировать и доказать теорему о разложении правильной дроби в сумму простейших. Так как вид простейших дробей над полями $\mathbb{C}$ и $\mathbb{R}$ различается, то и разложение выглядит по-разному. Это происходит от того, что над полем $\mathbb{R}$ существуют неприводимые квадратные трехчлены, а над полем $\mathbb{C}$ — нет.

Теорема о разложении правильных дробей на простейшие. *Всякая правильная дробь с коэффициентами из $\mathbb{C}$ или $\mathbb{R}$ разлагается в сумму простейших дробей и притом единственным с точностью до перестановки слагаемых способом.*

Над полем $\mathbb{C}$ такое разложение выглядит следующим образом:

$$\frac{P(z)}{(z - a_1)^{\alpha_1} \cdot \dots \cdot (z - a_n)^{\alpha_n}} = \sum_{i=1}^n \sum_{j=0}^{\alpha_i-1} \frac{A_{ij}}{(z - a_i)^{\alpha_i-j}}, \quad (\text{П1.7})$$

где $P(z) \in \mathbb{C}[z]$, $a_i, A_{ij} \in \mathbb{C}$ при $1 \leq i \leq n$.

Над полем $\mathbb{R}$ разложение принимает несколько иной вид:

$$\frac{P(x)}{\prod_{i=1}^n (x - a_i)^{\alpha_i} \prod_{i=1}^m (x^2 + c_i x + d_i)^{\beta_i}} =$$

$$= \sum_{i=1}^n \sum_{j=0}^{\alpha_i-1} \frac{A_{ij}}{(x - a_i)^{\alpha_i-j}} + \sum_{i=1}^m \sum_{j=0}^{\beta_i-1} \frac{B_{ij}x + C_{ij}}{(x^2 + c_i x + d_i)^{\beta_i-j}}, \quad (\text{П1.8})$$

где $P(x) \in \mathbb{R}[z]$, $a_i, c_i, d_i, A_{ij}, B_{ij}, C_{ij} \in \mathbb{R}$.

Доказательство. Без ограничения общности рассуждений можно считать знаменатель правильной дроби нормированным, т. е. имеющим старший коэффициент, равный единице.

Докажем сначала справедливость разложения (П1.7). Возьмем правильную дробь $\frac{P(z)}{Q(z)}$ над $\mathbb{C}$. Пусть степень знаменателя $Q(z)$ равна N . По следствию П1.1 основной теоремы алгебры знаменатель $Q(z)$ имеет в точности N (не обязательно различных) комплексных корней a_k и представляется в виде

$$Q(z) = (z - a_1)^{\alpha_1} \cdot \dots \cdot (z - a_n)^{\alpha_n},$$

где α_i — кратность корня a_i , $\alpha_1 + \dots + \alpha_n = \deg Q = N$. Разложение (П1.7) проводится последовательным применением леммы П1.2. Так как степень знаменателя все время уменьшается, то этот процесс рано или поздно закончится. При этом возможно, что некоторые коэффициенты A_{ij} в (П1.7) окажутся нулевыми. Равенство (П1.7) доказано.

Справедливость разложения (П1.8) над $\mathbb{R}$ доказывается аналогично при помощи индуктивного применения леммы П1.3 для поля $\mathbb{F} = \mathbb{R}$.

Единственность разложений (П1.7) и (П1.8) следует из однозначности разложения знаменателя в произведение неприводимых множителей над $\mathbb{C}$ и $\mathbb{R}$. Теорема доказана. $\square$

Лемма П1.4. Когда числитель и знаменатель правильной дроби $\frac{P(x)}{Q(x)}$ в левой части разложения (П1.7) действительны, коэффициенты при простейших дробях из его правой части, соответствующих действительным корням знаменателя, также действительны, а при дробях, соответствующих корням с ненулевой мнимой частью, будут попарно комплексно сопряжены.

Доказательство. По следствию П1.3 основной теоремы алгебры для действительных многочленов разложим знаменатель $Q(x)$ на неприводимые над $\mathbb{R}$ множители:

$$Q(x) = (x - a_1)^{\alpha_1} \dots (x - a_n)^{\alpha_n} \times \\ \times (x^2 + c_1x + d_1)^{\beta_1} \dots (x^2 + c_mx + d_m)^{\beta_m},$$

где α_i — кратность корня a_i , $\alpha_1 + \dots + \alpha_n + 2(\beta_1 + \dots + \beta_m) = \deg Q$. Каждый неприводимый трехчлен $x^2 + c_ix + d_i \in \mathbb{R}[x]$, $1 \leq i \leq m$ из этого произведения разлагается, в свою очередь, над полем $\mathbb{C}$ на двучлены

$$x^2 + c_ix + d_i = (x - b_i)(x - \bar{b}_i),$$

здесь b_i и $\bar{b}_i$ — комплексно сопряженные корни.

К дроби $\frac{P(x)}{Q(x)}$ со знаменателем

$$Q(x) = \prod_{i=1}^n (x - a_i)^{\alpha_i} \prod_{i=1}^m (x - b_i)(x - \bar{b}_i)$$

применим разложение (П1.7):

$$\frac{P(x)}{\prod_{i=1}^n (x - a_i)^{\alpha_i} \prod_{i=1}^m (x - b_i)(x - \bar{b}_i)} = \\ = \sum_{i,j} \frac{A_{ij}}{(x - a_i)^{\alpha_i - j}} + \sum_{i,j} \left(\frac{B_{ij}}{(x - b_i)^{\beta_i - j}} + \frac{C_{ij}}{(x - \bar{b}_i)^{\beta_i - j}} \right), \quad (\text{П1.9})$$

где A_{ij}, B_{ij}, C_{ij} , вообще говоря, являются комплексными.

Покажем, что коэффициенты B_{ij} и C_{ij} комплексно сопряжены. Действительно, рассмотрим две серии простейших дробей из правой части равенства (1.9), соответствующие паре сопряженных корней b и $\bar{b}$:

$$\frac{B_\beta}{(x - b)^\beta} + \frac{C_\beta}{(x - \bar{b})^\beta} + \frac{B_{\beta-1}}{(x - b)^{\beta-1}} + \\ + \frac{C_{\beta-1}}{(x - \bar{b})^{\beta-1}} + \dots + \frac{B_1}{x - b} + \frac{C_1}{x - \bar{b}}. \quad (\text{П1.10})$$

Будем рассуждать аналогично тому, как мы получили равенство (П1.3) из доказательства леммы П1.2. Пусть

$$Q(x) = (x - b)^\beta (x - \bar{b})^\beta R(x),$$

причем $R \in \mathbb{R}[x]$ и $R(b), R(\bar{b}) \neq 0$. Домножая обе части равенства (П1.9) на $(x - b)^\beta$ или $(x - \bar{b})^\beta$ и полагая $x = b$ или соответственно $x = \bar{b}$, получим

$$B_\beta = \frac{P(b)}{(b - \bar{b})^\beta R(b)}$$

и

$$\begin{aligned} C_\beta &= \frac{P(\bar{b})}{(\bar{b} - b)^\beta R(\bar{b})} = \frac{\overline{P(b)}}{(\bar{b} - b)^\beta \overline{R(b)}} = \frac{\overline{P(b)}}{(b - \bar{b})^\beta \overline{R(b)}} = \\ &= \frac{\overline{P(b)}}{(b - \bar{b})^\beta \overline{R(b)}} = \frac{\overline{P(b)}}{(b - \bar{b})^\beta R(b)} = \overline{B_\beta}. \quad (\text{П1.11}) \end{aligned}$$

При выводе равенства (П1.11) мы воспользовались тем, что числа $b - \bar{b}$ и $\bar{b} - b$ сопряжены, леммой П1.1, а также очевидными равенствами $\overline{z_1 z_2} = \overline{z_1} \overline{z_2}$ и $\overline{z_1 / z_2} = \overline{z_1} / \overline{z_2}$.

Таким образом, мы показали, что старшие коэффициенты B_β и C_β из (П1.10) сопряжены. Обозначим $B = B_\beta$, $\bar{B} = C_\beta$ и рассмотрим разность

$$\begin{aligned} &\frac{P(x)}{(x - b)^\beta (x - \bar{b})^\beta R(x)} - \frac{B}{(x - b)^\beta} - \frac{\bar{B}}{(x - \bar{b})^\beta} = \\ &= \frac{P(x) - (\bar{B}(x - b)^\beta + B(x - \bar{b})^\beta) R(x)}{(x - b)^\beta (x - \bar{b})^\beta R(x)}. \quad (\text{П1.12}) \end{aligned}$$

С одной стороны, эта разность является действительной дробью. Это так, поскольку

$$\begin{aligned} \frac{B}{(x - b)^\beta} + \frac{\bar{B}}{(x - \bar{b})^\beta} &= \frac{\bar{B}(x - b)^\beta + B(x - \bar{b})^\beta}{(x - b)^\beta (x - \bar{b})^\beta} = \\ &= \frac{\bar{B}(x - b)^\beta + B(x - \bar{b})^\beta}{(x^2 + c_j x + d_j)^\beta}, \end{aligned}$$

а

$$\begin{aligned} \bar{B}(x-b)^\beta + B(x-\bar{b})^\beta &= \bar{B} \sum_{i=0}^{\beta} (-1)^{\beta-i} C_{\beta}^i x^i b^{\beta-i} + \\ &+ B \sum_{i=0}^{\beta} (-1)^{\beta-i} C_{\beta}^i x^i \bar{b}^{\beta-i} = \sum_{i=0}^{\beta} (-1)^{\beta-i} C_{\beta}^i x^i \times \\ &\times \left(\bar{B} b^{\beta-i} + B \bar{b}^{\beta-i} \right) = \sum_{i=0}^{\beta} (-1)^{\beta-i} C_{\beta}^i x^i \left(\bar{B} b^{\beta-i} + \overline{B b^{\beta-i}} \right), \quad (\text{П1.13}) \end{aligned}$$

где $\bar{B} b^{\beta-i} + \overline{B b^{\beta-i}} \in \mathbb{R}$, а также $P(x)$, $R(x)$ и $(x-b)^\beta (x-\bar{b})^\beta = (x^2 + c_j x + d_j)^\beta$ являются многочленами с действительными коэффициентами.

С другой стороны, в представление разности (П1.12) суммой простейших дробей входят все дроби из (П1.10), кроме $\frac{B_{\beta}}{(x-b)^{\beta}}$ и $\frac{C_{\beta}}{(x-\bar{b})^{\beta}}$. Поэтому можно еще раз повторить все сказанное для правильной действительной дроби (П1.12). Тогда мы получим $B_{\beta-1} = \bar{C}_{\beta-1}$ и т.д. В итоге по индукции найдем, что $B_{ij} = \bar{C}_{ij}$ для всех i, j .

Применяя все тот же прием домножения на знаменатель простейшей дроби, легко показать, что все ненулевые коэффициенты A_{kj} в разложении (П1.9) на самом деле являются действительными числами как значения рациональных дробей над $\mathbb{R}$ в точках $a_k \in \mathbb{R}$. Лемма доказана. $\square$

П1.3. Решение линейных рекуррентных уравнений

Пусть последовательность $\{x_n\}_{n=0}^{\infty}$ удовлетворяет однородному линейному рекуррентному соотношению порядка k с постоянными коэффициентами $a_j, j = 0, \dots, k$ при $a_0, a_k \neq 0$

$$a_k x_{n+k} + a_{k-1} x_{n+k-1} + \dots + a_1 x_{n+1} + a_0 x_n = 0 \quad (\text{П1.14})$$

с некоторыми начальными условиями, задающими k первых членов последовательности. Нашей задачей будет найти замкнутое выражение для общего члена x_n . Разберем вначале случай, когда $x_j, a_j \in \mathbb{C}$.

Рассмотрим производящую функцию $X(z)$ последовательности $\{x_n\}$:

$$X(z) = \sum_{n=0}^{\infty} x_n z^n. \quad (\text{П1.15})$$

Обсудим вопрос сходимости формального степенного ряда $X(z)$.

Лемма П1.5. *Каковы бы ни были выбраны коэффициенты в соотношении (П1.14) и его начальные параметры, степенной ряд (П1.15) с коэффициентами, удовлетворяющими этому рекуррентному соотношению, является абсолютно сходящимся на некотором круге на комплексной плоскости $\mathbb{C}$ с центром в нуле, при этом радиус ε этого круга сходимости положителен и зависит только от коэффициентов рекуррентного соотношения.*

Доказательство. В силу ограниченности k найдется такое положительное действительное число N , что $|a_j| < N$ для всех j , $j = 0, \dots, k$. Также, очевидно, найдется такое число $M = M(k)$, что каждый из первых k членов последовательности $\{|x_n|\}$ не превосходит M . Обозначим $c = \frac{Nk}{|a_k|}$. Будем считать, что $c \geq 1$, а иначе положим $c = 1$.

Докажем по индукции, что неравенство $|x_n| < Mc^n$ выполнено при всех n . Предположение индукции выполняется в силу выбора M для всех $n < k$. Пусть это неравенство верно при значениях индекса, не превосходящих некоторого числа $n - 1$. Оценим x_n :

$$\begin{aligned} |x_n| &= \left| \frac{a_{k-1}x_{n-1} + \dots + a_1x_{n-k+1} + a_0x_{n-k}}{a_k} \right| \leq \\ &\leq \frac{|a_{k-1}||x_{n-1}| + \dots + |a_1||x_{n-k+1}| + |a_0||x_{n-k}|}{|a_k|} < \\ &< N \frac{|x_{n-1}| + \dots + |x_{n-k+1}| + |x_{n-k}|}{|a_k|} < \\ &< \frac{Nk}{|a_k|} \max_{n-k \leq j \leq n-1} |x_j| = c \max_{n-k \leq j \leq n-1} |x_j| < \\ &< cMc^{n-1} = Mc^n. \end{aligned}$$

Итак, неравенство $|x_n| < Mc^n$ выполняется для всех $n \geq 0$. Тогда по известному признаку сходимости степенных рядов $\sum x_n z^n$ абсолютно сойдется в любой точке внутри круга радиуса $\varepsilon = \frac{1}{c} > 0$. Лемма доказана. $\square$

Значение леммы П1.5 в том, что она позволяет корректно обращаться со степенным рядом (П1.15) как с обычной функцией: дифференцировать, интегрировать (внутри круга сходимости почленно), подставлять его в различные выражения и составлять функциональные уравнения.

Рассмотрим, в частности, следующие преобразования производящей функции последовательности $\{x_n\}$. Домножим обе части равенства (П1.15) на одночлены $a_{k-j}z^j$ при $j = 0, \dots, k$:

$$\begin{aligned} a_k X(z) &= a_k x_0 + a_k x_1 z + a_k x_2 z^2 + \dots + a_k x_n z^n + \dots \\ a_{k-1} z X(z) &= a_{k-1} x_0 z + a_{k-1} x_1 z^2 + \dots + a_{k-1} x_{n-1} z^n + \dots \\ a_{k-2} z^2 X(z) &= a_{k-2} x_0 z^2 + \dots + a_{k-2} x_{n-2} z^n + \dots \\ &\dots \dots \dots \\ a_0 z^k X(z) &= \dots + a_0 x_{n-k} z^n + \dots \end{aligned}$$

Сложим все полученные равенства, приводя подобные слагаемые:

$$\left(\sum_{j=0}^k a_{k-j} z^j \right) X(z) = \sum_{n=0}^{\infty} z^n \left(\sum_{j=0}^{\min(n,k)} a_{k-j} x_{n-j} \right).$$

Перепишав соотношение (П1.14) в виде

$$\begin{aligned} a_k x_n + a_{k-1} x_{n-2} + \dots + a_1 x_{n-k+1} + a_0 x_{n-k} &= \\ &= \sum_{j=0}^k a_{k-j} x_{n-j} = 0, \quad n \geq k, \end{aligned}$$

нетрудно убедиться, что все коэффициенты при одночлене z^n в правой части полученного равенства равны нулю, начиная с $n = k$.

Отсюда следует, что функция $X(z)$ удовлетворяет уравнению

$$Q(z)X(z) = P(z), \quad (\text{П1.16})$$

где $P(z), Q(z) \in \mathbb{C}[z]$ — некоторые многочлены. Отметим, что коэффициенты многочлена $Q(z)$ определяются коэффициентами соотношения (П1.14) и он имеет вид

$$Q(z) = a_k + a_{k-1}z + \dots + a_1z^{k-1} + a_0z^k,$$

а коэффициенты многочлена $P(z)$ — первыми k членами последовательности $\{x_n\}$, причем $\deg P < k = \deg Q$. Таким образом, из (П1.16) получаем, что $X(z)$ — правильная дробь:

$$X(z) = \frac{P(z)}{Q(z)}.$$

Дальнейший план наших действий таков: к полученной правильной дроби, знаменатель которой раскладывается на линейные сомножители, применим теорему о разложении правильных дробей на простейшие и представим ее как сумму простейших дробей. Каждую простейшую дробь легко разложить в степенной ряд, эти ряды почленно сложим и получим искомым ответ — замкнутое выражение для величины x_n .

Для начала выясним, как раскладываются в ряды простейшие дроби.

Лемма П1.6.¹⁾ Для произвольного $\alpha \in \mathbb{N}$ справедливо равенство

$$\frac{1}{(1-z)^\alpha} = \sum_{n=0}^{\infty} \bar{C}_\alpha^n z^n = \sum_{n=0}^{\infty} C_{\alpha+n-1}^n z^n, \quad (\text{П1.17})$$

где $\bar{C}_\alpha^n = C_{\alpha+n-1}^n$ — число сочетаний с повторениями из α по n .

Доказательство. Первый способ: докажем равенство индукцией по степени α . В случае базиса индукции, при $\alpha = 1$, равенство становится очевидным:

$$\frac{1}{1-z} = \sum_{n=0}^{\infty} z^n.$$

¹⁾ Этот результат уже был получен в п. 4.1.2 с помощью метода производящих функций.

Предположим, что

$$\frac{1}{(1-z)^{\alpha-1}} = \sum_{n=0}^{\infty} C_{\alpha+n-2}^n z^n.$$

Тогда

$$\begin{aligned} \frac{1}{(1-z)^{\alpha}} &= \frac{1}{(1-z)^{\alpha-1}} \frac{1}{1-z} = \left(\sum_{n=0}^{\infty} C_{\alpha+n-2}^n z^n \right) \left(\sum_{m=0}^{\infty} z^m \right) = \\ &= \sum_{l=0}^{\infty} (C_{\alpha-2}^0 + C_{\alpha-1}^1 + \dots + C_{\alpha+l-2}^l) z^l = \sum_{l=0}^{\infty} C_{\alpha+l-1}^l z^l. \end{aligned}$$

Здесь мы воспользовались равенствами

$$\begin{aligned} C_{n-1}^0 + C_n^1 + C_{n+1}^2 + \dots + C_{n+t-1}^t &= C_n^0 + C_n^1 + \\ &+ C_{n+1}^2 + \dots + C_{n+t-1}^t = C_{n+1}^1 + C_{n+1}^2 + \dots + C_{n+t-1}^t = \\ &= C_{n+2}^2 + \dots + C_{n+t-1}^t = \dots = C_{n+t}^t, \end{aligned}$$

которые следуют из известного рекуррентного соотношения $C_n^{t-1} + C_n^t = C_{n+1}^t$.

Второй способ: докажем равенство (П1.17) комбинаторно. Рассмотрим наш ряд $\frac{1}{(1-z)^{\alpha}}$ как произведение α одинаковых сомножителей $\frac{1}{1-z} = \sum_{n=0}^{\infty} z^n$. Перемножим их и соберем коэффициенты при одинаковых степенях z .

Коэффициент при z^n будет равен числу способов выбора по одному члену вида z^{k_j} из каждого из α рядов-сомножителей так, чтобы сумма всех показателей степеней k_j равнялась n . Число способов выбора, как известно, $\bar{C}_{\alpha}^n = C_{\alpha+n-1}^n$. Лемма доказана.

Замечание. Равенство (П1.17) позволяет несколько расширить понятие биномиального коэффициента, т.е. распространить его на случай отрицательных индексов. Действительно, пусть $n \in \mathbb{N}$. Рассмотрим бином $(1+x)^{-n}$ в отрицательной степени $(-n)$. Обозначим по аналогии символом C_{-n}^t коэффициент при x^t в сумме после раскрытия скобок и приведения подобных слагаемых. Тогда, согласно (П1.17),

$$C_{-n}^t = (-1)C_{n+t-1}^t,$$

и это равенство можно принять за определение C_{-n}^t . В качестве упражнения предлагаем продолжить «вверх» треугольник Паскаля (см. разд. 1.2.2).

Следствие. Для всех $a \in \mathbb{C}$ и всех $\alpha \in \mathbb{N}$ справедливо равенство

$$\frac{1}{(1-az)^\alpha} = \sum_{n=0}^{\infty} C_{\alpha+n-1}^n a^n z^n.$$

Пусть знаменатель $Q(z)$ имеет комплексные корни $z_1, \dots, z_m$ с кратностями $\alpha_1, \dots, \alpha_m$ соответственно, тогда

$$Q(z) = a_0(z-z_1)^{\alpha_1} \dots (z-z_m)^{\alpha_m}.$$

Представим правильную дробь $X(z)$ суммой простейших дробей, а каждую из них, согласно следствию леммы П1.6, разложим в степенной ряд

$$\begin{aligned} X(z) &= \frac{P(z)}{Q(z)} = \frac{P(z)}{a_0(z-z_1)^{\alpha_1} \dots (z-z_m)^{\alpha_m}} = \\ &= \sum_{i=1}^m \sum_{j=0}^{\alpha_i-1} \frac{A_{ij}}{(z-z_i)^{\alpha_i-j}} = \\ &= \sum_{i=1}^m \sum_{j=0}^{\alpha_i-1} \frac{B_{ij}}{\left(1 - \frac{z}{z_i}\right)^{\alpha_i-j}} = \sum_{i=1}^m \sum_{j=0}^{\alpha_i-1} \sum_{n=0}^{\infty} C_{\alpha_i-j+n-1}^n B_{ij} \left(\frac{z}{z_i}\right)^n = \\ &= \sum_{n=0}^{\infty} \left(\sum_{i=1}^m \left(\frac{1}{z_i}\right)^n \cdot \sum_{j=0}^{\alpha_i-1} B_{ij} C_{\alpha_i-j+n-1}^n \right) z^n = \\ &= \sum_{n=0}^{\infty} \left(\sum_{k=1}^m \lambda_k^n \cdot \sum_{j=0}^{\alpha_k-1} D_{kj} n^j \right) z^n, \quad (\text{П1.18}) \end{aligned}$$

где $A_{ij}, B_{ij}, D_{ij} \in \mathbb{C}$ — некоторые постоянные коэффициенты; $\lambda_i = \frac{1}{z_i} \in \mathbb{C}$ — величины, обратные корням знаменателя $Q(z)$. В последнем равенстве мы воспользовались тем, что биномиальный коэффициент

$$C_{\alpha_i-j+n-1}^n = C_{\alpha_i-j-1+n}^{\alpha_i-j-1} = \frac{(n + \alpha_i - j - 1) \cdot \dots \cdot (n + 1)}{(\alpha_i - j - 1)!}$$

относительно переменной n является многочленом степени $\alpha_i - j - 1$, поэтому и сумма $\sum_{j=0}^{\alpha_i-1} B_{ij} C_{\alpha_i-j+n-1}^n$ многочленов степени не выше $(\alpha_i - 1)$ с коэффициентами B_{kj} является многочленом $\sum_{j=0}^{\alpha_k-1} D_{kj} n^j$ от переменной n степени $(\alpha_i - 1)$ с некоторыми коэффициентами D_{ij} .

Нетрудно заметить, что комплексные числа $\lambda_i = \frac{1}{z_i}$, $i = 1, \dots, m$, являются корнями многочлена

$$T(\lambda) = a_k \lambda^k + a_{k-1} \lambda^{k-1} + \dots + a_1 \lambda + a_0, \quad (\text{П1.19})$$

связанного со знаменателем $Q(z)$ производящей функции $X(z)$ соотношением

$$Q(z) = z^{\deg T} T\left(\frac{1}{z}\right). \quad (\text{П1.20})$$

Заметим, что $T(\lambda)$ является *характеристическим многочленом* линейного однородного рекуррентного соотношения (П1.14), а $Q(z)$ часто называют *двойственным характеристическим многочленом* того же соотношения. Из равенств (П1.19) и (П1.14) следует, что

$$T(\lambda) = a_k (\lambda - \lambda_1)^{\alpha_1} \dots (\lambda - \lambda_m)^{\alpha_m}.$$

Сравнивая равенства (П1.15) и (П1.18), получаем замкнутое выражение для общего члена решения уравнения (П1.14):

$$x_n = \sum_{j=1}^m \lambda_j^n \cdot (D_{j,0} + D_{j,1} \cdot n + \dots + D_{j,\alpha_j-1} \cdot n^{\alpha_j-1}), \quad (\text{П1.21})$$

где $D_{j,s}$ — некоторые комплексные коэффициенты.

Таким образом, мы доказали следующую замечательную теорему.

Теорема об общем решении рекуррентного соотношения. *Решение однородного линейного рекуррентного уравнения (П1.14) с постоянными коэффициентами всегда имеет вид (П1.21), т. е. является суммой n -х степеней корней характеристического многочлена, умноженных на многочлены от переменной n , сте-*

пень которых на единицу меньше кратности соответствующего корня.

Из доказательства этой теоремы вытекает простой алгоритм решения уравнения (П1.14).

Алгоритм. Пусть из начальных условий уже найдены первые k членов последовательности $x_0, \dots, x_{k-1}$.

1. Записать характеристический многочлен $T(\lambda)$, определяемый равенством (П1.19), и найти его корни $\lambda_1, \dots, \lambda_m$ и их кратности $\alpha_1, \dots, \alpha_m$, где $\sum_j \alpha_j = k$.

2. Общее решение, как было доказано выше, имеет вид (П1.21). Подставить в него $n = 0, 1, \dots, k - 1$. Тогда в левой части будут известные числа, а в правой — некоторая линейная комбинация относительно величин D_{jl} . Нетрудно понять, что количество всевозможных коэффициентов D_{jl} в правой части равенства (П1.21) равно степени знаменателя производящей функции $X(z)$, т. е. порядку уравнения (П1.14), иначе говоря равно k . Таким образом, мы получили систему из k линейных уравнений с k неизвестными D_{jl} над полем $\mathbb{C}$. По теореме о разложении правильных дробей на простейшие эта система имеет единственное решение, так как неизвестные D_{jl} однозначно выражаются через коэффициенты A_{ij} разложения (П1.18) производящей функции $X(z)$ на простейшие дроби, а разложение на простейшие дроби единственно.

3. Решить полученную систему линейных уравнений порядка k над полем $\mathbb{C}$. Для малых k это можно сделать, например, методом Крамера. При $k \geq 4$ целесообразно использовать метод Гаусса (или модификацию Жордана).

4. Подставив найденные коэффициенты в (П1.21), получим ответ.

П1.4. Обсуждения и примеры

Рассмотрим пример применения предложенного алгоритма.

Пример П1.1. Найти общий член линейной рекуррентной последовательности

$$\begin{cases} x_n + 2x_{n-1} + 3x_{n-2} + 2x_{n-3} + x_{n-4} = 0 \\ x_0 = x_1 = x_3 = 0, \quad x_2 = -\sqrt{3}. \end{cases}$$

Многочлен $T(\lambda) = \lambda^4 + 2\lambda^3 + 3\lambda^2 + 2\lambda + 1$ будет характеристическим многочленом данной последовательности. Решив уравнение $\lambda^4 + 2\lambda^3 + 3\lambda^2 + 2\lambda + 1 = 0$ (например, сведя к биквадратному заменой $z = \lambda + (1/\lambda)$), найдем его корни:

$$\begin{aligned}\lambda_1 &= \frac{-1 + i\sqrt{3}}{2} = \cos\left(\frac{2\pi}{3}\right) + i\sin\left(\frac{2\pi}{3}\right) = e^{i[(2\pi)/3]}, \\ \lambda_2 &= \frac{-1 - i\sqrt{3}}{2} = \cos\left(\frac{2\pi}{3}\right) - i\sin\left(\frac{2\pi}{3}\right) = e^{-i[(2\pi)/3]}.\end{aligned}$$

Кратность каждого корня равна двум.

Заметим, что числа λ_1, λ_2 являются комплексными корнями 3-й степени из единицы и к тому же примитивными. Обозначим $\omega = \lambda_1$, тогда $\lambda_2 = \omega^2$. Общее решение данной рекурренты по теореме имеет вид

$$x_n = \lambda_1^n(c_1 + c_2n) + \lambda_2^n(c_3 + c_4n). \quad (\text{П1.22})$$

Чтобы вычислить константы c_j , составим систему линейных уравнений. Для этого подставим в равенство (П1.22) $n = 0, 1, 2, 3$ и воспользуемся начальными условиями:

$$\begin{cases} 0 = c_1 + c_3, \\ 0 = \omega(c_1 + c_2) + \omega^2(c_3 + c_4), \\ -\sqrt{3} = \omega^2(c_1 + 2c_2) + \omega(c_3 + 2c_4), \\ 0 = c_1 + 3c_2 + c_3 + 3c_4. \end{cases}$$

Здесь учтено, что $\omega^3 = 1$, поэтому $[1/\omega] = \omega^2$ и $(\omega^2)^2 = \omega$.

Решим данную систему в матричном виде:

$$\begin{aligned}&\begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ \omega & \omega & \omega^2 & \omega^2 & 0 \\ \omega^2 & 2\omega^2 & \omega & 2\omega & -\sqrt{3} \\ 1 & 3 & 1 & 3 & 0 \end{pmatrix} \sim \\ &\sim \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & \omega & \omega & 0 \\ 1 & 2 & \omega^2 & 2\omega^2 & -\omega\sqrt{3} \\ 1 & 3 & 1 & 3 & 0 \end{pmatrix} \sim\end{aligned}$$

$$\begin{aligned}
& \sim \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & \omega-1 & \omega & 0 \\ 0 & 2 & \omega^2-1 & 2\omega^2 & -\omega\sqrt{3} \\ 0 & 3 & 0 & 3 & 0 \end{pmatrix} \sim \\
& \sim \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & \omega-1 & \omega & 0 \\ 0 & 2 & \omega^2-1 & 2\omega^2 & -\omega\sqrt{3} \end{pmatrix} \sim \\
& \sim \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & \omega-1 & \omega-1 & 0 \\ 0 & 0 & \omega^2-1 & 2(\omega^2-1) & -\omega\sqrt{3} \end{pmatrix} \sim \\
& \sim \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 2 & \frac{-\omega\sqrt{3}}{\omega^2-1} \end{pmatrix} \sim \\
& \sim \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & \frac{-\omega\sqrt{3}}{\omega^2-1} \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & 0 & i \\ 0 & 1 & 0 & 0 & -i \\ 0 & 0 & 1 & 0 & -i \\ 0 & 0 & 0 & 1 & i \end{pmatrix}.
\end{aligned}$$

Видно, что

$$\frac{-\omega\sqrt{3}}{\omega^2-1} = \frac{\frac{-1+i\sqrt{3}}{2}\sqrt{3}}{\frac{-1-i\sqrt{3}}{2}-1} = \frac{3i-\sqrt{3}}{3+i\sqrt{3}} = i.$$

Таким образом, $c_1 = c_4 = i$, $c_2 = c_3 = -i$, поэтому

$$\begin{aligned}
x_n &= \lambda_1^n(i-in) + \lambda_2^n(-i+in) = \\
&= e^{i2n\pi/3}(i-in) + e^{-i2n\pi/3}(-i+in) = 2(n-1) \sin(2n\pi/3).
\end{aligned}$$

Даже не вычисляя явно константы c_1, c_2, c_3, c_4 в равенстве (П1.22), можно заранее утверждать, что они попарно сопряжены: $c_1 = \bar{c}_3, c_2 = \bar{c}_4$. Так как начальные условия – действительные числа, и коэффициенты рекуррентного соотношения тоже, вся последовательность является действительной: $\forall n \ x_n \in \mathbb{R}$. Значит, и ее производящая функция, имеющая вид

$$X(z) = \frac{P(z)}{1 + 2z + 3z^2 + 2z^3 + z^4},$$

где $P(z)$ – некоторый многочлен степени не выше трех, также является действительной. По лемме П1.4 коэффициенты разложения $X(z)$ в сумму простейших дробей будут попарно сопряжены, поэтому будут попарно сопряжены и соответствующие коэффициенты разложения каждой простейшей дроби в степенной ряд и их линейные комбинации. Аккуратное доказательство этого факта предоставляется читателю в качестве упражнения.

Сумму произведений показательных функций и многочленов будем называть *квазимногочленом*. Например, квазимногочленами являются выражения $n^2, e^n, n^2 + e^n, 2^n(1 - n), [(1 + n + n^2)/(2^n)] - \sqrt{2^n} - n2^n$ и $\cos n = [(e^{in} + e^{-in})/2]$. Выражения $\sqrt{n}, 2^{1+n+n^2}$ и $\frac{1}{n} + 2^n$ квазимногочленами не являются.

Используя это новое понятие, теорему можно переформулировать так: *общий член однородной линейной рекуррентной последовательности всегда является квазимногочленом.*

Верно и обратное утверждение: *если общий член x_n некоторой последовательности — квазимногочлен, то последовательность является линейной рекуррентой*, т. е. удовлетворяет линейному соотношению вида (П1.14) с некоторыми k и a_j . Действительно,

производящая функция $X(z) = \sum_{n=0}^{\infty} x_n z^n$ в данном случае есть ли-

нейная комбинация простейших дробей вида $[1/(1 - az)]$ и их производных и, следовательно, является рациональной. Коэффициенты же ряда Тейлора рациональной функции аналогично полученному равенству (П1.16) удовлетворяют некоторому линейному рекуррентному соотношению.

Таким образом, рациональные функции и только они являются производящими функциями для линейных рекуррентных последовательностей.

Пример П1.2. Записать какое-либо однородное линейное рекуррентное соотношение, которому удовлетворяет последовательность $x_n = (1+n)2^n - n$.

Первый способ. Рассмотрим производящую функцию

$$\begin{aligned} X(z) &= \sum_{n=0}^{\infty} x_n z^n = \sum_{n=0}^{\infty} ((1+n)2^n - n)z^n = \\ &= \sum_{n=0}^{\infty} (1+n)(2z)^n - \sum_{n=0}^{\infty} n z^n = \sum_{n=0}^{\infty} (1+n)(2z)^n - z \sum_{n=1}^{\infty} n z^{n-1} = \\ &= \sum_{n=0}^{\infty} \frac{1}{2} ((2z)^{n+1}) - z \sum_{n=1}^{\infty} z^n = z \sum_{n=0}^{\infty} (2z)^n - z \sum_{n=1}^{\infty} z^n = \\ &= \left(\frac{z}{1-2z} \right) - z \left(\frac{z}{1-z} \right) = \frac{1}{(1-2z)^2} - \frac{z}{(1-z)^2} = \\ &= \frac{(1-z)^2 - z(1-2z)^2}{(1-2z)^2 - (1-z)^2} = \frac{1-3z+5z^2-4z^3}{1-6z+13z^2-12z^3+4z^4}. \end{aligned}$$

По знаменателю $Q(z) = 1 - 6z + 13z^2 - 12z^3 + 4z^4$, используя (П1.20), найдем характеристический многочлен

$$T(\lambda) = \lambda^4 - 6\lambda^3 + 13\lambda^2 - 12\lambda + 4,$$

а зная коэффициенты $T(\lambda)$, выпишем и само соотношение

$$x_n - 6x_{n-1} + 13x_{n-2} - 12x_{n-3} + 4x_{n-4} = 0$$

с начальными условиями $x_0 = 1$, $x_1 = 2$, $x_2 = 10$, $x_3 = 29$.

Второй способ. Сравнивая

$$x_n = (1+n)2^n - n = (1+n)2^n + (0-n)1^n$$

с выражением (П1.22), выясняем, что характеристический многочлен $T(\lambda)$ имеет корень $\lambda_1 = 2$ кратностью 2 и корень $\lambda_2 = 1$ кратностью 2, т. е.

$$T(\lambda) = (\lambda - 2)^2(\lambda - 1)^2 = \lambda^4 - 6\lambda^3 + 13\lambda^2 - 12\lambda + 4.$$

Далее аналогично первому способу.

Полученное рекуррентное соотношение с $k = 4$ имеет наименьший возможный порядок среди всех линейных однородных соотношений, которым удовлетворяет данная последовательность $\{x_n\}$ (вообще говоря, таких соотношений бесконечно много).

Пример П1.3. Является ли линейной рекуррентой некоторого порядка k последовательность $x_n = \{1/(n+1)\}$?

Ответ: Нет, так как x_n — не квазимногочлен. Вычислив сумму соответствующего ряда, можно убедиться, что производящая функция $X(z)$ не рациональна.

П1.5. Задачи

1. Пусть все коэффициенты $\{a_j\}$ линейного однородного соотношения (П1.14) и все члены последовательности $\{x_n\}_{n=0}^{\infty}$ действительны. Доказать, что если два корня λ_r и λ_s характеристического многочлена (П1.19) комплексно сопряжены, т. е. $\lambda_r = \bar{\lambda}_s$, то соответствующие коэффициенты в выражении (П1.21) также сопряжены, т. е. $D_{rj} = \bar{D}_{sj}$ для всех j . (Указание: воспользоваться леммой П1.5.)

2. Найти производящие функции последовательностей $\{a_n\}$ и $\{b_n\}$, если

$$\begin{cases} a_{n+2} + a_{n+1} - a_n + b_{n+2} - 2b_{n+1} - b_n = 0, \\ a_{n+1} + a_n - b_{n+2} - b_{n+1} + 3b_n = 0, \\ a_0 = a_1 = b_1 = 1, \quad b_0 = 0. \end{cases}$$

П2. ЧИСЛА КАТАЛАНА

Задача 1. В кассу за билетами стоит очередь из $2n$ человек, у каждого по купюре в 100 или 50 руб., причем этих купюр в очереди поровну — n полтинников и n сторублевок. Билет стоит 50 руб., в начале продажи касса пуста. Найти число способов расположить очередь так, чтобы кассир всегда мог выдать сдачу.

Ответ к задаче называется n -м числом Каталана и обозначается c_n . Рассмотрим другую формулировку задачи об очереди в кассу.

Задача 2. Найти число различных двоичных наборов длины $2n$, в которых поровну нулей и единиц, и обладающих вдобавок ограничением: на любом начальном отрезке каждого такого набора число нулей не меньше числа единиц¹⁾.

Ясно, что ответом ко второй задаче также является число c_n . Действительно, очередь с купюрами можно закодировать двоичным набором, заменяя пятидесятирублевки нулями, а сторублевки единицами. Такое соответствие взаимно однозначно, поэтому число очередей равно числу $(0,1)$ -наборов. Если очередь удовлетворяла условию задачи 1, то соответствующий ей набор удовлетворяет условию задачи 2, и наоборот (например, набор 011001 не подходит, так как на его начальном отрезке 011 нулей меньше, чем единиц).

Перебором можно легко найти несколько первых чисел Каталана. Так $c_0 = 1$ (в пустом наборе λ нулевой длины нет нулей и единиц); $c_1 = 1$ (набор 01); $c_2 = 2$ (наборы 0101 и 0011); $c_3 = 5$ (наборы 010101, 010011, 001101, 001011, 000111).

П2.1. Метод производящих функций

Решим задачу о числах Каталана в формулировке о $(0,1)$ -наборах. Рассмотрим энумератор C , содержащий все наборы, удовлетворяющие условию задачи 2:

¹⁾ Заметим, что если бы ограничения не было, то ответом, очевидно, было бы число $C_{2n}^n = \frac{(2n)!}{n!n!}$.

$$\begin{aligned}
C &= \lambda + \\
&+ 01 + \\
&+ 0101 + 0011 + \\
&+ 010101 + 010011 + 001101 + 001011 + 000111 + \dots \quad (\text{П2.1})
\end{aligned}$$

С нашей точки зрения C представляет собой просто множество двоичных слов, даже не обязательно упорядоченное. Знак «+» понимается как (дизъюнктивное) объединение.

Нетрудно видеть, что энумератор C удовлетворяет равенству

$$C = 0 \cdot C \cdot 1 \cdot C + \lambda, \quad (\text{П2.2})$$

где умножение означает конкатенацию множеств. Строго говоря, C удовлетворяет еще очень многим равенствам, например, $C = C^2$ или $C = C^3$.

Центральным в решении является наблюдение, что каждый набор из C порождается регулярным выражением $C = 0 \cdot C \cdot 1 \cdot C + \lambda$ *однозначно* (чего не скажешь, например, о выражении C^2). Действительно, каждый непустой набор $a = a_1 \dots a_{2n} \in C$ начинается с нуля и для любого $a \neq \lambda$ множество всех таких m , для которых

$$\sum_{i=1}^m a_i = \frac{m}{2}, \text{ непусто (например, всегда можно взять } m = 2n). \text{ Сре-}$$

ди всех таких m найдется минимальное $\hat{m}$. Осталось заметить, что $a_1 = 0$, $a_{\hat{m}} = 1$. Поэтому набор a представим конкатенацией наборов a' и a'' , где $a' = a_1 \dots a_{\hat{m}} \in 0 \cdot C \cdot 1$ и $a'' = a_{\hat{m}+1} \dots a_{2n} \in C$, и представление $a = a' a''$ единственно, так как наборы a' и a'' определяют по набору a однозначно. Например, для набора $a = 001101$, очевидно, $m = 4$, $a' = 0011$, $a'' = 01$; а для набора $a = 00100111$ получаем $m = 8$, $a' = a$, $a'' = \lambda$.

Заменив каждый символ 0 и 1 в равенстве (П2.1) на переменную z , а λ — на $z^0 = 1$ и приведя подобные члены, получим степенной ряд $l(z)$, в котором коэффициентом при z^{2n} служит искомая величина c_n , а коэффициенты при нечетных степенях равны нулю. Замена $z^2 = x$ позволит записать этот ряд в более удобной форме $C(x) = l(\sqrt{x})$ без нулевых членов.

Из равенства (П2.2), пользуясь свойством однозначности регулярного выражения $C = 0 \cdot C \cdot 1 \cdot C + \lambda$, получаем соотношение, которому удовлетворяет ряд $C(x) = \sum_{k=0}^{\infty} c_k x^k$:

$$C(x) = xC^2(x) + 1. \quad (\text{П2.3})$$

Решая это квадратное уравнение относительно $C(x)$, получим

$$C_1(x) = \frac{1 + \sqrt{1 - 4x}}{2x}, \quad C_2(x) = \frac{1 - \sqrt{1 - 4x}}{2x}.$$

Обе функции удовлетворяют уравнению (П2.3), но решение дает лишь одна из них. Выбрать ее позволяет наблюдение, что $C(0) = c_0 = 1$, однако

$$\lim_{x \rightarrow 0} \frac{1 + \sqrt{1 - 4x}}{2x} = \infty.$$

Таким образом,

$$C(x) = \frac{1 - \sqrt{1 - 4x}}{2x} \quad (\text{П2.4})$$

является производящей функцией для последовательности Каталана $\{1, 1, 2, 5, \dots\}$, $x = 0$ — ее устранимая точка разрыва.

Дальнейшее — дело техники. Осталось разложить функцию $C(x)$ в степенной ряд, определив его коэффициенты. Отличникам рекомендуется сделать дальнейшие выкладки самостоятельно.

Итак, воспользуемся известной теоремой Тейлора

$$f(x) = \sum_{k=0}^{\infty} \frac{f^{(k)}(x_0)}{k!} (x - x_0)^k,$$

разложив в ряд с центром в нуле функцию $f(x) = \sqrt{1 - x}$. Индукцией по k нетрудно доказать, что

$$f^k(0) = (-1)^n \frac{1}{2} \left(\frac{1}{2} - 1 \right) \left(\frac{1}{2} - 2 \right) \cdot \dots \cdot \left(\frac{1}{2} - k + 1 \right).$$

Учитывая это, получаем

$$\begin{aligned}
& \sqrt{1-4x} = \\
& = 1 + \sum_{k=1}^{\infty} \frac{\frac{1}{2} \left(\frac{1}{2} - 1 \right) \left(\frac{1}{2} - 2 \right) \cdot \dots \cdot \left(\frac{1}{2} - k + 1 \right)}{k!} (-4x)^k = \\
& = 1 + \sum_{k=1}^{\infty} \frac{\frac{1}{2} \left(-\frac{1}{2} \right) \left(-\frac{3}{2} \right) \left(-\frac{5}{2} \right) \cdot \dots \cdot \left(-\frac{2k-3}{2} \right)}{k!} (-4x)^k = \\
& = 1 + \sum_{k=1}^{\infty} \frac{(-1)^{k-1} \cdot 1 \cdot 3 \cdot 5 \cdot \dots \cdot (2k-3)(2k-2)}{2^k k!} (-4x)^k = \\
& = 1 - \sum_{k=1}^{\infty} \frac{1 \cdot 2 \cdot 3 \cdot 5 \cdot \dots \cdot (2k-3)(2k-2)}{2 \cdot 4 \cdot 6 \cdot \dots \cdot (2k-4)(2k-2)k!} 2^k x^k = \\
& = 1 - \sum_{k=1}^{\infty} \frac{(2k-2)!}{(k-1)! 2^{k-1} k!} 2^k x^k = 1 - 2 \sum_{k=1}^{\infty} \frac{1}{2k-1} C_{2k-1}^k x^k.
\end{aligned}$$

Подставляя результат в выражение для $C(x)$, найдем

$$\begin{aligned}
C(x) &= \frac{1 - \sqrt{1-4x}}{2x} = \frac{1 - \left(1 - 2 \sum_{k=1}^{\infty} C_{2k-1}^k \frac{x^k}{2k-1} \right)}{2x} = \\
&= \sum_{k=1}^{\infty} \frac{C_{2k-1}^k}{2k-1} x^{k-1} = \sum_{n=0}^{\infty} \frac{C_{2n+1}^n}{2n+1} x^n = \sum_{n=0}^{\infty} \frac{C_{2n}^n}{n+1} x^n.
\end{aligned}$$

Таким образом, получено замкнутое выражение для числа Каталана

$$c_n = \frac{1}{n+1} C_{2n}^n. \quad (\text{П2.5})$$

Следствие П2.4. Число C_{2n}^n делится на $(n+1)$ при любом $n \in \mathbb{N}$.

Следствие П2.5. Вероятность того, что очередь в кассу задержится, равна $\frac{n}{n+1}$ и стремится к единице с ростом ее длины.

П2.2. Метод траекторий

Многие комбинаторные задачи удобно решать геометрически, что мы и проиллюстрируем ниже. Приведем еще один способ получения равенства (П2.5), в котором не будут использоваться понятия производящей функции и регулярного выражения.

Каждую двоичную последовательность (или очередь в кассу) представим ломаной на координатной плоскости. Ломаная состоит из ориентированных звеньев. Ее началом является начало координат $O(0, 0)$. Пусть нулевому символу (или полтиннику) соответствует звено — единичный отрезок $\nearrow$, а единице (или сторублевой купюре) — звено $\searrow$. Тогда каждому $(0,1)$ -набору $\mathbf{a}$ (и каждой очереди) соответствует своя ломаная $\gamma = \gamma(\mathbf{a})$, и по ломаной можно однозначно найти соответствующий набор. Например, набору **00110111001000001111** соответствует ломаная, изображенная на рис. П2.1.

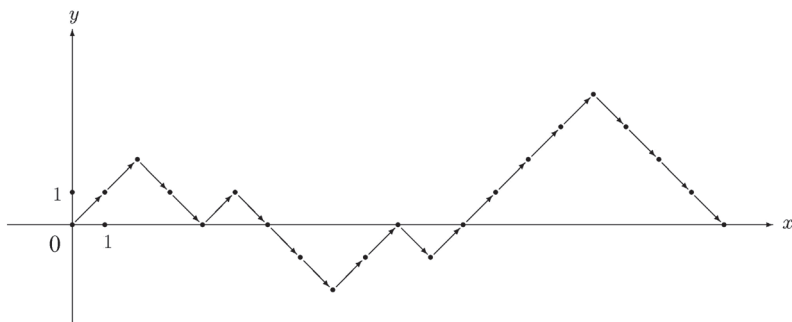


Рис. П2.1

Условие «на любом начальном отрезке двоичного набора число нулей не меньше числа единиц» геометрически означает, что в ломаной нет точек с отрицательными ординатами (например, ломаная на рис. П2.1 ему не удовлетворяет). Таким образом, мы приходим к следующей эквивалентной задаче.

Задача 3. Найти число c_n различных ломаных на координатной плоскости, соединяющих начало координат с точкой $(2n, 0)$,

состоящих из направленных единичных отрезков $\nearrow$ и $\searrow$ и не опускающихся ниже оси Ox .

Здесь, как часто бывает в комбинаторных задачах, выгоднее искать число неблагоприятных случаев, т. е. случаев, когда ломаная опускается ниже оси абсцисс. Если мы найдем их число, то, вычтя его из числа C_{2n}^n всех ломаных, состоящих из n отрезков $\nearrow$ и n отрезков $\searrow$, получим ответ для нашей задачи.

Отметим два очевидных факта. Во-первых, координаты конца ломаной зависят только от числа нулей и единиц в соответствующем наборе и не зависят от их порядка в нем. Во-вторых, любая неблагоприятная ломаная имеет общие точки с прямой $l: y = -1$. Обозначим начало координат O , а точку с координатами $(2n, 0)$, в которой оканчиваются все ломаные, обозначим A .

Найдем теперь число неподходящих по условию ломаных $\gamma: O \rightarrow A$. Каждая такая ломаная имеет хотя бы одну общую точку с прямой l . Пусть $B = B(\gamma)$ — крайняя слева точка среди всех таких точек. Она существует для каждой неподходящей ломаной и определяется по ней однозначно (рис. П2.2).

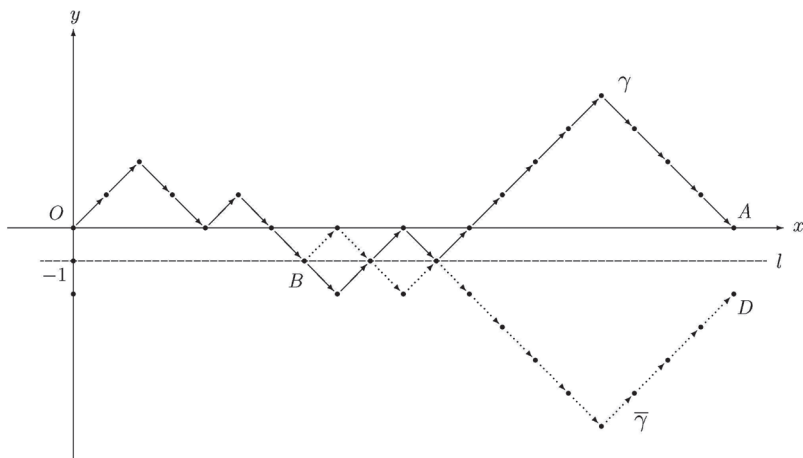


Рис. П2.2

Пусть γ' — часть ломаной γ от точки O до точки B , а γ'' — оставшаяся часть ломаной γ от точки B до точки A . Таким образом,

$\gamma = O\gamma'B\gamma''A$. Обозначим через γ''' ломаную, симметричную γ'' относительно прямой l (на рис. П2.2 она изображена пунктиром). Рассмотрим ломаную $\bar{\gamma} = O\gamma'B\gamma'''D$, начало которой до точки B совпадает с ломаной γ . Конец этой ломаной находится в некоторой точке D , по построению симметричной точке A относительно прямой l . Координаты точки A $(2n, 0)$ одинаковы для всех ломаных γ , поэтому и координаты точки D также одинаковы для всех ломаных $\bar{\gamma}$. Легко видеть, что ордината точки D равна -2 .

Заметим, что соответствие $\gamma \leftrightarrow \bar{\gamma}$ взаимно однозначно. Действительно, ломаную $\bar{\gamma}$ всегда можно получить из ломаной γ вышеописанной процедурой. Наоборот, каждая ломаная $\bar{\gamma} : O \rightarrow D$ пересекает прямую l хотя бы в одной точке, так как ее концы лежат по разные стороны прямой. Среди всех точек пересечения есть крайняя левая точка B , а отражением относительно прямой l отрезка γ''' , заключенного между точками B и D , получим ломаную $\gamma : O \rightarrow A$.

Итак, число ломаных, соединяющих точку O с точкой A и не пересекающих прямую $y = -1$, равно числу всевозможных ломаных, ведущих из точки O в точку D .

Осталось найти число ломаных $\bar{\gamma}$. Их будет в точности C_{x+y}^x , где x — число нулей, а y — число единиц в соответствующих ломаным $\bar{\gamma}$ двоичных наборах (числа x и y одинаковы для всех ломаных и зависят только от координат их начала и конца). Зная координаты концов ломаной $\bar{\gamma}$, составим систему уравнений

$$\begin{cases} x + y = 2n, \\ x - y = -2, \end{cases}$$

решив которую, найдем $x = n - 1$, $y = n + 1$.

Таким образом, число неподходящих ломаных равно $C_{2n}^{n-1} = C_{2n}^{n+1}$.

Число же ломаных, не пересекающих прямую l , выражается разностью числа всех ломаных и пересекающих ее, т. е.

$$\begin{aligned} c_n &= C_{2n}^n - C_{2n}^{n-1} = \frac{(2n)!}{n!n!} - \frac{(2n)!}{(n-1)!(n+1)!} = \\ &= \frac{(2n)!}{(n-1)!n!} \left(\frac{1}{n} - \frac{1}{n+1} \right) = \frac{1}{n+1} C_{2n}^n. \end{aligned}$$

Мы получили тот же ответ, что и раньше, но из совершенно других соображений.

Заключительное замечание. Выбор прямой $l: y = -1$ однозначен. Действительно, если мы возьмем в качестве l прямую, лежащую выше, например прямую $y = 0$, то неподходящими станут все ломаные, так как все они выходят из начала координат, лежащего на прямой. Если мы возьмем в качестве l прямую, лежащую ниже, например $y = -2$, то в числе неподходящих не будет ломаных с начальными отрезками, на которых число единиц превышает число нулей на 1, а такие ломаные не удовлетворяют условию.

П2.3. Приложения чисел Каталана

Рассмотрим несколько задач, решаемых с использованием последовательности Каталана.

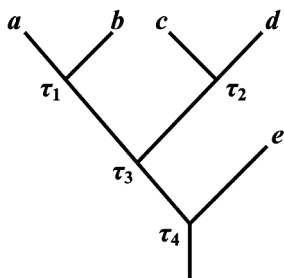


Рис. П2.3

П2.3.1. Тривалентные деревья. Построим соответствие между плоскими тривалентными деревьями с корнем и последовательностями, рассмотренными на примере дерева, изображенного на рис. П2.3 и содержащего пять вершин валентности 1 (кроме основания). Упорядочим вершины согласно порядку их обхода слева направо, начиная с корневой (которую для краткости записи исключим из списка, так как

она будет стоять на первом месте в любом случае).

У изображенного дерева вершины будут упорядочены следующим образом:

$$\tau_4, \tau_3, \tau_1, a, b, \tau_2, c, d, e.$$

Обозначим вершины валентности 3 (соединенные с тремя другими) единицей, а остальные — нулем, опустив последнюю одновалентную вершину (так как при выбранном порядке обхода тривалентная вершина не может быть последней, т. е. опущенным знаком всегда будет ноль). Рассмотренному дереву будет соответствовать такая последовательность: 11100100.

Очевидно, что каждому такому дереву можно однозначно поставить в соответствие двоичную последовательность, состоящую из $2(n - 1)$ знаков ($n - 1$ тривалентных вершин и $n - 1$ одновалентных).

Рассмотрим алгоритм построения дерева по заданной последовательности. Каждая единица преобразуется в тривалентную вершину, причем следующая вершина будет непосредственно с ней связана, каждый нуль — в одновалентную, причем следующая вершина будет связана с ближайшей свободной тривалентной. Таким образом, каждая единица увеличивает на единицу количество свободных тривалентных вершин (добавляя одну новую, расходуя одну связь предыдущей тривалентной и две собственные связи), а каждый нуль — уменьшает на единицу. Рассмотрим построение дерева по последовательности на основе приведенного выше примера (табл. П2.1).

Таблица П2.1

Знак	Создаваемая вершина	Свободные тривалентные вершины
1	τ_4	τ_4
1	τ_3	τ_4, τ_3
1	τ_1	τ_4, τ_3, τ_1
0	a	τ_4, τ_3
0	b	τ_4
1	τ_2	τ_4, τ_2
0	c	τ_4
0	d	Нет

Тривалентная вершина считается свободной, если связана менее чем с тремя другими, причем при создании следующей вершины число связей текущей не станет равно трем.

Очевидно, для взаимно однозначного соответствия двоичной последовательности четной длины такому дереву необходимо и достаточно, чтобы эта последовательность содержала равное чи-

сло нулей и единиц и при этом на любом ее начальном отрезке нулей было не больше, чем единиц, причем последовательности длиной $2n$ будет соответствовать дерево с $n+1$ одновалентными вершинами. Число таких последовательностей равно n -му числу Каталана, следовательно, число рассматриваемых деревьев с n одновалентными вершинами равно $(n-1)$ -му числу Каталана.

П2.3.2. Расстановка скобок в алгебраическом выражении.

Рассмотрим последовательность $\lambda_1, \lambda_2, \lambda_3, \dots, \lambda_n$, состоящую из n чисел. Найдем количество способов расстановки между этими числами скобок, причем внутри любой пары скобок должны находиться два объекта, каждый из которых может быть числом либо другим выражением, заключенным в скобки.

Поставим каждому числу во взаимно однозначное соответствие одновалентную вершину. Когда два числа находятся внутри пары скобок, создадим трехвалентную вершину, связанную с вершинами, соответствующими этим числам, и поставим ее в соответствие этой паре скобок. Если вместо одного или обоих чисел присутствует выражение, заключенное в скобки, вместо одновалентной вершины возьмем трехвалентную, соответствующую этой паре скобок. Рассмотренному выше в примере дереву будет соответствовать следующий способ расстановки скобок:

$$((ab)(cd))e.$$

Приведем таблицу соответствия вершин дерева и элементов выражения (табл. П2.2).

Таблица П2.2

Элемент выражения	Вершина
a	a
$\vdots$	$\vdots$
e	e
(ab)	τ_1
(cd)	τ_2
$((ab)(cd))$	τ_3
$((((ab)(cd))e)$	τ_4

Поскольку рассмотренное соотношение является взаимно однозначным и выражению, состоящему из n чисел, будет соответствовать дерево с n одновалентными вершинами, количество способов расстановки скобок будет равно $(n - 1)$ -му числу Каталана на c_{n-1} .

П2.3.3. Триангуляции. *Триангуляцией* называют разбиение плоского выпуклого многоугольника на треугольники непересекающимися отрезками, попарно соединяющими вершины этого многоугольника. Поставим во взаимно однозначное соответствие триангуляции $(n+1)$ -угольника и деревья, содержащие n одновалентных вершин. Изобразим триангуляцию, соответствующую дереву из первого примера (рис. П2.4).

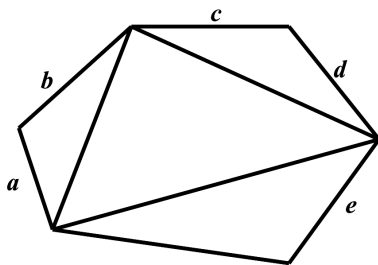


Рис. П2.4

Каждая диагональ многоугольника стягивает два ребра, ребро и другую диагональ либо две диагонали. Поставим в соответствие каждой диагонали вершину дерева из первого примера, причем вершина будет связана с теми вершинами, которые сопоставлены ребрам или диагоналям, которые она стягивает. Очевидно, что соответствие будет взаимно однозначным. Следовательно, число триангуляции k -угольника равно $(k - 1)$ -му числу Каталана c_{k-1} .

П2.4. Задачи

1. На окружности расставлены $2n$ пронумерованных точек. Сколькими способами их можно попарно соединить непересекающимися хордами?

2. Доказать следующее рекуррентное соотношение для чисел Каталана:

$$c_{n+1} = c_0 c_n + c_1 c_{n-1} + c_2 c_{n-2} + \dots + c_n c_0.$$

3. Доказать равенство $c_{n+1} = \frac{4n+2}{n+2} c_n = \frac{(4n+2)!!!!}{(n+2)!}$.

4. Найти число различных последовательностей из n единиц и $n + 10$ нулей, в которых среди первых i знаков, при всех $i = 1, 2, \dots, 2n + 10$ число единиц может превышать число нулей не более чем на три.

5. Упростить выражение $\sum_{k=0}^n C_{2k}^k C_{2n-2k}^{n-k}$. (Указание: какова производящая функция последовательности $\{C_{2n}^n\}_{n=0}^{\infty}$?)

6. Найти число различных последовательностей из n нулей и n единиц, в которых среди первых i знаков, при всех $i = 1, 2, \dots, n$ число нулей отличается от числа единиц не более чем на k .

ЛИТЕРАТУРА

1. *Андерсон Дж. А.* Дискретная математика и комбинаторика. М.: Вильямс, 2004.
2. *Виленкин Н.Я., Виленкин А.Н., Виленкин П.А.* Комбинаторика. М.: МЦНМО, 2006.
3. *Гаврилов Г.П., Сапоженко А.А.* Задачи и упражнения по дискретной математике. М.: Физматлит, 2005.
4. *Грэхем Р., Кнут Д., Паташник О.* Конкретная математика. Основание информатики. М.: Мир, 1998.
5. *Гульден Я., Джексон Д.* Перечислительная комбинаторика. М.: Наука, 1990.
6. *Ильин В.А., Позняк Э.Г.* Основы математического анализа: Учебник: В 2 т. Т. 1. М.: Наука, 1971.
7. *Кнут Д.* Искусство программирования: В 3 т. Т. 1. М.: Вильямс, 2000.
8. Комбинаторный анализ. Задачи и упражнения / Под ред. К.А. Рыбникова М.: Наука, 1982.
9. *Кострикин А.И.* Введение в алгебру. Основы алгебры. М.: Физматлит, 1994.
10. *Ландо С.К.* Лекции о производящих функциях. М.: МЦНМО, 2004.
11. *Риордан Дж.* Введение в комбинаторный анализ. М.: Изд-во иностр. лит., 1963.
12. *Рыбников К.А.* Введение в комбинаторный анализ. М.: Московский университет, 1985.
13. *Феллер В.* Введение в теорию вероятностей и ее приложения. Учебник: В 2 т. Т. 1. М.: Мир, 1984.
14. *Холл М.* Комбинаторика. М.: Мир, 1970.
15. *Яблонский С.В.* Введение в дискретную математику. 2-е изд. М.: Наука, 1986.
16. *Roberts F.S.* Applied Combinatorics. Prentice-Hall Inc., New Jersey, 1984.

ОГЛАВЛЕНИЕ

Предисловие	3
Глава 1. Основные комбинаторные понятия и схемы	4
1.1. Основные перечислительные правила	4
1.2. Основные комбинаторные схемы	5
1.3. Числа Стирлинга второго рода	11
1.4. Подстановки на конечном множестве	14
1.5. Числа Стирлинга первого рода	15
1.6. Урновые схемы	18
1.7. Схемы отображений конечных множеств	20
1.8. Задачи	21
Глава 2. Формула включения-исключения	23
2.1. Характеристическая функция множества	23
2.2. Число элементов, удовлетворяющих тем или иным свойствам	26
2.3. Приложения формулы включения-исключения	27
2.4. Задачи	29
Глава 3. Линейные рекуррентные последовательности	31
3.1. Основные понятия и определения	31
3.2. Линейное пространство линейных рекуррентных последовательностей	32
3.3. Решение линейных рекуррентных соотношений	36
3.4. Задачи	42
Глава 4. Производящие функции	44
4.1. Энумераторы	44
4.2. Формальные степенные ряды	51
4.3. Получение производящих функций	56
4.4. Задачи	65
Приложения	67
Литература	101

Учебное издание

Жуков Алексей Евгеньевич
Жуков Дмитрий Александрович

Элементы комбинаторики

Редактор *В.М. Царев*
Корректор *Е.В. Николаева*
Компьютерная верстка *В.И. Товстоног*

Подписано в печать 26.02.2014. Формат 60×84/16.

Усл. печ. л. 6,05. Тираж 100 экз. Изд. № 46.

Заказ

Издательство МГТУ им. Н.Э. Баумана.
Типография МГТУ им. Н.Э. Баумана.
105005, Москва, 2-я Бауманская ул., д. 5, стр. 1.

ДЛЯ ЗАМЕТОК