Московский Государственный Университет
имени М. В. Ломоносова
Факультет Вычислительной Математики и Кибернетики
Кафедра Математической Кибернетики

Дополнительные главы дискретной математики

лектор — старший преподаватель В. П. Воронин
составитель — А. Д. Поспелов

Москва — 2002

Содержание

Глава 1

Комбинаторика

Основным объектом изучения комбинаторики является как правило конечное (хотя, возможно, и счетное) множество, из элементов которого составляются различные комбинаторные конфигурации. Основными вопросами при этом являются существование требуемых конфигураций, алгоритмы их построения, оптимизация алгоритмов (если таковые существуют), а также задачи перечислительного характера (например, количество конфигураций с требуемыми свойствами).

Одним из наиболее популярных примеров комбинаторной постановки может служить *задача о магическом квадрате*. Она ставится следующим образом: для данного натурального n расположить числа от 1 до n^2 в целочисленных точках квадрата плоскости $Oxy : 1 \leqslant x \leqslant n,\ 1 \leqslant y \leqslant n$ так, чтобы сумма всех чисел, расположенных в любом столбце, была равна сумме всех чисел, расположенных в любой строке и равнялась сумме всех чисел, стоящих на каждой из диагоналей. К положительным достижениям в решении этой задачи относится, например, факт существования алгоритма, строящего магический квадрат для любого заданного n. В то же время открытым остается вопрос о количестве различных магических квадратов для $n \geqslant 5$. Примером магического квадрата для $n = 3$ может выступать следующий:

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

Другим известным примером является *задача о шести офицерах*, которая ставится следующим образом: имеется шесть полков, в каждом полку имеется шесть офицеров, причем все имеют разные звания. Вопрос заключается в том, возможно ли расположить всех этих офицеров в квадрате 6×6 так, чтобы на любой линии стояли офицеры из разных полков и с разными званиями. Задача обобщается на случай $n = 4k + 2$ полков и званий. Доказано, что при $k = 1$ решения не существует, а при $k \geqslant 2$ решение имеется.

Бинарное отношение.

Определение 1.0.1. Декартовым произведением множеств X и Y называется множество

$$X \times Y = \{(x,y) \mid x \in X,\ y \in Y\}.$$

Определение 1.0.2. Любое подмножество декартова произведения $\rho \subseteq X \times Y$ называется *бинарным отношением*.

Примерами бинарного отношения могут служить равенство $x = y$, предшествование $x \leqslant y$ и другие. *Областью определения бинарного отношения* ρ называется множество

$$D_\rho = \{x \in X \mid \exists (x,y) \in \rho\}.$$

Областью значений бинарного отношения ρ называется множество

$$R_\rho = \{y \in Y \mid \exists (x,y) \in \rho\}.$$

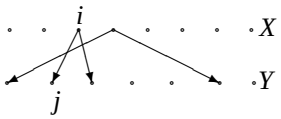
Из определения следует, что пустое множество $\varnothing$ также считается бинарным отношением.

Бинарное отношение может задаваться также в виде прямоугольной (вообще говоря, бесконечной) $0,1$-матрицы:

$$\begin{matrix} & & j & \\ & \begin{pmatrix} & \vdots & \\ \cdots & 1 & \cdots \\ & \vdots & 0 \\ & \vdots & \end{pmatrix}_{n \times m} \\ i & \end{matrix}$$

где n — мощность множества X, а m — мощность множества Y могут, вообще говоря, равняться счетной бесконечности. Считается, что все элементы каждого из множеств X и Y пронумерованы натуральными числами. Элемент матрицы с индексом (i, j) равняется единице тогда и только тогда, когда пара $(x_i, y_j) \in \rho$, где x_i — элемент из X, занумерованный числом i, а y_j — элемент из Y, занумерованный числом j; и равняется нулю в противном случае.

Бинарное отношение можно задать в виде двудольного орграфа:



при этом дуга из элемента из X с номером i идет к элементу из Y с номером j тогда и только тогда, когда $(x_i, y_j) \in \rho$. Такое задание бинарного отношения позволяет рассматривать его как многозначное отображение.

Определение 1.0.3. *Обратным бинарным отношением к* ρ называется бинарное отношение

$$\rho^{-1} = \{(y,x) \mid (x,y) \in \rho\}.$$

Определение 1.0.4. *Композицией бинарных отношений* ρ_1 *и* ρ_2 называется бинарное отношение

$$\rho = \rho_2 \circ \rho_1 = \{(x,z) \mid \exists y : (x,y) \in \rho_1,\ (y,z) \in \rho_2\}.$$

Очевидны простейшие свойства этих операций:

$$\left(\rho^{-1}\right)^{-1} = \rho$$

и

$$(\rho_2 \circ \rho_1)^{-1} = \rho_1^{-1} \circ \rho_2^{-1}.$$

В дальнейшем будем рассматривать частный случай бинарного отношения — $X = Y$ — бинарное отношение на декартовом квадрате. Введем для него следующие аксиомы.

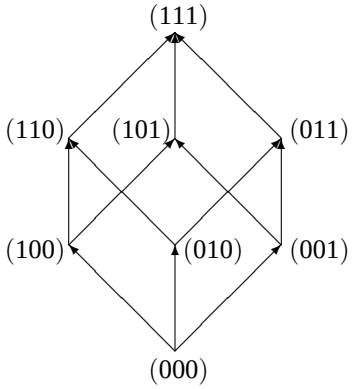
1. Аксиома *рефлексивности*: для любого $x \in X$ выполняется $x \rho x$. Иными словами в матрице, задающей это бинарное отношение, на диагонали стоят единицы.
2. Аксиома *симметричности*: для любых $x, y \in X$ выполняется $x \rho y \Rightarrow y \rho x$. Иными словами, матрица, задающая это бинарное отношение, является симметрической.
3. Аксиома *транзитивности*: для любых $x, y, z \in X$ выполняется $x \rho y \,\&\, y \rho z \Rightarrow x \rho z$.
4. Аксиома *антисимметричности*: для любых $x, y \in X$ выполняется $x \rho y \,\&\, y \rho x \Rightarrow x = y$.

Определение 1.0.5. Аксиомы 1, 2 и 3 определяют *отношение эквивалентности*. Такое отношение разбивает множество X, на котором оно задано, на *классы эквивалентности*, множество которых в свою очередь называется *фактормножеством*.

Часто в комбинаторных постановках требуется узнать по заданному основному множеству и отношению эквивалентности на нем число классов эквивалентности. Отношение эквивалентности можно задавать группой перестановок. В этом случае возможен вопрос о числе элементов в множестве по известной группе перестановок.

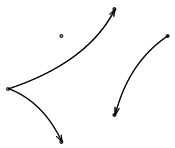
Определение 1.0.6. Аксиомы 1, 3 и 4 определяют *бинарное отношение частичного порядка*. Примером может служить упорядочение множества натуральных чисел по делимости: $y \mid x$ или $x \vdots y$ означает, что y является делителем числа x. Множество с заданным на нем частичным порядком называется *частично упорядоченным*.

Частично упорядоченное по делимости множество натуральных чисел обозначается $(\mathbb{N}, \mid)$. Бинарные отношения частичного порядка удобно изображать с помощью *диаграмм Хассе*. Диаграмма Хассе представляет собой ориентированный ациклический граф, множеством вершин которого является исходное множество, а дуга между вершинами x и y рисуется тогда и только тогда, когда $x \rho y$ и $\nexists z : x \rho z \,\&\, z \rho y$. Например, частичный порядок наборов из нулей и единиц, определяющий монотонность функций алгебры логики, будет выглядеть на диаграмме Хассе следующим образом:



В некоторых случаях можно обойтись без дуг, располагая элементы множества по ярусам. Так, например, вышеописанное частично упорядоченное множество $(\mathbb{N}, |)$ можно изобразить так:

Также в случае $X = Y$ граф, описывающий частично упорядоченное множество, не обязательно будет двудольным и может выглядеть по-другому:



По индукции можно определить также n-арные отношения. Помимо аксиом 1, 2, 3 и 4 может оказаться также, что $x \rho y \,\&\, x \rho z \Rightarrow y = x$. Если рассматривать бинарное отношение как функцию f, ставящую в соответствие множеству X некоторое другое множество D_f, то в этом случае она будет инъективной. Область определения $f : X \to Y$ совпадает с X, область значений в то же время не обязательно совпадает с Y. В случае $X = Y$ и $D_f = X$ при конечных множествах f взаимно однозначна. На функции распространяются определенные на бинарных отношениях композиции и обратные элементы. Таким образом, появляется связь комбинаторных чисел с функциями.

Часто бывает удобным исследовать не саму комбинаторную конфигурацию, а в некотором роде изоморфную ей. С тем, чтобы сделать это рассмотрение корректным, сформулируем *принцип взаимно однозначного соответствия*. Если одному множеству комбинаторных конфигураций с определенными свойствами изоморфно относительно этих свойств ставится в соответствие другое множество комбинаторных конфигураций, то число комбинаций, обладающих определенными свойствами в обоих множествах одно и то же.

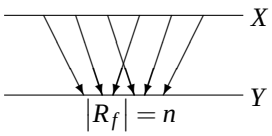
1.1 Простейшие комбинаторные числа

Пусть $X = \{1, 2, \ldots, n\}, Y = \{y_1, \ldots, y_m\}$. Множество всех отображений множества X во множество Y обозначается Y^X. Оно имеет мощность m^n. Это множество изоморфно множеству раскладок n шаров, помеченных числами $1, \ldots, n$ по m ящикам, помеченным элементами $y_1, \ldots, y_m$, также оно изоморфно множеству слов $y_{i_1} y_{i_2} \ldots y_{i_n}$ длины n в алфавите Y. Отображение f называется *инъективным*, если $i \neq j \,\&\, i \to y_s,\ j \to y_\ell \Rightarrow y_s \neq y_\ell$. Для того, чтобы отображение было инъективно, очевидно, необходимо, чтобы $|X| \leqslant |Y|$, то есть $n \leqslant m$. Число инъективных отображений равно *убывающему факториалу* $[m]_n = m(m-1)(m-2)\cdots(m-n+1)$. В терминах шаров и ящиков этому множеству соответствует множество раскладок n различимых шаров по m различимым ящикам так, чтобы в каждом ящике было бы не более одного шара. В терминах слов в алфавите Y этому множеству соответствует множество слов длины n в алфавите Y, все буквы в котором различны. Отображение f называется *сюръективным*, если $R_f = Y$, то есть каждый элемент из Y имеет хотя бы один прообраз. Для того, чтобы отображение было сюръективным, очевидно, необходимо, чтобы $|X| \geqslant |Y|$. По принципу взаимно однозначного соответствия этой комбинаторной конфигурации соответствует множество раскладок n различимых шаров по m различимым ящикам так, чтобы в каждом ящике оказалось хотя бы по одному шару или множество слов длины n в алфавите из m букв таких, что каждая буква алфавита присутствует в слове хотя бы один раз. Число сюръективных отображений X в Y равно $\binom{n}{m} \cdot m! \cdot m^{n-m}$. Отображение, являющееся одновременно сюръективным и инъективным, называется *биективным (взаимно однозначным, биекцией)*. Для того, чтобы отображение было биективным, очевидно, необходимо, чтобы $|X| = |Y|$. В случае конечных множеств следующие три утверждения эквивалентны:

1. f биективно;
2. f сюръективно и $|X| = |Y|$;
3. f инъективно и $|X| = |Y|$.

Определение 1.1.1. Биективные отображения конечных множеств в себя называются *перестановками*.

Введем бинарное отношение на множестве инъективных отображений: $f \rho g \Leftrightarrow R_f = R_g$.



Очевидно, это будет являться отношением эквивалентности. Оно разбивает все множество инъективных отображений на $n!$ классов эквивалентности. В силу свойств фактормножества, его мощность будет равна *биномиальному коэффициенту* $\frac{[m]_n}{n!} = \frac{m!}{n!(m-n)!} = C_m^n = \binom{m}{n}$. По принципу взаимно однозначного соответствия вышеописанное фактормножество эквивалентно множеству n-элементных подмножеств m-элементного множества или множеству наборов из нулей и единиц длины m ровно с n единицами.

Этот результат можно обобщить, если допустить вхождение элементов в подмножество с кратностью. *Мультимножеством* называется множество, у каждого элемента которого есть *кратность* — натуральное число, символизирующее количество вхождений данного элемента в мультимножество. Мощностью мультимножества называется сумма кратностей всех его элементов. Иными словами необходимо найти число мультиподмножеств мощности n множества $Y, |Y| = m$. Используя принцип взаимно однозначного соответствия, подсчет можно перенести на наборы целых неотрицательных чисел:

$$\begin{cases} \alpha_1 + \alpha_2 + \cdots + \alpha_m = n, \\ \alpha_i \geqslant 0,\ \alpha_i \in \mathbb{Z},\ i = \overline{1,m}. \end{cases} \tag{1.1}$$

Число различных решений этой системы и будет равно числу мультиподмножеств мощности n множества мощности m. Число решений в данном случае будет также являться биномиальным коэффициентом. Действительно, применяя принцип взаимно однозначного соответствия, можно каждому решению $(\alpha_1, \ldots, \alpha_m)$ взаимно однозначно поставить в соответствие набор длины $n+m-1$ из нулей и единиц $\left(\underbrace{1\ldots1}_{\alpha_1}0\underbrace{1\ldots1}_{\alpha_2}0\ldots0\underbrace{1\ldots1}_{\alpha_m}\right)$. Таким образом, число решений равно числу наборов указанной длины с $m-1$ нулем, то есть биномиальному коэффициенту $\binom{n+m-1}{m-1} = \binom{n+m-1}{n}$. Это число называется *числом сочетаний с повторениями*. Ему можно придать несколько другой содержательный смысл: число различных последовательностей шаров, извлекаемых из урны с возвращением.

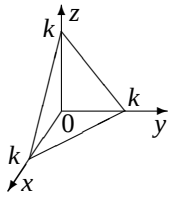
Число мультиподмножеств, содержащих каждый элемент исходного множества по крайней мере один раз, совпадает с числом решений системы

$$\begin{cases} \alpha_1 + \alpha_2 + \cdots + \alpha_m = n, \\ \alpha_i \in \mathbb{N},\ i = \overline{1,m}, \end{cases}$$

которое по принципу взаимно однозначного соответствия совпадает с числом решений системы

$$\begin{cases} \alpha_1' + \alpha_2' + \cdots + \alpha_m' = n - m, \\ \alpha_i' \geqslant 0,\ \alpha_i \in \mathbb{Z},\ i = \overline{1,m}, \end{cases}$$

то есть равно $\binom{n-1}{n-m}$. Используя полученные результаты можно, например, найти число целочисленных точек в тетраэдре $x, y, z \geqslant 0,\ x+y+z \leqslant k$.



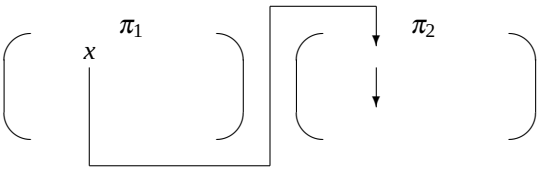
Их число равно $\binom{k+2}{k} = \frac{(k+1)(k+1)}{2}$.

Введем еще одно комбинаторное число: $[m]^n = m(m+1)\cdots(m+n-1) = [m+n-1]_n$ — *возрастающий факториал*. Это число имеет следующий содержательный смысл: имеется m-ярусный стеллаж, на который надо расставить n книг, причем порядок книг на полке имеет значение. Действительно, для первой книги имеется ровно m различных возможностей поставить ее на одну из полок. Для второй книги возможностей уже на одну больше, так как на одной из полок есть уже две неравнозначные позиции. И так далее. В результате получится возрастающий факториал.

Перестановки. Рассмотрим теперь подробней взаимно однозначные отображения множества

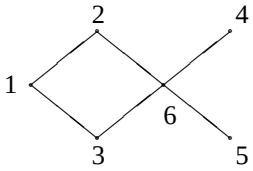
$$X = \{1, 2, \ldots, n\}$$

на себя, то есть перестановки. Всего их $n!$. Множество перестановок n-элементного множества называется *симметрической группой* степени n и обозначается S_n. Чтобы мотивировать такое определение, введем *произведение (композицию)* двух перестановок $\pi_1, \pi_2 \in S_n \Rightarrow \pi_1 \cdot \pi_2 = \pi$ по следующему правилу: $\pi_1 \cdot \pi_2(x) = \pi_2(\pi_1(x))$.



Иногда в литературе композицию определяют наоборот: $\pi_1 \cdot \pi_2(x) = \pi_1(\pi_2(x))$, однако, мы будем придерживаться введенных выше обозначений. Таким образом, S_n — группа с введенным выше внутренним законом композиции. Единичным элементом в этой группе служит единичная перестановка $e = \left(\begin{smallmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{smallmatrix}\right)$. Для каждой перестановки $\pi = \left(\begin{smallmatrix} 1 & 2 & \dots & n \\ a_1 & a_2 & \dots & a_n \end{smallmatrix}\right) \in S_n$ существует обратная перестановка $\pi^{-1} = \left(\begin{smallmatrix} a_1 & a_2 & \dots & a_n \\ 1 & 2 & \dots & n \end{smallmatrix}\right) \in S_n$, при это подразумевается, что столбцы последней переупорядочены так, что элементы первой строчки расположены по возрастанию. Действительно, в этом случае $\pi \cdot \pi^{-1} = \pi^{-1} \cdot \pi = e$. Можно показать, что операция композиции ассоциативна, но некоммутативна. Также справедливо утверждение о том, что любая конечная группа изоморфна симметрической группе подходящего порядка n.

Перестановками можно описывать всевозможные повороты и симметрии. Так, например, группа симметрий графа (группа перестановок вершин, приводящих к графу, изоморфному исходному)

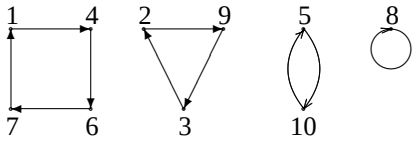


содержит всего четыре элемента: e, $\pi_1 = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 2 & 4 & 5 & 6 \end{smallmatrix}\right)$, $\pi_2 = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 5 & 4 & 6 \end{smallmatrix}\right)$, $\pi_3 = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 2 & 5 & 4 & 6 \end{smallmatrix}\right)$.

Граф, задающий перестановку имеет достаточно простой вид. Поясним это на примере: пусть дана перестановка

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 9 & 2 & 6 & 10 & 7 & 1 & 8 & 3 & 5 \end{pmatrix}.$$

Тогда ей можно поставить в соответствие набор непересекающихся контуров



В этом случае говорят, что перестановка распадается на соответствующие циклы. В общем случае, начиная последовательно применять перестановку к элементу i, затем к $\pi(i)$, и так далее, в силу конечности исходного множества рано или поздно наступит повтор, а в силу взаимной однозначности перестановки этот повтор наступит тогда, когда значение перестановки станет равным i. Таким образом, для любой перестановки допустимо представление в виде произведения своих простых циклов. Перестановка из примера представляется в виде произведения следующим образом: $[1,4,6,7]\,[2,9,3]\,[5,10]\,[8]$. При этом порядок элементов внутри цикла важен, а порядок циклов в произведении не играет никакой роли. По договоренности в дальнейшем будем писать циклы в порядке возрастания их наименьших элементов. Также часто не будем выделять циклы единичной длины, то есть неподвижные элементы. Тогда, если $\pi_1 = [C_1]$, где C_1 — упорядоченный набор элементов, образующих цикл, а $\pi_2 = [C_2]$, при условии $C_1 \cap C_2 = \varnothing \Rightarrow \pi = \pi_1 \cdot \pi_2 = \pi_2 \cdot \pi_1 = [C_1]\,[C_2]$. Заметим, что в данном случае перестановки, представляющие простые циклы, коммутируют в силу того, что на любой элемент в таком произведении будет действовать только одна перестановка.

Определение 1.1.2. *Типом перестановки π множества $X = \{1,2,\dots,n\}$* называется вектор длины n с целыми неотрицательными компонентами $\lambda(\pi) = (\lambda_1, \lambda_2, \dots, \lambda_n)$, где λ_1 — число петель (неподвижных элементов), λ_i для $i = \overline{2,n}$ — число циклов длины i.

Тип рассмотренной в примере перестановки будет $(1,1,1,1,0,0,0,0,0,0)$.

Компоненты вектора типа перестановки удовлетворяют простому соотношению:

$$\sum_{i=1}^{n} i\lambda_i = n.$$

Зададимся вопросом, сколько перестановок из S_n имеют заданный тип. Ответом на него служит следующее число: $\frac{n!}{\lambda_1! \cdots \lambda_n! 1^{\lambda_1} \cdots n^{\lambda_n}}$.

$$\underbrace{[\dots][\dots]}_{\lambda_n}\underbrace{[\dots][\dots]}_{\lambda_{n-1}}\cdots\underbrace{[\dots][\dots]}_{\lambda_1}$$

Расставляем все n элементов по местам ($n!$ способов). Затем отождествляем порядок циклов внутри группы циклов одной длины, то есть делим на $\lambda_1!\cdots\lambda_n!$. Также отождествляем порядки элементов внутри цикла, если они определяют один и тот же цикл: для конкретного цикла длины k число различных способов его определить в одной группе равно k (k циклических сдвигов), то есть делим на $1^{\lambda_1}\cdots n^{\lambda_n}$. Получаем утверждаемое число.

Будем говорить, что элементы a_i и a_j в перестановке $\begin{pmatrix}\cdots & i & \cdots & j & \cdots\\ \cdots & a_i & \cdots & a_j & \cdots\end{pmatrix}$ образуют *инверсию*, если $i<j$ & $a_i>a_j$. Число инверсий перестановки π будем обозначать через $I(\pi)$. Так, например, $I(e)=0$, $I\left(\begin{pmatrix}1 & \cdots & n\\ n & \cdots & 1\end{pmatrix}\right)=\frac{n(n-1)}{2}=\binom{n}{2}$. Для перестановки определяется знак:

$$\operatorname{sgn}(\pi)=(-1)^{I(\pi)}=\begin{cases}1, & \text{если перестановка } \textit{четная},\\ -1, & \text{если перестановка } \textit{нечетная}.\end{cases}$$

Для знака перестановки выполняется очевидное свойство $\operatorname{sgn}(\pi_1\cdot\pi_2)=\operatorname{sgn}(\pi_1)\cdot\operatorname{sgn}(\pi_2)$. Транспозиция двух элементов i и j обозначается просто $[i,j]$, частным случаем транспозиции выступает транспозиция двух соседних элементов $[i,i+1]$. Справедливо утверждение, что любую перестановку можно представить в виде произведения транспозиций двух соседних элементов, число которых равно числу инверсий перестановки. Действительно,

$$\begin{pmatrix}\cdots & i & i+1 & \cdots\\ \cdots & a & b & \cdots\end{pmatrix}[i,i+1]=\begin{pmatrix}\cdots & i & i+1 & \cdots\\ \cdots & b & a & \cdots\end{pmatrix}$$

Берем произвольную перестановку и смотрим, что переводится ею в единицу: $\pi=\begin{pmatrix}\cdots & i & \cdots\\ \cdots & 1 & \cdots\end{pmatrix}$. Тогда $\pi\cdot[i-1,i]\cdot[i-2,i-1]\cdots[1,2]=\pi_1$ единицу переводит в единицу, причем в силу того, что единица образовывала транспозиции со всеми элементами левее, число транспозиций уменьшилось ровно на $i-1$. Поступаем также со всеми остальными элементами и получаем, что $\pi\cdot t_1\cdot t_2\cdots t_{I(\pi)}=e$. Далее, так как обратным элементом к транспозиции двух элементов является она сама, $\pi=t_{I(\pi)}\cdots t_2\cdot t_1$. Умножение на каждую транспозицию изменяет знак, следовательно, для любых двух перестановок $\pi_1=t_{I(\pi_1)}\cdots t_1$ и $\pi_2=t'_{I(\pi_2)}\cdots t'_1$ верно, что $\operatorname{sgn}(\pi_1\cdot\pi_2)=\operatorname{sgn}(\pi_1)(-1)^{I(\pi_2)}=\operatorname{sgn}(\pi_1)\operatorname{sgn}(\pi_2)$.

Все четные перестановки образуют подгруппу симметрической группы. Знак любой транспозиции вида

$$\underbrace{\begin{pmatrix}\dots & i & \dots & j & \dots\\ \dots & j & \dots & i & \dots\end{pmatrix}}_{k}$$

равен $(-1)^{2k+1}=-1$. Определим знак произвольного простого цикла как произведение знаков простых транспозиций, композицией которых является данный цикл:

$$[a_1a_2\dots a_k]=[a_1a_2][a_2a_3]\cdots[a_{k-1}a_k]\Rightarrow\operatorname{sgn}([a_1\dots a_k])=(-1)^{k-1}.$$

Таким образом, чтобы определить знак перестановки, нужно знать число циклов четной длины:

$$\lambda(\pi)=(\lambda_1,\lambda_2,\dots,\lambda_n)\Rightarrow\operatorname{sgn}(\pi)=(-1)^{\sum\limits_{i=1}^{\left\lfloor\frac{n}{2}\right\rfloor}\lambda_{2i}}.$$

Принцип включения и исключения. Из теории множеств известны простейшие мощностные равенства: $|A\cup B|=|A|+|B|-|A\cap B|$, $|A\cup B\cup C|=|A|+|B|+|C|-|A\cap B|-|B\cap C|-|C\cap A|+|A\cap B\cap C|$ и так далее. Следующее предложение докажем по индукции. Пусть есть исходное множество $\mathscr{N}$, $|\mathscr{N}|=N$ и набор свойств $P_1,\dots,P_n$, кодируемые набором $\{1,2,\dots,n\}=[n]$. Для каждого элемента формулируем n высказываний относительно обладания им каждого из этих свойств. Пусть $I=\{i_1,i_2,\dots,i_s\}\subseteq[n]$ — подмножество кодов свойств. Обозначим

$$N[I]=\sharp\{a\in\mathscr{N}\mid a\ \text{обладает в точности свойствами } P_{i_1},\dots,P_{i_s}\text{ и больше не обладает никакими}\}$$

Так, например, $N[\varnothing]$ равно числу элементов $\mathscr{N}$, не обладающих ни одним из указанных свойств. Далее, обозначим

$$N(I)=\sum_{I\subseteq J\subseteq[n]}N[J]$$

— число элементов, обладающих заданными свойствами $P_{i_1},\dots,P_{i_s}$ с кодами из I и, быть может, еще какими-то. В терминах n-мерного булева куба, все вершины которого помечены неотрицательными целыми числами, показывающими сколько элементов из $\mathscr{N}$ обладают соответствующими свойствами, эти числа имеют следующий содержательный смысл: $N[I]$ — это число, приписанное вершине, у которой все разряды с номерами из I равны единице, а оставшиеся равны нулю; $N(I)$ — это сумма чисел, приписанных всем вершинам грани между вершиной $N[I]$ и единичной. Пусть теперь

$$N_{[r]}=\sum_{\substack{J\subseteq[n]\\ |J|=r}}N[J]$$

— число элементов, обладающих ровно r (неважно какими) свойствами. В n-мерном булевом кубе это сумма чисел, приписанных вершинам r-го слоя;

$$N_{(r)} = \sum_{\substack{J\subseteq(n)\\|J|=r}} N(J)$$

— число элементов, обладающих не менее r (неважно какими) свойствами. В n-мерном булевом кубе это сумма чисел, приписанных вершинам всех слоев, начиная с r-го.

Теперь можно сформулировать *принцип включения и исключения*:

Теорема 1.1 (Принцип включения и исключения).

$$N_{[0]} = N_{(0)} - N_{(1)} + \cdots + (-1)^i N_{(i)} + \cdots + (-1)^n N_{(n)}, \tag{1.2}$$

$$N_{[m]} = \binom{m}{m} N_{(m)} - \binom{m+1}{m} N_{(m+1)} + \cdots + (-1)^i \binom{m+i}{m} N_{(m+i)} + \cdots + (-1)^{n-m} \binom{n}{m} N_{(n)}. \tag{1.3}$$

□ *Док-во.* При $n=1$ $N_{[0]} = N_{(0)} - N_{(1)} = N - N_{(1)}$ и формула (1.2), очевидно, справедлива. Пусть формула справедлива для $n-1$ свойств. Имеем

$$N_{[0]} = N_{(0)} - N_{(1)} + N_{(2)} - N_{(3)} + \cdots + (-1)^{n-1} N_{(n-1)}. \tag{1.4}$$

Эта формула справедлива и для совокупности объектов, обладающих свойством n:

$$N[n] = N(n) - N^n_{(1)} + \cdots + (-1)^{n-1} N^n_{(n-1)}, \tag{1.5}$$

где $N^n_{(j)}$ — число объектов, обладающих свойством n и еще какими-то другими свойствами, число которых не меньше j. Вычитая формулу (1.5) из (1.4), получаем формулу (1.2).

Докажем теперь формулу (1.3). Перепишем ее следующим образом:

$$N_{[m]} = \sum_{k=0}^{n-m} (-1)^k \binom{m+k}{m} \sum_{i=m+k}^{n} N_{[i]}.$$

Докажем, что каждый предмет, обладающий в точности m свойствами, будет учтен в ней ровно один раз. В самом деле, элементы, обладающие $s < m$ свойствами, не учитываются очевидным образом. Элемент, обладающий заданными $s = m+t$ свойствами, будет учитываться во внутренней сумме $\binom{m+t}{m+k}$ раз. Но

$$\sum_{k=0}^{n-m} (-1)^k \binom{m+k}{k}\binom{m+t}{m+k} = \binom{m+t}{m} \sum_{k=0}^{t} (-1)^k \binom{t}{k} = \begin{cases} 1 & \text{при } t=0,\\ 0 & \text{при } t>0. \end{cases}$$

Таким образом, в (1.3) ровно по одному разу учитываются элементы, обладающие в точности m свойствами, а остальные не учитываются. ■

Принцип включения и исключения имеет весовой аналог. Пусть задана некоторая весовая функция $\omega : \mathscr{N} \to \mathsf{K}$, где K — кольцо, ставящая каждому элементу $a \in \mathscr{N}$ в соответствие его вес $\omega(a)$. Тогда если во всех обозначениях поменять N на значение веса W, то суммарный вес элементов, обладающих ровно m свойствами будет равен

Теорема 1.2 (Весовой вариант принципа включения и исключения).

$$W_{[m]} = \binom{m}{m} W_{(m)} - \binom{m+1}{m} W_{(m+1)} + \cdots + (-1)^i \binom{m+i}{m} W_{(m+i)} + \cdots + (-1)^{n-m} \binom{n}{m} W_{(n)}. \tag{1.6}$$

□ *Док-во.* Доказательство формулы (1.6) полностью аналогично доказательству формул (1.2) и (1.3) с тем лишь различием, что считать необходимо не число элементов, а их суммарный вес. ■

Перестановки с ограничениями. Будем рассматривать взаимно однозначные отображения множества $X = \{1,2,\ldots,n\}$ в себя *с ограничениями*, то есть для каждого элемента будем запрещать его отображение в какие-то другие. В нижеприведенной таблице под чертой указаны запреты для каждого элемента.

1	2	…	j	…	n
a_1^1	a_1^2	…	a_1^j	…	a_1^n
a_2^1	a_2^2	…	a_2^j	…	a_2^n
. . . . .					
$a_{i_1}^1$	$a_{i_2}^2$	…	$a_{i_j}^j$	…	$a_{i_n}^n$

Некоторые запреты вполне могут быть пустыми.

Примером задачи на перестановки с ограничениями может служить *задача о беспорядках*. В ней требуется найти число перестановок со следующими ограничениями:

$$\begin{array}{cccc} 1 & 2 & \dots & n \\ \hline 1 & 2 & \dots & n \end{array}$$

Такие перестановки называются *беспорядками*. Число беспорядков n-элементного множества обозначим D_n.

Задачи на перестановки с ограничениями часто сводятся к подсчету *перманента* $0,1$-*матрицы*. Вспомним, что определителем квадратной матрицы A_n размера $n \times n$ называется следующее число:

$$\det(A_n) = \sum_{\pi \in S_n} \operatorname{sgn}(\pi) \cdot a_{1,\pi(1)} \cdot a_{2,\pi(2)} \cdots a_{n,\pi(n)}.$$

Обобщениями определителя служат числа, получаемые заменой в правой части знака перестановки $\operatorname{sgn}(\pi)$ некоторой другой функцией перестановки $f(\pi)$, называемой в этом случае *функцией Шура*. Из всех таких функций рассмотрим одну: $f(\pi) \equiv 1$. Выражение

$$\operatorname{per}(A_n) = \sum_{\pi \in S_n} a_{1,\pi(1)} \cdot a_{2,\pi(2)} \cdots a_{n,\pi(n)},$$

получаемое в этом случае, называется *перманентом матрицы*. Он обладает некоторыми свойствами, схожими со свойствами определителя. Так, например, если матрицу транспонировать, то ее перманент не изменится. Также, при вычислении перманента можно использовать разложение по строке или столбцу. Но есть и различия: если переставить две строки (два столбца), перманент не изменится в отличии от определителя, который поменяет знак. Также, добавление к одной из строк (одному из столбцов) линейной комбинации других строк (столбцов), вообще говоря, меняет перманент. Определение перманента можно обобщить на случай прямоугольной матрицы: если, например, число столбов m больше числа строк n, то перманент будет равен сумме всевозможных различных произведений элементов, взятых из разных строк и разных столбцов. В добавление к вышесказанному заметим, что вычисление перманента является NP-полной задачей (в настоящий момент известны только экспоненциальные алгоритмы вычисления перманента), в то время как задача вычисления определителя полиномиальна (известный метод Гаусса требует $O(n^2)$ умножений).

Для таблицы запретов строим $0-1$-матрицу размера $n \times n$, в которой столбцам припишем элементы исходного множества, а строкам — запреты на отображения. Единицу в позиции (i, j) ставим тогда и только тогда, когда элемент i может отображаться перестановкой в элемент j, в противном случае (если отображение i в j запрещено), ставим нуль. Между перестановками и слагаемыми в перманенте устанавливается взаимно однозначное соответствие. Если перестановка нарушает хотя бы один запрет, то соответствующее ей слагаемое будет равно нулю, в противном случае оно будет равно единице. Таким образом, число перестановок с запретами будет просто равно перманенту соответствующей матрицы.

Для задачи о беспорядках перманент выглядит следующим образом:

$$\begin{pmatrix} 0 & 1 & 1 & \dots & 1 \\ 1 & 0 & 1 & \dots & 1 \\ 1 & 1 & 0 & \dots & 1 \\ \dots & \dots & \dots & \ddots & \dots \\ 1 & 1 & 1 & \dots & 0 \end{pmatrix}$$

При $n = 2$

$$\operatorname{per}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = 1;$$

При $n = 3$

$$\operatorname{per}\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} = 2.$$

Вызывает интерес поведение величины числа беспорядков n-элементного множества D_n при $n \to \infty$. Возможны четыре варианта:

$$\frac{D_n}{n!} \to 0; \qquad \frac{D_n}{n!} \to a, \quad 0 < a < \frac{1}{2}; \qquad \frac{D_n}{n!} \to a, \quad \frac{1}{2} \leqslant a < 1; \qquad \frac{D_n}{n!} \to 1.$$

Воспользуемся принципом включения и исключения. Обозначим для $i = \overline{1,n}$ свойством P_i перестановки тот факт, что $i \to i$. Задача свелась к подсчету общего числа перестановок, не обладающих ни одним из этих свойств:

$$N_{[0]} = N_{(0)} - N_{(1)} + \dots + (-1)^i N_{(i)} + \dots + (-1)^{n-m} N_{(n)} =$$
$$n! - \binom{n}{1}(n-1)! + \binom{n}{2}(n-2)! + \dots + (-1)^m \binom{n}{m}(n-m)! + \dots + (-1)^n \binom{n}{n}(n-n)! =$$
$$n! - \frac{n!}{1!} + \frac{n!}{2!} + \dots + \frac{(-1)^m n!}{m!} + \dots + \frac{(-1)^n n!}{n!} = n!\left(1 - \frac{1}{1!} + \frac{1}{2!} + \dots + \frac{(-1)^m}{m!} + \dots + \frac{(-1)^n}{n!}\right).$$

Устремляя n к бесконечности получаем асимптотику числа беспорядков:

$$\frac{D_n}{n!} \xrightarrow[n\to\infty]{} S = \sum_{m=0}^{\infty} (-1)^m \cdot \frac{1}{m!} = e^{-1} = \frac{1}{e}.$$

Таким образом, правильным оказался второй вариант. Задачу о числе беспорядков называют также *задачей Монмора*.

Другой известной задачей на перестановки с ограничениями является *задача Люка*, или *задача о супружеских парах*. Она заключается в нахождении числа рассадок за круглый $2n$-местный стол n супружеских пар так, чтобы никакая супружеская пара не оказалась на соседних стульях. Иногда эту задачу называют также *задачей мажордома*.

Пусть все стулья пронумерованы символами $1, 1', 2, 2', \ldots, n, n'$. Будем без ограничения общности рассуждений считать, что на стульях со штрихами могут сидеть персоны лишь одного пола. Для начала заметим, что перед тем, как будут рассажены все пары, можно рассмотреть всевозможные рассадки дам и относительно уже их искать допустимые рассадки мужчин. Таким образом, число разрешенных рассадок супружеских пар равно $2 \cdot n! \cdot U_n$, где U_n — число способов рассадить n мужчин так, чтобы супруги не сидели рядом. Таблица запретов будет в данном случае выглядеть следующим образом:

$$\begin{array}{cccccccc} 1 & 2 & \ldots & i & \ldots & n-1 & n \\ \hline 1 & 2 & \ldots & i & \ldots & n-1 & n \\ 2 & 3 & \ldots & i+1 & \ldots & n & 1 \\ \hline p_1 & p_2 & \cdots & p_i & \cdots & p_{n-1} & p_n \\ p'_1 & p'_2 & \cdots & p'_i & \cdots & p'_{n-1} & p'_n \end{array} \tag{1.7}$$

Задача сводится к вычислению перманента матрицы

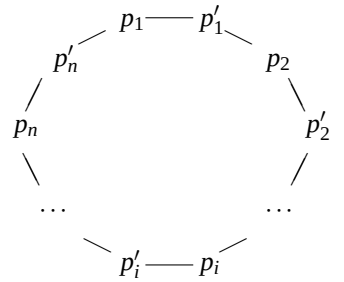
$$\begin{pmatrix} 0 & 0 & 1 & 1 & \ldots & 1 & 1 \\ 1 & 0 & 0 & 1 & \ldots & 1 & 1 \\ 1 & 1 & 0 & 0 & \ldots & 1 & 1 \\ 1 & 1 & 1 & 0 & \ldots & 1 & 1 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & 1 & 1 & 1 & \ldots & 0 & 0 \\ 0 & 1 & 1 & 1 & \ldots & 1 & 0 \end{pmatrix}$$

Если обозначить через J матрицу, все элементы которой суть единицы, I — единичную (на диагонали которой стоят единицы, а вне диагонали нули), C — *циркулярную матрицу*, у которой над диагональю, а также на месте элемента первого столбца последней строки стоят единицы, а остальные элементы равны нулю, то задача Люка сводится к вычислению $\operatorname{per}(J-I-C)$, а задача Монмора к $\operatorname{per}(J-I)$.

Введем $2n$ вообще говоря противоречивых свойств, причем противоречивыми являются любые наборы, содержащие хотя бы одну из пар

$$\{p_1, p'_1\}, \{p'_1, p_2\}, \{p_2, p'_2\}, \{p'_2, p_3\}, \ldots, \{p_i, p'_i\}, \{p'_i, p_{i+1}\}, \ldots, \{p'_{n-1}, p_n\}, \{p_n, p'_n\}, \{p'_n, p_1\}.$$

Это легко представить на рисунке, расположив эти свойства в круг:



(1.8)

Из этих $2n$ объектов, расположенных в круге, выбирается k, не расположенных рядом. Решим сначала вспомогательную задачу: найдем число способов выбрать из n расположенных в ряд объектов k, не расположенных рядом.

Лемма 1.1.1 (Капланский).

$$f(n,k) = \sharp\left\{\widetilde{\alpha} \in \mathbb{B}^n \mid \forall\, i = \overline{1,n-1} \Longrightarrow \alpha_i \alpha_{i+1} = 0\right\} = \binom{n-k+1}{k}.$$

□ *Док-во.* Очевидно, что $f(1,0) = f(1,1) = 1$, $k \geqslant 2 \Rightarrow f(1,k) = 0$. Докажем по индукции следующее предложение:

$$f(n,k) = f(n-1,k) + f(n-2,k-1) \tag{1.9}$$

Действительно, способы выбрать k несоседствующих объектов распадаются на два непересекающихся варианта: последний элемент не выбран, но тогда число способов выбрать k объектов среди $n-1$ первых равно как раз $f(n-1,k)$; последний элемент выбран, в этом случае выбирать $k-1$ объектов можно только среди первых $n-2$, то есть число способов $f(n-2,k-1)$. Предложение доказано. Для полного определения $f(n,k)$ осталось определить вторую строчку и первые два столбца:

$$f(2,0)=1,\ f(2,1)=2,\ k\geqslant 3\Rightarrow f(2,k)=0,\ f(n,0)=1,\ f(n,1)=n.$$

Наглядно это можно представить на таблице:

n \ k	0	1	2	3	4	5	…
0	1	0	0	0	0	0	…
1	1	1	0	0	0	0	…
2	1	2	0	0	0	0	…
3	1	3	.	0	.	.	.
4	1	4	.	.	0	.	.
5	1	5	.	.	.	.	.
6	1	6	.	.	.	.	.
⋮	⋮	⋮					

(1.10)

Теперь легко понять, что решением такого рекуррентного уравнения будет являться как раз требуемый биномиальный коэффициент $\binom{n-k+1}{k}$. ■

Лемма 1.1.2 (Капланский).

$$g(n,k)=\sharp\left\{\widetilde{\alpha}\in\mathbb{B}^n\mid\forall\, i=\overline{1,n-1}\Longrightarrow\alpha_i\alpha_{i+1}=0,\ \alpha_1\alpha_n=0\right\}=\frac{n}{n-k}\binom{n-k}{k}.$$

□ *Док-во.* При выборе k объектов из цикла (1.8) возможны два случая: последний объект не выбран — в этом случае число вариантов просто равно $f(n-1,k)$; последний объект выбран — тогда число вариантов $f(n-3,k-1)$, так как помимо последнего нельзя выбирать также теперь предпоследний и первый. Таким образом,

$$g(n,k)=f(n-1,k)+f(n-3,k-1)=\binom{n-k}{k}+\binom{n-k-1}{k-1}=\binom{n-k}{k}\left(1+\frac{k}{n-k}\right)=\frac{n}{n-k}\binom{n-k}{k},\quad(1.11)$$

что и требовалось доказать ■

Теперь мы готовы дать ответ на вопрос задачи Люка: $M_n=2n!U_n$, где U_n — число перестановок с ограничениями, входящими в противоречие друг с другом в соответствии с (1.8). Число выбрать из $2n$ свойств k непротиворечивых равно $v_k=\frac{2n}{2n-k}\binom{2n-k}{k}$. Тогда легко видеть, что согласно принципу включения и исключения

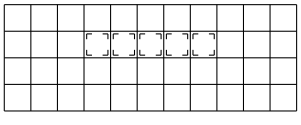
$$U_n=v_0\cdot n!-v_1\cdot(n-1)!+v_2\cdot(n-2)!-\cdots+(-1)^k v_k\cdot(n-k)!+\cdots+(-1)^n v_n\cdot(n-n)!=\sum_{k=0}^{n}(-1)^k\frac{2n}{2n-k}\binom{2n-k}{k}(n-k)!.$$

Примеры.

1. Имеется колода из $4n\,(n\geqslant 5)$ карт, которая содержит карты четырех мастей по n карт каждой масти, занумерованных числами $1,2,\ldots,n$. Подсчитать, сколькими способами можно выбрать пять карт так, что среди них окажутся:

   (а) Пять последовательных карт одной масти.

   □ *Решение.* Если представить колоду в виде таблицы $4\times n$, строки которой будут содержать карты одной масти, упорядоченные по возрастанию, то легко увидеть, что число искомых способов равно $4(n-4)$.

   n

   Действительно, одним из 4 способов можно выбрать одну строку, а затем одним из $n-4$ способов — последовательность из 5 подряд идущих карт. ■

(b) Пять последовательных карт, из которых по крайней мере две разных мастей.

□ *Решение.* Снова обращаясь к таблице, можно понять, что всего подряд идущих пятерок $4^5(n-4)$, из которых согласно (1a) $4(n-4)$ состоят из карт одной масти. Следовательно, неоднородных пятерок всего $4^5(n-4)-4(n-4)=1020(n-4)$. ■

(c) Четыре карты из пяти с одинаковыми номерами.

□ *Решение.* Снова из таблицы видно, что такому выбору соответствует выбор целого столбца таблицы (n способов) и выбор еще одной карты среди оставшихся $n-1$ столбцов, то есть всего возможностей $n(4n-4)=4n(n-1)$. ■

(d) Три карты с одним номером и две карты с другими.

□ *Решение.* Такой выбор равносилен выделению в таблице одного столбца (n способов), в котором затем выбираются 3 элемента ($\binom{4}{3}$ способов), после чего выбираются два других столбца ($\binom{n-1}{2}$), в каждом из которых выбирается по 1 элементу ($\binom{4}{1}$ способов независимо для каждого столбца). Таким образом, всего $n\cdot\binom{4}{3}\cdot\binom{n-1}{2}\cdot\binom{4}{1}^2=32n(n-1)(n-2)$ способов. ■

2. Найти число способов раскладки n различных шаров по m различным урнам.

□ *Решение.* Это число, очевидно, равно найденному в параграфе 1.1 числу различных отображений n-элементного множества в m-элементное, то есть m^n. ■

3. Сколькими способами можно разместить n одинаковых шаров по m различным урнам?

□ *Решение.* Это число является числом решений системы (1.1), то есть числу сочетаний с повторениями $\binom{n+m-1}{n}$. ■

4. Сколькими способами можно разложить $n=n_1+n_2+\cdots+n_k$ различных шаров по k различным урнам так, чтобы в первую урну попало n_1 шаров, во вторую — n_2 и так далее, в k-ю — n_k?

□ *Решение.* Это число вычисляется непосредственно: сначала из n шаров выбираем n_1 шаров ($\binom{n}{n_1}$ способами) и помещаем их в первую урну. Затем из оставшихся $n-n_1$ шаров выбираем n_2 шаров ($\binom{n-n_1}{n_2}$ способами) и помещаем их во вторую урну и так далее, из оставшихся невыбранными $n-n_1-\cdots-n_{k-1}$ шаров выбираем n_k шаров ($\binom{n-n_1-\cdots-n_{k-1}}{n_k}=1$ способами) и помещаем их в k-ю урну. Всего способов получается $\binom{n}{n_1}\binom{n-n_1}{n_2}\cdots\binom{n-n_1-\cdots-n_{k-1}}{n_k}=\frac{n!}{n_1!n_2!\cdots n_k!}$. Это число называется *полиномиальным коэффициентом* и обозначается $\binom{n}{n_1n_2\cdots n_k}$. По аналогии с биномиальными коэффициентами, являющимися коэффициентами разложения бинома Ньютона $(1+x)^n=\sum\limits_{k=0}^{n}\binom{n}{k}x^k$ или, что то же самое, $(a+b)^n=\sum\limits_{k=0}^{n}\binom{n}{k}a^kb^{n-k}$, полиномиальные коэффициенты являются коэффициентами разложения аналогичного полинома:

$$(a_1+a_2+\cdots+a_k)^n=\sum_{\substack{n_1+n_2+\cdots+n_k=n\\ n_i\geqslant 0,\ i=\overline{1,k}}}a_1^{n_1}a_2^{n_2}\cdots a_k^{n_k}.$$

■

5. $n\,(n>2)$ человек садятся за круглый стол. Два размещения по местам будем считать совпадающими, если каждый человек имеет одних и тех же соседей в обоих случаях. Сколько существует способов сесть за стол?

□ *Решение.* Каждой рассадке взаимно однозначно соответствует перестановка n целых чисел $0,1,\ldots,n-1$. Все $n!$ перестановок разбиваются на классы эквивалентности по следующему принципу: две перестановки π_1 и π_2 эквивалентны в том и только в том случае, когда либо $\pi_1(x)=\pi_2(x+i)$ для некоторого $i\in\{0,\ldots,n-1\}$ (сложение производится по модулю n) и для всех $x=\overline{1,n}$, либо $\pi_1(x)=\pi_2(i-x)$ для некоторого $i\in\{0,\ldots,n-1\}$ (вычитание производится по модулю n) и для всех $x=\overline{1,n}$. В каждом классе эквивалентности $2n$ перестановок, n сдвигов и n отраженных сдвигов. Таким образом, всего классов эквивалентности $\frac{n!}{2n}=\frac{(n-1)!}{2}=[n-1]_{n-2}$. ■

6. Сколькими способами можно посадить за круглый стол n мужчин и n женщин так, чтобы никакие два лица одного пола не сидели рядом?

□ *Решение.* Будем обозначать множество женщин числами $1,\dots,n$, а множество мужчин — числами $n+1,\dots,2n$. Каждая рассадка являются перестановкой объединения этих множеств. Перестановка, соответствующая рассадке, удовлетворяющей условию, должна числа $1,\dots,n$ сопоставлять либо только четным числам, либо нечетным (2 возможности), при этом автоматически числа $n+1,\dots,2n$ сопоставятся только нечетным, либо только четным числам. Переставить первые n чисел указанным образом можно $n!$ способами, при этом для каждой их перестановки вторые n чисел можно переставить также $n!$ способами. Таким образом, всего искомых перестановок $2\,(n!)^2$. ■

7. Сколькими способами можно составить три пары из n шахматистов?

□ *Решение.* Первую пару можно выбрать $\binom{n}{2}$ способами, вторую $\binom{n-2}{2}$, третью $\binom{n-4}{2}$. При этом порядок пар не имеет значения. Одну и ту же тройку пар можно упорядочить $3!$ способами, то есть всего способов составить три пары $\frac{\binom{n}{2}\binom{n-2}{2}\binom{n-4}{2}}{3!} = 15\binom{n}{6} = \frac{[n]_6}{48}$. ■

8. Сколько делителей имеет число $q = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$, где p_i — различные простые числа, α_i — некоторые натуральные числа? Чему равна сумма делителей?

□ *Решение.* Очевидно, что число r является делителем числа q в том и только в том случае, когда $q = p_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n}, \beta_i \leqslant \alpha_i$. Следовательно, что всего делителей $\prod\limits_{i=1}^{n} (\alpha_i + 1)$. Далее, суммой всех делителей является

$$\sum_{\substack{\beta_i \leqslant \alpha_i \\ i=\overline{1,n}}} p_1^{\beta_1} \cdots p_n^{\beta_n}. \tag{1.12}$$

Очевидно, что эта сумма равна

$$\left(1 + p_1 + \cdots + p_1^{\alpha_1}\right) \cdots \left(1 + p_n + \cdots + p_n^{\alpha_n}\right) = \prod_{i=1}^{n} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}, \tag{1.13}$$

так как всякое слагаемое из (1.12) можно найти в (1.13) и наоборот. ■

9. Сколько можно составить перестановок из n элементов, в которых данные m элементов не стоят рядом в любом порядке?

□ *Решение.* Всего перестановок $n!$. Фиксированные m элементов можно поставить рядом $m!$ способами. Оставшиеся элементы можно упорядочить $(n-m)!$ различными способами. Разместить группу выделенных m элементов среди n элементов можно $n - m + 1$ способом. Таким образом, число искомых перестановок равно $n! - m!\,(n-m+1)!$. ■

10. Сколько существует чисел от 0 до 10^n, в которые не входят две идущие друг за другом одинаковые цифры?

□ *Решение.* Рассмотрим k-разрядные числа, в которых никакие две подряд идущие цифры не повторяются. Найдем их количество. Первый разряд может быть произвольным из множества $\{1,2,3,4,5,6,7,8,9\}$. Второй разряд может быть произвольным из этого же множества или нулем, но не равен первому и так далее. Таким образом, каждый разряд при построенном предыдущем принадлежит девятиэлементному множеству, то есть всего чисел длины k, удовлетворяющих условию задачи 9^n. Будем также считать число 0 состоящим их 0 разрядов. Поскольку искомые числа имеют в десятичной записи от 1 до n цифр (10^n имеет $n+1$ цифру, но не подходит при $n \geqslant 2$), всего чисел

$$\sum_{k=0}^{n} 9^k = \frac{9^{n+1} - 1}{8}$$

■

11. Сколько существует n-значных натуральных чисел, у которых цифры расположены в неубывающем порядке?

□ *Решение.* Каждому n-значному числу в десятичной системе счисления, у которого цифры расположены в неубывающем порядке, можно взаимно однозначно поставить в соответствие последовательность из нулей и единиц длины $n+9$ следующим образом: числу $\underbrace{1\cdots1}_{k_1}\cdots\underbrace{9\cdots9}_{k_9}$ соответствует $\underbrace{1\cdots1}_{k_1}0\underbrace{1\cdots1}_{k_2}0\cdots0\underbrace{1\cdots1}_{k_9}$, то есть сначала идет столько единиц, сколькими единицами начинается число, затем идет нуль, затем столько единиц, сколько двоек, и так далее. Очевидно, что длина такой последовательности будет $n+8$, так как каждой из n цифр исходного

числа соответствует одна единица, а разделителями выступают нули. Обратно, по каждой такой последовательности можно однозначно восстановить число: сначала пишем столько единиц, сколько единиц стоит перед первым нулем в последовательности, затем пропускаем нуль и пишем столько двоек, сколько стоит в последовательности между первым и вторым нулями и так далее. Итак, искомых чисел столько же, сколько последовательностей из нулей и единиц длины $n+8$, содержащих 8 нулей, то есть $\binom{n+8}{n}$. ■

12. Доказать свойство биномиальных коэффициентов

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}. \tag{1.14}$$

□ *Решение.* Пусть $n \geqslant 2$, $k \geqslant 1$. Тогда множество наборов длины n с k единицами распадается на два непересекающихся множества: заканчивающихся нулем и заканчивающихся единицей. Число наборов длины n с k единицами, заканчивающихся нулем, равно $\binom{n-1}{k}$, а заканчивающихся единицей $\binom{n-1}{k-1}$. Так как мощность объединения двух непересекающихся множеств равна сумме их мощностей, свойство доказано.

Все вышесказанное дает возможность рекуррентно определить биномиальные коэффициенты. Будем считать, что существует одна последовательность длины нуль, содержащая нуль единиц, и не существует ни одной последовательности той же длины, содержащей больше единиц. Также, вполне естественно полагать, что существует одна последовательность длины единица, содержащая нуль единиц, одна последовательность той же длины, содержащая одну единицу, и иных последовательностей той же длины не существует. Таким образом, биномиальные коэффициенты могут быть определены следующей системой:

$$\begin{cases} \binom{0}{0} = 1, & \\ \binom{n}{k} = 0, & \text{если } n < 0 \text{ или } k < 0, \\ \binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}, & \text{иначе} \end{cases}$$

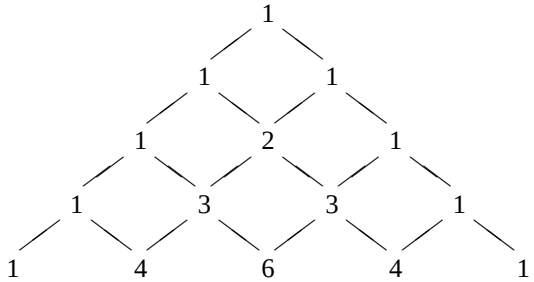
или

$$\begin{cases} \binom{n}{0} = 1, & n \geqslant 0, \\ \binom{0}{k} = 0, & k \geqslant 1, \\ \binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}, & n,k \geqslant 1. \end{cases}$$

Наглядно это можно представить на таблице:

n \ k	0	1	2	3	4	5	…
0	1	0	0	0	0	0	…
1	1	1	0	0	0	0	…
2	1	2	1	0	0	0	…
3	1	3	. . . . .				
4	1	4	. . . . .				
5	1	5	. . . . .				
6	1	6	. . . . .				
						$\binom{n-1}{k-1}$	$\binom{n-1}{k}$
⋮	⋮	⋮					$\binom{n}{k}$

Иногда бывает удобно представить в виде треугольника:



■

13. Доказать равенство $\sum\limits_{k=1}^{n} \frac{(-1)^{k-1}}{k}\binom{n}{k} = 1+\frac{1}{2}+\cdots+\frac{1}{n}$.

□ *Решение.* Обозначим $* = \sum\limits_{k=1}^{n} \frac{(-1)^{k-1}}{k}\binom{n}{k}$. Рассмотрим функцию $t\sum\limits_{k=1}^{n}(-1)^{k-1}\binom{n}{k}t^{k-1}$ и интеграл от нее:

$$\int\limits_0^1 \sum_{k=1}^{n}(-1)^{k-1}\binom{n}{k}t^{k-1}dt = \int\limits_0^1 \frac{1-(1-t)^n}{t}dt = \int\limits_0^1 \frac{1-t^n}{1-t}dt = \int\limits_0^1 \left(1+t+\cdots+t^{n-1}\right)dt$$
$$= \left(t+\frac{t^2}{2}+\cdots+\frac{t^n}{n}\right)\Big|_0^1 = 1+\frac{1}{2}+\cdots+\frac{1}{n}.$$

С другой стороны

$$\int\limits_0^1 \sum_{k=1}^{n}(-1)^{k-1}\binom{n}{k}t^{k-1}dt = \sum_{k=1}^{n}(-1)^{k-1}\binom{n}{k}\frac{t^k}{k}\Big|_0^1 = *.$$

Таким образом, равенство доказано. ■

14. Доказать тождества:

(a) $\sum\limits_k \binom{n}{2k} = \sum\limits_k \binom{n}{2k+1} = 2^{n-1}$.

□ *Решение.* Это равенство отражает очевидный факт, что число наборов равной длины из нулей и единиц с четным числом единиц равно числу наборов из нулей и единиц с нечетным числом единиц и равно половине полного числа наборов. ■

(b) $4\sum\limits_k \binom{n}{4k} = 2^n + 2^{n/2+1}\cos\frac{\pi n}{4}$.

□ *Решение.* Число в левой части равно учетверенному числу вершин n-мерного единичного куба, число единиц в которых кратно четырем. Рассмотрим вспомогательную сумму

$$S = \frac{1}{4}(1+1)^n + (1-1)^n + (1+i)^n + (1-i)^n.$$

Заметим, что

$$4S = 2^n + 2\left(\sqrt{2}\right)^n \cos\frac{\pi n}{4} = 2^n + 2^{\frac{n}{2}+1}\cos\frac{\pi n}{4}.$$

Составим таблицу сумм степеней

	1	-1	i	$-i$	сумма
0	1	1	1	1	4
1	1	-1	i	$-i$	0
2	1	1	-1	-1	0
3	1	-1	$-i$	i	0

Получаем

$$4S = \sum_{k=0}^{n}\binom{n}{k}1^{n-k}1^k + \sum_{k=0}^{n}\binom{n}{k}1^{n-k}(-1)^k + \sum_{k=0}^{n}\binom{n}{k}1^{n-k}i^k + \sum_{k=0}^{n}\binom{n}{k}1^{n-k}(-i)^k$$
$$= \sum_{k=0}^{n}\binom{n}{k}1^{n-k}\left(1^k+(-1)^k+i^k+(-i)^k\right) = 4\sum_{k=0}^{\lfloor\frac{n}{4}\rfloor}\binom{n}{4k}.$$

■

15. При обследовании читательских вкусов студентов оказалось, что 60% студентов читают журнал A, 50% — журнал B, 50% — журнал C, 30% — журналы A и B, 20% — журналы B и C, 40% — журналы A и C, 10% — журналы A, B и C. Сколько процентов студентов:

(a) не читает ни одного из журналов?

□ *Решение.* Согласно принципу включения и исключения

$$N_{[0]} = N_{(0)} - N_{(1)} + N_{(2)} - N_{(3)} = \\ 100\% - (60\% + 50\% + 50\%) + (30\% + 20\% + 40\%) - 10\% = 20\%.$$

■

(b) читает в точности 2 журнала?

□ *Решение.* Согласно принципу включения и исключения

$$N_{[2]} = \binom{2}{2} N_{(2)} - \binom{3}{2} N_{(3)} = 30\% + 20\% + 40\% - 3 \cdot 10\% = 60\%.$$

■

(c) читает не менее 2 журналов?

□ *Решение.* Согласно принципу включения и исключения

$$N_{[2]} + N_{[3]} = \binom{2}{2} N_{(2)} - \binom{3}{2} N_{(3)} + \binom{3}{3} N_{(3)} = 30\% + 20\% + 40\% - 3 \cdot 10\% + 10\% = 70\%.$$

■

Упражнения.

1. Имеется колода из $4n\,(n \geqslant 5)$ карт, которая содержит карты четырех мастей по n карт каждой масти, занумерованных числами $1, 2, \ldots, n$. Подсчитать, сколькими способами можно выбрать пять карт так, что среди них окажутся:
   (a) три карты с одним номером и две карты с другим;
   (b) пять карт одной масти;
   (c) пять последовательно занумерованных карт;
   (d) три карты из пяти с одним и тем же номером;
   (e) не более двух карт каждой масти.
2. Доказать следующие свойства биномиальных коэффициентов:
   (a) $\binom{n}{k} = \binom{n}{n-k}$;
   (b) $\binom{n}{k}\binom{k}{r} = \binom{n-r}{k-r}\binom{n}{r}$;
   (c) $\binom{n}{k-r} \Big/ \binom{n}{k} = \frac{[k]_r}{[n-k+r]_r}$;
   (d) $\binom{n}{k} = \sum\limits_{r=0}^{n} \binom{n-r-1}{k-r}$;
   (e) $\binom{n-r}{k-r} \Big/ \binom{n}{k} = \frac{[k]_r}{[n]_r}$;
   (f) $\binom{n+1}{k} \Big/ \binom{n}{k} = \frac{n+1}{n-k+1}$;
   (g) $\sum\limits_{r=k}^{n} \binom{r}{k} = \binom{n+1}{k+1}$.
3. Доказать, что
   (a) $\binom{n}{k}$ возрастает по n при фиксированном k;
   (b) $\binom{n-r}{k-r}$ убывает по r при фиксированных n и k;
   (c) если n фиксировано, то $\binom{n}{k}$ возрастает по k при $k \leqslant \lfloor n/2 \rfloor$ и убывает при $k > \lceil n/2 \rceil$;
   (d) $\max\limits_{0 \leqslant k \leqslant n} \binom{n}{k} = \binom{n}{\lfloor n/2 \rfloor}$;
   (e) минимальное значение суммы $\binom{n_1}{k} + \binom{n_2}{k} + \cdots + \binom{n_s}{k}$ при условии $\sum\limits_{i=1}^{s} n_i = n$ равно $(s-r)\binom{q}{r} + r\binom{q+1}{k}$, где $q = \lfloor n/s \rfloor, r = n - s\lfloor n/s \rfloor$;

(f) максимальное значение суммы $\binom{n}{k_1}+\binom{n}{k_2}+\cdots+\binom{n}{k_s}$ при условии $0\leqslant k_1<\cdots<k_s\leqslant n$ $(1\leqslant s\leqslant n+1)$ равно $\sum\limits_{\frac{n-s}{2}\leqslant j<\frac{n+s}{2}}\binom{n}{j}$;

(g) при простом p и любом $p>k\geqslant 1$ число $\binom{p}{k}$ кратно p;

(h) $\prod\limits_{n<p_i\leqslant 2n} p_i\leqslant\binom{2n}{n}$, где произведение берется по всем простым числам p_i $(n<p_i\leqslant 2n)$.

4. Индукцией по n с использованием соотношения (1.14) доказать тождество

$$(1+t)^n=\sum_{k=0}^{n}\binom{n}{k}t^k. \tag{1.15}$$

5. Пусть n и m — целые положительные числа. С использованием тождества (1.15) или иным способом доказать следующие равенства:

(a) $\sum\limits_{k=0}^{n}\binom{n}{k}=2^n$;

(b) $\sum\limits_{k=0}^{n}(-1)^k\binom{n}{k}=0$;

(c) $\sum\limits_{k=1}^{n}k\binom{n}{k}=n2^{n-1}$;

(d) $\sum\limits_{k=2}^{n}k(k-1)\binom{n}{k}=n(n-1)2^{n-2}$;

(e) $\sum\limits_{k=0}^{n}(2k+1)\binom{n}{k}=(n+1)2^n$;

(f) $\sum\limits_{k=0}^{n}\frac{1}{k+1}\binom{n}{k}=\frac{1}{n+1}\left(2^{n+1}-1\right)$;

(g) $\sum\limits_{k=0}^{n}(-1)^k\frac{1}{k+1}\binom{n}{k}=\frac{1}{n+1}$;

(h) $\sum\limits_{r=0}^{k}\binom{m}{r}\binom{m}{k-r}=\binom{n+m}{k}$;

(i) $\sum\limits_{k=0}^{n}\binom{n}{k}^2=\binom{2n}{n}$;

(j) $\sum\limits_{k=0}^{n}\frac{(2n)!}{(k!)^2((n-k)!)^2}=\binom{2n}{n}^2$;

(k) $\sum\limits_{k=0}^{n}\sum\limits_{r=0}^{n-k}\binom{n}{k}\binom{n-k}{r}=3^n$;

(l) $\sum\limits_{r=k}^{n}(-1)^{k-r}\binom{n}{r}=\sum\limits_{r=0}^{n-k}(-1)^{n-k-r}\binom{n}{r}$;

(m) $\sum\limits_{r=0}^{n-k}\binom{n}{k+r}\binom{m}{r}=\binom{m+n}{n-k}$;

(n) $\sum\limits_{k=n}^{m}(-1)^{k-n}\binom{k}{n}\binom{m}{k}=\begin{cases}0 & \text{при } m\neq n,\\ 1 & \text{при } m=n.\end{cases}$

6. Доказать тождества:

(a) если $0\leqslant r<m$, то $m\sum\limits_{k}\binom{n}{mk+r}=\sum\limits_{\nu=0}^{m-1}e^{-2\pi ir\nu/m}\left(1+e^{2\pi i\nu/m}\right)^n$, где $i^2=-1$;

(b) $\sum\limits_{k}\binom{n}{4k+r}=\frac{1}{4}\left(2^n+2^{n/2+1}\cos\left(\frac{\pi}{4}(n-2r)\right)\right)$, $0\leqslant r\leqslant 3$.

7. На одной из кафедр университета работают 13 человек, причем каждый из них знает хотя бы один иностранный язык. Десять человек знают английский, семеро — немецкий, шестеро — французский. Пятеро знают английский и немецкий, четверо — английский и французский, трое — немецкий и французский.

(a) Сколько человек знают все 3 языка?

(b) Сколько человек знают ровно 2 языка?

(c) Сколько человек знают только английский язык?

8. (a) Показать, что количество целых положительных чисел, делящихся на n и не превосходящих x равно $\lfloor x/n \rfloor$.

(b) Найти число целых положительных чисел, не превосходящих 1000, и не делящихся ни на одно из чисел 3, 5 и 7.

(c) Найти число целых положительных чисел, не превосходящих 1000, и не делящихся ни на одно из чисел 6, 10 и 15.

(d) Показать, что если $n = 30m$, то количество целых положительных чисел, не превосходящих n и не делящихся ни на одно из чисел 6, 10, 15, равно $22m$.

(e) Пусть $p_1, \ldots, p_r$ — все простые числа, не превосходящие $\sqrt{n}$. Показать, что число простых чисел p таких, что $\sqrt{n} < p \leqslant n$, равно $n - 1 + \sum\limits_{k=1}^{r} (-1)^k S_k$, где сумма

$$S_k = \sum \left[\frac{n}{p_1^{\alpha_1} \cdots p_r^{\alpha_r}} \right]$$

берется по всевозможным $\binom{r}{k}$ наборам показателей $\alpha_1, \ldots, \alpha_r$, в которых ровно k из показателей равны 1, а остальные равны 0.

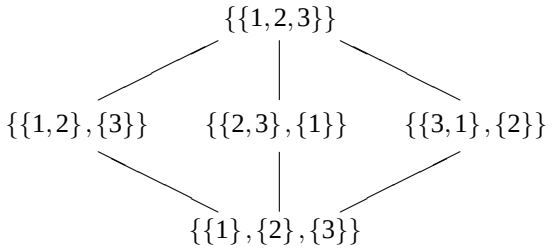
(f) Найти число простых чисел, не превосходящих 100.

1.2 Производящие функции

Разбиения множества. Пусть X — некоторое конечное множество, $|X| = n$, на котором задано разбиение $X = X_1 \cup X_2 \cup \cdots \cup X_k$, то есть $\forall\, i = \overline{1,k} \Rightarrow X_i \neq \varnothing \;\&\; i \neq j \Rightarrow X_i \cap X_j = \varnothing$. Заметим, что порядок блоков и элементов в блоке не важен.

Определение 1.2.1. *Числом Стирлинга второго рода* $S(n,k)$ для $n \geqslant 1$, $k \geqslant 1$ называется число разбиений n-элементного множества на k блоков.

В качестве примера рассмотрим случай $n = 3$. Заметим предварительно, что разбиения можно упорядочить: разбиение D_2 предшествует разбиению D_1 ($D_2 \preccurlyeq D_1$), если D_2 можно получить из D_1, разбивая блоки последнего на подблоки. Иными словами, любой блок из D_2 содержится лишь в одном блоке D_1. Это отношение можно рассматривать как уточнение эквивалентности: из эквивалентности по разбиению D_2 следует эквивалентность по разбиению D_1, но не наоборот. Итак, диаграмма Хассе частично упорядоченного множества разбиений выглядит следующим образом:



Отсюда видно, что $S(3,1) = 1$, $S(3,2) = 3$, $S(3,3) = 1$.

Вообще, очевидны следующие тривиальные равенства:

$$S(n,n) = 1 \ (n \geqslant 1),\ S(n,1) = 1 \ (n \geqslant 1),\ S(n,k) = 0 \ (k > n \geqslant 1).$$

Опираясь на эти начальные условия, найдем рекуррентное соотношение для чисел Стирлинга второго рода, доказав следующую формулу:

$$S(n,k) = S(n-1,k-1) + k \cdot S(n-1,k). \tag{1.16}$$

□ *Док-во.* Действительно, выделим в n-элементном множестве последний элемент и рассмотрим всевозможные разбиения оставшегося множества. Возможны два случая:

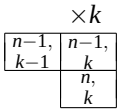
1. последний элемент составляет отдельный блок. Но всего таких разбиений столько, сколько существует разбиений оставшегося $(n-1)$-элементного множества на $k-1$ блоков.

2. Последний элемент не составляет отдельного блока. Но тогда он принадлежит одному из k блоков разбиения $(n-1)$-элементного оставшегося множества.

Поскольку эти два случая несовместны, получаем (1.16). ■

Таким образом, числа Стирлинга второго рода могут задаваться следующей таблицей:

n \ k	0	1	2	3	4	5	6	7	…
0	1	0	0	0	0	0	0	0	…
1	0	1	0	0	0	0	0	0	…
2	0	1	1	0	0	0	0	0	…
3	0	1	3	1	0	0	0	0	…
4	0	1	7	6	1	0	0	0	…
5	0	1	15	25	10	1	0	0	…
6	0	1	31	90	65	15	1	0	…
7	0	1	63	301	350	140	21	1	…
⋮	⋮	⋮							



Эти числа растут очень быстро. Так, например, $S(10,5) = 42525$. Начальные условия могут задаваться по-другому:

$$\begin{cases} S(0,0) = 1, \\ S(n,n) = 1, \quad n \geqslant 0, \\ S(n,0) = 0, \quad n \geqslant 1; \end{cases}$$

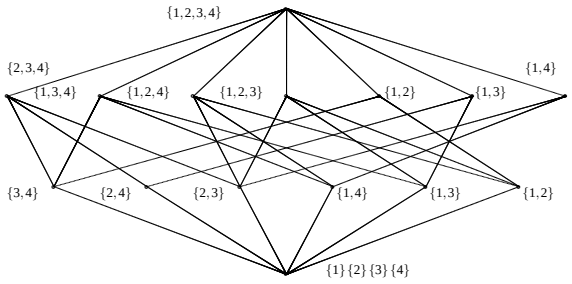
или

$$\begin{cases} S(0,0) = 1, \\ S(0,k) = 0, \quad k \geqslant 1 \\ S(n,0) = 0, \quad n \geqslant 1. \end{cases}$$

В качестве следующего примера найдем все разбиения четырехэлементного множества $\{1,2,3,4\}$:

$$\begin{aligned} D_{1,1} &= \{1,2,3,4\}, \\ D_{2,1} &= \{1\}\{2,3,4\}, \\ D_{2,2} &= \{2\}\{1,3,4\}, \\ D_{2,3} &= \{3\}\{1,2,4\}, \\ D_{2,4} &= \{4\}\{1,2,3\}, \\ D_{2,5} &= \{1,2\}\{3,4\}, \\ D_{2,6} &= \{1,3\}\{2,4\}, \\ D_{2,7} &= \{1,4\}\{2,3\}, \\ D_{3,1} &= \{1\}\{2\}\{3,4\}, \\ D_{3,2} &= \{1\}\{3\}\{2,4\}, \\ D_{3,3} &= \{1\}\{4\}\{2,3\}, \\ D_{3,4} &= \{2\}\{3\}\{1,4\}, \\ D_{3,5} &= \{2\}\{4\}\{1,3\}, \\ D_{3,6} &= \{3\}\{4\}\{1,2\}, \\ D_{4,1} &= \{1\}\{2\}\{3\}\{4\}. \end{aligned}$$

Диаграмма Хассе этого частичного упорядоченного множества будет иметь следующий вид:



Теорема 1.3. *Для $k \geqslant 2$ справедливо следующее соотношение:*

$$S(n,k) = \sum_{i=k-1}^{n-1} \binom{n-1}{i} S(i,k-1). \tag{1.17}$$

□ *Док-во.* Выделяем последний элемент и объявляем его уникальным. Затем, для каждого $j = \overline{0, n-k}$ выделяем среди оставшихся элементов блок размера j (это можно сделать $\binom{n-1}{j}$ способами) и присоединяем уникальный элемент этому блоку. После этого (для каждого j) рассматриваем все возможные разбиения оставшегося $(n-j-1)$-элементного множества $S(n-j-1, k-1)$. Ввиду уникальности последнего элемента и одного из блоков все вышеописанные ситуации несовместны, то есть перебирают различные разбиения. Таким образом,

$$S(n,k) = \sum_{j=0}^{n-k} \binom{n-1}{j} S(n-j-1, k-1).$$

Выполняя формальную замену переменной $i = n-j-1$, получаем

$$S(n,k) = \sum_{i=k-1}^{n-1} \binom{n-1}{n-i-1} S(i,k-1) = \sum_{i=k-1}^{n-1} \binom{n-1}{i} S(i,k-1),$$

что и требовалось доказать. ■

Заметим, что равенство 1.17 не может использоваться для корректного задания чисел Стирлинга второго рода.

Обозначим для разбиения n-элементного множества на k блоков для $i = \overline{1,n}$ через $k_i \geqslant 0$ число блоков, содержащих i элементов. При этом

$$\sum_{i=1}^{n} i k_i = n, \qquad \sum_{i=1}^{n} k_i = k.$$

Обозначим за $B(n; k_1, \ldots, k_n)$ число разбиений n-элементного множества, содержащих k_i блоков из i элементов для $i = \overline{1,n}$. При условиях $\sum_{i=1}^{n} i k_i = n$, $\sum_{i=1}^{n} k_i = k$

$$B(n; k_1, \ldots, k_n) = \frac{n!}{k_1! \cdots k_n! \, (1!)^{k_1} \ldots (n!)^{k_n}}.$$

Действительно, раскидываем n элементам по n позициям.

$$\underbrace{[\ldots]\ldots[\ldots]}_{k_n}\underbrace{[\ldots]\ldots[\ldots]}_{k_{n-1}}\cdots\underbrace{[\ldots]\ldots[\ldots]}_{k_1}$$

Это можно сделать $n!$ различными способами. Затем отождествляем порядок блоков внутри групп блоков одного размера и отождествляем порядок элементов в каждом блоке. Очевидно, при этом получается требуемое число. Очевидно, что согласно определению

$$S(n,k) = \sum_{\sum_{i=1}^{n} i k_i = n} B(n; k_1, \ldots, k_n).$$

Определение 1.2.2. *Числом Белла* B_n называется число всевозможных разбиений n-элементного множества на блоки:

$$B_n = \sum_{k=0}^{\infty} S(n,k), \qquad B_0 = 1.$$

В терминах диаграмм Хассе частично упорядоченного множества разбиений число Белла равно числу вершин в диаграмме.

Теорема 1.4. *Для чисел Белла выполняется следующее равенство:*

$$B_{n+1} = \sum_{i=0}^{n} \binom{n}{i} B_i. \tag{1.18}$$

□ *Док-во.* Действительно, выбираем последний из $n+1$ элементов исходного множества и называем его особым. Для любого $i = \overline{0,n}$ рассматриваем всевозможные различные блоки размера i оставшегося n-элементного множества и присоединяем к каждому из них по очереди особый элемент. Для оставшихся $n-i$ элементов рассматриваем их всевозможные разбиения. Заметим, что таким образом перебираются различные разбиения ввиду различности выбираемых блоков среди первых n неособых элементов. Далее, для разных i будут перебираться также все различные разбиения, так как в них особый элемент принадлежит блокам разных размеров. Таким образом, доказана справедливость (1.18). ■

Заметим, что из симметричности биномиальных коэффициентов следует

$$B_{n+1} = \sum_{j=0}^{n} \binom{n}{j} B_{n-j} = \sum_{i=0}^{n} \binom{n}{i} B_i.$$

Числа Белла растут быстрей чисел Стирлинга второго рода: так, например, $B_{20} = 51724158235372$.

Рассмотрим два базиса полиномов над некоторым полем: стандартный

$$1,\ x,\ x^2,\ \ldots,\ x^n,\ \ldots$$

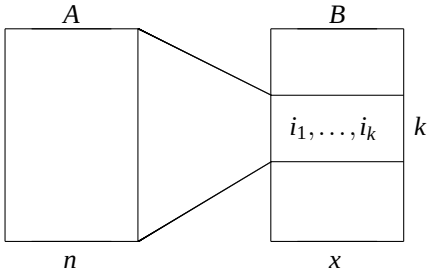
и базис из убывающих факториалов

$$[x]_0,\ [x]_1,\ [x]_2,\ \ldots,\ [x]_n,\ \ldots$$

Теорема 1.5. *Числа Стирлинга второго рода суть коэффициенты перехода от второго базиса к первому:*

$$x^n = \sum_{k=0}^{n} S(n,k)\,[x]_k. \tag{1.19}$$

□ *Док-во.* Докажем это по индукции. Для $n = 0$ равенство (1.19) превращается в очевидное: $1 = x^0 = \sum\limits_{k=0}^{0} S(0,k)\,[x]_k = S(0,0)\,[x]_0 = 1$. Докажем индуктивный переход. Рассмотрим для этого конечные множества A и B с мощностями соответственно $|A| = n \in \mathbb{N}$ и $|B| = x \in \mathbb{N}$, $x \geqslant n$. Рассматриваем далее всевозможные отображения $f : A \to B$. Их число равно x^n.



В то же время каждое отображение f с областью значений $D_f = \{i_1, \ldots, i_k\} \subseteq B$, $|D_s| = k$ можно единственным образом представить следующим образом: выбираем какие-то k различных элементов множества B ($\binom{x}{k}$ способов) и разбиение множества A на k блоков ($S(n,k)$ способов) и рассматриваем все взаимно однозначные отображения множества блоков на D_f (их число — $k!$). При этом функция f будет очевидным образом всюду определена. Далее заметим, что разным k, разным разбиениям A на k блоков, разным биекциям разбиений A на D_f соответствуют разные функции, отображающие A в B. Таким образом,

$$x^n = \sum_{k=1}^{x} \binom{x}{k} k! \cdot S(n,k) = \sum_{k=1}^{x} \frac{[x]_k}{k!} k! \cdot S(n,k) = \sum_{k=0}^{n} S(n,k)\,[x]_k, \tag{1.20}$$

поскольку $S(n,0) = 0,\ n \geqslant 1$. Равенство (1.20) справедливо для всех натуральных n и k. Теперь заметим, что если два полинома равны во всех целочисленных точках, то они равны тождественно на всей числовой оси. ■

Определение 1.2.3. *Числом Стирлинга первого рода* $s(n,k)$ называется коэффициент перехода от стандартного базиса полиномов к базису из убывающих факториалов:

$$[x]_n = \sum_{k=0}^{n} s(n,k)\,x^k.$$

Очевидно, $s(0,0) = 1,\ s(n,0) = 1,\ n \geqslant 1$. Также понятно, что $s(n,n) = 1,\ \forall\, n \in \mathbb{N},\ s(n,k) = 0,\ k > n$, так как коэффициенты при любых равных степенях, в том числе и при старшей, у тождественно равных полиномов должны совпадать. Запишем определение числа Стирлинга первого рода:

$$[x]_n = [x]_{n-1}\,(x-n+1) = \left(\sum_{k=0}^{n-1} s(n-1,k) \cdot x^k\right)(x-n+1) = \sum_{k=0}^{n} s(n,k)\,x^k.$$

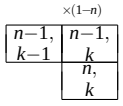
Приравнивая коэффициенты при равных степенях в последнем равенстве, получаем тождество, которое может служить рекуррентным определением чисел Стирлинга первого рода:

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

Видно, что если n и k одной четности, то $s(n,k) > 0$, если же n и k разной четности, что $s(n,k) < 0$. Поведение этих чисел

можно показать на таблице.

$n \backslash k$	0	1	2	3	4	5	6	…
0	1	0	0	0	0	0	0	…
1	0	1	0	0	0	0	0	…
2	0	−1	1	0	0	0	0	…
3	0	2	−3	1	0	0	0	…
4	0	−6	11	−6	1	0	0	…
5	0	24	−50	35	−10	1	0	…
6	0	−120	274	−225	85	−15	1	…
⋮	⋮	⋮						



Из свойств коэффициентов перехода от одного базиса к другому вытекает справедливость равенства

$$\sum_{k=0}^{\infty} s(n,k)\,S(k,m) = \delta_{nm}.$$

Начальные условия в свою очередь могут задаваться двумя способами:

$$\begin{cases} s(0,0) = 1, \\ s(n,n) = 1, \quad n \geqslant 0, \\ s(n,0) = 0, \quad n \geqslant 1; \end{cases}$$

или

$$\begin{cases} s(0,0) = 1, \\ s(0,k) = 0, \quad k \geqslant 1 \\ s(n,0) = 0, \quad n \geqslant 1. \end{cases}$$

Перед тем, как перейти к содержательному смыслу, связанному с числами Стирлинга первого рода, отметим, что их модулю растет достаточно быстро, значительно быстрей, чем числа Стирлинга второго рода. Так, например, $s(10,3) = -1026576$.

Обозначим за $c(n,k)$ число перестановок из n элементов, которые представляются в виде произведения k простых циклов (перестановки вида $\pi = [\ldots]_1 [\ldots]_2 \cdots [\ldots]_k$). Понятно, что

$$c(n,n) = 1,\ c(n,1) = n!/n = (n-1)! = |s(n,1)|.$$

Далее, очевидно, что

$$c(n,k) = c(n-1,k-1) + (n-1)\,c(n-1,k).$$

Это равенство доказывается тем же самым приемом с уникальным элементом, что и теоремы 1.3 и 1.5. В то же время

$$c(n,k) = (-1)^{n-k} s(n,k) = |s(n,k)|.$$

Таким образом, если знакопеременной двухиндексной последовательности чисел Стирлинга первого рода трудно приписать комбинаторный смысл, то модули этих чисел имеют вполне конкретный содержательный смысл: они выражают число перестановок, представляющихся в виде произведения заданного числа циклов.

Рекуррентные соотношения и производящие функции. Пусть $u_0, u_1, \ldots, u_n, \ldots$ — последовательность (например, из поля комплексных чисел). Тогда формальный степенной ряд

$$f(x) = u_0 + u_1 x + u_2 x^2 + \cdots + u_n x^n + \cdots$$

называется *производящей функцией последовательности* $\{u_n\}_{n=0}^{\infty}$. Если этот степенной ряд сходится, то следующие формально введенные операции приобретают общепринятый смысл. Для производящей функции

$$g(x) = v_0 + v_1 x + v_2 x^2 + \cdots + v_n x^n + \cdots$$

последовательности $v_0, v_1, \ldots, v_n, \ldots$ над тем же полем естественным образом вводятся линейные комбинации производящих функций $\alpha f(x) + \beta f(x)$, а также произведение:

$$f(x) \cdot g(x) = h(x) = \sum_{n=0}^{\infty} w_n x^n,$$

где

$$w_n = u_0v_n + u_1v_{n-1} + \cdots + u_iv_{n-i} + \cdots + u_nv_0 = \sum_{i=0}^{n} u_iv_{n-i}.$$

Если $u_0 \neq 0$, то для производящей функции последовательности $\{u_n\}_{n=0}^{\infty}$ существует обратный элемент $f^{-1}(x)$: $f(x) \cdot f^{-1}(x) = 1$, формальный ряд которого определяется следующим образом:

$$\begin{aligned}
0 &= v_0 \cdot u_0 && \Rightarrow v_0 = \frac{1}{u_0} \\
0 &= v_0 \cdot u_1 + v_1 \cdot u_0 && \Rightarrow v_1 = -\frac{v_0 \cdot u_1}{u_0} \\
& && \cdots \\
0 &= u_0 \cdot v_n + u_1v_{n-1} + \cdots + u_iv_{n-i} + \cdots + u_nv_0 && \Rightarrow v_n = -\frac{u_1v_{n-1} + \cdots + u_iv_{n-i} + \cdots + u_nv_0}{u_0} \\
& && \cdots
\end{aligned}$$

Рассмотрим известный пример последовательности Фибоначчи $F_0, F_1, \ldots$, задаваемой начальными условиями $F_0 = F_1 = 1$ и рекуррентным соотношением $F_{n+2} = F_{n+1} + F_n$. Первые ее пять членов будут равны:

$$F_0 = 1, \qquad F_1 = 1, \qquad F_2 = 2, \qquad F_3 = 3, \qquad F_4 = 5, \qquad F_5 = 8.$$

Найдем ее производящую функцию. Поскольку последовательность, легко видеть положительная и строго возрастающая ($F_{n+1} > F_n$), а $F_{n+1} = F_n + F_{n-1}$, легко заключить, что $F_{n+1} < 2F_n \Rightarrow F_n < 2^n$. Таким образом, производящая функция последовательности

$$f(x) = \sum_{n=0}^{\infty} F_n x^n \tag{1.21}$$

сходится в открытом круге $R < \frac{1}{2}$. В нем допустимы следующие действия:

$$\begin{array}{rcccccc}
f(x) &=& F_0 & +F_1x & +F_2x^2 & +F_3x^3 + \cdots & +F_nx^n + \cdots \\
-xf(x) &=& & -F_0x & -F_1x^2 & -F_2x^3 - \cdots & -F_{n+1}x^{n+2} - \cdots \\
-x^2f(x) &=& & & -F_0x^2 & -F_1x^3 - \cdots & -F_nx^{n+3} - \cdots
\end{array}$$

Сложим эти три равенства. Заметим при этом, что согласно рекуррентному определению чисел Фибоначчи коэффициенты при всех степенях, начиная со второй, обнулятся:

$$\left(1 - x - x^2\right) f(x) = F_0 + (F_1 - F_0)x \implies f(x) = \frac{1}{1 - x - x^2}.$$

Обозначим $k(x) = 1 - x - x^2$ — многочлен, обратный к производящей функции последовательности. Характеристическим многочленом называется функция

$$h(x) = x^2k\left(\frac{1}{x}\right) = x^2 - x - 1 = (x - \alpha_1)(x - \alpha_2), \quad \text{где} \quad \alpha_1 = \frac{1 - \sqrt{5}}{2},\ \alpha_2 = \frac{1 + \sqrt{5}}{2}.$$

Отсюда легко видеть, что

$$k(x) = x^2h\left(\frac{1}{x}\right) = (1 - \alpha_1x)(1 - \alpha_2x).$$

Таким образом, производящую функцию можно разложить на простые дроби следующим образом:

$$f(x) = \frac{1}{1 - x - x^2} = \frac{1}{(1 - \alpha_1x)(1 - \alpha_2x)} = \frac{A}{1 - \alpha_1x} + \frac{B}{1 - \alpha_2x},$$

где A и B определяются из системы линейных уравнений

$$\begin{cases} A + B & = 1, \\ -\alpha_2A - \alpha_1B & = 0. \end{cases}$$

Решением являются значения $A = \frac{1+\sqrt{5}}{2\sqrt{5}} = \frac{\alpha_1}{\sqrt{5}}$, $B = -\frac{1-\sqrt{5}}{2\sqrt{5}} = -\frac{\alpha_2}{\sqrt{5}}$. Теперь можно разложить производящую функцию в степенной ряд по степеням x, используя то, что $\frac{1}{1-z} = 1 + z + z^2 + \cdots$.

$$f(x) = A\sum_{n=0}^{\infty} \alpha_1^n x^n + B\sum_{n=0}^{\infty} \alpha_2^n x^n = \sum_{n=0}^{\infty} (A\alpha_1^n + B\alpha_2^n)x^n = \sum_{n=0}^{\infty} \left(\frac{\alpha_1^{n+1}}{\sqrt{5}} - \frac{\alpha_2^{n+1}}{\sqrt{5}}\right)x^n. \tag{1.22}$$

Приравнивая коэффициенты при равных степенях в (1.21) и (1.22), получаем

$$F_n = \frac{1}{\sqrt{5}}\left(\alpha_1^{n+1} - \alpha_2^{n+1}\right) = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n+1}\right).$$

Числа Фибоначчи имеют понятный содержательный смысл: для $n \geqslant 1$ это число двоичных последовательностей длины $n-1$, у которых никакие две единицы не стоят рядом. Легко понять, что $f_{n+2} = F_{n+3}$ путем выделения последнего разряда складывается из последовательностей длины $n+1$, у которых никакие две единицы не стоят рядом с выделенным разрядом нулем и последовательностей длины n, у которых никакие две единицы не стоят рядом с выделенным разрядом единицей: $f_{n+2} = f_{n+1} + f_n$.

Пусть дана последовательность $\{u_n\}_{n=0}^{\infty}$ над некоторым полем. Линейных однородным рекуррентным соотношением с постоянными коэффициентами порядка r называется равенство вида

$$u_{n+r} - p_1 u_{n+r-1} - p_2 u_{n+r-2} - \cdots - p_{r-1} u_{n+1} - p_r u_n = 0.$$

При известных начальных условиях $u_0, u_1, \ldots, u_{r-1}$ при его помощи может быть достаточно легко найден общий вид u_k. Действительно, если производящая функция для этой последовательности равна

$$u(x) = \sum_{n=0}^{\infty} u_n x^n, \quad x \in \mathbb{C},$$

то, поступая также, как и в случае последовательности Фибоначчи, получим

$$k(x) = 1 - p_1 x - p_2 x^2 - \cdots - p_r x^r.$$

Имеем,

$$k(x) \cdot u(x) = C(x), \quad \deg C(x) \leqslant r-1,$$

что также ясно из рассмотренного выше примера последовательности Фибоначчи. Поступаем далее аналогично:

$$h(x) = x^r k\left(\frac{1}{x}\right) = x^r - p_1 x^{r-1} - \cdots - p_r, \quad k(x) = x^r h\left(\frac{1}{x}\right)$$

и по основной теореме алгебры существует единственное представление

$$h(x) = x^r - p_1 x^{r-1} - \cdots - p_r = (x-\alpha_1)^{s_1}(x-\alpha_2)^{s_2}\cdots(x-\alpha_q)^{s_q}, \quad s_1 + s_2 + \cdots + s_q = r.$$

Отсюда способ нахождения явного выражения для степенного ряда производящей функции

$$u(x) = \frac{C(x)}{(1-\alpha_1 x)^{s_1}\cdots(1-\alpha_q x)^{s_q}} = \sum_{i=1}^{q}\sum_{j=1}^{s_i}\frac{\beta_{ij}}{(1-\alpha_i x)^j}. \tag{1.23}$$

В качестве еще одного примера можно найти, какую последовательность определяет производящая функция

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

Для этого воспользуемся разложением в ряд функции

$$(1+z)^{-n} = 1 + (-n)z + (-n)(-n-1)\cdot\frac{1}{2}z^2 + \cdots + \frac{(-1)(-n-1)\cdots(-n-m+1)}{m!}z^m + \cdots.$$

Тогда

$$\frac{1}{(1-\alpha x)^n} = \sum_{m=0}^{\infty}\frac{(-n)(-n-1)\cdots(-n-m+1)}{m!}(-\alpha x)^m = \sum_{m=0}^{\infty}\frac{(n+m-1)\cdots(n+1)n}{m!}\alpha^m x^m =$$
$$\sum_{m=0}^{\infty}\binom{n+m-1}{n-1}\alpha^m x^m = \sum_{m=0}^{\infty}\binom{n+m-1}{m}\alpha^m x^m, \tag{1.24}$$

то есть это — производящая функция чисел сочетаний с повторениями. Заметим, что $\binom{n+m-1}{n-1} = P_{n-1}(m)$, выступающий в роли коэффициента при $\alpha^m x^m$ в сумме (1.24), является многочленом от m степени $n-1$. Используя этот факт, окончательное выражение для производящей функции можно переписать несколько иначе, подставив разложение (1.24) в (1.23):

$$u(x) = \sum_{i=1}^{q}\sum_{j=1}^{s_i}\frac{\beta_{ij}}{(1-\alpha_i x)^j} = \sum_{n=0}^{\infty}\left(\sum_{i=1}^{q} Q_{\leqslant s_{i-1}}(n)\,\alpha_i^n\right)x^n.$$

Исходя из r начальных условий можно получить общий член последовательности из линейной системы уравнений:

$$u_n = \sum_{i=1}^{q} Q_{\leqslant s_i - 1}(n)\,\alpha_i^n.$$

Найдем теперь производящую функцию

$$F(x,y) = \sum_{n=0}^{\infty}\sum_{k=0}^{\infty} f_{n,k} x^n y^k$$

двухиндексной последовательности чисел сочетаний с повторениями $f_{n,k} = \binom{n-k+1}{k}$, задаваемой линейным рекуррентным соотношением $f_{n,k} - f_{n-1,k} - f_{n-2,k-1} = 0$, что продемонстрировано на таблице (1.10). Легко получить, что $\left(1 - x - x^2 y\right) F(x,y) = 1 + xy$. Тогда

$$F(x,y) = \frac{1+xy}{1-x(1+xy)} = (1+xy)\sum_{\ell=0}^{\infty} x^\ell (1+xy)^\ell = \sum_{\ell=0}^{\infty} x^\ell (1+xy)^{\ell+1} =$$

$$\sum_{\ell=0}^{\infty} x^\ell \sum_{m=0}^{\ell+1} \binom{\ell+1}{m} x^m y^m = \sum_{\ell=0}^{\infty} x^\ell \sum_{m=0}^{\infty} \binom{\ell+1}{m} x^m y^m = \sum_{\ell=0}^{\infty}\sum_{m=0}^{\infty} \binom{\ell+1}{m} x^{\ell+m} y^m.$$

Выполняя замену переменных $n = \ell + m,\ k = m$, получаем

$$F(x,y) = \sum_{n=0}^{\infty}\sum_{k=0}^{\infty} \binom{n-k+1}{k} x^n y^k.$$

Таким образом, получено, что единственным решением линейного однородного рекуррентного соотношения с постоянными коэффициентами (1.9) является $f_{n,k} = \binom{n-k+1}{k}$.

Определение 1.2.4. *Числом Каталана* u_n называется число способов корректной расстановки скобок в произведении n сомножителей

$$x_1 \cdot x_2 \cdots x_n.$$

Очевидно, что $u_0 = 0$, $u_1 = u_2 = u_1 \cdot u_2 = 1$ и числа Каталана удовлетворяют следующему соотношению $u_n = u_1 \cdot u_{n-1} + u_2 \cdot u_{n-2} + \cdots + u_{n-1} \cdot u_1, \quad n \geqslant 2$. Действительно, первый сомножитель в каждом слагаемом указывает число способов расстановки скобок слева, а второй — справа. Заметим, что ничего не изменится, если это соотношение дополнить двумя нулевыми слагаемыми:

$$u_n = u_0 \cdot u_n + u_1 \cdot u_{n-1} + \cdots + u_n \cdot u_0, \quad n \geqslant 2.$$

Производящая функция последовательности чисел Каталана

$$u(x) = \sum_{n=0}^{\infty} u_n x^n$$

удовлетворяет простому соотношению: $u^2(x) = -x + u(x)$. Действительно, возведем ее в квадрат и соберем коэффициенты при равных степенях: $u^2(x) = 0 + 0 \cdot x + u_2 \cdot x^2 + u_3 \cdot x^3 + \cdots = -x + u(x)$. Заметим, что это тождество выполняется как формальное для рядов. В действительности решить это функциональное уравнение традиционными методами не удается, так как неизвестно, сходится этот формальный ряд или нет. Поэтому прибегают к следующему приему: рассмотрим функцию

$$v(x) = \frac{1 - \sqrt{1-4x}}{2}; \qquad |x| < \frac{1}{4},$$

удовлетворяющую этому же функциональному отношению и аналитическую в открытом круге с центром в нуле ненулевого радиуса. Осталось доказать только начальные условия: очевидно, что коэффициент разложения $v(x)$ в ряд по степеням x

$$v(x) = \sum_{n=0}^{\infty} v_n \cdot x^n$$

и $v_0 = v(0)$. Надо найти v_1. Разложим для этого в ряд функцию $\frac{1}{2}\sqrt{1-4x}$. Используем известное разложение

$$(1+z)^m = \sum_{n=0}^{\infty} a_n \cdot z^n, \quad a_n = \frac{m(m-1)\cdots(m+1-n)}{n!} \cdot z^n.$$

Отсюда

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

$$\frac{1\cdot 3\cdots(2n-3)}{n!}2^{n-1} = \frac{1\cdot 3\cdots(2n-3)\cdot 2\cdot 4\cdots(2n-2)}{n!\,(n-1)!} = \frac{(2n-2)!}{n!\,(n-1)!}.$$

Отсюда получается, что $v_1 = u_1 = 1$. Таким образом, $v(x)$ — действительно производящая функция последовательности чисел Каталана. Сразу можно показать общую формулу для них:

$$u_n = \frac{(2n-2)!}{n!\,(n-1)!} = \binom{2n-1}{n} \cdot \frac{1}{2n-1} = \frac{1}{n}\binom{2n-2}{n-1}.$$

Числа Каталана играют важную роль во многих комбинаторных задачах. Так, например, если обозначить a_n — число способов разбить $(n+2)$-угольник на треугольники, то оно будет являться числом Каталана индекса на единицу больше:

$$a_n = \sum_{\ell=1}^{n-1} a_l a_{n-\ell}, \quad a_n = u_{n+1} = \frac{(2n)!}{n!\,(n+1)!} = \frac{1}{n+1}\binom{2n}{n}.$$

Другим примером является точная оценка числа деревьев (имеется ввиду их укладок на плоскости) на n вершинах. Действительно, между последовательностями из нулей и единиц длины $2n$, кодирующими деревья и расстановками скобок можно установить изоморфизм: в каждом префиксе число единиц (открывающихся скобок) не меньше числа нулей (закрывающихся скобок). Этот же результат может быть сформулирована по-другому: число путей в целочисленной решетке от вершины $(0,0)$ к вершине (n,n), проходящих под диагональю.

Рассмотрим для последовательности $\{a_n\}_{n=0}^{\infty}$ линейное неоднородное рекуррентное соотношение с постоянными коэффициентами:

$$a_{n+r} - p_1 a_{n+r-1} - \cdots - p_r a_n = f(n).$$

Общее решение неоднородного соотношения a_n представляется в виде суммы общего решения однородного соотношения a'_n и некоторого частного решения неоднородного: $a_n = a'_n + a''_n$. Частное решение ищется достаточно просто в случае $f(n) = \lambda^n P_m(n)$. Тогда если $h(\lambda) = 0$ кратности k, где $h(x) = 0$ — характеристическое уравнение, то частное решение ищется в виде $n^k Q_m(n)\,\lambda^n$, где $Q_m(m)$ — полином степени m.

Рассмотрим некоторую последовательность чисел $\{a_n\}_{n=0}^{\infty}$ из поля $\mathbb{F}$. Наряду с обычной производящей функцией

$$A(x) = \sum_{n=0}^{\infty} a_n x^n$$

введем *экспоненциальную производящую функцию*:

$$A^e(x) = \sum_{n=0}^{\infty} \frac{a_n}{n!} x^n.$$

Для производящих функций этих двух видов последовательностей $\{a_n\}_{n=0}^{\infty}$, $\{b_n\}_{n=0}^{\infty}$, $\{c_n\}_{n=0}^{\infty}$ выполняются очевидные свойства:

$$A(x) = B(x) \Longleftrightarrow a_n = b_n, \qquad A^e(x) = B^e(x) \Longleftrightarrow a_n = b_n; \tag{1.25}$$

$$A(x) + B(x) = C(x) \Longleftrightarrow a_n + b_n = c_n, \qquad A^e(x) + B^e(x) = C^e(x) \Longleftrightarrow a_n + b_n = c_n; \tag{1.26}$$

$$A(x) \cdot B(x) = C(x) \Longleftrightarrow \sum_{k=0}^{n} a_k b_{n-k} = c_n, \qquad A^e(x) \cdot B^e(x) = C^e(x) \Longleftrightarrow \sum_{k=0}^{n} \binom{n}{k} a_k b_{n-k} = c_n. \tag{1.27}$$

Соотношение (1.25) называется также *принципом равенства*, а случай экспоненциальных производящих функций (1.27) легко запомнить, используя следующее мнемоническое правило: надо раскрыть правую часть $(a+b)^n = c^n$, используя формулу бинома Ньютона, и перевести все степени в индексы. В случае полей $\mathbb{R}$ или $\mathbb{C}$ соответствующие бесконечные алгебры многочленов $\mathbb{R}[[x]]$ и $\mathbb{C}[[x]]$ получили название *алгебры Коши*, а $\mathbb{R}^e[[x]]$ и $\mathbb{C}^e[[x]]$ — *формального исчисления Блиссара*.

Принцип Лагранжа. *Если формальные степенные ряды существуют в некоторой ненулевой окрестности нуля как аналитические функции, то над ними можно осуществлять любые допустимые операции как над функциями.*

Из принципа Лагранжа вытекает в частности, что в случае сходимости ряда его можно дифференцировать по следующему правилу:

$$A(x) = \sum_{n=0}^{\infty} a_n x^n \Longrightarrow \frac{d}{dx} A(x) = \sum_{n=1}^{\infty} n a_n x^{n-1}.$$

Это корректно в силу теоремы Коши-Адамара, утверждающей, что если степенной ряд сходится в некоторой ненулевой окрестности нуля, то он сходится абсолютно, и того факта, что сходимость ряда из производных равномерна.

Пусть дана последовательность $\{a_n\}_{n=0}^{\infty}$ чисел с известной производящей функцией $A(x)$. Требуется найти последовательность $S_n = a_0 + a_1 + \cdots + a_n$. Легко видеть, что производящая функция этой последовательности будет выглядеть так:

$$S(x) = \frac{A(x)}{1-x}.$$

Пусть для начала $a_i = i$, $\forall\, i \geqslant 0$. Для любого $0 < \varepsilon < 1$ ряд $A(x)$ сходится в окрестности нуля $(-1+\varepsilon, 1-\varepsilon)$ к

$$A^1(x) = x \cdot \frac{d}{dx}\left(\frac{1}{1-x}\right) = 0 + 1 \cdot x + 2 \cdot x^2 + \cdots + n \cdot x^n + \cdots = \frac{x}{(1-x)^2}.$$

Тогда

$$S^1(x) = \frac{x}{(1-x)^3}$$

и

$$S_n^1 = \frac{(-3)(-3-1)\cdots(-3-n+1)}{n!} \cdot (-1)^n = \frac{(n+2)(n+1)}{2!} = \binom{n+1}{2}.$$

В качестве еще одного примера рассмотрим $a_i = i^2$, $\forall\, i \geqslant 0$. Для любого $0 < \varepsilon < 1$ ряд $A(x)$ сходится в окрестности нуля $(-1+\varepsilon, 1-\varepsilon)$ к

$$A^2(x) = x \cdot \frac{d}{dx}\left(x \cdot \frac{d}{dx}\left(\frac{1}{1-x}\right)\right) = 0 + 1 \cdot x + 4 \cdot x^2 + \cdots + n^2 \cdot x^n + \cdots = \frac{x(x+1)}{(1-x)^3}.$$

Тогда

$$S^2(x) = \frac{x(x+1)}{(1-x)^4} = \left(x^2+x\right) \sum_{n=0}^{\infty} \frac{(-4)(-5)\cdots(-4-n+1)}{n!} (-1)^n x^n =$$

$$\left(x^2+x\right) \sum_{n=0}^{\infty} \frac{(n+3)(n+2)(n+1)}{3!} x^n$$

и

$$S_n^2 = \frac{1}{6}\left((n+2)(n+1)n + (n+1)n(n-1)\right) = \frac{n(n+1)(2n+1)}{6}.$$

Сумму первых n кубов можно также найти, используя аппарат производящих функций, но есть и более изящный способ, основанный на тождестве, которое легко доказывается по индукции: $(1+2+\cdots+n)^2 = 1^3 + 2^3 + \cdots + n^3$, то есть

$$S_n^3 = \binom{n+1}{2}^2.$$

Основные свойства обычных производящих функций.

$$f_n^1 = f_n^2 \qquad \Longleftrightarrow f_1(x) = f_2(x); \tag{1.28}$$

$$f_n = f_n^1 + f_n^2 \qquad \Longleftrightarrow f(x) = f_1(x) + f_2(x); \tag{1.29}$$

$$F_n = \begin{cases} 0, & n = 0, \\ f_{n-1} & \text{иначе;} \end{cases} \qquad \Longleftrightarrow F(x) = x \cdot f(x); \tag{1.30}$$

$$F_n = f_{n+1} \qquad \Longleftrightarrow F(x) = \frac{f(x) - f_0}{x}, \quad (f_0 = f(0)); \tag{1.31}$$

$$F_n = f_{n+k} \qquad \Longleftrightarrow F(x) = \frac{f(x) - \sum\limits_{r=0}^{k-1} f_r x^r}{x^k}; \tag{1.32}$$

$$F_n = k \cdot f_n \qquad \Longleftrightarrow F(x) = k \cdot f(x); \tag{1.33}$$

$$F_n = \alpha^n f_n \qquad \Longleftrightarrow F(x) = f(\alpha x); \tag{1.34}$$

$$F_n = n \cdot f_n \qquad \Longleftrightarrow F(x) = x \frac{d}{dx} f(x); \tag{1.35}$$

$$F_n = \sum_{r=0}^{n} f_r \qquad \Longleftrightarrow F(x) = \frac{f(x)}{1-x}; \tag{1.36}$$

$$F_n = \begin{cases} 0, & n = \overline{1, k-1}, \\ f_{n-k}, & n \geqslant k, \end{cases} \qquad \Longleftrightarrow F(x) = x^k f(x); \tag{1.37}$$

$$F_n = \sum_{r=0}^{n} f_r g_{n-r} \qquad \Longleftrightarrow F(x) = f(x) \cdot g(x); \tag{1.38}$$

$$F_n = f_{n+1} - f_n \qquad \Longleftrightarrow F(x) = \frac{(1-x) f(x) - f_0}{x}; \tag{1.39}$$

$$\exists \lim_{N\to\infty} \frac{1}{N} \sum_{n=0}^{N} f_n \qquad \Longrightarrow \lim_{N\to\infty} \frac{1}{N} \sum_{n=0}^{N} f_n = \lim_{x\to 1} (1-x) \cdot f(x); \tag{1.40}$$

$$\exists \lim_{n\to\infty} f_n \qquad \Longrightarrow \lim_{n\to\infty} f_n = \lim_{x\to 1} (1-x) f(x). \tag{1.41}$$

Основные преобразования обычных производящих функций.

$$f_n = \begin{cases} 1, & n = 0, \\ 0, & n \geqslant 1, \end{cases} \qquad \Longleftrightarrow f(x) \equiv 1; \tag{1.42}$$

$$f_n = \begin{cases} 1, & n = k, \\ 0, & n \neq k, \end{cases} \qquad \Longleftrightarrow f(x) = x^k; \tag{1.43}$$

$$f_n \equiv 1 \qquad \Longleftrightarrow f(x) = \frac{1}{1-x}; \tag{1.44}$$

$$f_n = \alpha^n \qquad \Longleftrightarrow f(x) = \frac{1}{1-\alpha x}; \tag{1.45}$$

$$f_n = n \cdot \alpha^n \qquad \Longleftrightarrow f(x) = \frac{\alpha x}{(1-\alpha x)^2}; \tag{1.46}$$

$$f_n = a \cdot n \qquad \Longleftrightarrow f(x) = \frac{ax}{(1-x)^2}; \tag{1.47}$$

$$f_n = \binom{n+p-1}{n} \alpha^n,\ n \geqslant 0,\ p \geqslant 1 \qquad \Longleftrightarrow f(x) = \frac{1}{(1-\alpha x)^p}; \tag{1.48}$$

$$f_n = n^2 \qquad \Longleftrightarrow f(x) = \frac{1}{(1-\alpha x)^p}; \tag{1.49}$$

$$f_n = n^k \qquad \Longleftrightarrow f(x) = x \cdot \frac{d}{dx} g(x), \quad \text{где } g_n = n^{k-1}; \tag{1.50}$$

$$f_n = n^2 \alpha^n \qquad \Longleftrightarrow f(x) = \frac{\alpha x(1+\alpha x)}{(1-\alpha x)^3}; \tag{1.51}$$

$$f_n = n^3 \alpha^n \qquad \Longleftrightarrow f(x) = \frac{\alpha x\left(\alpha^2 x + 4\alpha x + 1\right)}{(1-\alpha x)^4}; \tag{1.52}$$

$$f_n = n^k \alpha^n \qquad \Longleftrightarrow f(x) = x\frac{d}{dx} g(\alpha x), \quad \text{где } g_n = n^{k-1}; \tag{1.53}$$

$$f_n = \begin{cases} \binom{k}{n} \alpha^n \beta k - n, & k \geqslant n, \\ 0, & n > k, \end{cases} \qquad \Longleftrightarrow f(x) = (\beta + \alpha x)^k; \tag{1.54}$$

$$f_n = \begin{cases} 0, & n = 0, \\ \frac{\alpha^n}{n}, & n \geqslant 1, \end{cases} \qquad \Longleftrightarrow f(x) = -\ln(1-\alpha x); \tag{1.55}$$

$$f_n = \begin{cases} 0, & n \text{ — четное}, \\ \frac{\alpha^n}{n}, & n \text{ — нечетное}, \end{cases} \qquad \Longleftrightarrow f(x) = \operatorname{Arctg}(\alpha x) = \frac{1}{2}\ln\left(\frac{1+\alpha x}{1-\alpha x}\right); \tag{1.56}$$

$$f_n = \begin{cases} 0, & n = 0 \ \vee\ n \text{ — нечетное}, \\ \frac{\alpha^n}{n}, & n \geqslant 2\ \&\ n \text{ — четное}, \end{cases} \qquad \Longleftrightarrow f(x) = -\frac{1}{2}\ln\left(1-\alpha^2 x^2\right); \tag{1.57}$$

$$f_n = \frac{\alpha^n}{n!} \qquad \Longleftrightarrow f(x) = e^{\alpha x}; \tag{1.58}$$

$$f_n = \begin{cases} 0, & n \text{ — четное}, \\ \frac{\alpha^n}{n!}, & n \text{ — нечетное}, \end{cases} \qquad \Longleftrightarrow f(x) = \frac{e^{\alpha x} - e^{-\alpha x}}{2} = \operatorname{sh} x; \tag{1.59}$$

$$f_n = \begin{cases} 0, & n = 0 \ \vee\ n \text{ — нечетное}, \\ \frac{\alpha^n}{n!}, & n \geqslant 2\ \&\ n \text{ — четное}, \end{cases} \qquad \Longleftrightarrow f(x) = \frac{e^{\alpha x} + e^{-\alpha x}}{2} = \operatorname{ch} x; \tag{1.60}$$

$$f_n = \frac{(\ln \alpha)^n}{n!} \qquad \Longleftrightarrow f(x) = \alpha^x; \tag{1.61}$$

$$f_n = \sin \alpha n \qquad \Longleftrightarrow f(x) = \frac{x \sin \alpha}{x^2 - 2x\cos\alpha + 1}; \tag{1.62}$$

$$f_n = \cos \alpha n \qquad \Longleftrightarrow f(x) = \frac{1 - x\cos\alpha}{x^2 - 2x\cos\alpha + 1}; \tag{1.63}$$

$$f_n = a^{-\beta n} \sin \alpha n \qquad \Longleftrightarrow f(x) = \frac{x \sin \alpha}{a^{-\beta} x^2 - 2x\cos\alpha + a^{\beta}}; \tag{1.64}$$

$$f_n = a^{-\beta n} \cos \alpha n \qquad \Longleftrightarrow f(x) = \frac{a^{\beta} - x\cos\alpha}{a^{-\beta} x^2 - 2x\cos\alpha + a^{\beta}}; \tag{1.65}$$

$$f_n = \operatorname{sh}\alpha n \qquad \Longleftrightarrow f(x) = \frac{x\operatorname{sh}\alpha}{x^2 - 2x\operatorname{ch}\alpha + 1}; \tag{1.66}$$

$$f_n = \operatorname{ch}\alpha n \qquad \Longleftrightarrow f(x) = \frac{1 - x\operatorname{ch}\alpha}{x^2 - 2x\operatorname{ch}\alpha + 1}; \tag{1.67}$$

$$f_n = a^{-\beta n}\operatorname{sh}\alpha n \qquad \Longleftrightarrow f(x) = \frac{x\operatorname{sh}\alpha}{a^{-\beta}x^2 - 2x\operatorname{ch}\alpha + a^{\beta}}; \tag{1.68}$$

$$f_n = a^{-\beta n}\operatorname{ch}\alpha n \qquad \Longleftrightarrow f(x) = \frac{a^{\beta} - x\operatorname{ch}\alpha}{a^{-\beta}x^2 - 2x\operatorname{ch}\alpha + a^{\beta}}. \tag{1.69}$$

Примеры.

1. Найти a_n по рекуррентным соотношениям и начальным условиям:

   (a) $a_{n+2} - 4a_{n+1} + 3a_n = 0,\ a_1 = 10,\ a_2 = 16.$

   □ *Решение.* Для начала найдем, что $a_0 = 8$, и заменим начальные условия на эквивалентные $a_0 = 8,\ a_1 = 10$. Характеристическим уравнением этой последовательности является $x^2 - 4x + 3 = 0$. Оно имеет два вещественных корня кратности один: $\alpha_1 = 1,\ \alpha_2 = 3$. Таким образом, общее решение данного линейного однородного рекуррентного соотношения с постоянными коэффициентами выписывается в виде $a_n = C_1 + C_2 \cdot 3^n$. Из начальных условий получаем, что $C_1 + C_2 = 8,\ C_1 + 3C_2 = 10 \Rightarrow C_1 = 7,\ C_2 = 1$. Таким образом, окончательно $a_n = 7 + 3^n$. ■

   (b) $a_{n+3} - 3a_{n+1} + 2a_n = 0,\ a_1 = a,\ a_2 = b,\ a_3 = c.$

   □ *Решение.* Для начала найдем, что $a_0 = \frac{3a-c}{2}$ и заменим начальные условия на эквивалентные $a_0 = \frac{3a-c}{2},\ a_1 = a,\ a_2 = b$. Характеристическим уравнением для последовательности является $x^3 - 3x + 2 = 0$. Оно имеет вещественный корень $\alpha_1 = 1$ кратности два и вещественный корень $\alpha_2 = -2$ кратности один. Таким образом, общее решение данного линейного однородного рекуррентного соотношения с постоянными коэффициентами выписывается в виде $a_n = C_1 + C_2 n + C_3 (-2)^n$. Из начальных условий получаем, что

   $$\begin{cases} C_1 + C_3 = \frac{3a-c}{2}, \\ C_1 + C_2 - 2C_3 = a, \\ C_1 + 2C_2 + 4C_3 = b; \end{cases} \Longleftrightarrow \begin{cases} C_1 = \frac{14a-b-4c}{9}, \\ C_2 = \frac{b-2a+c}{3}, \\ C_3 = \frac{2b-a-c}{18}. \end{cases}$$

   Таким образом, окончательно $a_n = \frac{14a-b-4c}{9} + \frac{b-2a+c}{3}n + \frac{2b-a-c}{18}(-2)^n$. ■

   (c) $a_{n+2} - 2\cos\alpha a_{n+1} + a_n = 0,\ a_1 = \cos\alpha,\ a_2 = \cos 2\alpha.$

   □ *Решение.* Для начала найдем, что $a_0 = 1$ и заменим начальные условия на эквивалентные $a_0 = 1,\ a_1 = \cos\alpha$. Характеристическим уравнением для последовательности является $x^2 - 2x\cos\alpha + 1 = 0$. Оно имеет два комплексно сопряженных корня $\alpha_1 = \cos\alpha - i\sin\alpha$ и $\alpha_2 = \cos\alpha + i\sin\alpha$ кратности один каждый. Таким образом, общее решение данного линейного однородного рекуррентного соотношения с постоянными коэффициентами выписывается в виде $a_n = C_1(\cos\alpha - i\sin\alpha)^n + C_2(\cos\alpha + i\sin\alpha)^n$. Из начальных условий получаем, что $C_1 + C_2 = 1,\ (C_1 + C_2)\cos\alpha - (C_1 - C_2)\sin\alpha = \cos\alpha \Rightarrow C_1 = C_2 = \frac{1}{2}$. Таким образом, окончательно

   $$a_n = \frac{1}{2}\left((\cos\alpha - i\sin\alpha)^n + (\cos\alpha + i\sin\alpha)^n\right) = \frac{e^{-in\alpha} + e^{in\alpha}}{2} = \cos n\alpha.$$

   ■

2. Вывести общее выражение для определителя трехдиагональной матрицы порядка n.

   □ *Решение.* Трехдиагональная матрица порядка n имеет следующий вид:

   $$A_n = \begin{pmatrix} a & b & 0 & 0 & \dots & 0 & 0 & 0 \\ c & a & b & 0 & \dots & 0 & 0 & 0 \\ 0 & c & a & b & \dots & 0 & 0 & 0 \\ 0 & 0 & c & a & \dots & 0 & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 & \dots & a & b & 0 \\ 0 & 0 & 0 & 0 & \dots & c & a & b \\ 0 & 0 & 0 & 0 & \dots & 0 & c & a \end{pmatrix}_{n\times n}$$

Обозначим $\det A_n = \Delta_n$. Начальные условия для нее выписываются достаточно просто:

$$\begin{cases} \Delta_0 = 1 \quad (\text{по договоренности}), \\ \Delta_1 = \det(a) = a. \end{cases}$$

Далее, для $n \geqslant 2$, используя разложение по первой строке, а затем по первому столбцу легко получить, что $\Delta_n = a\Delta_{n-1} - bc\Delta_{n-2} \Leftrightarrow \Delta_{n+2} - a\Delta_{n+1} + bc\Delta_n = 0$. Характеристическое уравнение для данного линейного однородного рекуррентного соотношения с постоянными коэффициентами имеет вид $x^2 - ax + bc = 0$. В зависимости от того, равен или не равен нулю его дискриминант $D = a^2 - 4bc$, возможны два случая:

(a) $D \neq 0$. Тогда

$$\Delta_n = C_1 \left(\frac{a - \sqrt{a^2 - 4bc}}{2} \right)^n + C_2 \left(\frac{a + \sqrt{a^2 - 4bc}}{2} \right)^n,$$

где C_1 и C_2 определяются из уравнений

$$\begin{cases} C_1 + C_2 = 0, \\ -C_1 + C_2 = \frac{a}{\sqrt{a^2 - 4bc}}. \end{cases}$$

Решением являются

$$C_1 = -\frac{1}{\sqrt{a^2 - 4bc}} \frac{a - \sqrt{a^2 - 4bc}}{2}, \quad C_2 = \frac{1}{\sqrt{a^2 - 4bc}} \frac{a + \sqrt{a^2 - 4bc}}{2},$$

где квадратные корни являются алгебраическими и во всех случаях их значения полагаются одинаковыми. Таким образом, в случае некратных корней

$$\Delta_n = -\frac{1}{\sqrt{a^2 - 4bc}} \left(\frac{a - \sqrt{a^2 - 4bc}}{2} \right)^{n+1} + \frac{1}{\sqrt{a^2 - 4bc}} \left(\frac{a + \sqrt{a^2 - 4bc}}{2} \right)^{n+1}.$$

(b) $D = 0$. Тогда

$$\Delta_n = (C_1 + C_2 n) \left(\frac{a}{2} \right)^n,$$

где C_1 и C_2 определяются из уравнений

$$\begin{cases} C_1 = 1, \\ C_1 + C_2 = 2. \end{cases}$$

Решением являются $C_1 = C_2 = 1$. Таким образом, в случае кратных корней

$$\Delta_n = (1 + n) \left(\frac{a}{2} \right)^n.$$

■

3. Найти общие решения рекуррентных соотношений:

(a) $a_{n+2} + 3a_n = 0$.

□ *Решение.* Характеристическое уравнение для данной последовательности $x^2 + 3 = 0$ имеет два комплексно сопряженных мнимых корня кратности один: $\alpha_1 = -i\sqrt{3}$ и $\alpha_2 = i\sqrt{3}$. Таким образом, общее решение данного линейного однородного рекуррентного соотношения с постоянными коэффициентами выписывается в виде

$$a_n = C_1 \left(-i\sqrt{3} \right)^n + C_2 \left(i\sqrt{3} \right)^n = C_1 3^{\frac{n}{2}} \left(i^n + (-i)^n \right) =$$
$$C_1 3^{\frac{n}{2}} \left(\cos \frac{\pi n}{2} - i \sin \frac{\pi n}{2} \right) + C_2 3^{\frac{n}{2}} \left(\cos \frac{\pi n}{2} + i \sin \frac{\pi n}{2} \right).$$

■

(b) $a_{n+2} + 2a_{n+1} + a_n = 0$.

□ *Решение.* Характеристическое уравнение для данной последовательности $x^2 + 2x + 1 = 0$ имеет один вещественный корень $\alpha = -1$ кратности два. Таким образом, общее решение данного линейного однородного рекуррентного соотношения с постоянными коэффициентами выписывается в виде $a_n = (C_1 + C_2 n)(-1)^n$. ■

(c) $a_{n+3}+10a_{n+2}+32a_{n+1}+32a_n=0$.

□ *Решение.* Характеристическое уравнение для исходной последовательности имеет вид $x^3+10x^2+32x+32=0$. Оно имеет вещественный корень $\alpha_1=-2$ кратности один и вещественный корень $\alpha_2=-4$ кратности два. Таким образом, общее решение данного линейного однородного рекуррентного соотношения с постоянными коэффициентами выписывается в виде $a_n=C_1(-2)^n+(C_2+C_3n)(-4)^n=(-2)^n(C_1+(C_2+C_3n)2^n)$. ■

4. (a) Пусть $\{a_n\}$ и $\{b_n\}$ — две последовательности, члены которых связаны соотношениями

$$\begin{aligned} a_{n+1}&=p_1a_n+q_1b_n,\\ b_{n+1}&=p_2a_n+q_2b_n,\\ \Delta&=p_1q_2-p_2q_1\neq 0, \end{aligned}$$

где p_1, q_1, p_2, q_2 — данные числа. Найти выражения для a_n и b_n, считая, что a_1 и b_1 заданы.

□ *Решение.* Найдем a_0, b_0 из системы уравнений

$$\begin{cases} a_1=p_1a_0+q_1b_0,\\ b_1=p_2a_0+q_2b_0; \end{cases}\iff\begin{cases} a_0=\frac{q_2a_1-q_1b_1}{\Delta},\\ b_0=-\frac{p_2a_1-p_1b_1}{\Delta}. \end{cases}$$

и заменим начальные условия на эквивалентные при $n=0$. Пусть $q_1\neq 0$. Выражаем из первого уравнения

$$b_n=\frac{1}{q_1}(a_{n+1}-p_1a_n),\quad b_{n+1}=\frac{1}{q_1}(a_{n+2}-p_1a_{n+1})$$

и подставляем их во второе:

$$\frac{1}{q_1}(a_{n+2}-p_1a_{n+1})=p_2a_n+q_2\frac{1}{q_1}(a_{n+1}-p_1a_n).$$

Преобразуем последнее равенство и получаем

$$a_{n+2}-(p_1+q_2)a_{n+1}+\Delta a_n=0.$$

Корни этого характеристического уравнения равны $\alpha_1=\frac{1}{2}\left(p_1+q_2-\sqrt{(p_1+q_2)^2-4\Delta}\right)$ и $\alpha_2=\frac{1}{2}\left(p_1+q_2+\sqrt{(p_1+q_2)^2-4\Delta}\right)$, где корень алгебраический и один и тот же в обоих случаях. Таким образом, в случае некратных корней

$$\begin{aligned} a_n&=C_1\left(\frac{p_1+q_2-\sqrt{(p_1+q_2)^2-4\Delta}}{2}\right)^n+C_2\left(\frac{p_1+q_2+\sqrt{(p_1+q_2)^2-4\Delta}}{2}\right)^n,\\ b_n&=C_3\left(\frac{p_1+q_2-\sqrt{(p_1+q_2)^2-4\Delta}}{2}\right)^n+C_4\left(\frac{p_1+q_2+\sqrt{(p_1+q_2)^2-4\Delta}}{2}\right)^n. \end{aligned}$$

В случае кратных корней

$$\begin{aligned} a_n&=(C_1+C_2n)\left(\frac{p_1+q_2}{2}\right)^n,\\ b_n&=(C_3+C_4n)\left(\frac{p_1+q_2}{2}\right)^n. \end{aligned}$$

Подставляя эти выражения в исходную систему, находим зависимость между C_1, C_2, C_3 и C_4, оставляющую две степени свободы (поскольку система не вырождена). Затем, подставляем начальные условия a_0, b_0 и находим константы.

Если $q_1=0$, то проведем те же рассуждения, поменяв a на b и b на a. При этом необходимо $p_2\neq 0$. Если же $p_2=0$ & $q_1=0$, то $\Delta=0$, что противоречит условию. Таким образом, решение найдено. ■

(b) Найти решение системы рекуррентных соотношений

$$\begin{aligned} a_{n+1} &= 3a_n + b_n, \\ b_{n+1} &= -a_n + b_n, \\ a_1 &= 14, \quad b_1 = -6. \end{aligned}$$

□ *Решение.* Воспользуемся результатом упражнения 4a (в данном случае корни кратные).

$$a_n = (C_1 + C_2 n)\,2^n, \quad b_n = (C_3 + C_4 n)\,2^n.$$

Подставляя в исходную систему, находим $C_4 = -C_2$, $C_3 = -C_1 + 2C_2$, то есть

$$a_n = (C_1 + C_2 n)\,2^n, \quad b_n = (-C_1 + 2C_2 - C_2 n)\,2^n.$$

Далее, учитывая, что $a_0 = 5$, $b_0 = -1$, получаем $C_1 = 5$, $C_2 = 2$. Таким образом, окончательно

$$a_n = (5 + 2n)\,2^n, \quad b_n = (-1 - 2n)\,2^n.$$

■

5. Найти решение системы рекуррентных соотношений

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

□ *Решение.* Решим задачу на языке матриц. Система задается матрицей

$$A = \begin{pmatrix} -1 & 2 \\ 2 & 2 \end{pmatrix}$$

и начальным вектором

$$X_0 = \begin{pmatrix} 3 \\ 1 \end{pmatrix}$$

Собственные значения A равны $\lambda_1 = -2$, $\lambda_2 = 3$ с собственными векторами соответственно $\begin{pmatrix} 1 \\ 2 \end{pmatrix}$ и $\begin{pmatrix} 2 \\ -1 \end{pmatrix}$. Из собственных векторов составим матрицу $Q = \begin{pmatrix} 1 & 2 \\ 2 & -1 \end{pmatrix} \Rightarrow Q^{-1} = \begin{pmatrix} \frac{1}{5} & \frac{2}{5} \\ \frac{2}{5} & -\frac{1}{5} \end{pmatrix}$. Далее,

$$A = Q\Lambda Q^{-1}, \quad Y_n = Q^{-1}X_n \Longrightarrow Y_{n+1} = \Lambda Y_n, \quad Y_n = \Lambda^n Y_0 \Longrightarrow X_n = Q\Lambda^n Q^{-1} X_0.$$

В то же время

$$A^n = Q\Lambda^n Q^{-1} \begin{pmatrix} 1 & 2 \\ 2 & -1 \end{pmatrix} \begin{pmatrix} 3^n & 0 \\ 0 & (-2)^n \end{pmatrix} \begin{pmatrix} \frac{1}{5} & \frac{2}{5} \\ \frac{2}{5} & -\frac{1}{5} \end{pmatrix} = \begin{pmatrix} \frac{1}{5}\cdot 3^n + \frac{4}{5}\cdot(-2)^n & \frac{2}{5}\cdot 3^n - \frac{2}{5}(-2)^n \\ \frac{2}{5}\cdot 3^n - \frac{2}{5}\cdot(-2)^n & \frac{4}{5}\cdot 3^n + \frac{1}{5}(-2)^n \end{pmatrix}.$$

Таким образом,

$$\begin{cases} a_n = 3^n - (-2)^{n+1}, \\ b_n = 2\cdot 3^n - (-2)^n. \end{cases}$$

■

6. Решить рекуррентное соотношение $a_{n+3} - 6a_{n+2} + 11a_{n+1} - 6a_n = 4n$, $a_0 = 1$, $a_1 = 3$, $a_2 = 4$.

□ *Решение.* Характеристическое уравнение для решения однородного соотношения последовательности $x^3 - 6x^2 + 11x - 6 = 0$ имеет три различных вещественных корня кратности один каждый: $\alpha_1 = 1$, $\alpha_2 = 2$, $\alpha_3 = 3$. Таким образом, общее решение однородного соотношения имеет вид $a'_n = A\cdot 1^n + B\cdot 2^n + C\cdot 3^n$. Частное решение имеет смысл искать в виде $a''_n = n(\alpha n + \beta)\cdot 1^n$. Подставляя его в исходное уравнение и приравнивая коэффициенты при равных степенях, получаем $\alpha = 1$, $\beta = 2$, откуда $a_n = a'_n + a''_n = A + B\cdot 2^n + C\cdot 3^n + n(n+2)$. Теперь можно определить константы A, B, C, исходя из начальных условий:

$$\begin{cases} A + B + C = 1, \\ A + 2B + 3C = 0, \\ A + 4B + 9C = -4; \end{cases} \Longleftrightarrow \begin{cases} A = 1, \\ B = 1, \\ C = -1. \end{cases}$$

Итак, окончательно, $a_n = 1 + 2^n - 3^n + n(n+2)$. ■

7. Решить рекуррентные соотношения:

   (a) $a_{n+1} - a_n = n$, $a_1 = 1$.

   □ *Решение.* Легко видеть, что $a_0 = 1$. Заменим начальное условие на эквивалентное $a_0 = 1$. Характеристическое уравнение для однородного соотношения $x - 1 = 0$ имеет один корень $\alpha = 1$ кратности один. Таким образом, общее решение однородного соотношения имеет вид $a'_n = A$. Частное решение имеет смысл искать в виде $a''_n = n(\beta n + \gamma)$. Подставляя его в исходное уравнение и приравнивая коэффициенты при равных степенях, получаем $\beta = \frac{1}{2}$, $\gamma = -\frac{1}{2}$, откуда $a_n = a'_n + a''_n = A + \frac{1}{2}n(n-1)$. Из начальных условий находим, что $A = 1$ и $a_n = 1 + \binom{n}{2}$. ■

   (b) $a_{n+2} + 2a_{n+1} - 8a_n = 27 \cdot 5^n$, $a_1 = -9$, $a_2 = 45$.

   □ *Решение.* Легко видеть, что $a_0 = 0$. Заменим начальные условия на эквивалентные $a_0 = 0$, $a_1 = -9$. Характеристическое уравнение для однородного соотношения $x^2 + 2x - 8 = 0$ имеет два корня кратности один каждый $\alpha_1 = -4$, $\alpha_2 = 2$. Таким образом, общее решение однородного соотношения имеет вид $a'_n = A(-4)^n + B \cdot 2^n$. Частное решение имеет смысл искать в виде $a''_n = \beta \cdot 5^n$. Подставляя его в исходное уравнение и приравнивая коэффициенты при равных степенях, получаем $\beta = 1$, откуда $a_n = a'_n + a''_n = A(-4)^n + B \cdot 2^n + 5^n$. Из начальных условий находим, что $A = 2$, $B = -3$ и $a_n = 2 \cdot (-4)^n - 3 \cdot 2^n + 5^n$. ■

8. Решить систему линейных рекуррентных соотношений:

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

□ *Решение.* Заметим предварительно, что $b_1 = -2$. Далее, выражая из второго уравнения $b_{n+2} = a_{n+1} + 2b_{n+1} + 1$ и подставляя туда $a_{n+1} = -b_n + n$, получаем линейное рекуррентное соотношение относительно b_n: $b_{n+2} - 2b_{n+1} + b_n = n + 1$. Его характеристическое уравнение имеет корень $\alpha = 1$ кратности два, в связи с чем общим решением однородного соотношения является $b'_n = A + Bn$, а частное решение имеет смысл искать в виде $b''_n = n^2(\beta n + \gamma)$. Подставляя последнее в уравнение, находим $\alpha = \frac{1}{6}$, $\beta = 0$. Таким образом, $b_n = b'_n + b''_n = A + Bn + \frac{n^2}{6}$. Используя начальные условия на b_n, получаем $A = -2$, $B = -\frac{1}{6}$. Таким образом,

$$b_n = -2 - \frac{n}{6} + \frac{n^3}{6}, \quad a_n = 2 + \frac{7(n-1)}{6} - \frac{(n-6)^3}{6} = 1 + \frac{2}{3}n + \frac{1}{2}n^2 - \frac{1}{6}n^3.$$

■

Упражнения.

1. Найти числа Стирлинга второго рода:

   (a) $S(n, n-1)$ и

   (b) $S(n, n-2)$.

2. Найти общие решения рекуррентных соотношений:

   (a) $a_{n+2} - 4a_{n+1} + 3a_n = 0$;

   (b) $a_{n+2} - a + n + 1 - a_n = 0$;

   (c) $a_{n+3} + 3a_{n+2} + 3a_{n+1} + a_n = 0$.

3. Найти общее решение системы рекуррентных соотношений

$$\begin{cases} a_{n+1} &= b_n + 5, \\ b_{n+1} &= -a_n + 3. \end{cases}$$

4. Решить рекуррентные соотношения:

   (a) $a_{n+2} - 2a_{n+1} + 2a_n = 2^n$, $a_0 = 1$, $a_1 = 2$;

   (b) $a_{n+2} + a_{n+1} - 2a_n = n$, $a_0 = 1$, $a_1 = -2$;

   (c) $a_{n+2} - 4a_{n+1} + 2a_n = 2^n$, $a_0 = 1$, $a_1 = 2$;

   (d) $a_{n+2} + a_{n+1} - 6a_n = 5 \cdot 2^{n+1}$, $a_0 = 2$, $a_1 = 1$.

5. Пользуясь аппаратом производящих функций, вывести формулу суммы кубов первых n натуральных чисел.

1.3 Простейшие перечислительные задачи

Вводные замечания. В этом параграфе рассматриваются задачи, представляющие собой нахождение числа классов эквивалентности комбинаторных конфигураций. Чтобы пояснить это, рассмотрим пример. Найдем число раскрасок граней куба в два разных цвета (например, в белый и черный): всего (не учитывая симметрий куба) их $2^6 = 64$. Теперь отождествим раскраски, получающиеся друг из друга поворотами куба. Тогда все различные раскраски описываются в следующем списке:

1. все грани белые (1 раскраска),
2. одна грань белая, остальные — черные (1 раскраска),
3. две грани белые, четыре — черные (2 раскраски: в одной белые грани имеют общее ребро, а в другой не имеют),
4. три грани белые, три — черные (2 раскраски: в одной белые грани имеют общую вершину, а в другой не имеют),
5. четыре грани белые, две — черные (2 раскраски: в одной черные грани имеют общее ребро, а в другой не имеют),
6. пять граней белых, одна — черная (1 раскраска),
7. все грани черные (1 раскраска).

Таким образом, всего 10 классов эквивалентности и столько же соответствующих им неэквивалентных раскрасок.

Чтобы обосновать многие из последующих рассуждений, сформулируем и докажем следующую теорему.

Теорема 1.6 (Кэли). *Любая конечная группа G изоморфна некоторой подходящей подгруппе симметрической группы S_n.*

□ *Док-во.* Пусть $|G| = n$; $G = \{g_0 = e, g_1, \ldots, g_{n-1}\}$. Для любого $g \in G$ рассмотрим подстановку

$$\widehat{g} = \begin{pmatrix} g_0 & g_1 & \cdots & g_{n-1} \\ g\cdot g_0 & g\cdot g_1 & \cdots & g\cdot g_{n-1} \end{pmatrix}$$

Она является инъективным отображением $G \to \widehat{G} \subseteq S_n$. Действительно,

$$g\cdot g_i = g\cdot g_j \Longrightarrow g^{-1}\cdot g\cdot g_i = g^{-1}\cdot g\cdot g_j \Longrightarrow g_i = g_j.$$

Таким образом, отображение $\widehat{g}$ является перестановкой, а, следовательно, и взаимно однозначным. Осталось проверить только, что в $\widehat{G}$ выполняется равенство $\widehat{g_1}\cdot\widehat{g_2} = \widehat{g_1\cdot g_2}\ \forall\, g_1, g_2$, то есть $\widehat{G}$ — группа. Действительно, пусть

$$g_1 \leftrightarrow \widehat{g_1} = \begin{pmatrix} g_0 & \cdots & y & \cdots & g_{n-1} \\ g_1\cdot g_0 & \cdots & z & \cdots & g_1\cdot g_{n-1} \end{pmatrix},$$

$$g_2 \leftrightarrow \widehat{g_2} = \begin{pmatrix} g_0 & \cdots & x & \cdots & g_{n-1} \\ g_2\cdot g_0 & \cdots & y & \cdots & g_2\cdot g_{n-1} \end{pmatrix},$$

$$g_1\cdot g_2 \leftrightarrow \widehat{g_1\cdot g_2} = \begin{pmatrix} g_0 & \cdots & g_{n-1} \\ (g_1\cdot g_2)\cdot g_0 & \cdots & (g_1\cdot g_2)\cdot g_{n-1} \end{pmatrix}.$$

Тогда согласно определению композиции перестановок

$$\widehat{g_1}\cdot\widehat{g_2}\,(x) = \widehat{g_1}\,(\widehat{g_2}\,(x)) = \widehat{g_1}\,(y) = z,$$
$$\widehat{g_1\cdot g_2}\,(x) = (g_1\cdot g_2)\,(x) = g_1\,(g_2\cdot x) = g_1\cdot y = z.$$

Таким образом, между G и $\widehat{G}$ установлено взаимно однозначное отображение, сохраняющее внутренний закон композиции, то есть изоморфизм. ■

Построенное в теореме 1.6 представление конечной группы называется *левым регулярным представлением Кэли*. Правое регулярное представление, которое может быть построено по аналогии, называется *антиизоморфизмом*.

Теорема 1.7 (Лагранж). *Пусть $G = \{\alpha_0 = e, \alpha_1, \ldots, \alpha_{n-1}\}$ — некоторая конечная группа, а множество $H = \{\beta_0 = e, \beta_1, \ldots, \beta_{m-1}\} \subseteq G$ — ее подгруппа ($m \leqslant n$). Тогда $m \mid n$.*

□ *Док-во.* Обозначив $S_0 = H$, $\gamma_0 = e$, рассмотрим множество $G \setminus S_0$. Если оно пусто, то теорема выполнена, в противном случае выбираем из него произвольный элемент γ_1.

$$\begin{array}{lllllll} S_0 & \gamma_0 = e: & \beta_0, & \beta_1, & \ldots, & \beta_{m-1} \\ S_1 & \gamma_1: & \gamma_1\beta_0, & \gamma_1\beta_1, & \ldots, & \gamma_1\beta_{m-1} \\ S_2 & \gamma_2: & \gamma_2\beta_0, & \gamma_2\beta_1, & \ldots, & \gamma_2\beta_{m-1} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ S_k & \gamma_k: & \gamma_k\beta_0, & \gamma_k\beta_1, & \ldots, & \gamma_k\beta_{m-1} \end{array} \tag{1.70}$$

Обозначим $S_1 = \left\{\gamma_1\beta_i,\ \forall\, i = \overline{0, m-1}\right\}$. Среди них нет одинаковых и $S_0 \cap S_1 = \varnothing$: действительно, если $\gamma_1\beta_i = \gamma_1\beta_j \Rightarrow \beta_i = \beta_j \Rightarrow i = j$ (домножением справа на γ_1^{-1}), а если $\gamma_1\beta_i = \beta_j \Rightarrow \gamma_1 = \beta_j\beta_i^{-1} \in H$. Если $(G\setminus S_0)\setminus S_1 = \varnothing$, то теорема доказана: порядок группы равен удвоенному порядку подгруппы. В противном случае выбираем произвольный $\gamma_2 \in (G\setminus S_0)\setminus S_1$ и повторяем те же рассуждения. На k-ом шаге мы получаем набор $S_k = \{\gamma_k\beta_0, \gamma_k\beta_1, \ldots, \gamma_k\beta_{m-1}\}$, причем все элементы в нем различны и не встречались во множествах S_i, $\forall\, i = \overline{0, k-1}$. Действительно пусть $\ell < k$ и

$$\gamma_k\beta_i = \gamma_\ell\beta_j \Rightarrow \gamma_k = \gamma_\ell \underbrace{\beta_j\beta_i^{-1}}_{\in H} = \gamma_\ell\beta_r \in S_\ell,$$

но γ_k выбиралось из дополнения S_ℓ. Остановка этого процесса может произойти только в случае

$$(\cdots((G\setminus S_0)\setminus S_1)\setminus\cdots)\setminus S_m = \varnothing,$$

но тогда $\ell\cdot m = n$, где m — порядок H, что и требовалось доказать. ■

Основные леммы.

Определение 1.3.1. *Индексом подгруппы H группы G* называется число

$$[G:H] = \frac{|G|}{|H|}.$$

Пусть $N = \{1, 2, \ldots, n\}$, G — подгруппа S_n. Введем следующее бинарное отношение на элементах множества N:

$$a \sim b \pmod G \Longleftrightarrow \exists\, \pi \in G : \pi(a) = b.$$

Легко проверить, что оно удовлетворяет аксиомам

1. рефлексивности:
$$\pi = e \in G \Longrightarrow a \sim a \pmod G,$$
2. симметричности:
$$\pi \in G \Longleftrightarrow \pi^{-1} \in G \Longrightarrow a \sim b \pmod G \Longleftrightarrow b \sim a \pmod G,$$
3. транзитивности:
$$\pi_1, \pi_2 \in G \Longrightarrow \pi_1\cdot\pi_2 = \pi \in G \Longrightarrow (a \sim b \pmod G)\,\&\,(b \sim c \pmod G) \Longrightarrow a \sim c \pmod G.$$

Иными словами, оно является отношением эквивалентности. Оно разбивает исходное множество N на классы эквивалентности. В двух крайних случаях $G = S_n$ и $G = \{e\}$ соответственно все элементы эквивалентны и никакие два не являются эквивалентными.

Определение 1.3.2. *Орбитой элемента $a \in N$* называется множество

$$\mathscr{O}_a = \{b \in N \mid a \sim b \pmod G\}.$$

Так как класс эквивалентности порождается любым своим представителем, допустимо обозначать через $\mathscr{O}_a$ орбиту произвольного элемента $a \in N$. Найдем ее. Пусть $G = \{\alpha_0 = e, \alpha_1, \ldots, \alpha_{r-1}\}$, $r = \ell\cdot m$. Тогда среди элементов $e(a) = \alpha_0(a), \alpha_1(a), \ldots, \alpha_{r-1}(a)$ могут быть повторы, но среди них содержатся все элементы, эквивалентные a и только они. То есть, множество этих элементов и составляет $\mathscr{O}_a$. Далее, $a \sim b \pmod G \Leftrightarrow \mathscr{O}_a = \mathscr{O}_b \Rightarrow |\mathscr{O}_a| = |\mathscr{O}_b|$.

Определение 1.3.3. *Стабилизатором элемента a* называется множество элементов

$$G_a = \{\alpha_i \in G \mid \alpha_i(a) = a\}.$$

Легко проверить, что G_a — подгруппа G.

Утверждение 1.3.1.

$$[G:G_a] = |\mathscr{O}_a| \qquad (|G_a|\,|\mathscr{O}_a| = |G|).$$

□ *Док-во.* Пусть $G_a = \{\beta_0 = e, \beta_1, \ldots, \beta_{m-1}\}$. Покажем, что среди элементов (1.70) не встречается одинаковых. Этим мы и покажем, что мощность орбиты является индексом стабилизатора.

$$\begin{array}{llcccc|c}
S_0 & \gamma_0 = e: & \beta_0, & \beta_1, & \ldots, & \beta_{m-1} & e(a)\\
S_1 & \gamma_1: & \gamma_1\beta_0, & \gamma_1\beta_1, & \ldots, & \gamma_1\beta_{m-1} & \gamma_1(a)\\
S_2 & \gamma_2: & \gamma_2\beta_0, & \gamma_2\beta_1, & \ldots, & \gamma_2\beta_{m-1} & \gamma_2(a)\\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots\\
S_k & \gamma_k: & \gamma_k\beta_0, & \gamma_k\beta_1, & \ldots, & \gamma_k\beta_{m-1} & \gamma_k(a)\\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots\\
S_\ell & \gamma_\ell: & \gamma_\ell\beta_0, & \gamma_\ell\beta_1, & \ldots, & \gamma_\ell\beta_{m-1} & \gamma_\ell(a)
\end{array}$$

Пусть $i \geqslant 1$, $k > s \geqslant 1$. Тогда

$$\gamma_i\beta_j(a) = \beta_s(a) = a \Longrightarrow \gamma_i\beta_i \in G_a \Longrightarrow \gamma_i \in G_a \quad \text{(противоречие)}$$
$$\gamma_k\beta_j(a) = \gamma_s\beta_j(a) \Longrightarrow \gamma_k(a) = \gamma_s(a) \Longrightarrow \exists\, \beta \in G_a : \gamma_s^{-1}\gamma_k = \beta \Longrightarrow k = s \quad \text{(противоречие.)}$$

Таким образом, действительно, $\mathscr{O}_a = \ell + 1$. ■

Если $a \sim b \pmod G$, то $|G_a| = |G_b|$ и между стабилизаторами этих двух элементов можно установить изоморфизм. Действительно, пусть $\pi(a) = b$, $g \in G_a$. Тогда $\pi g \pi^{-1} \in G_b$.

Лемма 1.3.1 (Бернсайд). *Пусть $N(G)$ — число орбит по группе G. Тогда*

$$N(G) = \frac{1}{|G|}\sum_{\pi\in G}\lambda_1(\pi),$$

где $\lambda_1(\pi)$ — число неподвижных элементов перестановки π (первая координата вектора типа перестановки).

□ *Док-во.* Рассмотрим таблицу из нулей и единиц, строки которой соответствуют элементам N, а столбцы — перестановкам из G.

N \ G	π_0	. . . . .	π_{m-1}	
1	1	. . . . .	…	$\lvert G_1\rvert$
2	1	. . . . .	…	$\lvert G_2\rvert$
⋮	…	… 0 …	…	⋮
⋮	…	… 1 …	…	⋮
n	1	. . . . .	…	$\lvert G_n\rvert$
	$\lambda_1(\pi_0)$	. . . . .	$\lambda_1(\pi_{m-1})$	

Элемент этой таблицы t_{ij} для $i = \overline{1,n}$, $j = \overline{0,m-1}$ определяется по следующему правилу:

$$t_{ij} = \begin{cases} 0, & \pi_j(i) \neq i, \\ 1, & \pi_j(i) = i. \end{cases}$$

Число единиц в i-ой строке есть порядок стабилизатора элемента i, а число единиц в j-ом столбце есть число неподвижных элементов j-ой перестановки. Обозначим через $\mathscr{O}^i$ орбиту i-го класса эквивалентности для $i = \overline{1, N(G)}$. Далее, в силу того, что мощности стабилизаторов эквивалентных элементов равны, а также того, что $|G_a|\,|\mathscr{O}_a| = |G|$ получаем,

$$\sum_{\pi\in G}\lambda_1(\pi) = \sum_{i=1}^{n}|G_i| = \underbrace{|G_a| + \cdots + |G_a|}_{\mathscr{O}^1} + \underbrace{|G_b| + \cdots + |G_b|}_{\mathscr{O}^2} + \cdots + \underbrace{|G_c| + \cdots + |G_c|}_{\mathscr{O}^{N(G)}} = |G|\cdot N(G)$$
$$\Longrightarrow N(G) = \frac{1}{|G|}\sum_{\pi\in G}\lambda_1(\pi),$$

где a из первого класса эквивалентности, b — из второго, c — из $N(G)$-го. ■

Введем на N весовую функцию $\omega : N \to \mathbb{R}$ такую, что $a \sim b \pmod G \Rightarrow \omega(a) = \omega(b)$. Весом орбиты назовем вес ее произвольного представителя: $W(\mathscr{O}_a) = \omega(a)$. Тогда справедлива следующая лемма.

Лемма 1.3.2 (Бернсайд, весовой вид).

$$\sum_{j=1}^{N(G)} W\left(\mathscr{O}^j\right) = \frac{1}{|G|}\sum_{\pi\in G}\sum_{a=\pi(a)}\omega(a).$$

□ *Док-во.* Рассмотрим таблицу весов, аналогичную используемой в лемме 1.3.1.

N \ G	π_0	…	π_{m-1}	
1	$\omega(1)$	…	…	$\lvert G_1\rvert$
2	$\omega(2)$	…	…	$\lvert G_2\rvert$
. . . . .				
n	$\omega(n)$	…	…	$\lvert G_n\rvert$

Элементы этой таблицы определяются по правилу: $w_{ij} = \omega(\pi_j(i))$ для $i = \overline{1,n},\ j = \overline{0,m-1}$. Отметим, что если i — неподвижный элемент перестановки π_j, то $w_{ij} = \omega(i)$. Воспользуемся теперь тем же приемом: перейдем от суммы по всем элементам к сумме по классам эквивалентности. Внутри каждого класса эквивалентности веса элементов одинаковы и равны весу орбиты, но каждый такой элемент участвует в сумме $|G|$ раз, так как (далее a — элемент из первой орбиты, b — из последней)

$$\sum_{\pi\in G}\sum_{a:a=\pi(a)}\omega(a) = \sum_{i=1}^{n}\sum_{\pi:\pi(i)=i}\omega(i) = \sum_{i=1}^{n}\omega(i)\sharp\{\pi\in G:\pi(i)=i\} = \sum_{i=1}^{n}\omega(i)|G_i| =$$

$$\underbrace{\omega(1)+\cdots+\omega(1)}_{|G_1|}+\underbrace{\omega(2)+\cdots+\omega(2)}_{|G_2|}+\cdots+\underbrace{\omega(n)+\cdots+\omega(n)}_{|G_n|} =$$

$$\underbrace{W\left(\mathscr{O}^1\right)+\cdots+W\left(\mathscr{O}^1\right)}_{\sum\limits_{i\in\mathscr{O}^1}|G_i|=\left|\mathscr{O}^1\right||G_a|=|G|}+\cdots+\underbrace{W\left(\mathscr{O}^{N(G)}\right)+\cdots+W\left(\mathscr{O}^{N(G)}\right)}_{\sum\limits_{i\in\mathscr{O}^{N(G)}}|G_i|=\left|\mathscr{O}^{N(G)}\right||G_b|=|G|} = |G|\sum_{j=1}^{N(G)}W\left(\mathscr{O}^j\right)$$

$$\Longrightarrow \sum_{j=1}^{N(G)}W\left(\mathscr{O}^j\right) = \frac{1}{|G|}\sum_{\pi\in G}\sum_{a=\pi(a)}\omega(a),$$

что и требовалось доказать. ■

Лемма 1.3.3 (Бернсайд, ограниченная форма). *Пусть N' — некоторое подмножество множества N. Если определить эквивалентность в ограниченной форме:*

$$a\sim' b \pmod G \Longleftrightarrow a\sim b \pmod G \ \&\ a,b\in N',$$

то число орбит по группе G на множестве N' равно

$$N\left(G|\,N'\right) = \frac{1}{|G|}\sum_{\pi\in G}\lambda_1\left(\pi|\,N'\right),$$

где $\lambda_1\left(\pi|\,N'\right)$ — число петель перестановки π на множестве N'.

□ *Док-во.* Аналогично основной лемме 1.3.1 с тем лишь отличием, что рассуждения проводятся для части орбит. ■

Теорема Пойа. Обозначим $N = \{1,\ldots,n\}$ — множество вершин, $M = \{1,\ldots,m\}$ — множество красок. Функции вида $f: N\to M$ будем называть *раскрасками множества N в цвета из M*. Их множество — $\operatorname{map}(N,M)$ с числом элементов $\sharp\operatorname{map}(N,M) = m^n$. Для некоторой подгруппы $G\subseteq S_n$ будем называть раскраски f и g эквивалентными и обозначать

$$f\sim g \pmod G \Longleftrightarrow \exists\,\pi\in G:\forall x\in N\Rightarrow f(\pi(x)) = g(x).$$

Определение 1.3.4. *Цикловым индексом группы перестановок G* будем называть многочлен

$$Z(G;x_1,\ldots,x_n) = \frac{1}{|G|}\sum_{\pi\in G}x_1^{\lambda_1(\pi)}x_2^{\lambda_2(\pi)}\cdots x_n^{\lambda_n(\pi)},$$

где $\overline{\lambda(\pi)} = (\lambda_1(\pi),\lambda_2(\pi),\ldots,\lambda_n(\pi))$ — тип перестановки π.

В примере 5 рассмотрено значение $Z(G;k,\ldots,k)$ циклового индекса групп вращений и вращений с отражениями для простого p. В общем виде они выглядят для простых p следующим образом:

$$Z(G;x_1,\ldots,x_p) = \frac{1}{p}\left(x_1^p+(p-1)x_p\right), \qquad \text{для группы вращений;}$$

$$Z(G;x_1,\ldots,x_p) = \frac{1}{p}\left(x_1^p+(p-1)x_p+px_1x_2^{\frac{p-1}{2}}\right), \qquad \text{для группы вращений с отражениями.}$$

Установим изоморфизм между элементами $\pi\in G$ и перестановками S_{m^n}. Определим для начала раскраске f и перестановке π функцию f^π по следующему правилу: $\forall\, j=\pi(i)\Rightarrow f^\pi(j) = f(i)$. Легко убедиться, что такое соответствие инъективно: действительно, если

$$f_1\to f_1^\pi,\ f_2\to f_2^\pi \quad \text{и} \quad f_1^\pi(j) = f_2^\pi(j)\ \forall j=\overline{1,n}\Longrightarrow f_1(i) = f_2(i)\ \forall\, i=\pi^{-1}(j).$$

Так поставим в соответствие группе G некоторое множество раскрасок $\{f^\pi\}$. При этом перестановке π ставится в соответствие некоторая другая перестановка раскрасок $\widehat{\pi}\in\widehat{G}$. Легко видеть, что это соответствие изоморфно (поэтому

можно говорить о подгруппе $\widehat{G}$ симметрической группы S_{m^n}), так как $(\widehat{\pi})^{-1} = \widehat{\left(\pi^{-1}\right)}$, $\widehat{e}$ — единичный элемент в $\widehat{G}$, а $\widehat{\pi_2 \cdot \pi_1} = \widehat{\pi}_2 \cdot \widehat{\pi}_1$. Осталось показать, что это соответствие взаимно однозначно: пусть $G \ni \pi_1 \neq \pi_2 \in G$, а π_1, π_2 порождают соответственно $\widehat{\pi}_1$, $\widehat{\pi}_2$. Тогда $\exists\, i : j = \pi_1(i) \neq \pi_2(i) = k$. Рассмотрим раскраску, окрашивающую i-ый элемент в первый цвет, а все остальные во второй. Тогда $\widehat{\pi}_1$ окрасит все элементы, кроме j-го в первый цвет, а j-ый элемент во второй, а $\widehat{\pi}_2$ все элементы, кроме k-го окрасит в первый цвет, а k-ый элемент во второй. Следовательно, $\widehat{\pi}_1$, $\widehat{\pi}_2$ — разные перестановки раскрасок. Таким образом, можно окончательно утверждать, что между G и $\widehat{G}$ установлен изоморфизм.

Теорема 1.8 (Пойа, упрощенный вид). *Число орбит раскрасок по группе G (подгруппе S_n) равно значению циклового индекса $Z(G; m, m, \cdots, m)$.*

□ *Док-во.* Заметим предварительно, что в силу изоморфизма

$$f_1 \sim f_2 \pmod{\widehat{G}} \Longleftrightarrow f_1 \sim f_2 \pmod{G}.$$

Пусть $\mathscr{F} = \{F_1, \ldots, F_t\}$ — множество орбит. Тогда по лемме Бернсайда 1.3.1 и в силу изоморфизма групп G и $\widehat{G}$

$$t = \frac{1}{\left|\widehat{G}\right|} \sum_{\widehat{\pi} \in \widehat{G}} \sum_{f = \widehat{\pi}(f)} 1 = \frac{1}{|G|} \sum_{\pi \in G} m^{\lambda_1(\pi)} m^{\lambda_2(\pi)} \cdots m^{\lambda_n(\pi)} = Z(G; m, m, \ldots, m).$$

Последнее равенство вытекает из того, что петля в перестановке группы G при изоморфно переходит в окрашивание всех циклов в один цвет раскраской группы $\widehat{G}$ ■

Пусть $W = \{w_1, \ldots, w_r\}$ — множество цветов. Введем все окрасок $\omega : M \to \mathsf{K}(W)$, то есть $\omega(i) = w_i$. Весом раскраски будем называть произведение весов ее цветов:

$$\omega(f) = \prod_{i \in N} \omega(f(i)).$$

Очевидно, что $f_1 \sim f_2 \pmod{G} \Rightarrow \omega(f_1) = \omega(f_2)$:

$$\omega(f_2) = \prod_{i \in N} \omega(f_2(i)) = \prod_{i \in N} \omega(f_1(\pi(i))) = \prod_{i \in N} \omega(f_1(i)) = \omega(f_1).$$

По аналогии с обычными группами перестановок, весом орбиты назовем вес любой ее раскраски: $W(F_i) = \omega(f)\ \forall f \in F_i$.

Теорема 1.9 (Пойа).

$$\sum_{F \in \mathscr{F}} W(F) = Z\left(G; \sum_{i=1}^{m} \omega(i), \sum_{i=1}^{m} \omega^2(i), \ldots, \sum_{i=1}^{m} \omega^n(i)\right).$$

□ *Док-во.* Пусть $W = \{W_1, \ldots, W_r\}$ — множество всех возможных весов раскрасок (весов орбит), $r \leqslant m^n$. Тогда

$$\begin{aligned}\sum_{F \in \mathscr{F}} W(F) &= \sum_{i=1}^{r} W_i \sum_{\substack{F \in \mathscr{F} \\ W(F) = W_i}} 1 = \sum_{i=1}^{r} W_i \cdot \frac{1}{\left|\widehat{G}\right|} \sum_{\widehat{\pi} \in \widehat{G}} \sum_{\substack{F \in \mathscr{F} \\ W(F) = W_i}} 1 \\ &= \frac{1}{\left|\widehat{G}\right|} \sum_{\pi \in G} (\omega(1) + \cdots + \omega(m))^{\lambda_1} \left(\omega^2(1) + \cdots + \omega^2(m)\right)^{\lambda_2} \cdots (\omega^n(1) + \cdots + \omega^n(m))^{\lambda_n} \\ &= Z\left(G; \sum_{i=1}^{m} \omega(i), \sum_{i=1}^{m} \omega^2(i), \ldots, \sum_{i=1}^{m} \omega^n(i)\right).\end{aligned}$$

Последнее равенство вытекает из того, что петля в перестановке группы G при изоморфно переходит в окрашивание всех циклов в один цвет раскраской группы $\widehat{G}$ ■

В дальнейшем под *витражом* будем понимать прозрачную прямоугольник, разлинованный квадратами, которые могут быть окрашены в цвета. При этом окраска квадрата с двух сторон одинаковая. По *пластиной* будем понимать непрозрачный (двусторонний) прямоугольник, разлинованный квадратами, которые могут быть окрашены в цвета с обеих сторон независимо друг от друга.

Примеры.

1. Найти число орбит на множестве $S = \{a, b, c, d\}$ по группе

$$G = \left\{ \begin{pmatrix} a & b & c & d \\ a & b & c & d \end{pmatrix}, \begin{pmatrix} a & b & c & d \\ b & a & c & d \end{pmatrix}, \begin{pmatrix} a & b & c & d \\ a & b & d & c \end{pmatrix}, \begin{pmatrix} a & b & c & d \\ b & a & d & c \end{pmatrix} \right\}.$$

□ *Решение.* Нетрудно проверить, что G — группа. Действительно, первый ее элемент является единицей, оставшиеся три являются сами себе обратными, композицией второго и третьего является четвертый, второго и четвертого — третий, третьего и четвертого — второй. Легко видеть, что орбитами здесь являются лишь два множества: $\{a,b\}$ и $\{c,d\}$. Согласно лемме 1.3.1 число орбит равно

$$N(G) = \frac{1}{4}(4+2+2+0) = 2.$$

■

2. Найти число орбит на множестве $\{a,b,c,d,e,f,g,h\}$ по группе.

$$G = \left\{\widehat{e} = \begin{pmatrix} a & b & c & d & e & f & g & h \\ a & b & c & d & e & f & g & h \end{pmatrix}, \pi = \pi^{-1} = \begin{pmatrix} a & b & c & d & e & f & g & h \\ b & a & d & c & f & e & g & h \end{pmatrix}\right\}.$$

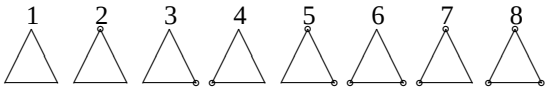
□ *Решение.* По лемме 1.3.1, очевидно,

$$N(G) = \frac{1}{2}(8+4) = 6$$

■

3. Найти число различных вершинных раскрасок треугольников в два цвета (используется модель "ожерелья", то есть орбиты определяются по группе вращений).

□ *Решение.* Здесь легко представить себе все эти раскраски:



(обведены вершины, раскрашенные в один цвет, отличный от цвета необведенных). Группа вращений в данном случае содержит три перестановки: тождественную и вращения на углы $2pi/3$ и $4\pi/3$:

$$\begin{aligned} G = \{\widehat{e} &= \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{smallmatrix}\right) = [1]\,[2]\cdots[8]\,, \\ \pi &= \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 3 & 4 & 2 & 6 & 7 & 5 & 8 \end{smallmatrix}\right) = [234]\,[567]\,[1]\,[8]\,, \\ \pi^{-1} = \pi^2 &= \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 4 & 2 & 3 & 7 & 5 & 6 & 8 \end{smallmatrix}\right) = [423]\,[756]\,[1]\,[8]\,\}. \end{aligned}$$

Таким образом, по лемме 1.3.1

$$N(G) = \frac{1}{3}(8+2+2) = 4.$$

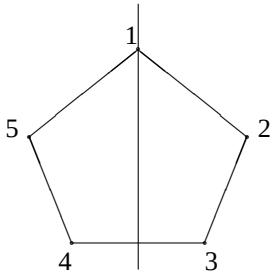
Действительно, неэквивалентными раскрасками являются, например, раскраски $1,2,5,8$. ■

4. Найти число различных вершинных раскрасок правильного пятиугольника в три цвета по группе вращений и по группе вращений и симметрий.

□ *Док-во.* Группа вращений в данном случае состоит из пяти перестановок: тождественной, которая оставляет все раскраски неподвижными, и поворотов на $\pi \cdot n/5$, где $n = 2,4,6,8$, которые оставляют неподвижными лишь одноцветные раскраски (потому что 5 — простое число). Тогда по лемме 1.3.1

$$N(G) = \frac{1}{5}\left(3^5+3+3+3+3\right) = \frac{255}{5} = 51.$$

Добавляя также симметрии, имеем еще пять перестановок, соответствующих каждой из пяти осей симметрии, каждая из которых сохраняет 3^3 раскрасок.



Действительно, можно выбрать любой цвет для вершины, через которую проходит ось, а также два любых цвета для вершин, лежащих по одну сторону от оси. В этом случае

$$N(G)=\frac{1}{10}\left(3^5+3+3+3+3+3^3+3^3+3^3+3^3+3^3\right)=\frac{390}{10}=39.$$

■

5. Найти число различных вершинных раскрасок правильного p-угольника, где p — простое в k цветов, отождествляя раскраски, получающиеся друг из друга вращениями и вращениями с симметриями.

□ *Решение.* Группа вращений будет состоять из p перестановок, из которых одна (единичная) сохраняет все k^p раскрасок, а остальные ($p-1$ различных поворотов, совмещающих вершины) в силу простоты p сохраняют лишь одноцветные раскраски. Таким образом, число раскрасок по группе вращений равно для простого числа вершин

$$N(G)=\frac{1}{p}\left(k^p+(p-1)k\right).$$

Группа симметрий будет содержать p перестановок (для начал пусть p — нечетное), каждая из которых соответствует оси, проходящей через выделенную вершину (в силу простоты p все оси различны). Каждая симметрия сохраняет раскраски, у которых выделенная вершина имеет произвольный цвет, а оставшиеся $\frac{p-1}{2}$ вершин, лежащих по одну сторону от оси определяют однозначно раскраску оставшихся $\frac{p-1}{2}$, лежащих по другую сторону оси, то есть в этом случае

$$N(G)=\frac{1}{2p}\left(k^p+(p-1)k+p\cdot k^{\frac{p+1}{2}}\right).$$

В случае четного простого $p=2$ симметрий наблюдаться не будет, поэтому

$$N(G)=\frac{1}{2}=\frac{k(k+1)}{2},$$

также, как и по группе вращений. ■

6. Найти число различных вершинных раскрасок правильного шестиугольника в 2 цвета, отождествляя раскраски, получающиеся друг из друга сначала только вращениями, а затем вращениями с симметриями.

□ *Решение.* Группа вращений будет содержать 6 перестановок, где единичная сохраняет все 2^6 раскрасок, повороты на $\pi/3$ и $5\pi/3$ сохраняют только одноцветные раскраски (так как 1 и 5 взаимно просты с числом вершин 6), повороты на $2\pi/3$ и $4\pi/3$ сохраняет четыре раскраски (четные вершины раскрашены в один цвет, а нечетные — в другой), поворот на π сохраняет восемь раскрасок (противоположные вершины окрашены в один цвет). Таким образом, в случае группы вращений

$$N(G)=\frac{1}{6}\left(2^6+2\cdot2+2\cdot2^2+2^3\right)=\frac{84}{6}=14.$$

Группа симметрий содержит шесть перестановок (3 оси, проходящие через две противоположные вершины и 3 оси через середины противоположных ребер). Симметрии, соответствующие осям, проходящим через вершины, сохраняют 2^4 раскрасок (две вершины на оси и две вершины по одну сторону оси произвольны), а симметрии, соответствующие осям, проходящим через середины ребер, сохраняют 2^3 раскрасок (три вершины по одну сторону оси определяют однозначно остальные). В случае вращений с симметриями

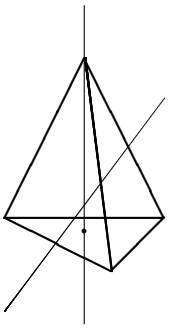
$$N(G)=\frac{1}{12}\left(2^6+2\cdot2+2\cdot2^2+2^3+3\cdot2^4+3\cdot2^3\right)=\frac{156}{12}=13.$$

■

7. Найти цикловой индекс групп вращений вершин и ребер тетраэдра.

□ *Решение.* Группы вращений вершин и ребер тетраэдра содержат по 12 перестановок: тождественную, восемь перестановок, отвечающих выбору одной из четырех осей, проходящих через одну из вершин и середину противоположной грани, а затем вращения вершин тетраэдра на $2\pi/3$ и $4\pi/3$, а также три перестановки, отвечающие

выбору одной из трех осей, проходящих через середины противоположных ребер, а затем вращения вершин тетраэдра на π.



Рассмотрим случай вращения вершин. Тождественная перестановка образует 4 цикла единичной длины. Каждое вращение вокруг оси, проходящей через вершину, образует одну петлю и один цикл длины 3, а вращения вокруг реберных осей образуют два цикла длины 2. Таким образом,

$$Z(G_V; x_1, x_2, x_3, x_4) = \frac{1}{12}\left(x_1^4 + 8x_1x_3 + 3x_2^2\right).$$

В случае вращения ребер тождественная перестановка образует шесть петель, вращения вокруг вершинных осей образуют по два цикла длины 3, а вращения вокруг реберных осей — две петли и два цикла длины 2. Таким образом,

$$Z(G_E; x_1, x_2, x_3, x_4, x_5, x_6) = \frac{1}{12}\left(x_1^6 + 8x_3^2 + 3x_1^2x_2^2\right).$$

■

8. Найти вес орбит раскрасок граней куба по группе вращений в два цвета с весами 1, x.

□ *Решение.* Группа вращений и симметрий состоит из 24 перестановок: тождественной, трех поворотов на π вокруг прямых, соединяющих центры противоположных граней, шести поворотов на $\pi/2$ вокруг прямых, соединяющих центры противоположных граней, шести поворотов на π вокруг прямых, соединяющих середины противоположных ребер и восьми поворотов на $2\pi/3$ вокруг прямых, соединяющих противоположные вершины. Они образуют соответственное число циклов: восемь петель, две петли и два цикла длины 2, две петли и один цикл длины 4, три цикла длины 2 и два цикла длины 3. Соответственно цикловой индекс группы вращений равен

$$Z(G; x_1, x_2, x_3, x_4, x_5, x_6) = \frac{1}{24}\left(x_1^6 + 3x_1^2x_2^2 + 6x_1^2x_4 + 6x_2^3 + 8x_3^2\right).$$

Вес раскраски по теореме Пойа 1.9 равен

$$\begin{aligned} Z\left(G; 1+x, 1+x^2, 1+x^3, 1+x^4\right) &= \frac{1}{24}\left((1+x)^6 + 3(1+x)^2\left(1+x^2\right)^2 + 6(1+x)^2\left(1+x^4\right) + 6\left(1+x^2\right)^3 + 8\left(1+x^3\right)^2\right) \\ &= 1 + x + 2x^2 + 2x^3 + 2x^4 + x^5 + x^6. \end{aligned}$$

■

9. Найти вес раскрасок пирамиды из 10 шариков (основание составляют шесть шариков, сложенных в виде правильного треугольника, поверх них лежат, касаясь друг друга еще три, пирамиду замыкает десятый, лежащий на трех верхних) по группе вращений в два цвета с весами 1, x.

□ *Решение.* Группа вращений здесь совпадает с группой вращений тетраэдра. При этом тождественная перестановка образует 10 петель, вращения вокруг вершинных осей образуют одну петлю и три цикла длины 3, а вращения вокруг реберных осей — две петли и четыре цикла длины 2. Таким образом,

$$Z(G, x_1, \ldots, x_{10}) = \frac{1}{12}\left(x_1^{10} + 8x_1x_3^3 + 3x_1^2x_2^4\right).$$

Вес раскраски по теореме Пойа 1.9 равен

$$\begin{aligned} Z\left(G, 1+x, 1+x^2, 1+x^3\right) &= \frac{1}{12}\left((1+x)^{10} + 8(1+x)\left(1+x^3\right)^3 + 3(1+x)^2\left(1+x^2\right)^4\right) \\ &= 1 + 2x + 5x^2 + 14x^3 + 22x^4 + 24x^5 + 22x^6 + 14x^7 + 5x^8 + 2x^9 + x^{10}. \end{aligned}$$

■

10. Найти вес орбит по группе вращений и симметрий раскрасок витража 2×2 в три цвета с весами 1, x, y.

□ *Решение.* Группа вращений содержит 8 перестановок: тождественную, образующую 4 петли, вращения на $\pi/2$ и $3\pi/2$, образующие один цикл длины 4, вращение на π, образующее два цикла длины 2, две симметрии относительно диагоналей, образующие две петли и один цикл длины 2, а также две симметрии относительно осей, проходящих через середины противоположных ребер, образующие по два цикла длины 2. Таким образом,

$$Z(G;x_1,x_2,x_3,x_4)=\frac{1}{8}\left(x_1^4+2x_4+3x_2^2+2x_1^2x_2\right).$$

Вес раскраски по теореме Пойа 1.9 равен

$$\begin{aligned}Z\left(G;1+x+y,1+x^2+y^2,1+x^3+y^3,1+x^4+y^4\right)&\\ =\frac{1}{8}\left((1+x+y)^4+2\left(1+x^4+y^4\right)+3\left(1+x^2+y^2\right)^2+2\left(1+x+y\right)^2\left(1+x^2+y^2\right)\right)&\\ =1+x+y+2x^2+2xy+2y^2+x^3+2x^2y+2xy^2+y^3+x^4+x^3y+2x^2y^2+xy^3+y^4.&\end{aligned}$$

■

Упражнения.

1. Найти цикловой индекс группы вращения вершин куба.
2. Найти цикловой индекс группы вращения ребер куба.
3. Найти цикловой индекс группы вращения вершин октаэдра.
4. Найти цикловой индекс группы вращения ребер октаэдра.
5. Найти цикловой индекс группы вращения граней октаэдра.
6. Найти цикловой индекс группы вращения витража.
7. Найти цикловой индекс группы вращения пластины.

1.4 Частично упорядоченные множества

Основные понятия. В параграфе, посвященном бинарным отношениям, уже вводилось понятие частично упорядоченного множества, и рассматривался пример $(\mathbb{N},\leqslant)$. Напомним, что частично упорядоченным множество называется пара

$$(P,\leqslant),$$

где P — некоторое множество, а $\leqslant$ — бинарное отношение частичного порядка, то есть бинарное отношение, удовлетворяющее аксиомам рефлексивности, транзитивности и антисимметричности:

1. для любого $x\in P$ выполняется $x_\rho x$;
2. для любых $x,y,z\in P$ выполняется $x_\rho y\ \&\ y_\rho z\Rightarrow x_\rho z$;
3. для любых $x,y\in P$ выполняется $x_\rho y\ \&\ y_\rho x\Rightarrow x=y$.

Если вдобавок выполняется еще и $\forall\, x,y\in P\Rightarrow x\leqslant y\ \vee\ y\leqslant x$, то пара $(P,\leqslant)$ называется вполне упорядоченным множеством. Если же это не верно, то элементы, для которых $x\not\leqslant y\ \ \&\ \ y\not\leqslant x$, будем называть *несравнимыми* и обозначать $x\supset\subset y$. Введем также уточняющие знаки: если $x\leqslant y$, $x\neq y$, то $x<y$. Введем также очень важное в дальнейшем понятие *интервала*: это множество

$$[x,y]=\{z\in P\,|\,x\leqslant z\leqslant y\}.$$

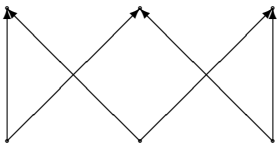
В случае $[x,y]=\{x,y\}$ и $x\neq y$, будем говорить о непосредственном предшествовании $x\lessdot y$. В терминах диаграммы Хассе это означает, что между x и y есть дуга.

Важным примером частичного порядка является множество всех подмножеств булева куба $\mathbb{B}^n$, упорядоченных по включению $(\mathbb{B}^n,\subseteq)$. Он изоморфен множеству всех (2^n) подмножеств конечного n-элементного множества, упорядоченных по включению, а также множеству всех наборов из нулей и единиц длины n, упорядоченных лексикографически при $1>0$.

Определение 1.4.1. *Частичным порядком, двойственным к частичному порядку* $(P,\leqslant)$ называется частичный порядок $(P,\leqslant_1)$, где $x\leqslant_1 y\Leftrightarrow y\leqslant x$. В дальнейшем, определяя что-то для частичного порядка $(P,\leqslant)$ *по двойственности*, будем подразумевать, что определяется то же самое, но для частичного порядка $(P,\leqslant_1)$.

Определение 1.4.2. Элемент частично упорядоченного множества $(P,\leqslant)$, называется *минимальным*, если $\nexists\, y \in P$: $y < x$. Иными словами, $\forall\, y \in P \Rightarrow x < y \vee x \supset\subset y$. По двойственности определяется понятие *максимального элемента*.

Заметим, что минимального элемента может и не быть, а в случае существования минимальных элементов, их может быть несколько.



(1.71)

Так, например, на рисунке (1.71) все элементы нижнего слоя являются минимальными.

Определение 1.4.3. Элемент z частично упорядоченного множества $(P,\leqslant)$, называется *наименьшим (нулем)*, если $\forall\, x \in P : z < x$. По двойственности определяется понятие *наибольшего элемента (единицы)*.

Заметим, что наименьший элемент (если он есть) является минимальным. Также, если минимальный элемент существует, то он единственен. На диаграмме Хассе (1.71) нет наименьшего элемента.

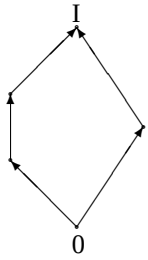
Определение 1.4.4. Подмножество $Q \subseteq P$ частично упорядоченного множества $(P,\leqslant)$ называется *цепью*, если любые два элемента из Q сравнимы.

Определение 1.4.5. Подмножество $Q \subseteq P$ частично упорядоченного множества $(P,\leqslant)$ называется *антицепью*, если любые два элемента из Q не сравнимы.

Сформулируем теперь условие на частично упорядоченные множества, с которыми мы в дальнейшем будем работать.

Цепное условие Жордана-Дедекинда. *Каждый интервал конечен и длины максимальной неуплотняемой цепи между любыми двумя элементами одна и та же.*

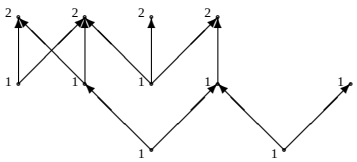
Это условие определяет так называемые *ранжированные частично упорядоченные множества*. Сразу оговоримся, что существуют множества, на которых ввести функцию ранга невозможно — неранжированные, такие, как пентагон:



Пусть частично упорядоченное множество удовлетворяет условию Жордана-Дедекинда и имеет наименьший элемент 0. Тогда можно по индукции определить функцию ранга:

1. $\operatorname{rank}(0) = 0$;
2. $a \lessdot b \Longrightarrow \operatorname{rank}(a) + 1 = \operatorname{rank}(b)$.

На содержательном уровне, такое множество должно иметь слои.



Так, например, частично упорядоченное множество натуральных чисел по делимости ранжируемо: для любого числа $n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ функция ранга равна $\operatorname{rank} n = \sum\limits_{i=1}^{s} \alpha_i$. Заметим при этом, что мощность интервала $[1,n] = \{m \mid m \mid n\}$ равна $\prod\limits_{i=1}^{s} (1+\alpha_i)$, а интервал $[m,n]$ изоморфен интервалу $\left[1, \frac{n}{m}\right]$. Если множество ранжируемо, то любой его слой является антицепью.

Определение 1.4.6. Длина цепи от нуля до единицы (если оба элемента существуют) называется *длиной множества*.

Определение 1.4.7. Наибольшая длина антицепи называется *шириной множества*.

Уже изучавшееся в параграфе 1.2 частично упорядоченное множество (неупорядоченных) разбиений конечного множества, упорядоченное по подразбиениям, носит название Беллиана, а диаграммы Хассе, соответствующие этим частичным порядкам называются диаграммами Юнга. Соответственно диаграммы Хассе, соответствующие частично упорядоченным по подразбиениям множествам упорядоченных разбиений, называются графами Феррера.

Введем ряд операций над частичными порядками. Пусть имеются два частично упорядоченных множества $(P, \leqslant_P)$ и $(Q, \leqslant_Q)$, $P \cap Q = \varnothing$.

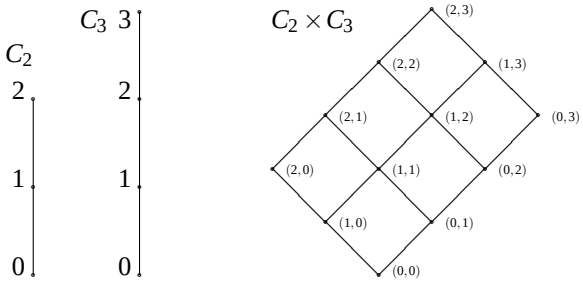
Определение 1.4.8. *Суммой (объединением) частичных порядков P и Q* называется частично упорядоченное множество $P \cup Q, \leqslant$ такое, что

1. $a, b \in P \Longrightarrow a \leqslant b \Leftrightarrow a \leqslant_P b$;
2. $a, b \in Q \Longrightarrow a \leqslant b \Leftrightarrow a \leqslant_Q b$;
3. $a \in P,\ b \in Q \Longrightarrow a \supset\subset b$.

Определение 1.4.9. *Декартовым произведением частичных порядков P и Q* называется частично упорядоченное множество $(P \times Q, \leqslant)$ такое, что

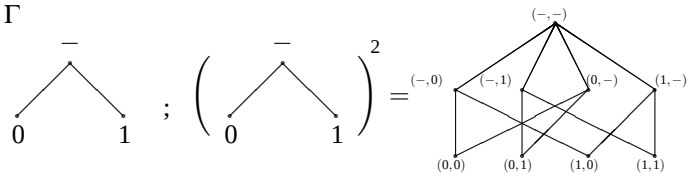
$$a_1, a_2 \in P,\ b_1, b_2 \in Q \Longrightarrow (a_1, a_2) \leqslant (b_1, b_2) \Leftrightarrow a_1 \leqslant_P a_2,\ b_1 \leqslant_Q b_2.$$

Примером декартова произведения может случить произведение цепей C_2 и C_3.



В частном случае $C_1 = \mathbb{B}$, а $\mathbb{B}^n$ — n-мерный булев куб — можно трактовать как частично упорядоченное множество n-ой декартовой степени цепи C_1.

Рассмотрим n-мерный единичный куб $\mathbb{B}^n$, на котором задан описанный выше частичный порядок. Если $\widetilde{\alpha} \leqslant \widetilde{\beta}$ и расстояние Хэмминга $\rho\left(\widetilde{\alpha}, \widetilde{\beta}\right) = k$, то интервал $\left[\widetilde{\alpha}, \widetilde{\beta}\right]$ является гранью этого куба размерности k. Ее можно обозначать следующим образом: те $n-k$ разрядов, в которых наборы $\widetilde{\alpha}$ и $\widetilde{\beta}$ совпадают сохраним, а оставшиеся — те, в которых в наборе $\widetilde{\alpha}$ стоят нули, а в наборе $\widetilde{\beta}$ стоят единицы, заменим прочерками: $\left[\widetilde{\alpha}, \widetilde{\beta}\right] = (\alpha_1, \ldots, -, \ldots)$, при этом первая компонента с прочерком называется *направлением грани*. В качестве еще одного примера рассмотрим частично упорядоченное множество Γ, состоящее из трех элементов.



Таким образом, легко видеть, что Γ^2 представляет собой частично упорядоченное множество граней двумерного куба по включению. По аналогии можно заявить, что Γ^n является частичным порядком также по включению граней n-мерного единичного куба.

Определение 1.4.10. Отображение $\varphi : P \to Q$ называется *монотонным (изотонным)*, если

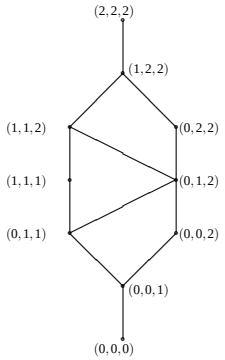
$$\forall a, b \in P : a \leqslant_P b \Longrightarrow \varphi(a) \leqslant_Q \varphi(b).$$

Примерами монотонных отображения являются монотонные функции алгебры логики.

Определение 1.4.11. Пусть S — множество всех монотонных отображений $P \to Q$ (иногда пишут $S = Q^P$). Тогда *кардинальной степенью частично упорядоченных множеств P и Q* называется частично упорядоченное множество $(S, \leqslant)$ такое, что

$$\forall \varphi_1, \varphi_2 \in S \Longrightarrow \varphi_1 \leqslant \varphi_2 \Leftrightarrow \forall a \in P : \varphi_1(a) \leqslant_Q \varphi_2(a).$$

В качестве примера построим кардинальную степень двух цепей: $C_2^{C_2}$. Чтобы представить все монотонные функции, отображающие C_2 в C_2, перейдем к их представлению векторами длины 3: $(a,b,c) : a \leqslant b \leqslant c,\ a,b,c \in \{0,1,2\}$. Частичный порядок этих векторов представлен на диаграмме Хассе:



Этот частичный порядок изоморфен множеству векторов из нулей и единиц длины 5, упорядоченных по перестановке единиц справа налево. В дальнейшем при изучении решеток станет ясен комбинаторный смысл этой аналогии.

Определение 1.4.12. Пусть $C_1,\dots,C_n$ суть цепи частично упорядоченного множества $(P,\leqslant)$. Будем говорить, что они образуют *покрытие этого частично упорядоченного множества*, если $C_i \neq \varnothing$, $i=\overline{1,n}$, для любых $1 \leqslant i < j \leqslant n \Rightarrow C_i \cap C_j = \varnothing$, $\bigcup_{i=1}^{n} C_i = P$.

Очевидно, что для любого частичного порядка всегда существует покрытие: достаточно рассмотреть тривиальное — каждый элемент объявить цепью. Справедливо утверждение о том, что число цепей в покрытии не может быть меньше ширины множества. Действительно, ширина множества равна наибольшей длине антицепи, но все элементы в ней несравнимы, следовательно, никакие два не могут находится в одной цепи покрытия. Таким образом, каждый элемент наибольшей антицепи должен содержаться в своей отдельной цепи покрытия. Справедливо и обратное неравенство.

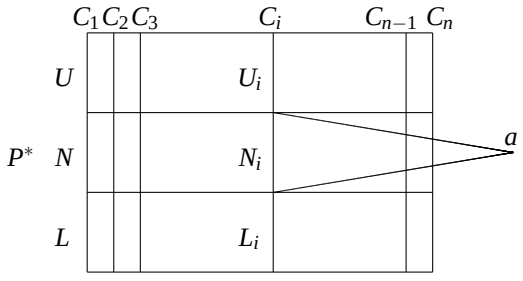
Теорема 1.10 (Дилуорс). *Пусть $(P,\leqslant)$ — конечное частично упорядоченное множество. Тогда его ширина равна минимальному числу цепей, его покрывающих.*

□ *Док-во.* Проведем индукцию по числу элементов в P. Базис индукции (случай $|P|=1$) очевиден. Пусть теорема справедлива при $|P| \leqslant k$, то есть частично упорядоченное множество, содержащее не более k элементов можно покрыть цепями, число которых равно ширине P. Докажем случай $|P| = k+1$. Возьмем произвольный элемент $a \in P$ и рассмотрим другой носитель $P^* = P \setminus \{a\}$. Возможно два случая:

1. Ширина частично упорядоченного множества $(P^*,\leqslant)$ меньше ширины исходного множества, то есть не превосходит k. Тогда по индуктивному предположению существует покрытие $(P^*,\leqslant)$ не более, чем k цепями, добавив к которым цепь, состоящую из единственного элемента a, получим покрытие $(P,\leqslant)$ не более, чем $k+1$ цепями, что и требовалось доказать.

2. Ширина частично упорядоченного множества $(P^*,\leqslant)$ равна ширине $(P,\leqslant)$. В этом случае разобьем P^* относительно a на три части:

$$U = \{b \in P \mid a < b\}, \quad L = \{b \in P \mid b < a\}, \quad N = \{b \in P \mid a \supset\subset b\}.$$



По транзитивности каждый элемент из L предшествует любому элементу из U. В дальнейшем n — ширина частично упорядоченного множества P^*. По индуктивному предположению существуют n цепей $C_1,\dots,C_n$, покрывающих P^*. Разобьем каждую цепь также на три части: $C_i = U_i \cup N_i \cup L_i$, где $U_i = U \cap C_i$, $N_i = N \cap C_i$, $L_i = L \cap C_i$, $\forall i = \overline{1,n}$. Возможно два подслучая:

(a) $\exists i \in [1,n] \cap \mathbb{N} : N_i = \varnothing$. В этом случае уплотним цепь C_i элементом a, при этом получим покрытие n цепями множества $(P,\leqslant)$. Таким образом, построено покрытие цепями, число которых равно ширине множества, что и утверждалось в теореме.

(b) $\forall i = \overline{1,n}\ N_i \neq \varnothing$. Прежде чем перейти к рассмотрению следующих двух подслучаев заметим, что любая цепь покрытия целиком лежит либо в $U \cup N$, либо в $L \cup N$ (докажите).

i. Если найдется номер j такой, что частично упорядоченное множество $(P^* \setminus U_j, \leqslant)$ имеет ширину, меньшую n, то искомым покрытием является покрытие $(P^* \setminus U_j, \leqslant)$, объединенное с цепью $U_j \cup \{a\}$. Аналогичен случай, когда найдется номер ℓ такой, что частично упорядоченное множество $(P^* \setminus L_\ell, \leqslant)$ имеет ширину, меньшую n. Таким образом, и в этом случае искомое покрытие существует.

ii. Не ограничивая общности рассуждений, будем считать, что все цепи лежат в $U \cap N$. Предположим, при удалении любого U_i, $i = \overline{1,n}$ ширина множества сохраняется. В это случае для любого i множество $(U \cup N) \setminus U_i$ имеет ширину n, а его максимальной антицепью является цепь A_i длины n, причем на каждой из цепей C_j присутствует один элемент каждой антицепи A_i, $\forall i = \overline{1,n}$. Важно, что один из элементов каждой антицепи находится на N_i: $A_i \cap N_i \neq \varnothing$, $\forall i = \overline{1,n}$. Рассмотрим объединение всех таких антицепей $A = \bigcup_{i=1}^{n} A_i$. В цепях $U_i \cup N_i$ выбираем наименьший элемент из $A \cap (U_i \cup N_i)$ — $a_i \in N_i$. Утверждается, что $A^* = \{a_1, \ldots, a_n\}$ — антицепь. Доказательство от противного: пусть $\exists b, c \in A^*$, $b < c$. Если $b \in A_s$, то возьмем $d \in A_s$ — элемент, лежащий на той же цепи, что и c но выше (так как c наименьший из элементов A_s, лежащих на той же цепи). Тогда по транзитивности $c < d \Rightarrow b < d$, что противоречит тому, что A_s антицепь. Таким образом, в P^* антицепью является A^*, а в P — $A^* \cup \{a\}$, что противоречит предположению о том, что ширина P равна ширине P^* и равна n.

Теорема доказана. ■

Цепи Анселя. Рассмотрим единичный n-мерный куб $\mathbb{B}^n$ с традиционным частичным порядком. Обозначим $\mathbb{B}_k^n = \{\widetilde{\alpha} \in \mathbb{B}^n : \|\widetilde{\alpha}\| = k\}$ — k-ый слой для $k = \overline{0,n}$. Очевидно, для любого k слой $\mathbb{B}_k^n$ является антицепью длины $\left|\mathbb{B}_k^n\right| = \binom{n}{k}$. Покажем, что последовательность $\left\{\left|\mathbb{B}_k^n\right| = a_k\right\}_{k=0}^{n}$ монотонно убывает. Действительно,

$$\frac{a_{k+1}}{a_k} = \frac{\binom{n}{k+1}}{\binom{n}{k}} = \frac{n-k}{k+1}$$

монотонно убывает. Покажем, что в случае четного n последовательность $\{a_k\}_{k=0}^{n}$ является унимодальной, а в случае нечетного — два серединных элемента последовательности являются максимальными. Действительно, если $n = 2m$, то

$$k < m \Rightarrow \frac{n-k}{k+1} > 1, \quad k \geqslant m \Rightarrow \frac{n-k}{k+1} < 1$$
$$\binom{n}{0} < \binom{n}{1} < \cdots < \binom{n}{m} > \binom{n}{m+1} > \cdots > \binom{n}{n}.$$

Если же $n = 2m+1$, то

$$k < m \Rightarrow \frac{n-k}{k+1} > 1, \quad k = m \Rightarrow \frac{n-k}{k+1} = 1, \quad k > m \Rightarrow \frac{n-k}{k+1} < 1$$
$$\binom{n}{0} < \binom{n}{1} < \cdots < \binom{n}{m-1} < \binom{n}{m} = \binom{n}{m+1} > \binom{n}{m+2} > \cdots > \binom{n}{n}.$$

В любом случае можно утверждать, что ширина $\mathbb{B}^n$ не меньше, чем $\binom{n}{\lfloor \frac{n}{2} \rfloor}$. Покажем, что в действительности справедливо равенство: ширина $\mathbb{B}^n$ в точности равна $\binom{n}{\lfloor \frac{n}{2} \rfloor}$. Для этого проведем следующую цепочку рассуждений: в n-мерном единичном кубе существует ровно $n!$ максимальных цепей из $\widetilde{0}$ в $\widetilde{1}$. Это вытекает из того, что число путей из нуля в единицу равно числу способов упорядоченной расстановки n единиц по n позициям (замена каждого нуля единицей добавляет ребро к уже существующей цепи, а всего ребер — n). Аналогично, число максимальных цепей из $\widetilde{0}$ в $\widetilde{1}$, проходящих через заданную вершину $\widetilde{\alpha}$: $\|\widetilde{\alpha}\| = k$ равно $k!\,(n-k)!$. Используя эти факты, рассмотрим произвольную антицепь $A = \{\widetilde{\alpha}_1, \ldots, \widetilde{\alpha}_s\}$, причем $\|\widetilde{\alpha}_i\| = k_i$, $i = \overline{1,s}$. Всего различных цепей, проходящих через A

$$k_1!\,(n-k_1)! + k_2!\,(n-k_2)! + \cdots + k_s!\,(n-k_s)! \leqslant n!$$

Отсюда имеем

$$\sum_{i=1}^{s} \frac{1}{\binom{n}{k_i}} \leqslant 1, \text{ в то же время } \sum_{i=1}^{s} \frac{1}{\binom{n}{k_i}} \geqslant \frac{s}{\binom{n}{\lfloor \frac{n}{2} \rfloor}} \Longrightarrow s \leqslant \binom{n}{\lfloor \frac{n}{2} \rfloor},$$

причем, если хотя бы одно $\widetilde{\alpha}_\ell$ не лежит в среднем (в случае четного n) или в двух средних (в случае нечетного n) слоях, то неравенство будет строгим. Таким образом, помимо того, что показано равенство ширины n-мерного куба $\binom{n}{\lfloor \frac{n}{2} \rfloor}$, еще и указан общий вид максимальных антицепей. В случае четного n максимальная антицепь всего одна — $\binom{n}{2}$-ый слой. Случай нечетного $n = 2m+1$ требует особого рассмотрения. Очевидно, что если хотя бы один элемент антицепи лежит вне двух средних слоев, то данная антицепь не будет максимальной. Предположим, что максимальная антицепь

принадлежит одновременно обоим средним слоям: $A = X \cup Y$, $X \subset \mathbb{B}^n_{m+1}$, $Y \subset \mathbb{B}^n_m$, причем $X, Y \neq \varnothing$. Так как $\binom{n}{m} = \binom{n}{m+1}$, двудольный граф, долями которого являются $\mathbb{B}^n_{m+1}$ и $\mathbb{B}^n_m$, а ребрами — все ребра, соединяющие эти же слои в $\mathbb{B}^n$, будет однородным (каждой вершине инцидентно одинаковое число ребер). Для множества X рассмотрим его *тень*:

$$P(X) = \left\{ \widetilde{\alpha} \in \mathbb{B}^n_m \,\middle|\, \exists \widetilde{\beta} \in X : \widetilde{\alpha} < \widetilde{\beta} \right\}.$$

Очевидно, что число ребер, соединяющих множество X со своей тенью не превосходит числа ребер, соединяющих $P(X)$ с верхней долей:

$$|X| \cdot (m+1) \leqslant |P(X)| \cdot (m+1) \Longrightarrow |X| \leqslant |P(X)|,$$

причем равенство достигается только в том случае, когда X совпадает со всем слоем, иными словами, в случае $X \subsetneq \mathbb{B}^n_{m+1}$ верно строгое неравенство $|X| < |P(X)|$. Но $Y = \mathbb{B}^n_m \setminus P(X)$ и $|Y| < \left|\mathbb{B}^n_{m+1} \setminus X\right|$, следовательно, A не является максимальной антицепью, так как $|A| < |\mathbb{B}^n_m|$. Таким образом, по доказанному в случае нечетного n единичный куб $\mathbb{B}^n$ содержит всего две максимальные антицепи: соответственно $\left\lfloor \frac{n}{2} \right\rfloor$-ый и $\left\lceil \frac{n}{2} \right\rceil$-ый слои.

Единичный n-мерный куб является ранжированным частично упорядоченным множеством. Как оказалось, ширина $\mathbb{B}^n$ совпадает с мощностью наибольшего слоя. Такие ранжированные частично упорядоченные множества называются *шпернеровыми*. Рассмотрим еще один пример шпернерова множества.

Ранее было обозначено через Γ^n частично упорядоченное по включению множество граней n-мерного единичного куба. Также было показано, что всего граней 3^n. Проведем ту же цепочку рассуждений, что и в случае $\mathbb{B}^n$. Единицей в этом частичном порядке является тривиальная грань $\mathbb{B}^n$, а вот нуля здесь нет: минимальными являются 2^n элементов, являющихся также тривиальными гранями, состоящими из одной вершины каждая. Всего в Γ^n существует $2^n n!$ максимальных антицепей (спускаясь по частичному порядку, на k-ом шаге выбираем одну из $(n-k+1)$ ранее невыбранных координат и одним из двух способов заменяем ее либо на 0, либо на 1). Всего k-мерных граней $\binom{n}{k}2^{n-k}$, так как их число равно количеству способов выбора k степеней свободы из n возможных ($\binom{n}{k}$ способов), в каждом из которых возможны все допустимые значения фиксированных $n-k$ координат (2^{n-k} вариантов). Всего цепей, проходящих через выбранную грань размерности k равно $2^k k!\,(n-k)!$, так как их количество равно числу способов упорядоченного открывания $n-k$ фиксированных координат ($(n-k)!$ способов), после каждого из которых возможны все $2^k k!$ цепей до минимальных элементов.

Покажем унимодальность последовательности чисел $\{b_k\}_{k=0}^n$ k-мерных граней: $b_k = \binom{n}{k}2^{n-k}$. Действительно,

$$\frac{b_{k+1}}{b_k} = \frac{\binom{n}{k+1}2^{n-k-1}}{\binom{n}{k}2^{n-k}} = \frac{1}{2} \cdot \frac{n-k}{k+1}$$

монотонно убывает. Пусть $n \geqslant 3$. Тогда

$$k < \frac{n-1}{3} \Rightarrow \frac{b_{k+1}}{b_k} > 1, \quad k = \frac{n-1}{3} \Rightarrow \frac{b_{k+1}}{b_k} = 1, \quad k > \frac{n-1}{3} \Rightarrow \frac{b_{k+1}}{b_k} < 1.$$

Отсюда три случая: если $n \equiv 2 \pmod 3$, то наибольший слоев два: слой $\left\lfloor \frac{n}{3} \right\rfloor$-мерных и $\left\lceil \frac{n}{3} \right\rceil$-мерных граней; если же $n \not\equiv 2 \pmod 3$, то наибольший слой один: множество $\left\lfloor \frac{n}{3} \right\rfloor$-мерный граней. В дальнейшем нам понадобится лишь тот факт, что в любом случае $\left\lfloor \frac{n}{3} \right\rfloor$-ый слой является максимальным.

Найдем ширину множества Γ^n. Очевидно, она не меньше, чем ширина наибольшего слоя, то есть $\binom{n}{\left\lfloor \frac{n}{3} \right\rfloor} \cdot 2^{n-\left\lfloor \frac{n}{3} \right\rfloor}$. Покажем точное равенство. Для этого рассмотрим произвольную антицепь $A = \{\widetilde{\alpha}_1, \ldots, \widetilde{\alpha}_s\}$, причем размерность грани $\widetilde{\alpha}_i$ равна k_i для $i = \overline{1,s}$. Количество максимальных цепей, проходящих через элементы A, не превосходит общего числа максимальных цепей в Γ^n:

$$2^{k_1} k_1!\,(n-k_1)! + 2^{k_2} k_2!\,(n-k_2)! + \cdots + 2^{k_s} k_s!\,(n-k_s)! \leqslant n!\,2^n.$$

Отсюда имеем

$$\sum_{i=1}^{s} \frac{1}{\binom{n}{k_i}2^{n-k_i}} \leqslant 1, \text{ в то же время } \sum_{i=1}^{s} \frac{1}{\binom{n}{k_i}2^{n-k_i}} \geqslant \frac{s}{\binom{n}{\left\lfloor \frac{n}{3} \right\rfloor}2^{n-\left\lfloor \frac{n}{3} \right\rfloor}} \Longrightarrow s \leqslant \binom{n}{\left\lfloor \frac{n}{3} \right\rfloor}2^{n-\left\lfloor \frac{n}{3} \right\rfloor}.$$

Отсюда видно, что если хотя бы один элемент антицепи лежит вне $\left\lfloor \frac{n}{3} \right\rfloor$-ого слоя в случае $n \not\equiv 2 \pmod 3$ (вне $\left\lfloor \frac{n}{3} \right\rfloor$-ого и $\left\lceil \frac{n}{3} \right\rceil$-ого слоев в случае $n \equiv 2 \pmod 3$), то антицепь не будет максимальной, так как будет выполняться соответствующее строгое неравенство. Итак, Γ^n является также шпернеровым множеством и его ширина равна $\binom{n}{\left\lfloor \frac{n}{3} \right\rfloor}2^{\left\lceil \frac{2n}{3} \right\rceil}$.

Рассмотрим частично упорядоченное множество $\mathbb{B}^n$. Булевой функцией, заданной на нем называется любое отображение $\mathbb{B}^n \to \mathbb{B}^1$. Монотонной булевой функцией, заданной на $\mathbb{B}^n$ называется любая булева функция f, удовлетворяющая импликации

$$\widetilde{\alpha} \leqslant \widetilde{\beta} \Longrightarrow f(\widetilde{\alpha}) \leqslant f\left(\widetilde{\beta}\right).$$

Нас будет интересовать вопрос о числе таких отображений как о функции, зависящей от n. В дальнейшем условимся обозначать ее через $\psi(n)$. В случае $n=0$ все функции монотонны (так как они суть константы 0 и 1): $\psi(0)=2$. При $n=1$ немонотонной является лишь отрицание, так что $\psi(n)=3$. В дальнейшем $n\geqslant 2$. Для начал получим тривиальную нижнюю оценку на число монотонных функций для $n\geqslant 2$. Для этого рассмотрим в $\mathbb{B}^n$ два слоя: $\lfloor\frac{n}{2}\rfloor$-ый и $\left(\lfloor\frac{n}{2}\rfloor+1\right)$-ый. Определим семейство монотонных функций $\mathbf{\Phi}=\mathbf{\Phi}_1\cup\mathbf{\Phi}_2$ следующим образом: на всех слоях выше $\left(\lfloor\frac{n}{2}\rfloor+1\right)$-го определим все функции равными единице, а на всех слоях ниже $\lfloor\frac{n}{2}\rfloor$-го определим их равными нулю. Все функции из $\mathbf{\Phi}_1$ равны нулю на $\lfloor\frac{n}{2}\rfloor$-ом слое и определены произвольным образом на $\left(\lfloor\frac{n}{2}\rfloor+1\right)$-ом — всего таких столько же, сколько существует способов определить функцию на $\binom{n}{\lfloor\frac{n}{2}\rfloor+1}$ наборах, то есть $2^{\binom{n}{\lfloor\frac{n}{2}\rfloor+1}}$. Все функции из $\mathbf{\Phi}_1$ наоборот: равны единице на $\left(\lfloor\frac{n}{2}\rfloor+1\right)$-ом слое и определены произвольным образом на $\lfloor\frac{n}{2}\rfloor$-ом — всего таких столько же, сколько существует способов определить функцию на $\binom{n}{\lfloor\frac{n}{2}\rfloor}$ наборах, то есть $2^{\binom{n}{\lfloor\frac{n}{2}\rfloor}}$. Очевидно, что пересечение $\mathbf{\Phi}_1\cap\mathbf{\Phi}_2$ содержит лишь одну функцию: равную нулю вплоть до $\lfloor\frac{n}{2}\rfloor$-го слоя, и равную единице, начиная с $\left(\lfloor\frac{n}{2}\rfloor+1\right)$-ого слоя. Учитывая то, что все остальные функции в $\mathbf{\Phi}_1$ и $\mathbf{\Phi}_2$ различны, получена нижняя оценка на число булевых монотонных функций:

$$\psi(n)\geqslant 2^{\binom{n}{\lfloor\frac{n}{2}\rfloor}}+2^{\binom{n}{\lfloor\frac{n}{2}\rfloor+1}}-1.$$

Следующая, интересующая нас задача — это расшифровка монотонной булевой функции. Известно, что некоторая функция $f:\mathbb{B}^n\to\mathbb{B}$ является монотонной. Требуется ее расшифровать, то есть определить ее значения на всех вершинах $\mathbb{B}^n$. При этом разрешается задавать вопросы вида: чему равна функция на данном наборе. Нас будет интересовать наименьшее число вопросов как функция от n. Договоримся в дальнейшем обозначать ее $\varphi(n)$. Для получения нижней оценки на эту функцию воспользуемся семейством функций $\mathbf{\Phi}$, построенным при получении нижней оценки на число монотонных булевых функций: если задано вопросов меньше, чем $\binom{n}{\lfloor\frac{n}{2}\rfloor}+\binom{n}{\lfloor\frac{n}{2}\rfloor+1}$, то заведомо найдется вершина на одном из выделенных средних слоев, на котором значение функции не спрашивалось. В этом случае двумя монотонными функциями, неразличимыми таким тестом будут функции из $\mathbf{\Phi}$, различные лишь на вершине, на которой значение не спрашивалось. Таким образом,

$$\varphi(n)\geqslant\binom{n}{\lfloor\frac{n}{2}\rfloor}+\binom{n}{\lfloor\frac{n}{2}\rfloor+1}.$$

Теорема 1.11 (Ансель). *$\mathbb{B}^n$ может быть покрыт $\binom{n}{\lfloor\frac{n}{2}\rfloor}$ максимальными цепями со следующими свойствами:*

1. *число цепей длины $n-2p+1$ для $p=\overline{0,\lfloor\frac{n}{2}\rfloor}$ равно $\binom{n}{p}-\binom{n}{p-1}$,*
2. *в наименьшей вершине цепи длины $n-2p+1$ как в наборе из нулей единиц содержится в точности p единиц и $n-p$ нулей, а в наибольшей — $n-p$ единиц и p нулей,*
3. *для любых наборов $\alpha_1\lessdot\alpha_2\lessdot\alpha_3$ на цепи длины $n-2p+1$*

$$\alpha_1=(\ldots\,0\ldots\,0\ldots)$$
$$\alpha_2=(\ldots\,0\ldots\,1\ldots)$$
$$\alpha_3=(\ldots\,1\ldots\,1\ldots)$$

их относительное дополнение до квадрата α:

$$\alpha=(\ldots\,1\ldots\,0\ldots)$$

лежит на цепи длины $n-2p-1$.

Замечание. Из пункта 1 видно, что все цепи имеют длину одной и той же четности, причем в случае нечетного n все цепи имеют четную длину, а в случае четного n — нечетную.

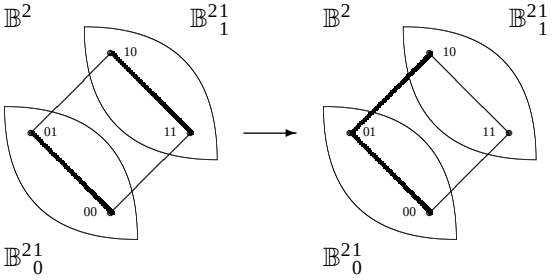
□ *Док-во.* Проведем индукцию по n. Для $n=0$ теорема, очевидно верна.

•

Покрытие состоит всего из одной цепи, для которой пункты 1, 2 и 3 тривиальны. Для $n=1$ утверждения также выполняются:

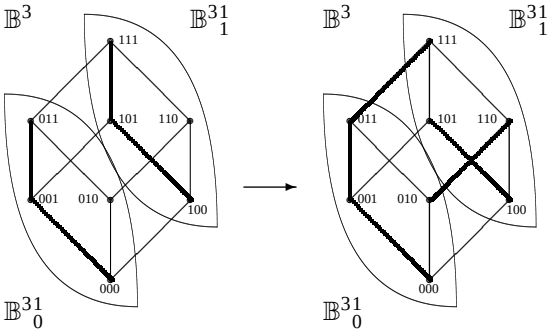
Покрытие содержит единственную цепь, для которой проверка условий 1, 2, 3 также не вызывает затруднений. Такие тривиальные цепи, образующие покрытия $\mathbb{B}^0$ и $\mathbb{B}^1$ называются цепями Анселя. Более интересны случаи $n=2$ и $n=3$, на которых можно наглядно продемонстрировать индуктивный переход.

Пусть $n=2$. Куб $\mathbb{B}^2$ получается соединением всех вершин одномерного куба $\mathbb{B}^{11}_0$ с одноименными вершинами одномерного куба $\mathbb{B}^{21}_1$, при этом все вершины $\mathbb{B}^{21}_0$ получают метки, начинающиеся нулем, а все вершины, принадлежавшие $\mathbb{B}^{21}_1$ получают метки, начинающиеся единицей. Рассмотрим в $\mathbb{B}^{21}_0$ и в $\mathbb{B}^{21}_1$ уже построенные на предыдущем шаге их покрытия цепями Анселя.



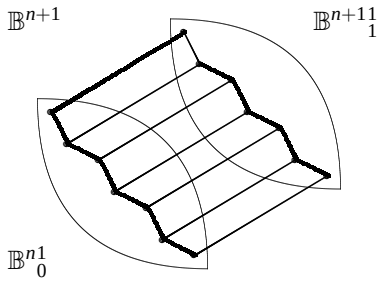
Разрываем цепь в $\mathbb{B}^{21}_1$ и соединяем ее бывший максимальный элемент с максимальным элементом цепи покрытия $\mathbb{B}^{21}_0$.

В случае $n=3$ алгоритм действий аналогичный. Куб $\mathbb{B}^3$ получается соединением всех вершин двумерного куба $\mathbb{B}^{21}_0$ с одноименными вершинами одномерного куба $\mathbb{B}^{31}_1$, при этом все вершины $\mathbb{B}^{31}_0$ получают метки, начинающиеся нулем, а все вершины, принадлежавшие $\mathbb{B}^{31}_1$ получают метки, начинающиеся единицей. Рассмотрим в $\mathbb{B}^{31}_0$ и в $\mathbb{B}^{31}_1$ уже построенные на предыдущем шаге их покрытия цепями Анселя.



Снова отрываем от каждой цепи в $\mathbb{B}^{31}_1$ максимальный элемент и делаем его максимальным соответствующей цепи $\mathbb{B}^{31}_0$.

Теперь мы можем формализовать индуктивный переход. Пусть существует способ покрывать $\mathbb{B}^n$ цепями Анселя, при котором выполняются условия 1, 2 и 3. Тогда искомое покрытие для $\mathbb{B}^{n+1}$ строится следующим образом: от каждой цепи в $\mathbb{B}^{n+11}_1$ отрывается максимальный элемент и присоединяется к соответствующей цепи в $\mathbb{B}^{n+11}_0$. При этом длины всех цепей в $\mathbb{B}^{n+11}_1$ увеличиваются на единицу, а длины всех цепей в $\mathbb{B}^{n+11}_0$ уменьшаются на единицу (цепи длины 1 в $\mathbb{B}^{n+11}_0$ исчезают).



Проверим, удовлетворяет ли такое покрытие условиям теоремы:

1. Цепи длины $(n+1)-2p+1$ получаются из цепей длины $n-2p+1$, лежащих в грани $\mathbb{B}^{n1}_0$ (всего их $\binom{n}{p}-\binom{n}{p-1}$) удлинением на единицу и из цепей длины $n-2(p-1)+1$, лежащих в грани $\mathbb{B}^{n1}_1$ (всего их $\binom{n}{p-1}-\binom{n}{p-2}$) укорочением на единицу. Итого, цепей такой длины ровно $\binom{n}{p}-\binom{n}{p-2}=\binom{n+1}{p}-\binom{n+1}{p-1}$.

2. Возможны два тривиальных подслучая:

   (а) цепь получена удлинением соответствующей из $\mathbb{B}^{n1}_0$. Тогда число нулей в наименьшей вершине увеличилось на единицу (из-за появившегося первого разряда), число единиц в ней сохранилось, а число единиц в наибольшей вершине увеличилось на единицу (тоже из-за первого разряда), в то время как число нулей в ней сохранилось. Таким образом, условие выполняется.

(b) Цепь получена укорочением соответствующей из $\mathbb{B}^{n1}_{1}$. Тогда число нулей в минимальной вершине цепи сохранилось, число единиц в ней же увеличилось из-за появившегося первого разряда, а число единиц в максимальной вершине осталось прежним (так как одна единица добавилась первым разрядом, но бывшая максимальная вершина удалена, поэтому новая лежит уровнем ниже, следовательно, в младших разрядах содержит на одну единицу меньше), в то время как число нулей в максимальной вершине увеличилось на единицу (из-за спуска ее на один уровень вниз). Таким образом, и в этом случае условие сохраняется.

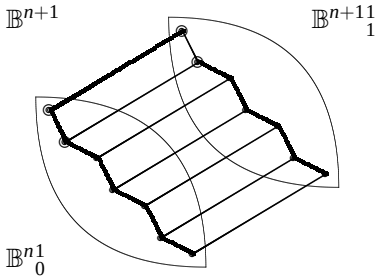
3. Берем три вершины с одной цепи, идущие подряд. Возможны два случая.

(a) Они взяты с укороченной цепи. Тогда, поскольку при индуктивном построении они были взяты с цепи $\mathbb{B}^{n1}_{1}$ длины на единицу больше, их дополнение до квадрата лежит (по индуктивному предположению) также в $\mathbb{B}^{n1}_{1}$ на цепи длины на 2 меньше (по индуктивному предположению соответствующая цепь, содержавшая нужное дополнение до квадрата, имела длину на 2 больше до отщепления максимальных элементов с каждой цепи, но после отщепления, как легко видеть, баланс длин сохранился).

(b) Они взяты с удлиненной цепи. Возможны два подслучая.

i. Все три вершины лежат в $\mathbb{B}^{n1}_{0}$. В этом случае по индуктивному предположению их дополнение до квадрата также находится в $\mathbb{B}^{n1}_{0}$, причем оно лежит на цепи длины на 2 меньше (по индуктивному предположению соответствующая цепь, содержавшая нужное дополнение до квадрата, имела длину на 2 меньше до добавления максимальных элементов к каждой цепи из $\mathbb{B}^{n1}_{1}$, но после их добавления, как легко видеть, баланс длин сохранился).

ii. Большая из этих трех вершин лежит в $\mathbb{B}^{n1}_{0}$. Тогда дополнением до квадрата, как легко видеть, будет служить максимальная вершина соответствующей укороченной цепи.



Поскольку при индуктивном построении сначала обе цепи были одной длины, а затем первая из них стала на одну вершину длиннее, а вторая — на одну вершину короче, то условие и в этом случае выполняется.

Теорема доказана. ■

Используя теорему Анселя можно получить верхнюю оценку на число монотонных булевых функций $\psi(n)$. Действительно, покроем $\mathbb{B}^n$ цепями Анселя. Рассмотрим все цепи Анселя наименьшей длины (это либо 1, либо 2). Определим на них не более, чем тремя способами монотонную функцию. Затем, возьмем на больших цепях (длины $n-2p+1$) три наименьшие вершины. Зная значения на всех цепях длины, не более, чем $n-2(p+1)+1$ по монотонности дополним их до квадрата и определим на них снова не более, чем тремя способами монотонную функцию. При этом, на всех вершинах, кроме двух функция определится однозначно, а на оставшихся останется как раз ровно три варианта. Таким образом, суммируя полученные результаты относительно $\psi(n)$, можно утверждать, что

$$2^{\left(\left\lfloor\frac{n}{2}\right\rfloor\right)}+2^{\left(\left\lfloor\frac{n}{2}\right\rfloor+1\right)}-1\leqslant\psi(n)\leqslant 3^{\left(\left\lfloor\frac{n}{2}\right\rfloor\right)}.$$

Также можно показать, что ранее полученная нижняя оценка на сложность расшифровки монотонной булевой функции $\varphi(n)$ совпадает с верхней оценкой. Действительно, в случае нечетного n сначала узнаем значения на цепях длины 2 (при этом зададим не более, чем по два вопроса на каждую цепь). Затем, используя снова продолжения до квадрата, узнаем значения на цепях большей длины (при этом зададим снова не более чем по два вопроса для каждой цепи). Итак, для нечетного случая

$$\varphi(n)\leqslant 2\cdot\binom{n}{\lfloor\frac{n}{2}\rfloor}=\binom{n}{\lfloor\frac{n}{2}\rfloor}+\binom{n}{\lfloor\frac{n}{2}\rfloor+1}.$$

В четном случае узнаем сначала значения функции на цепях длины 1, задав по одному вопросу для каждой цепи. Затем, для цепей большей длины узнаем значения не более, чем на двух вершинах, используя продолжения до квадрата. Таким образом, и в этом случае $\varphi(n)$ не превосходит своей нижней оценки:

$$\varphi(n)\leqslant 1\cdot\left(\binom{n}{\frac{n}{2}}-\binom{n}{\frac{n}{2}-1}\right)+2\cdot\binom{n}{\frac{n}{2}-1}=\binom{n}{\frac{n}{2}}+\binom{n}{\frac{n}{2}-1}=\binom{n}{\frac{n}{2}}+\binom{n}{\frac{n}{2}+1}.$$

Итак, окончательно можно утверждать, что

$$\varphi(n) = \binom{n}{\lfloor \frac{n}{2} \rfloor} + \binom{n}{\lfloor \frac{n}{2} \rfloor + 1}.$$

Алгебры инцидентности. Частичный порядок $(P, \leqslant)$ будем называть *локально конечным*, если любой интервал конечен. Пусть в дальнейшем $\mathbb{F}$ — некоторое бесконечное поле.

Определение 1.4.13. *Алгеброй инцидентности частично упорядоченного множества* $(P, \leqslant)$ называется множество

$$A(P) = \left\{ f : P^2 \to \mathbb{F} \,\middle|\, x \not\leqslant y \Rightarrow f(x,y) = 0 \right\}.$$

Алгебра инцидентности замкнута относительно *операции сложения*:

$$(f+g)(x,y) = f(x,y) + g(x,y),$$

операции умножения на число $r \in \mathbb{F}$:

$$(r \cdot f)(x,y) = r \cdot f(x,y),$$

а также операции свертки

$$(f \star g)(x,y) = \sum_{x \leqslant z \leqslant y} f(x,z) \cdot g(z,y).$$

Нейтральным элементом по сложению является функция, тождественно равная нулю и очевидным образом принадлежащая алгебре инцидентности. Свертка ассоциативна: $f \star (g \star h) = (f \star g) \star h$. Действительно,

$$\begin{aligned}(f \star (g \star h))(x,y) &= \sum_{x \leqslant z \leqslant y} f(x,z) \cdot (g \star h)(z,y) = \sum_{x \leqslant z \leqslant y} f(x,z) \left(\sum_{z \leqslant w \leqslant y} g(z,w) \cdot h(w,y) \right) \\ &= \sum_{x \leqslant z \leqslant y} \sum_{z \leqslant w \leqslant y} f(x,z) \cdot g(z,w) \cdot h(w,y) = \sum_{x \leqslant w \leqslant y} \sum_{x \leqslant z \leqslant y} f(x,z) \cdot g(z,w) \cdot h(w,y) \\ &= \sum_{x \leqslant w \leqslant y} \left(\sum_{x \leqslant z \leqslant w} f(x,z) \cdot g(z,w) \right) \cdot h(w,y) = \sum_{x \leqslant w \leqslant y} (f \star g)(x,w) \cdot h(w,y) = ((f \star g) \star h)(x,y).\end{aligned}$$

В то же время операция некоммутативна. Действительно, пусть

$$x < y,\ f(x,x) = f(x,y) = 0,\ f(y,y) = e,\ g(x,y) = a, \text{ где } a \in \mathbb{F},\ e \neq 0.$$

Тогда

$$\begin{aligned}(f \star g)(x,y) &= f(x,x) \cdot g(x,y) + f(x,y) \cdot g(y,y) = 0, \\ (g \star f)(x,y) &= g(x,x) \cdot f(x,y) + g(x,y) \cdot f(y,y) = a^2 \neq 0.\end{aligned}$$

Последнее равенство вытекает из того, что в поле нет делителей нуля.

Из определения свертки легко видеть, что она дистрибутивна относительно сложения:

$$\begin{aligned}(f+g) \star h &= f \star h + g \star h, \\ f \star (g+h) &= f \star g + f \star h.\end{aligned}$$

Нейтральной функцией по свертке будет дельта-функция: $\forall f \in A(P) \Rightarrow f \star \delta = \delta \star f = f$, где

$$\delta(x,y) = \begin{cases} 1, & x = y, \\ 0, & \text{иначе.} \end{cases}$$

Иногда можно говорить об обратных элементах по свертке f_Λ^{-1} и f_Π^{-1} (соответственно левом и правом обратных элементах), если $f_\Lambda^{-1} \star f = \delta$ и $f \star f_\Pi^{-1} = \delta$. Не всякий элемент алгебры инцидентности имеет обратный, однако если он все же существует, то левый обратный совпадает с правым обратным элементом:

$$f_\Lambda^{-1} = f_\Lambda^{-1} \star \delta = f_\Lambda^{-1} \star \left(f \star f_\Pi^{-1} \right) = \left(f_\Lambda^{-1} \star f \right) \star f_\Pi^{-1} = \delta \star f_\Pi^{-1} = f_\Pi^{-1}.$$

Теорема 1.12. *Элемент $f \in A(P)$ обратим тогда и только тогда, когда для любого $x \in P$ выполняется $f(x,x) \neq 0$.*

□ *Док-во.* Необходимость в данном случае очевидна: если $f \in A(P)$ обратим, то

$$f^{-1}(x,x) \cdot f(x,x) = 1$$

по определению операции свертки и дельта-функции. Поскольку в поле нет делителей нуля, для любого $x \in P$ выполняется $f(x,x) \neq 0$.

Покажем достаточность. Для этого определим для функции f обратную явным образом. Если $x \not\leqslant y$, очевидно, определим $f^{-1}(x,y) = 0$. Поскольку для любого x выполняется $f^{-1}(x,x) \cdot f(x,x) = 1$ и $f(x,x) \neq 0$, определим $f^{-1}(x,x) = \frac{1}{f(x,x)}$. Пусть теперь $x < y$ и для любого $z \in [x,y)$ обратная функция $f^{-1}(x,z)$ уже определена. Тогда по определению свертки

$$\sum_{x \leqslant z \leqslant y} f^{-1}(x,z) \cdot f(z,y) = \delta(x,y) = 0 \Longrightarrow f^{-1}(x,y) = -\frac{1}{f(y,y)} \sum_{x \leqslant z < y} f^{-1}(x,z) \cdot f(z,y).$$

Попутно доказано, что обратный элемент, если он существует, единственен.

Теорема доказана. ■

Перечислим теперь наиболее важные функции алгебра инцидентности.

1. $\delta(x,y) = \begin{cases} 1, & x = y, \\ 0, & \text{иначе.} \end{cases}$

2. $\zeta(x,y) = \begin{cases} 1, & x \leqslant y, \\ 0, & \text{иначе} \end{cases}$ — дзета-функция.

3. $\lambda(x,y) = \begin{cases} 1, & x = y,\ x \lessdot y, \\ 0, & \text{иначе} \end{cases}$ — лямбда-функция.

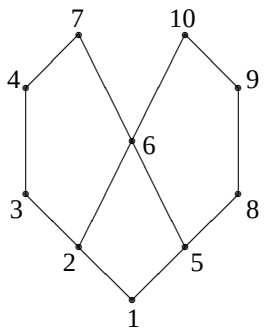
4. $\eta(x,y) = \zeta(x,y) - \delta(x,y) = \begin{cases} 1, & x < y, \\ 0, & \text{иначе} \end{cases}$ — эта-фунция.

5. $\kappa(x,y) = \lambda(x,y) - \delta(x,y) = \begin{cases} 1, & x \lessdot y, \\ 0, & \text{иначе} \end{cases}$ — каппа-функция.

6. $\mu(x,y) = \zeta^{-1}(x,y)$ — функция Мебиуса.

7. $\ell(x,y)$ — длина максимальной (x,y)-цепи.

Введем понятие *монотонной нумерации частичного порядка*. Нумерацией частично упорядоченного множества $(P,\leqslant)$ называется отображение $n : P \to \mathbb{N}$. Нумерация называется монотонной, если из $p_1 \leqslant p_2$ следует $n(p_1) \leqslant n(p_2)$. Алгоритм монотонной нумерации произвольного конечного частичного порядка чрезвычайно прост: на первом шаге выбираем произвольный минимальный элемент и нумеруем его единицей. Затем, на каждом последующем шаге выбираем элемент, ниже которого лежат только помеченные элементы, и нумеруем его следующим натуральным числом. Очевидно, выполняется $x < y \Rightarrow n(x) < n(y)$. Рассмотрим это на примере. Пусть $P = \{1,2,3,4,5,6,7,8,9,10\}$, а отношение частичного порядка задается диаграммой Хассе, представленной на рисунке.



Вершины частичного порядка пронумерованы, как легко проверить, монотонно. Важнейшим свойством монотонной нумерации является то, что матрицы введенных нами ранее функций имеют верхний треугольный вид. Так например,

матрица дзета-функции выглядит так (номера строк соответствуют номерам x, а номера столбцов — номерам y в монотонной нумерации):

$$\zeta = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Также можно найти матрицу функции Мебиуса, которая также будет иметь верхний треугольный вид:

$$\mu = \begin{pmatrix} 1 & -1 & 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 & -1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 & 0 & -1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Пусть частично упорядоченное множество $(P, \leqslant)$ локально конечно и имеет наименьший элемент. Пусть $\mathscr{F} : P \to \mathbb{F}$ — некоторая функция, определенная на этом частичном порядке. Предположим, что вместо $\mathscr{F}$ известны значения *суммирующей функции*:

$$S_{\mathscr{F}}(x) = \sum_{y \leqslant x} \mathscr{F}(y).$$

Задача заключается в расшифровке исходной функции по известным значениям суммирующей функции. Задача решается следующим образом: введем новую функцию

$$f(x,y) = \begin{cases} \mathscr{F}(z), & x = 0,\ y = z \\ 0, & \text{иначе.} \end{cases}$$

Выполним свертку этой функции и дзета-функции:

$$S_{\mathscr{F}}(x,y) = \sum_{x \leqslant z \leqslant y} f(x,z) \cdot \zeta(z,y) = (f \star \zeta)(x,y).$$

Очевидно, что $S_{\mathscr{F}}(0,x) = S_{\mathscr{F}}(x)$. Поскольку дзета-функция обратима, и обратной к ней является функция Мебиуса, можно выполнить следующую операцию, приводящую к *обращению Мебиуса*: $f(x,y) = (S_{\mathscr{F}} \star \mu)(x,y)$. Отсюда получаем основную формулу, определяющую значения $\mathscr{F}$ через значения суммирующей функции:

$$\mathscr{F}(x) = f(0,x) = \sum_{y \leqslant x} S_{\mathscr{F}}(0,y) \cdot \mu(y,x) = \sum_{y \leqslant x} S_{\mathscr{F}}(y) \cdot \mu(y,x).$$

Рассмотрим конечный алфавит $\{a_1, \ldots, a_r\}$, $r \geqslant 2$. Построим все r^n слов над этим алфавитом длины n и разобьем из на классы эквивалентности. Прежде всего определим понятие периода: слово $(b_1, \ldots, b_n)$ имеет период $d | n$, если для любого i выполняется $b_i = b_{i+d}$ $(i + d \pmod n)$ и для любого $d' < d$ это неверно. Классом эквивалентности является множество слов, получающихся одно из другого циклическим сдвигом.

Рассмотрим пример: пусть $r = 2$, $n = 4$. Всего существует 16 слов длины 4 над двухбуквенным алфавитом (пусть это $\{0,1\}$). Два из них имеют период 1: это (0000) и (1111), два слова имеют период 2: это (0101) и (1010), остальные же слова имеют период 3. Всего 6 классов эквивалентности:

$$(0000)$$
$$(1111)$$
$$(0101),\ (1010)$$
$$(0001),\ (1000),\ (0100),\ (0010)$$
$$(0011),\ (1001),\ (1100),\ (0110)$$
$$(0111),\ (1011),\ (1101),\ (1110)$$

Обозначим через $\mathrm{M}(d)$ число классов эквивалентности слов периода d. Так, для $r=2$, $n=4$ $\mathrm{M}(1)=2$, $\mathrm{M}(2)=1$, $\mathrm{M}(4)=3$. Нас будет интересовать вопрос, чему же равно $\mathrm{M}(n)$. В данном случае легко построить суммирующую функцию, после чего можно выполнить обращение Мебиуса:

$$\sum_{d|n} d\cdot \mathrm{M}(d)=r^n \Longrightarrow \mathrm{M}(n)\cdot n=\sum_{d|n} r^d\cdot \mu(d,n)=\sum_{d|n} r^d\cdot \mu\left(\frac{n}{d}\right)=\sum_{d|n} r^{\frac{n}{d}}\cdot \mu(d).$$

Отсюда получаем окончательную формулу

$$\mathrm{M}(n)=\frac{1}{n}\sum_{d|n} r^{\frac{n}{d}}\mu(d).$$

Это число замечательно тем, что оно равно числу неприводимых нормированных многочленов степени n над $F_p[x]$, если только $r=p$ — простое. Так, например, при $r=2$

$$\mathrm{M}(4)=\frac{1}{4}\left(2^4\cdot 1+2^2\cdot(-1)+2^1\cdot 0\right)=3.$$

Решетки. Пусть $(P,\leqslant)$ — некоторое частично упорядоченное множество и $X\subseteq P$.

Определение 1.4.14. *Верхней гранью множества X* называется элемент (если он существует) $a\in P$ такой, что $\forall x\in X\Rightarrow x\leqslant a$. По двойственности определяется *нижняя грань множества X*. *Точной верхней гранью множества X* называется наименьшая из верхних граней $\sup X$ (если такая существует). По двойственности определяется *точная нижняя грань* $\inf X$ *множества X*.

Определение 1.4.15. Частично упорядоченное множество $(P,\leqslant)$ называется *полной решеткой*, если у любого множества $X\subseteq P$ существуют $\sup X$ и $\inf X$. Если у каждого $X\subseteq P$ существует $\sup X$, то $(P,\leqslant)$ называется *верхней полурешеткой*, если же у каждого $X\subseteq P$ существует $\inf X$, то $(P,\leqslant)$ называется *нижней полурешеткой*.

Определение 1.4.16. Частично упорядоченное множество $(P,\leqslant)$ называется *решеткой*, если у любых $x,y\in P$ существуют $\sup\{x,y\}\stackrel{\text{def}}{=}x\vee y$ и $\inf\{x,y\}\stackrel{\text{def}}{=}x\wedge y$.

Замечание. Если $(P,\leqslant)$ — решетка, то для любых $x_1,\ldots,x_n\in P$ существуют

$$\sup\{x_1,\ldots,x_n\}=x_1\vee\cdots\vee x_n \quad\text{и}\quad \inf\{x_1,\ldots,x_n\}=x_1\wedge\cdots\wedge x_n.$$

Примером неполной решетки может выступать частично упорядоченное множество натуральных чисел по делимости $(\mathbb{N},|)$. Легко видеть, что в нем множество $X=\mathbb{N}$ не имеет верхних граней вообще, следовательно, не имеет и точной верхней грани.

Введенные выше обозначения точной верхней и точной нижней граней пар элементов решетки можно рассматривать как операцию над элементами исходного частичного порядка. Легко доказать, что выполняется простой закон ассоциативности, например, для точной верхней грани:

$$(x\vee y)\vee z=x\vee(y\vee z).$$

Действительно, пусть $x\vee y=a$ и $b=a\vee z$. Предположим, что $x\vee(y\vee z)=b_1<b$. Но тогда $x\leqslant b_1$, $y\vee z\leqslant b_1\Rightarrow y\leqslant b_1$, причем b_1 является верхней гранью как для x, так и для y. Тогда $a\leqslant b_1$, но $b\leqslant a$, откуда получаем противоречие с предположением $b\leqslant b_1$.

Решеткой является множество

$$\mathrm{M}(d_1,\ldots,d_n)=\left\{(x_1,\ldots,x_n)\,\middle|\, 0\leqslant x_i\leqslant d_i,\ x_i,d_i\in\mathbb{Z},\ i=\overline{1,n}\right\},$$

причем $(x_1,\ldots,x_n)\leqslant(y_1,\ldots,y_n)\Leftrightarrow x_i\leqslant y_i\ \forall i=\overline{1,n}$. Множество, состоящее из линейных подпространств пространства $\mathbb{R}^3$ (начало координат, три координатных оси, три координатных плоскости и все $\mathbb{R}^3$) также представляет собой решетку, причем изоморфную $\mathbb{B}^3$. Частично упорядоченное по включению множество всех подгрупп (включая тривиальные — пустую и саму группу) некоторой конечной группы G является также решеткой. При этом точной верхней гранью множества является наименьшая группа, содержащая все группы это множества, а точной нижней гранью — пересечение всех групп множества. Замкнутые классы функций k-значной логики ($k\geqslant 2$) также образуют решетку. По аналогии с группой точной верхней гранью множества классов выступает наименьший класс, всех их содержащий, а точной нижней гранью множества классов является их пересечение. При $k=2$ решетка замкнутых классов в P_k называется *решеткой Поста*.

Очевидным образом выполняются следующие пять свойств:

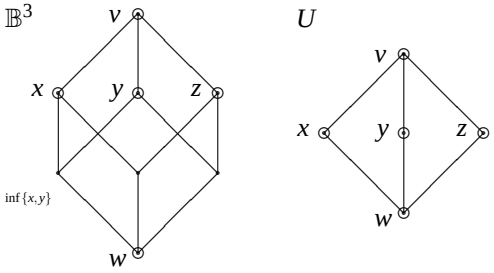
1. $x\wedge x=x$, $x\vee x=x$ — *идемпотентность*,
2. $x\wedge y=y\wedge x$, $x\vee y=y\vee x$ — *коммутативность*,

3. $(x \wedge y) \wedge z = x \wedge (y \wedge z)$, $(x \vee y) \vee z = x \vee (y \vee z)$ — *ассоциативность*,
4. $x \wedge (x \vee y) = x \vee (x \wedge y) = x$ — *поглощение*,
5. $x \leq y \Longleftrightarrow x = x \wedge y$ и $y = x \vee y$ — *совместимость*,
6. свойство *дистрибутивности*, которое, вообще говоря, выполняется не всегда:
   (a) $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ и
   (b) $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$.

Таким образом, можно перейти к рассмотрению алгебры $(P, \vee, \wedge)$, соотносящейся с частичным порядком $(P, \leqslant)$ согласно свойству 5.

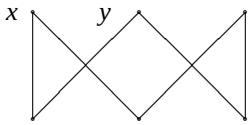
Определение 1.4.17. *Подрешеткой* решетки $(P, \vee, \wedge)$ называется решетка $(Q, \vee, wedge)$, где $Q \subseteq P$ замкнутая относительно операций взятия точной верхней и точной нижней граней в исходной решетке $(P, \vee, \wedge)$.

Чтобы подчеркнуть важность последнего требования приведем пример решетки U, носитель которой является подмножеством решетки $\mathbb{B}^3$, однако, U не является подрешеткой $\mathbb{B}^3$ согласно введенному определению.



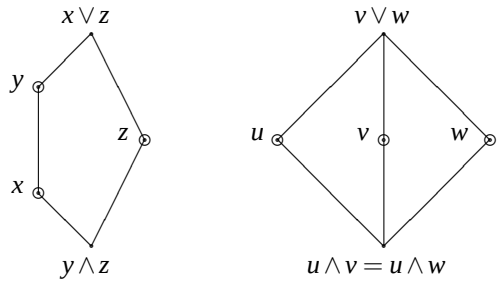
Действительно, $x, y \in U$, но $\inf\{x, y\} \notin U$.

Примером множества, не являющегося решеткой служит частично упорядоченное множество, заданное диаграммой Хассе: элементы x, y не имеют верхней грани вообще, а значит и точной верхней грани.



Определение 1.4.18. Если для любых трех элементов x, y, z решетки выполняются условия 6a и 6b, то решетка называется *дистрибутивной*.

Примерами дистрибутивных решеток являются $\mathbb{B}^n$, упорядоченный стандартным образом и $(\mathbb{N}, |)$. Примерами недистрибутивных решеток являются пентагон и решетка U, рассмотренная в качестве контрпримера подрешетки.



Действительно, в пентагоне:

$$x \vee (y \wedge z) = x \neq y = (x \vee y) \wedge (x \vee z),$$

в решетке U:

$$u \wedge (v \vee w) = u \neq 0 = (u \wedge v) \vee (u \wedge w).$$

Справедлив некий аналог теоремы Понтрягина-Куратовского: решетка является дистрибутивной тогда и только тогда, когда она не содержит в качестве подрешеток пентагона и U. Используя это утверждение, можно показать, например, что частично упорядоченное по подразбиениям множество разбиений конечного множества является решеткой, которая не дистрибутивна, если только исходное множество содержит не менее трех элементов.

Любая решетка с конечным носителем является полной. Элемент p решетки L называется *неприводимым*, если выполняется импликация

$$p = x \vee y \Longrightarrow p = x \text{ или } p = y.$$

Исключим по определению из множества неприводимых элементов наименьший (несмотря на то, что вышеприведенная импликация для него выполняется). На языке диаграмм Хассе из вершины, соответствующей неприводимому элементу, выходит вниз не более одного ребра: в противном случае он являлся бы точной верхней гранью двух непосредственно предшествующих ему элементов. Согласно определению любой элемент частично упорядоченного множества является либо неприводимым, либо приводимым, поэтому для произвольного элемента a частично упорядоченного множества допустимо представление его в виде точной верхней грани неприводимых элементов $a = p_1 \vee p_2 \vee \cdots \vee p_s$. Если для любого $i = \overline{1,s} \Rightarrow a \neq p_1 \vee p_2 \vee \cdots \vee p_{i-1} \vee p_{i+1} \vee \cdots \vee p_s$, то такое разложение называется несократимым. В этом случае очевидно, что множество неприводимых элементов $\{p_i\}_{i=1}^{s}$ образует антицепь. Разложением для нуля будем считать сам нуль: $0 = 0$.

Лемма 1.4.1. *Пусть p — неприводимый элемент дистрибутивной решетки L и*

$$p \leqslant \bigvee_{i=1}^{n} a_i.$$

Тогда найдется такое $1 \leqslant i \leqslant n$, что $p \leqslant a_i$.

□ *Док-во.* Из условия ясно, что для p справедливо представление

$$p = p \wedge \left(\bigvee_{i=1}^{n} a_i \right) = \bigvee_{i=1}^{n} (p \wedge a_i).$$

Поскольку все $p \wedge a_i \leqslant p$, должно найтись такое i, что выполнится в точности равенство $p \wedge a_i = p$. В этом случае по определению точной нижней грани и выполнится $p \leqslant a_i$.

Лемма доказана. ■

Лемма 1.4.2 (Биркгоф). *Несократимое разложение на неприводимые элементы для любого элемента $a \in L$ (L — дистрибутивная решетка) однозначно с точностью до порядка неприводимых элементов, участвующих в разложении.*

□ *Док-во.* Пусть найдутся два несократимых разложения некоторого элемента $a \in L$ на неприводимые элементы:

$$a = p_1 \vee p_2 \vee \cdots \vee p_s = q_1 \vee q_2 \vee \cdots \vee q_r.$$

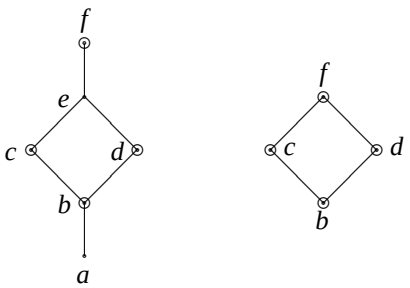
Из вида разложений следует, что

$$\forall i = \overline{1,s} \Rightarrow p_i \leqslant a = \bigvee_{i=1}^{r} q_i \Longrightarrow \exists j : p_i \leqslant q_j, \quad \text{аналогично } \exists k : q_j \leqslant p_k \Longrightarrow p_i \leqslant q_j \leqslant p_k.$$

Учитывая то, что элементы несократимого разложения на неприводимые элементы лежат на антицепи, получим $p_i = q_j = p_k$. Проведя эти рассуждения сначала для всех p_i, а затем для всех q_j, убедимся, что оба разложения состоят из одних и тех же неприводимых элементов и могут различаться лишь их порядком.

Лемма доказана. ■

Монотонная булева функция на частично упорядоченном множестве может быть задана следующим образом: выделяется произвольная максимальная по включению антицепь, выше которой функция определяется единицей, а на ней и ниже — нулем. По двойственности можно определить антимонотонную функцию. Это определение понадобится нам в дальнейшем при кодировании дистрибутивных решеток. Предварим это следующим примером. Пусть частично упорядоченное множество задается диаграммой Хассе.



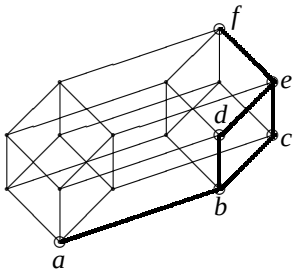
Выделим из этого множества подмножество всех неприводимые элементов — в данном случае это $\{b, c, d, f\}$. Неприводимые элементы находятся между собой в отношении частичного порядка, определяющемся в свою очередь своей диаграммой Хассе, представленной справа. Новый частичный порядок, образованный неприводимыми элементами можно упорядоченным образом покрыть цепями. Сделать это можно разными способами: например, пользуясь теоремой Дилуорса, покрыть числом цепей, равным ширине множества (в этом случае число цепей минимально), а можно тривиально: каждый неприводимый элемент объявить самостоятельной цепью (в этом случае число цепей максимально). Пусть уже имеется упорядоченное покрытие цепями $C_1, \ldots, C_n$ длин $\ell_1, \ldots, \ell_n$ соответственно. Пронумеруем элементы C_i по порядку числами от 1 до ℓ_i для $i = \overline{1,n}$. Теперь каждому элементу исходной дистрибутивной решетки поставим в соответствие набор чисел $(k_1, \ldots, k_n)$, где k_i для $i = \overline{1,n}$ — номер неприводимого элемента с i-ой цепи, участвующего в несократимом разложении элемента на неприводимые элементы ($k_i \leqslant \ell_i$). В случае, если ни один элемент с цепи C_i не участвует в несократимом разложении на неприводимые элементы данного элемента частично упорядоченного множества, положим $k_i = 0$. Таким образом, для данного покрытия цепями происходит вложение дистрибутивной решетки в n-мерный параллелепипед с целочисленными координатами:

$$P \to ([0,\ell_1] \cap \mathbb{Z}) \times ([0,\ell_2] \cap \mathbb{Z}) \times \cdots \times ([0,\ell_i] \cap \mathbb{Z}) \times \cdots \times ([0,\ell_n] \cap \mathbb{Z}).$$

Рассмотрим тривиальное покрытие множества неприводимых элементов, объявив каждый элемент самостоятельной цепью. В этом случае установится соответствие между всеми элементами исходного частично упорядоченного множества и наборами из нулей и единиц длины 4:

$$\begin{aligned} a &\longrightarrow (0,0,0,0) \\ b &\longrightarrow (1,0,0,0) \\ c &\longrightarrow (1,1,0,0) \\ d &\longrightarrow (1,0,1,0) \\ e &\longrightarrow (1,1,1,0) \\ f &\longrightarrow (1,1,1,1) \end{aligned}$$

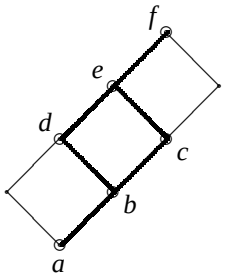
Это соответствие проинтерпретируем как вложение исходной дистрибутивной решетки в четырехмерный единичный куб $\mathbb{B}^4$:



Рассмотрим другое упорядоченное покрытие цепями, число которых равно ширине решетки. Пусть $C_1 = (b, c, f)$, $C_2 = (d)$. В этом случае устанавливается соответствие между элементами решетки и наборами длины 2 с целочисленными координатами, первая из которых меняется в диапазоне от 0 до 3, а вторая — от 0 до 1:

$$\begin{aligned} a &\longrightarrow (0,0) \\ b &\longrightarrow (1,0) \\ c &\longrightarrow (2,0) \\ d &\longrightarrow (1,1) \\ e &\longrightarrow (2,1) \\ f &\longrightarrow (3,1) \end{aligned}$$

Это соответствие проинтерпретируем как вложение дистрибутивной решетки в двумерный параллелепипед с целочисленными координатами $[0,3] \times [0,1]$:



Следующий интересующий нас вопрос — это кодирование дистрибутивных решеток. В задачах часто бывает удобно работать не с самой дистрибутивной решеткой, а с некоторой ее кодировкой, обладающей наименьшей избыточностью и, в то же время, однозначной. Ниже строится один из наиболее популярных способов кодировать дистрибутивные решетки.

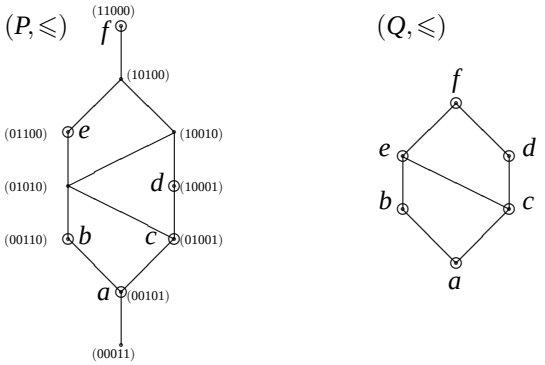
Пусть $(P,\leqslant)$ — дистрибутивная решетка. Выделим из нее множество всех неприводимых элементов Q и определим новое частично упорядоченное множество $(Q,\leqslant)$, где отношение частичного порядка то же, что и в исходной решетке. Каждому $a \in P$ однозначным образом ставится в соответствие подмножество из Q, являющееся его разложением. Отметим, что это подмножество обязательно является антицепью. Нулю поставим в соответствие пустую антицепь. Каждой такой антицепи S поставим в соответствие ее замыкание вниз $S_- = \{a \in Q \mid \exists a' \in S : a \leqslant a'\}$. Введем на Q антимонотонную булеву функцию f:

$$f(q) = \begin{cases} 1, & x \in S_-, \\ 0, & \text{иначе.} \end{cases}$$

При этом сама антицепь S окажется для f множеством верхних единиц. Множество S_- называется *идеалом*. В связи с тем, что все вышевведенные соответствия оказываются изоморфизмами, можно утверждать, что *дистрибутивная решетка изоморфна множеству идеалов своих неприводимых элементов*. Покроем Q упорядоченным набором цепей $C_1,\ldots,C_n$. Это можно сделать множеством способов, при этом количество цепей меняется от ширины Q до мощности Q. Относительно антимонотонной булевой функции f каждая цепь разбивается на два куска: нижний кусок погружен во множество единиц, а верхний — во множество нулей (какие-то из кусков вполне могут оказаться пустыми). В цепи C_i выберем наибольший элемент, погруженный в единицу — x_i (снова считаем, что все элементы цепи пронумерованы от единицы до длины цепи; если такового не оказалось, полагаем номер верхней единицы нулем). В этом случае *кодировкой решетки* назовем набор $x_1,\ldots,x_i,\ldots,x_n$.

Если покрывать решетку цепями длины единица, то будет получено ее вложение в соответствующий единичный n-мерный куб. Если брать покрытие меньшим числом цепей, то размерность параллелепипеда падает, однако растет число возможных значений координат.

Рассмотрим в качестве примера $\left(\mathbb{B}_2^5,\leqslant\right)$.



Неприводимыми в этой решетке являются элементы a,b,c,d,e,f, их частичный порядок указан на соответствующей диаграмме Хассе. Несократимые разложения элементов P на неприводимые элементы выглядят следующим образом:

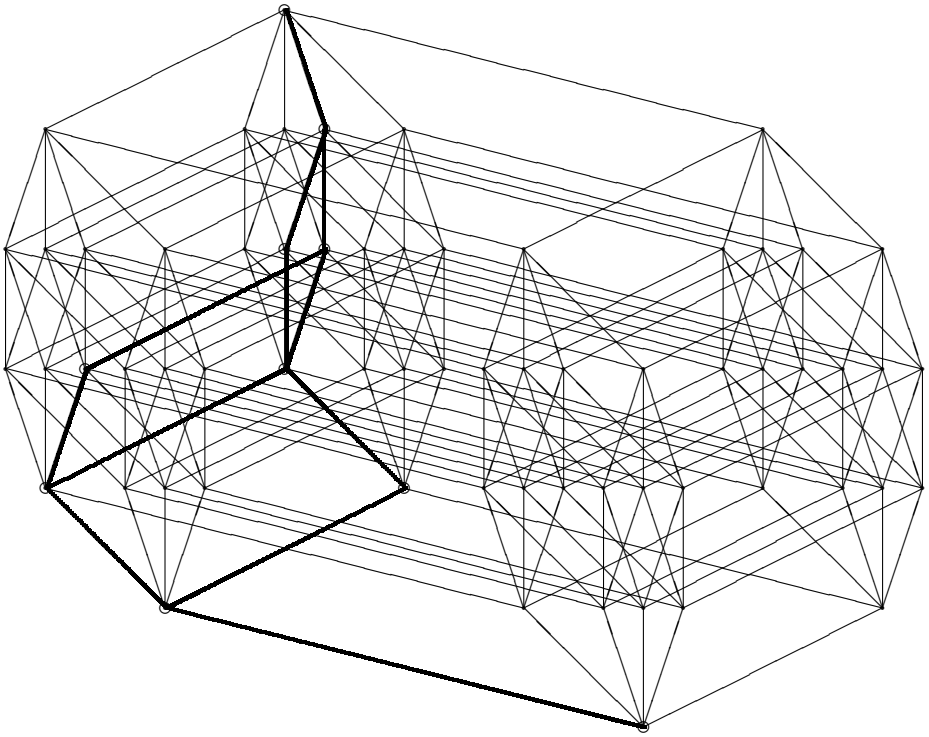
$$\begin{aligned}
(00011) &= \varnothing,\\
(00101) &= a,\\
(00110) &= b,\\
(01001) &= c,\\
(01010) &= b \vee c,\\
(10001) &= d,\\
(01100) &= e,\\
(10010) &= b \vee d,\\
(10100) &= e \vee d,\\
(11000) &= f.
\end{aligned}$$

В первый раз покроем Q цепями длины 1. Ниже указаны полученные кодировки.

$$\begin{aligned}
(00011) &\longrightarrow (0,0,0,0,0,0),\\
(00101) &\longrightarrow (1,0,0,0,0,0),\\
(00110) &\longrightarrow (1,1,0,0,0,0),\\
(01001) &\longrightarrow (1,0,1,0,0,0),
\end{aligned}$$

$$
\begin{aligned}
(01010) &\longrightarrow (1,1,1,0,0,0)\,,\\
(10001) &\longrightarrow (1,0,1,1,0,0)\,,\\
(01100) &\longrightarrow (1,1,1,0,1,0)\,,\\
(10010) &\longrightarrow (1,1,1,1,0,0)\,,\\
(10100) &\longrightarrow (1,1,1,1,1,0)\,,\\
(11000) &\longrightarrow (1,1,1,1,1,1)\,.
\end{aligned}
$$

Проинтерпретируем полученный результат как вложение $\mathbb{B}_2^5$ в шестимерный единичный куб (чтобы не загромождать и без того сложный рисунок мы опускаем кодировки элементов, предполагая, что вершины куба расположены по ярусам, при этом на i-ом ярусе снизу (отсчет начинается с нуля) расположены вершины с i единицами, упорядоченные согласно индуктивному построению).

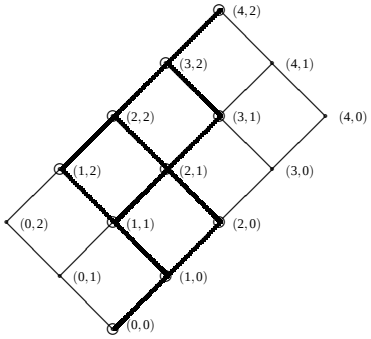


Рассмотрим другое упорядоченное покрытие цепями: на этот раз, опираясь на теорему Дилуорса, покроем решетку числом цепей, равным ее ширине. Пусть $C_1 = (a,b,e,f)$, $C_2 = (c,d)$. В этом случае вершины получат следующие кодировки:

$$
\begin{aligned}
(00011) &\longrightarrow (0,0)\,,\\
(00101) &\longrightarrow (1,0)\,,\\
(00110) &\longrightarrow (2,0)\,,\\
(01001) &\longrightarrow (1,1)\,,\\
(01010) &\longrightarrow (2,1)\,,\\
(10001) &\longrightarrow (1,2)\,,\\
(01100) &\longrightarrow (3,1)\,,\\
(10010) &\longrightarrow (2,2)\,,\\
(10100) &\longrightarrow (3,2)\,,\\
(11000) &\longrightarrow (4,2)\,.
\end{aligned}
$$

Такое отображение также имеет геометрическую интерпретацию: оно соответствует вложению указанной решетки в

двумерный параллелепипед с целочисленными координатами, лежащими в пределах $[0,4]\times[0,2]$.



Обычно двумерный параллелепипед такого вида называется *прямоугольной решеткой* и обозначается $L(4,2)$

Примеры.

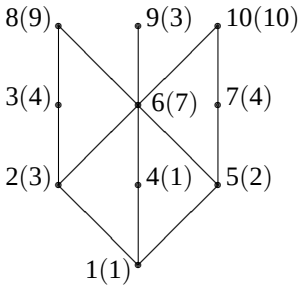
1. Доказать равенство $\sum\limits_{k\geqslant 0}\eta^k(x,y)=(2\delta-\zeta)^{-1}(x,y)$.

   □ *Решение.* Используя известные свойства сумм, легко преобразовать левую часть к правой:

   $$\sum_{k\geqslant 0}\eta^k(x,y)=\sum_{k\geqslant 0}(\zeta-\delta)^k(x,y)=(\delta-(\zeta-\delta))^{-1}(x,y)=(2\delta-\zeta)^{-1}(x,y).$$

   ■

2. На частичном порядке, представленном на диаграмме Хассе, ввести монотонную нумерацию, в ней найти матрицы дзета-функции и функции Мебиуса, а также определить функцию $\mathscr{F}$, если в скобках указаны значения суммирующей функции.



   □ *Решение.* Непосредственно по определению выписывается матрица дзета-функции:

   $$\zeta=\begin{pmatrix}1&1&1&1&1&1&1&1&1&1\\0&1&1&0&0&1&0&1&0&0\\0&0&1&0&0&0&0&1&0&0\\0&0&0&1&0&1&0&1&1&1\\0&0&0&0&1&1&1&1&1&1\\0&0&0&0&0&1&0&1&1&1\\0&0&0&0&0&0&1&0&0&1\\0&0&0&0&0&0&0&1&0&0\\0&0&0&0&0&0&0&0&1&0\\0&0&0&0&0&0&0&0&0&1\end{pmatrix}$$

   Из определяющего функцию Мебиуса свойства, подлежащего доказательству в пункте 2а упражнения 2, находим матрицу функции Мебиуса:

   $$\mu=\begin{pmatrix}1&-1&0&-1&-1&2&0&0&0&0\\0&1&-1&0&0&-1&0&1&0&0\\0&0&1&0&0&0&0&-1&0&0\\0&0&0&1&0&-1&0&0&0&0\\0&0&0&0&1&-1&-1&0&0&1\\0&0&0&0&0&1&0&-1&-1&-1\\0&0&0&0&0&0&1&0&0&-1\\0&0&0&0&0&0&0&1&0&0\\0&0&0&0&0&0&0&0&1&0\\0&0&0&0&0&0&0&0&0&1\end{pmatrix}$$

Вектор суммирующей функции равен (в данной монотонной нумерации)

$$S_{\mathscr{F}} = \begin{pmatrix} 1 & 3 & 4 & 1 & 2 & 7 & 4 & 9 & 3 & 10 \end{pmatrix}$$

Отсюда, используя обращение Мебиуса

$$\mathscr{F}(x) = \sum_{y \leqslant x} S_{\mathscr{F}}(y)\, \mu(y,x),$$

или, что то же самое, вектор функции $\mathscr{F}(x)$ равен произведению вектор-строки на матрицу

$$\mathscr{F} = S_{\mathscr{F}} \cdot \mu.$$

Выполнив необходимые вычисления, получаем, что вектор функции $\mathscr{F}(x)$ равен

$$\mathscr{F} = \begin{pmatrix} 1 & 2 & 1 & 0 & 1 & 3 & 2 & 1 & -4 & 1 \end{pmatrix}.$$

■

Упражнения.

1. Доказать, что для любой функции алгебры инцидентности справедливо соотношение
$$f^k(x,y) = \sum_{x \leqslant z_1 \leqslant z_2 \leqslant \cdots \leqslant z_k \leqslant y} f(x,z_1) \cdot f(z_1,z_2) \cdots f(z_k,y).$$
2. Доказать следующие равенства:
   (a) $\sum\limits_{x \leqslant z \leqslant y} \mu(x,z) = \sum\limits_{x \leqslant z \leqslant y} \mu(z,y) = \delta(x,y)$,
   (b) $\sum\limits_{k \geqslant 0} \kappa^k(x,y) = (2\delta - \lambda)^{-1}(x,y)$.
3. Обосновать следующие утверждения:
   (a) $\eta^k(x,y) = \sharp\{(x,y)\text{-цепи длины ровно } k\}$,
   (b) $\kappa^k(x,y) = \sharp\{\text{максимальные } (x,y)\text{-цепи длины ровно } k\}$,
   (c) $\zeta^k(x,y) = \sharp\{(x,y)\text{-цепи длины, не превосходящей } k\}$,
   (d) $\lambda^k(x,y) = \sharp\{\text{максимальные } (x,y)\text{-цепи длины, не превосходящей } k\}$.
4. Найти функцию Мебиуса для единичного n-мерного куба.
5. Доказать, что в частично упорядоченном по делимости множестве натуральных чисел функцией Мебиуса является
$$\mu(n) = \begin{cases} 1, & n = 1, \\ (-1)^s, & n = p_1 \cdots p_s \text{ — свободно от квадратов}, \\ 0, & \text{иначе}. \end{cases}$$
   Использовано следующее обозначение: $\mu(m,n) = \mu\left(1, \frac{n}{m}\right)$; $\quad \mu(1,n) = \mu(n)$.
6. Доказать, что свойства 6a и 6b эквивалентны и для определения дистрибутивности достаточно любого одного из них.

Глава 2

Конечнозначные логики

2.1 Функции конечнозначной логики

Определения и примеры. Множество $\mathfrak{U} = \{u_1, u_2, \ldots, u_\ell, \ldots\}$ назовем *алфавитом переменных*. Элементы этого множества называются соответственно *переменными*. При этом считается, что переменные с различными индексами различны (то есть могут принимать различные значения независимо друг от друга).

Определяется множество $E_k = \{0, 1, \ldots, k-1\}$ и рассматриваются функции вида $f : E_k^n \to E_k$. Функция от n различных переменных обозначается $f(u_{i_1}, \ldots, u_{i_n})$, при этом считается, что $j \neq s \Rightarrow u_{i_j} \neq u_{i_s}$. Такие функции называются *функциями k-значной логики*. В дальнейшем используются следующие метаобозначения: $f(x, y, \ldots, z)$ — при этом считается, что различным буквам соответствуют различные переменные, $f(x_1, \ldots, x_n)$ — при этом аналогично считается, что буквам с различными индексами соответствуют различные переменные и $f(\tilde{x}^n)$, что является альтернативным обозначением второго обозначения.

Множество всех функций k-значной логики обозначается P_k. Множество всех функций k- значной логики, зависящих от n переменных обозначается $P_k^{\langle n \rangle}$. Очевидно, $\left|P_k^{\langle n \rangle}\right| = k^{k^n}$. В дальнейшем левая часть предыдущего равенства будет записываться в несколько ином виде: $|P_k|^{\langle n \rangle}$. Доказывается это равенство при помощи *табличного задания функции k-значной логики*:

	x_1	…	x_{n-1}	x_n	$f(x_1, \ldots, x_{n-1}, x_n)$
k^n	0	…	0	0	← любое значение
	0	…	0	1	← любое значение
	…	…	…	…	…
	$k-1$	…	$k-1$	$k-1$	← любое значение

Упорядочив лексикографически в левой части таблицы все наборы длины n из E_k, легко видеть, что всего их k^n. Далее, каждому из наборов ставится в соответствие произвольное значение также из E_k. Это, в свою очередь можно сделать k^{k^n} различными способами.

Изучение функций k-значной логики существенно затрудняется тем, что с возрастанием числа переменных их количество растет заметно быстрее, чем, скажем, число функций алгебры логики. Так, например, число функций трехзначной логики двух переменных равно 3^9, что больше, чем 19000, в то время, как число функций алгебры логики того же числа переменных равно 16. Возникает вопрос о задании функции k-значной логики. Векторное задание, которое очень удобно для функции алгебры логики, представляется неприемлемым, так как длина вектора быстро растет. Для функций одного переменного наиболее часто используется представление в виде *подстановки*:

$$S(x) = \begin{pmatrix} 0 & 1 & \ldots & k-1 \\ a_0 & a_1 & \ldots & a_{k-1} \end{pmatrix}.$$

Напомним, что элементы нижней строчки в подстановке могут повторяться. Если же все элементы нижней строчки различны, то подстановка превращается в *перестановку*. Для функций двух переменных используется задание в виде двумерной таблицы:

x \ y	0	1	…	$k-1$
0			⋮	
1			⋮	
⋮	…	…	$f(i,j)$	
$k-1$				

Следующие функции называются *элементарными* функциями k-значной логики:

- *Константы* $0, 1, \ldots, k-1$ не имеют существенных переменных. Формально константу 0 можно задать в виде подстановки

$$0(x) = \begin{pmatrix} 0 & 1 & \ldots & k-1 \\ 0 & 0 & \ldots & 0 \end{pmatrix}.$$

- Функции, существенно зависящие от одной переменной: Обобщение отрицания алгебры логики — *отрицание Поста*
$$\overline{x} = \begin{pmatrix} 0 & 1 & \dots & k-2 & k-1 \\ 1 & 2 & \dots & k-1 & 0 \end{pmatrix} = x+1 \pmod k.$$
Оно обладает простыми свойствами: $\overline{\overline{x}} = x+2 \pmod k$, и вообще для любого натурального l отрицание Поста, примененное l раз к x, дает $x+l \pmod k$. Обратим внимание, что сложение *двух различных переменных* таким образом не определяется, так как мы определили лишь сложение с константой.

- Другим обобщением отрицания в P_2 является *отрицание Лукасевича* (в некоторых источниках — *Лукашевича*). Оно определяется как
$$\sim x = \begin{pmatrix} 0 & 1 & 2 & \dots & k-1 \\ k-1 & k-2 & k-3 & \dots & 0 \end{pmatrix} = (k-1)-x.$$
Для отрицания Лукасевича справедливо правило снятия двойного отрицания, как и у отрицания в P_2: $\sim(\sim x) = x$

- Функция $-x = \begin{pmatrix} 0 & 1 & 2 & \dots & k-1 \\ 0 & k-1 & k-2 & \dots & 1 \end{pmatrix}$, обладающая тем свойством, что если ее добавить к x, то получится константа 0. Векторное задание этой функции имеет вид $-x = \begin{pmatrix} 0 & k-1 & \dots & 1 \end{pmatrix}$. С другой стороны: $x = \begin{pmatrix} 0 & 1 & \dots & k-1 \end{pmatrix}, \sim x = \begin{pmatrix} k-1 & k-2 & \dots & 1 \end{pmatrix}$,
$$\overline{(\sim x)} = \begin{pmatrix} 0 & k-1 & \dots & 1 \end{pmatrix},$$
то есть $x = -\overline{(\sim x)}$.

- Семейство функций, являющихся также обобщениями отрицания
$$J_i(x) = \begin{cases} k-1 & x = i, \\ 0 & x \neq i, \end{cases} \qquad 0 \leqslant i \leqslant k-1$$
и
$$j_i(x) = \begin{cases} 1 & x = i, \\ 0 & x \neq i, \end{cases} \qquad 0 \leqslant i \leqslant k-1.$$

- *Разностью* переменной x и константы i назовем функцию $x-i = x+(k-i)$, иначе говоря, $(k-i)$ раз примененное отрицание Поста.

- Обобщение двухместной дизъюнкции — максимум: $\max(x,y)$. Эта функция, очевидно, коммутативна, а также ассоциативна: $\max(x,\max(y,z)) = \max(\max(x,y),z)$, что позволяется ввести по индукции n-местный максимум: $\max(x_1,\dots,x_{n-1},x_n) = \max(\max(x_1,\dots,x_{n-1}),x_n)$.

- Обобщение двухместной конъюнкции: $\min(x,y)$. Минимум обладает такими же свойствами, что и максимум. В частности, определяется $\min(x_1,\dots,x_n)$. Для минимума и максимума справедливы обобщения правил де Моргана:
$$\sim\max(\sim x,\sim y) = \min(x,y), \sim\min(\sim x,\sim y) = \max(x,y). \tag{2.1}$$

- Сложение по модулю k: $x+y \pmod k$. Эта операция коммутативна и ассоциативна. Можно ввести разность: $x+\underbrace{y+y+\dots+y}_{k-1} = x-y$

- Еще одним обобщением конъюнкции может служить произведение по модулю k: $x\cdot y \pmod k$.

- Усеченная разность
$$x \dot{-} y = \begin{cases} x-y & x \geqslant y, \\ 0 & x < y. \end{cases}$$
Таблица усеченной разности при $k=3$ имеет следующий вид:

x \ y	0	1	2
0	0	0	0
1	1	0	0
2	2	1	0

Очевидно, что из усеченной разности легко получить минимум: $\min(x,y) = x \dot{-} (x \dot{-} y)$. Действительно, если $x < y$, то выражение в скобке равно нулю и вся формула реализует функцию x. Если же $x \geqslant y$, то выражение в скобке реализует $x-y$, что заведомо меньше x, то есть вся формула реализует $x-(x-y) \equiv y$.

- Импликация $x \supset y = \sim (x \dot{-} y)$, которую можно записать также

$$x \supset y = \begin{cases} k-1-x+y & x \geqslant y, \\ k-1 & x < y. \end{cases}$$

Реализация функций формулами. Понятия формулы и ее глубины, а также функции, сопоставляющейся формуле над множеством функций определяются аналогично P_2.

Определение 2.1.1. Пусть $\mathscr{A}$ — некоторое множество функций из P_k.

1. Для любой функции $f \in \mathscr{A}$ справедливо: f является формулой глубины 1 над $\mathscr{A}$.
2. Если $\mathfrak{F}_1, \ldots, \mathfrak{F}_n$ — формулы над $\mathscr{A}$ или символы переменных из $\mathfrak{U}$ и $f(\tilde{x}^n) \in \mathscr{A}$, причем наибольшая глубина формулы среди $\mathfrak{F}_1, \ldots, \mathfrak{F}_n$ равна k, то $f(\mathfrak{F}_1, \ldots, \mathfrak{F}_n)$ — также формула над $\mathscr{A}$, глубина которой равна $k+1$.
3. Те и только те объекты называются формулами над $\mathscr{A}$, которые могут быть определены согласно пунктам 1 и 2 данного определения.

Дадим определение *реализации функций формулой*.

Определение 2.1.2. Пусть $\mathscr{A}$ — некоторое множество функций из P_k.

1. Если функция $f \in \mathscr{A}$, то формуле f сопоставляется функция $f \in \mathscr{A}$, иными словами, формула f реализует функцию f: $f \to f \in \mathscr{A}$.
2. Если $\mathfrak{F}_1 \to f_1, \ldots, \mathfrak{F}_n \to f_n$ и $f \in \mathscr{A}$, то формуле $f(\mathfrak{F}_1, \ldots, \mathfrak{F}_n)$ сопоставляется функция $f(f_1, \ldots, f_n)$, иными словами, $f(f_1, \ldots, f_n)$ реализуется формулой $f(\mathfrak{F}_1, \ldots, \mathfrak{F}_n)$.
3. Функции сопоставляются всем формулам, описанным в пунктах 1 и 2, и только им.

Первая и вторая формы. Система функций

$$\{0, 1, \ldots, k-1, J_0(x), \ldots, J_{k-1}(x), \min(x,y), \max(x,y)\}$$

называется системой *Россера-Туркетта*.

Теорема 2.1. *Система Россера-Туркетта полна в P_k.*

□ *Док-во.* Обозначим систему Россера-Туркетта символом $\mathscr{A}$. Так как $0 \in \mathscr{A}$, будем рассматривать функции $f(\tilde{x}^n) \not\equiv 0$. В этом случае справедливо представление

$$f(\tilde{x}^n) = \max_{\substack{(\alpha_1,\ldots,\alpha_n) \in E_k^n \\ f(\alpha_1,\ldots,\alpha_n) \neq 0}} (\min(J_{\alpha_1}(x_1), \ldots, J_{\alpha_n}(x_n), f(\alpha_1, \ldots, \alpha_n))). \tag{2.2}$$

Действительно, на любом наборе $\tilde{\alpha}^n \in E_k^n$ все минимумы обратятся в ноль, за исключением одного, который и примет значение, равное значению функции на этом наборе. Максимум из нулей и одного значения функции равен этому самому значению. ■

Реализация функции над системой Россера-Туркетта называется *первой формой* этой функции. Так, например, первая форма усеченной разности при $k = 3$ имеет следующий вид:

$$\max(\min(J_1(x), J_0(y), 1), \min(J_2(x), J_0(y), 2), \min(J_2(x), J_1(y), 1))$$

Отметим, что система функций

$$\{0, 1, \ldots, k-1, J_0(x), \ldots, J_{k-1}(x), x+y, \min(x,y)\}$$

также полна в P_k. Это следует из того, что доказательство теоремы 2.1 не изменится, если заменить в 2.2 максимум на сумму по модулю k:

$$f(\tilde{x}^n) = \sum_{\substack{(\alpha_1,\ldots,\alpha_n) \in E_k^n \\ f(\alpha_1,\ldots,\alpha_n) \neq 0}} \min(J_{\alpha_1}(x_1), \ldots, J_{\alpha_n}(x_n), f(\alpha_1, \ldots, \alpha_n)) \pmod{k}.$$

В этом случае суммироваться будут все нули и одно значение функции, что, очевидно, то же самое.

Рассмотрим теперь систему

$$\{0, 1, \ldots, k-1, j_0(x), \ldots, j_{k-1}(x), x+y, x \cdot y\} \tag{2.3}$$

и докажем ее полноту:

Теорема 2.2. *Система 2.3 полна в P_k.*

□ *Док-во.* Обозначим систему 2.3 символом $\mathscr{B}$. Так как $0 \in \mathscr{B}$, будем рассматривать функции $f(\tilde{x}^n) \not\equiv 0$. В этом случае справедливо представление

$$f(\tilde{x}^n) = \sum_{\substack{(\alpha_1,\ldots,\alpha_n)\in E_k^n \\ f(\alpha_1,\ldots,\alpha_n)\neq 0}} f(\alpha_1,\ldots,\alpha_n)\cdot j_{\alpha_1}(x_1)\cdots j_{\alpha_n}(x_n) \pmod{k}. \tag{2.4}$$

Действительно, на любом наборе $(\alpha_1,\ldots,\alpha_n)$, если $\exists i : x_i \neq \alpha_i$, то все слагаемое обратится в ноль. Если же все $x_i = \alpha_i$, что встретится не более одного раза, то все слагаемое станет равным значению функции. Таким образом, правая часть суммы 2.4 на фиксированном наборе равна просто значению функции на этом же наборе. ■

Представление 2.4 функции k-значной логики принято называть ее *второй формой*. Так, при $k = 3$ вторая форма усеченной разности имеет вид:

$$j_1(x)\cdot j_0(y) + 2\cdot j_2(x)\cdot j_0(y) + j_2(x)\cdot j_1(y).$$

Операция замыкания, свойства замыкания, замкнутые классы. Пусть $\mathscr{A}$ — некоторое множество функций из P_k. Множество $[\mathscr{A}]$ всех функций, реализуемых формулами над $\mathscr{A}$, называется *замыканием* множества $\mathscr{A}$. Для операции замыкания очевидны следующие тривиальные тождества:

1. экстенсивность: $\mathscr{A} \subseteq [\mathscr{A}]$,
2. монотонность (изотонность): $\mathscr{A} \subseteq \mathscr{B} \Rightarrow [\mathscr{A}] \subseteq [\mathscr{B}]$ и
3. идемпотентность: $[\mathscr{A}] = [[\mathscr{A}]]$.

Если множество $\mathscr{A}$ совпадает со своим замыканием: ($\mathscr{A} = [\mathscr{A}]$), то $\mathscr{A}$ называется *замкнутым классом*.

Пусть $\mathscr{A}, \mathscr{B} \subseteq P_k$. Тогда если $\mathscr{B} = [\mathscr{B}]$, $\mathscr{A} \subseteq \mathscr{B}$ и $[\mathscr{A}] = \mathscr{B}$, то говорят, что система функций $\mathscr{A}$ — *полная* в системе $\mathscr{B}$. Аналогично, если $\mathscr{A}$ — минимальная (по удалению) полная система в $\mathscr{B}$, то $\mathscr{A}$ называется *базисом*.

Очевидно, что замкнутые классы существуют. Тривиальными примерами замкнутых классов являются все P_k и пустое множество: $[P_k] = P_k$, $[\varnothing] = \varnothing$. Рассмотрим теперь некоторые нетривиальные замкнутые классы.

Определение 2.1.3. Пусть $\varnothing \subsetneq \mathscr{E} \subsetneq E_k$. $f(\tilde{x}^n) \in P_k$ *сохраняет множество* $\mathscr{E}$, если выполнена следующая импликация: $\alpha_1,\ldots,\alpha_n \in \mathscr{E} \Rightarrow f(\alpha_1,\ldots,\alpha_n) \in \mathscr{E}$. *Классом функций, сохраняющих множество* $\mathscr{E}$ называется $T(\mathscr{E})$.

Лемма 2.1.1. *Для любого множества $\mathscr{E} \subseteq E_k$ класс $T(\mathscr{E})$ замкнут.*

□ *Док-во.* Поскольку тождественная функция сохраняет любое множество, для доказательства замкнутости достаточно доказать, что суперпозиция функций, сохраняющих $\mathscr{E}$, также сохраняет $\mathscr{E}$. Пусть функции $f_1(x_1,\ldots,x_n),\ldots,f_m(x_1,\ldots,x_n) \in T(\mathscr{E})$ (без ограничения общности будем считать, что они зависят от одних и тех же переменных). Пусть также $f(x_1,\ldots,x_m) \in T(\mathscr{E})$. Для любого набора $\widetilde{\alpha} = (\alpha_1,\ldots,\alpha_n) \in \mathscr{E}$ значения функций $f_1(\alpha_1,\ldots,\alpha_n) = \beta_1 \in \mathscr{E},\ldots,f_m(\alpha_1,\ldots,\alpha_n) = \beta_m \in \mathscr{E}$. Но тогда и $f(\beta_1,\ldots,\beta_m) \in \mathscr{E}$. ■

Описанное семейство замкнутых классов обладает следующими свойствами.

Утверждение 2.1.1. *$T(\mathscr{E}) = P_k$, $T(\mathscr{E}) = P_k$, а также $\varnothing \subsetneq \mathscr{E} \subsetneq E_k \Rightarrow T(\mathscr{E})$ — непустое множество, не совпадающее с P_k.*

□ *Док-во.* Первое свойство очевидно, второе принимается по договоренности, а третье следует из того, что, например, отрицание Поста не сохраняет никакое непустое собственное подмножество E_k. ■

Функции максимума и минимума, очевидно, сохраняют любое $\mathscr{E} \subseteq E_k$.

Утверждение 2.1.2. *Всего в P_k существует $2^k - 2$ классов, сохраняющих непустые собственные множества, причем все они попарно различны и ни один из них не содержится в другом.*

□ *Док-во.* Действительно, пусть $\mathscr{E}_1 \neq \mathscr{E}_2$. Возможны 2 варианта:

1. Существуют такие a и b, что $a \in \mathscr{E}_1 \setminus \mathscr{E}_2$ и $b \in \mathscr{E}_2 \setminus \mathscr{E}_1$, то есть $\mathscr{E}_1 \not\subseteq \mathscr{E}_2$ и $\mathscr{E}_2 \not\subseteq \mathscr{E}_1$. В этом случае, очевидно, для функций констант выполняется $a \notin T(\mathscr{E}_2)$, $b \notin T(\mathscr{E})$, то есть эти классы не совпадают, и ни один из них не содержится во втором.
2. $\mathscr{E}_2 \subsetneq \mathscr{E}_1$, то есть существует такое a, что $a \in \mathscr{E}_1 \setminus \mathscr{E}_2$. В этом случае классы $T(\mathscr{E}_1)$ и $T(\mathscr{E}_2)$ различны, потому что константа a содержится в первом из них и не содержится во втором. Покажем, что во втором классе существует функция, не содержащаяся в первом. Поскольку $\mathscr{E}_2$ не пусто, существует $c \in \mathscr{E}_2$. Также, поскольку $\mathscr{E}_1 \neq E_k$, существует точка $d \in E_k \setminus \mathscr{E}_1$. Класс $T(\mathscr{E}_2)$, очевидно, содержит функцию такого вида: $f(x) = \begin{cases} c & \text{если } x \in \mathscr{E}_2, \\ d & \text{в противном случае.} \end{cases}$ Функция $f(x)$ по построению содержится в классе $T(\mathscr{E}_2)$, но, очевидно, не содержится в классе $T(\mathscr{E}_1)$, так как $f(a) = d \notin \mathscr{E}_2$.

Осталось только подсчитать число этих классов. Так как все они различны, то их число равно числу непустых собственных подмножеств E_k, то есть $2^k - 2$. ■

Определение 2.1.4. Множество функций $\mathscr{A}$ называется *предполным классом в* P_k, если оно само является замкнутым и неполным в P_k классом, но для любой функции f, не содержащейся в $\mathscr{A}$ выполняется $[\mathscr{A} \cup \{f\}] = P_k$.

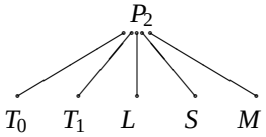
Утверждение 2.1.3. *Для любого непустого подмножества* $\mathscr{E} \subsetneq E_k$ *класс* $T(\mathscr{E})$ *является предполным в* P_k.

□ *Док-во.* Пусть $\mathscr{E}$ — любое собственное непустое подмножество E_k. Для произвольной функции $f \notin T(\mathscr{E})$ рассмотрим замыкание $[T(\mathscr{E}) \cup \{f\}]$. Для f справедливо $f \notin T(\mathscr{E}) \Rightarrow \exists \widetilde{\alpha} \in \mathscr{E}^n : f(\widetilde{\alpha}) = f(\alpha_1, \alpha_2, \ldots, \alpha_n) = b \notin \mathscr{E}$. С другой стороны, очевидно, классу $T(\mathscr{E})$ принадлежит такая функция (для $a \in \mathscr{E}$):

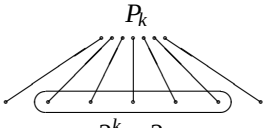
$$g(x,y,z) = \begin{cases} a & z \in \mathscr{E}, \\ V_k(x,y) & z \notin \mathscr{E}. \end{cases}$$

Таким образом, суперпозиция функций из объединения $g(x, y, f(\widetilde{\alpha}))$, реализует функцию Вебба. ■

Утверждение 2.1.3 показывает, что все замкнутые классы, сохраняющие непустые собственные подмножества E_k, являются предполными. Если вспомнить P_2, то там существовало ровно пять предполных классов: два класса сохраняющих константы, классы линейных, самодвойственных и монотонных функций и их структура условно выглядела так:



Аналогичная ситуация наблюдается и в P_k:



, (2.5)

где выделены как раз те $2^k - 2$ предполных классов.

Число функций, зависящих от n переменных в классе $T(\mathscr{E})$ при $|\mathscr{E}| = m$ для $1 \leqslant m < n$, очевидно, равно $m^{m^n} k^{k^n - m^n}$. Действительно, всего наборов длины n, составленных из символов $\mathscr{E}$, — m^n. Им могут соответствовать лишь значения из m-элементного множества. Остальным же $k^n - m^n$ наборам могут соответствовать любое из k значений. Таким образом получено, что

$$|T(\mathscr{E})|^{\langle n \rangle} = m^{m^n} k^{k^n - m^n}.$$

Рассмотрим теперь другое семейство замкнутых классов:

Определение 2.1.5. Пусть $D_1, D_2, \ldots, D_s$ — попарно непересекающиеся непустые множества (*блоки*), в объединении дающие все E_k. В этом случае представление $E_k = D_1 \cup D_2 \cup \ldots \cup D_s$ называется *разбиением* E_k.

Случаи $s = 1$ и $s = k$ порождают *тривиальные разбиения* E_k и $\{0\} \cup \{1\} \cup \ldots \cup \{k-1\}$ соответственно. Все остальные разбиения называются *нетривиальными*. По заданному разбиению D можно на множествах E_k и E_k^n ввести отношение эквивалентности следующим образом: $\forall a, b \in E_k : a \sim b \pmod{D}$ (a и b эквивалентны по разбиению D) тогда и только тогда, когда они в этом разбиении попадают в один блок; $\widetilde{\alpha} \sim \widetilde{\beta} \pmod{D} \Leftrightarrow \forall i = \overline{1,n} \Rightarrow \alpha_i \sim \beta_i \pmod{D}$, если $|\widetilde{\alpha}| = \left|\widetilde{\beta}\right| = n$.

Определение 2.1.6. Функция $f(\widetilde{x}^n)$ от n переменных *сохраняет разбиение* D, если

$$\widetilde{\alpha} \sim \widetilde{\beta} \pmod{D} \Rightarrow f(\widetilde{\alpha}) \sim f\left(\widetilde{\beta}\right) \pmod{D}.$$

Классом функций, сохраняющих разбиение D называется множество всех функций, сохраняющих заданное разбиение D.

Также, как и в случае сохранения множества, выделяются вырожденные случаи. Тривиальными называются разбиение в виде одного блока $U(P_k)$ и разбиение в виде k блоков

$$U(\{0\} \cup \{1\} \cup \ldots \cup \{k-1\}).$$

Все функции сохраняют тривиальные разбиения, иными словами, классы всех функций, сохраняющих тривиальные разбиения, являются полными в P_k, поэтому имеет смысл рассматривать эти классы только при $k \geqslant 3$. Любая тождественная функция сохраняет любое разбиение. Отрицание Поста не сохраняет никакое нетривиальное разбиение. Из этого следует, что для любого разбиения класс сохраняющих его функций не пуст. Справедливо более сильное утверждение, а именно, что $\varnothing \subsetneq U(D) \subsetneq P_k$ для любого нетривиального разбиения D. Действительно, если есть хотя бы два блока, один из которых содержит хотя бы два элемента a и b, а второй содержит хотя бы один элемент c, то достаточно в качестве примера функции, не сохраняющей данное разбиение, рассмотреть отображение a в a, b в c, а на остальных элементах — произвольно.

Лемма 2.1.2. *Для любого разбиения класс функций, его сохраняющих, замкнут.*

□ *Док-во.* Поскольку тождественная функция сохраняет любое разбиение, для доказательства замкнутости достаточно доказать, что суперпозиция сохраняющих разбиение функций также сохраняет разбиение. Рассмотрим произвольное разбиение D и пусть $f_1(\tilde{x}^n), \ldots, f_m(\tilde{x}^n), f(\tilde{x}^m) \in U(D)$. Докажем, что $F(\tilde{x}^n) = f(f_1(\tilde{x}^n), \ldots, f_m(\tilde{x}^n)) \in U(D)$. Рассмотрим для этого любые два эквивалентные по разбиению D набора $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_i, \ldots, \alpha_n)$ и $\tilde{\beta} = (\beta_1, \ldots, \beta_i, \ldots, \beta_n)$. Из $f_j(\tilde{x}^n) \in U(D)\ \forall j = \overline{1,m}$ следует, что $f_j(\tilde{\alpha}) \sim f_j\left(\tilde{\beta}\right) \pmod{D}\ \forall j = \overline{1,m}$, или, что то же самое,

$$(f_1(\tilde{\alpha}), f_2(\tilde{\alpha}), \ldots, f_i(\tilde{\alpha}), \ldots, f_m(\tilde{\alpha})) \sim \left(f_1\left(\tilde{\beta}\right), f_2\left(\tilde{\beta}\right), \ldots, f_i\left(\tilde{\beta}\right), \ldots, f_m\left(\tilde{\beta}\right)\right) \pmod{D}.$$

Из того, что $f(\tilde{x}^m) \in U(D)$, следует, что $f(f_1(\tilde{\alpha}), \ldots, f_m(\tilde{\alpha})) \sim f\left(f_1\left(\tilde{\beta}\right), \ldots, f_m\left(\tilde{\beta}\right)\right) \pmod{D}$, или, по-другому, $F(\tilde{\alpha}) \sim F\left(\tilde{\beta}\right) \pmod{D}$. ■

Два введенных выше замкнутых класса можно рассматривать как частные случаи *класса функций, сохраняющих предикат*.

Определение 2.1.7. *s-местным предикатом* называется функция k-значной логики $P(y_1, \ldots, y_s)$, принимающая только значения 0 или 1. Если на некотором наборе $\tilde{\alpha}$ предикат принимает значение, равное единице, то этот набор *удовлетворяет предикату*: $\tilde{\alpha} \in P$. Упорядоченная s-ка наборов удовлетворяет предикату P, если она удовлетворяет ему покомпонентно:

$$\begin{matrix} \tilde{\alpha}_1 = (\alpha_1^1, \ldots, \alpha_n^1) \\ \tilde{\alpha}_2 = (\alpha_1^2, \ldots, \alpha_n^2) \\ \cdots \\ \tilde{\alpha}_s = (\alpha_1^s, \ldots, \alpha_n^s) \end{matrix} \in P \Leftrightarrow \forall j = \overline{1,n} \Rightarrow (\alpha_j^1, \alpha_j^2, \ldots, \alpha_j^s) \in P$$

Рассматриваются только случаи $s \geqslant 1$. Предикаты, являющиеся тождественным нулем или тождественной единицей, называются *тривиальными*. В этом случае предикат существенно зависит от нуля переменных. В случае $s = 1$ предикат называется *характеристической функцией*. В случае $s = 2$ — *разбиением*.

Определение 2.1.8. *Функция $f(\tilde{x}^n)$ сохраняет предикат P*, если для любой упорядоченной s-ки наборов длины n $(\tilde{\alpha}_1, \ldots, \tilde{\alpha}_s)$ упорядоченная s-ка $(f(\tilde{\alpha}_1), \ldots, f(\tilde{\alpha}_s))$ также удовлетворяет предикату P. *Классом функций, сохраняющих предикат P*, называется множество $W(P)$ всех функций, сохраняющих предикат P.

Так как любой набор удовлетворяет предикату $P \equiv 1$, $W(P) = P_k$. Также, предикат, тождественно равный нулю, сохраняет любая функция. Очевидно, что класс, сохраняющий нетривиальный предикат не пуст и не совпадает со всем P_k, за некоторыми исключениями. Действительно, для любого нетривиального s-местного предиката существует упорядоченная s-ка, ему не удовлетворяющая. Тогда функцию, не сохраняющую предикат, определяем по следующему правилу: для некоторой упорядоченной s-ки различных наборов, удовлетворяющей предикату, ставим в соответствие упорядоченную s-ку, не удовлетворяющую предикату. Здесь существенно наличие s различных наборов, удовлетворяющих предикату. В противном случае, если предикат имеет следующий вид:

$$P(x_1, \ldots, x_s) = \begin{cases} 1 & x_{i_1} = x_{i_2} = \cdots = x_{i_l}\ 0 \leqslant l \leqslant s, \\ 0 & \text{иначе,} \end{cases},$$

то любая функция его сохраняет. Действительно, в этом случае из s наборов l должны быть равными. Но и значения любой функции на них будут равны. А поскольку на оставшихся $s - l$ наборах функция может принимать произвольные значения, любая функция такой предикат сохранит. С другой стороны, если потребовать, чтобы некоторые наборы были не просто равны друг другу, а еще и совпадали с вполне определенным фиксированным набором, то класс функций, сохраняющих такой предикат снова будет неполным.

Лемма 2.1.3. *Для любого предиката класс сохраняющих его функций замкнут.*

□ *Док-во.* Так как тождественная функция сохраняет любой предикат, для доказательства замкнутости этого класса достаточно доказать, что суперпозиция сохраняющих предикат функций также сохраняет предикат. Для этого рассмотрим функции

$$f_1(\tilde{x}^n), f_2(\tilde{x}^n), \ldots, f_m(\tilde{x}^n), f(z_1,\ldots,z_m) \in W(P)$$

для некоторого предиката s-местного предиката P и докажем, что суперпозиция

$$F(\tilde{x}^n) = f(f_1(\tilde{x}^n),\ldots,f_m(\tilde{x}^n)) \in W(P).$$

Предложим этой суперпозиции любой набор наборов $(\tilde{\alpha}_1,\tilde{\alpha}_2,\ldots,\tilde{\alpha}_j,\ldots,\tilde{\alpha}_s)$, сохраняющих предикат. Для каждого набора вычислим все f_l.

$$\begin{array}{lll}
\tilde{\alpha}_1 = (\alpha_1^1,\alpha_2^1,\ldots,\alpha_i^1,\ldots,\alpha_n^1) & (f_1(\tilde{\alpha}_1),f_2(\tilde{\alpha}_1),\ldots,f_i(\tilde{\alpha}_1),\ldots,f_m(\tilde{\alpha}_1)) & F(\tilde{\alpha}_1,) \\
\tilde{\alpha}_2 = (\alpha_1^2,\alpha_2^2,\ldots,\alpha_i^2,\ldots,\alpha_n^2) & (f_1(\tilde{\alpha}_2),f_2(\tilde{\alpha}_2),\ldots,f_i(\tilde{\alpha}_2),\ldots,f_m(\tilde{\alpha}_2)) & F(\tilde{\alpha}_2,) \\
\vdots & \vdots & \vdots \\
\tilde{\alpha}_j = \left(\alpha_1^j,\alpha_2^j,\ldots,\alpha_i^j,\ldots,\alpha_n^j\right) & (f_1(\tilde{\alpha}_j),f_2(\tilde{\alpha}_j),\ldots,f_i(\tilde{\alpha}_j),\ldots,f_m(\tilde{\alpha}_j)) & F(\tilde{\alpha}_j,) \\
\vdots & \vdots & \vdots \\
\tilde{\alpha}_s = (\alpha_1^s,\alpha_2^s,\ldots,\alpha_i^s,\ldots,\alpha_n^s) & (f_1(\tilde{\alpha}_s),f_2(\tilde{\alpha}_s),\ldots,f_i(\tilde{\alpha}_s),\ldots,f_m(\tilde{\alpha}_s)) & F(\tilde{\alpha}_s,)
\end{array}$$

Упорядоченная s-ка наборов, составленных из значений функций, очевидно, удовлетворяет предикату. Следовательно, и s-ка, составленная из значений суперпозиции также удовлетворяет предикату. ■

Предикаты могут описывать различные свойства функций. Можно легко, определив соответствующий предикат, предложить замкнутый класс монотонных функций: $P(x_1,x_2) = \begin{cases} 1 & x_1 \leqslant x_2, \\ 0 & x_1 > x_2. \end{cases}$ *Функцией, двойственной к* $f(x_1,\ldots,x_n)$, называется функций $f^*(x_1,\ldots,x_n) = \sim f(\sim x_1,\ldots,\sim x_n)$. Функция f называется *самодвойственной*, если $f = f^*$. Также можно описать замкнутый класс самодвойственных функций, определив соответствующий предикат: $P(x_1,x_2) = \begin{cases} 1 & x_1 = \sim x_2, \\ 0 & x_1 \neq \sim x_2. \end{cases}$ Несмотря на то, что предикаты являются достаточно мощным средством описания замкнутых классов, позже будет показано, что используя предикаты, нельзя описать *все* замкнутые классы.

Другими примерами замкнутых классов являются, например, класс линейных функций, класс функций, представимых полиномами **Pol**, класс функций, существенно зависящих не более, чем от одной переменной $P_k^{(1)}$. Эти классы не являются полными системами при любых значения k, за исключением второго, который является полной системой при любом простом k. Замыкание множества всех функций, зависящих от двух переменных, в свою очередь совпадает со всем P_k.

В заключение пункта приведем еще один пример замкнутого класса $T(\mathscr{E},s)$, $s = \overline{1,k}$. Фиксируются произвольные $\mathscr{E},A_0,A_1,A_2,\ldots,A_n \subseteq E_k$, $|A_i| = s$, $i = \overline{0,n}$, $\mathscr{E} \neq E_k$. Функция n переменных $f(x_1,\ldots,x_n) \in T(\mathscr{E},s)$ тогда и только тогда, когда $f(\mathscr{E}\cup A_1,\mathscr{E}\cup A_2,\ldots,\mathscr{E}\cup A_n) \in \mathscr{E}\cup A_0$. Этот класс также является неполным в нетривиальных случаях.

Полные системы, примеры полных систем. Пусть $\mathscr{A}$ — некоторое множество функций из P_k. Если $[\mathscr{A}] = P_k$, то говорят, что $\mathscr{A}$ образует *полную систему*. Минимальная (по удалению функций) полная система называется *базисом*. Полноту произвольной системы $\mathscr{B}$ будем доказывать сведением к заведомо полным системам, используя следующую схему:

$$\begin{cases} [\mathscr{A}] = P_k \\ \mathscr{A} \subseteq [\mathscr{B}] \end{cases} \Rightarrow [\mathscr{B}] = P_k.$$

Следующие системы являются полными в P_k при любом значении k:

1. система Россера-Туркетта (теорема 2.1);
2. $\{0,\ldots,k-1,j_0,\ldots,j_{k-1},+,\cdot\}$ (теорема 2.2);
3. система Поста (теорема 2.3);
4. $\{\bar{x},\min(x,y)\}$ (упражнение 1а);
5. $V_k(x,y)$ (следствие 2.1.1);
6. $\{1,k-1,x\dot{-}y\}$.

□ *Док-во.* Сведем эту систему к системе Поста. Минимум получается тривиально: $\min(x,y) = x\dot{-}(x\dot{-}y)$. Получим теперь все одноместные функции, в том числе и отрицание Поста. Реализуем для этого сначала все константы ($k-1$ и 1 уже есть):

$$k-2 = (k-1)\dot{-}1, \ldots, 3\dot{-}1 = 2, 1\dot{-}1 = 0.$$

Получим теперь все j_i:

$$j_0(x) = 1\dot{-}x;\ j_1(x) = ((2\dot{-}x)\dot{-}j_0(x))\dot{-}j_0(x);\ j_i(x) = j_0(x\dot{-}i)\dot{-}j_0(x\dot{-}(i-1)),\ i = \overline{1,k-1}.$$

Имея все j_i можно получить систему функций

$$g_{i,s}(x) = \begin{cases} s & x = i, \\ k-1 & x \neq i. \end{cases}$$

следующим образом:

$$g_{i,s}(x) = (\cdots((k-1)\underbrace{\dot{-}j_i(x))\dot{-}\cdots)\dot{-}}_{k-s-1 \text{ раз}} j_i(x).$$

Отсюда произвольную одноместную функцию строим по правилу

$$f(x) = \min\left(g_{0,f(0)}(x), \ldots, g_{l,f(l)}(x), \ldots, g_{k-1,f(k-1)}(x)\right).$$

Таким образом можно построить и отрицание Поста, следовательно, система полна. ■

7. $\{j_0(x), x+y\}$ при $k \geqslant 3$. Заметим, что при $k=2$ эта же система не полна, так как она целиком содержится в классе линейных функций ($j_0(x) = \bar{x}$, $x+y = x \oplus y$).

□ *Док-во.* Действительно, $\underbrace{x+x+\cdots+x}_{k \text{ раз}} = 0 \pmod{k}$, далее $j_0(0) = 1$; $x+1 = \bar{x}$, откуда получаются все константы и все $j_i(x)$. Отсюда можно получить систему функций $f_{l,s} = \underbrace{j_l(x)+\cdots+j_l(x)}_{s \text{ раз}}$. Таким образом, можно получить произвольную одноместную функцию:

$$f(x) = \sum_{i=0}^{k-1} f_{i,f(i)}(x),$$

в том числе и $\sim x$, $\bar{x}$. Получим теперь все двухместные функции. Для этого построим сначала вспомогательную систему функций:

$$j_{0,0}(x,y) = j_2(j_0(x) + j_0(y)) = \begin{cases} 1 & x = y = 0, \\ 0 & \text{иначе;} \end{cases} \tag{2.6}$$

$$j_{l,m}(x,y) = j_{0,0}(x+(k-l), y+(k-m)) = \begin{cases} 1 & x = l, y = m, \\ 0 & \text{в противном случае.} \end{cases}$$

Теперь мы готовы построить все функции двух переменных. Действительно,

$$f_{l,m,s}(x,y) = \underbrace{j_{l,m}(x,y)+\cdots+j_{l,m}(x,y)}_{s \text{ раз}} = \begin{cases} s & x = l, y = m, \\ 0 & \text{иначе.} \end{cases}$$

Тогда любая двухместная функция может быть представлена в виде

$$f(x,y) = \sum_{l=0}^{k-1}\sum_{m=0}^{k-1} f_{l,m,f(l,m)}(x,y),$$

в частности, функция Вебба. Следовательно, система 7 полна. ■

Отметим, что условие $k \geqslant 3$ существенно используется на шаге 2.6, где необходимо наличие в P_k функции $j_0(x)$, что, очевидно, выполняется тогда и только тогда, когда $k \geqslant 3$.

Теорема о полноте системы Поста. *Системой Поста* называется система функций

$$\{\overline{x}, \max(x,y)\}.$$

Теорема 2.3. *Система Поста полна в P_k.*

□ *Док-во.* Сведем систему Поста к системе Россера-Туркетта. Для начала получим константы. Имея отрицание Поста, можно получить функцию $x+i$ для любого i. Тогда справедливо равенство

$$\max(x, x+1, x+2, \ldots, x+k-1) = k-1.$$

Если есть одна константа и циклический сдвиг с шагом 1 (в нашем случае — отрицание Поста), то можно получить все константы: $\overline{k-1} = 0, \overline{0} = 1, \ldots, \overline{k-3} = k-2$. Получим все J_i:

$$\overline{\max(x+1, \ldots, x+k-1)} = \overline{\begin{pmatrix} 0 & 1 & \ldots & k-2 & k-1 \\ k-1 & k-2 & \ldots & k-1 & k-2 \end{pmatrix}} = J_{k-1}(x).$$

Аналогично, имея циклический сдвиг с шагом 1 и J_{k-1}, можно получить уже все J_i по следующему правилу: $J_{k-2}(x) = J_{k-1}(\overline{x}), \ldots, J_0(x) = J_1(\overline{x})$.

Таким образом, получены все константы, все J_i, а максимум входит в систему Поста. Осталось получить минимум. Заметим, что в силу 2.1 достаточно реализовать над системой Поста отрицание Лукасевича. Реализуем систему функций, над которой реализуются *все* функции одного переменного, в частности, и отрицание Лукасевича. Построим систему функций

$$f_{r,x}(x) = \begin{cases} s & x = r, \\ 0 & x \neq r. \end{cases}.$$

Действительно,

$$\begin{aligned} \max(J_0(x), k-2) + 2 = j_0(x) &= f_{0,1}(x) \\ \max(J_0(x), k-3) + 3 &= f_{0,2}(x) \\ &\ldots \\ \max(J_0(x), k-s-1) + s + 1 &= f_{0,s}(x) \\ &\ldots \\ \max(J_0(x), 0) &= f_{0,k-1}(x) \end{aligned}$$

Далее, для любого s

$$\begin{aligned} f_{k-1,s}(x) &= f_{0,s}(\overline{x}) \\ &\ldots \\ f_{1,s}(x) &= f_{2,s}(\overline{x}) \end{aligned}$$

Таким образом, для любых $0 \leqslant r, s \leqslant k-1$ построены $f_{r,s}(x)$ С помощью полученной системы, очевидно, можно построить любую одноместную функцию $f(x)$:

$$f(x) = \max\left(f_{0,f(0)}(x), f_{1,f(1)}(x), \ldots, f_{l,f(l)}(x), \ldots, f_{k-1,f(k-1)}(x)\right),$$

в том числе и отрицание Лукасевича:

$$\sim x = \max\left(f_{0,k-1}(x), f_{1,k-2}(x), \ldots, f_{l,k-l-1}(x), \ldots, f_{k-1,0}(x)\right).$$

Тогда, согласно 2.1, $\min(x,y) = \sim \max(\sim x, \sim y)$, что завершает доказательство. ■

Заметим, что эта система функций является полной при *любом* значении k. Дело в том, что некоторые системы полны лишь при определенных значениях k, например, при $k \geqslant 3$ или при только при простых k.

Функция Вебба. *Функцией Вебба* называется функция

$$\overline{\max(x,y)} = \max(x,y) + 1.$$

Эта функция является аналогом шефферовой функции в P_2: ее замыкание совпадает со всем P_k:

Следствие 2.1.1 (из теоремы 2.3). *Система $\{V_k(x,y)\}$ полна в P_k.*

□ *Док-во.* Сведем эту систему к системе Поста. Отождествим переменные: $V_k(x,x) = x+1 = \overline{x}$. Затем применим $k-1$ раз полученное отрицание Поста к самой функции Вебба: $V_k(x,y) - 1 = \max(x,y)$. ■

Следствие 2.1.2 (из следствия 2.1.1). *Из любой полной системы в P_k можно выделить полную конечную подсистему.*

□ *Док-во.* Действительно, если система $\mathscr{A}$ полна, то функция Вебба реализуется формулой над $\mathscr{A}$: $V_k(x,y) = \mathfrak{F}(f_{i_1}, \ldots, f_{i_r}), f_{i_j} \in \mathscr{A} \quad \forall j = \overline{1,r}$. Но тогда система функций $\{f_{i_1}, \ldots, f_{i_r}\}$ также полна. ■

Примеры.

1. Используя метод сведения к заведомо полным системам, доказать полноту в P_k следующих систем:

   (a) $\{J_0(x), J_1(x), \ldots, J_{k-1}(x), x^2, x \dot{-} y\}$.

   □ *Решение.* Отождествлением переменных в усеченной разности получаем константу 0: $x \dot{-} x = 0$. Далее, подставляя на место переменной функции $J_0(x)$ эту константу, получаем константу $k-1$. Подставляя $k-1$ в x^2, получаем константу 1. Таким образом, в исходной системе содержится заведомо полная система 6. ■

   (b) $\{k-1, x \dot{-} y, x+y\}$.

   □ *Решение.* Суммируя $k-1$ раз константу $k-1$, получаем константу 1: $\underbrace{k-1+\cdots+k-1}_{k-1} = 1$. Таким образом, в исходной системе содержится заведомо полная система 6. ■

   (c) $\{\sim x, x+2, x \dot{-} y\}$.

   □ *Решение.* Отождествлением переменных в усеченной разности получаем константу 0. Отрицание Лукасевича нуля равно константе $k-1$. Затем, $(k-1)+2=1$. Таким образом, в исходной системе содержится заведомо полная система 6. ■

   (d) $\{-x, 1-x^2, x \dot{-} y\}$.

   □ *Решение.* $x \dot{-} x = 0$, $1-0^2=1$, $-1=k-1$. Таким образом, в исходной системе содержится заведомо полная система 6. ■

   (e) $\{x+y, (\sim x) \dot{-} 2y\}$.

   □ *Решение.* Заметим, что при $k=2$ система не полна: $x+y = x \oplus y$, $(\sim x) \dot{-} 2y = \bar{x} = x \oplus 1$ — содержатся в классе линейных функций. При $k \geqslant 3$ верно следующее: $\underbrace{x+x+\cdots+x}_{k} = 0$, $(\sim 0) \dot{-} 2 \cdot 0 = k-1$, $x \dot{-} 2(k-1) = x \dot{-} (k-2) = j_{k-1}(x)$, $j_{k-1}(x+(k-1)) = j_0(x)$. Таким образом, исходная система сведена к системе 7, которая полна при $k \geqslant 3$. ■

2. Подобрав подходящий класс типа $T(\mathscr{E})$ или $U(D)$, доказать, что система $\mathscr{A}$ не полна в P_k.

   (a) $\mathscr{A} = \{\sim s, \min(x,y), x \cdot y^2\}$.

   □ *Решение.* Утверждается, что для $\mathscr{E} = \{0, k-1\}$ система $\mathscr{A} \subseteq T(\mathscr{E})$. Действительно, $\sim 0 = k-1$, $\sim (k-1) = 0$, функция минимум сохраняет любое множество, $0 \cdot 0^2 = 0 \cdot (k-1)^2 = (k-1) \cdot 0^2 = 0$, $(k-1) \cdot (k-1)^2 = k-1$. Следовательно, при $k \geqslant 3$ система не полна. При $k=2$, очевидно, система полна, так как первые две функции превращаются в отрицание и конъюнкцию и образуют базис в P_2. ■

   (b) $\mathscr{A} = \left\{1, 2, \overline{x \dot{-} j_2(x)}, \max(x,y)\right\}$.

   □ *Решение.* Утверждается, что для $\mathscr{E} = \{1,2\}$ система $\mathscr{A} \subseteq T(\mathscr{E})$. Действительно, константы сохраняют это множество, максимум сохраняет любое множество, а $\overline{1 \dot{-} j_2(1)} = \overline{2 \dot{-} j_2(2)} = 2$. Следовательно, при $k \geqslant 3$ система полна. При $k=2$ рассматривать систему не имеет смысла, так как она содержит константу 2. ■

   (c) $\mathscr{A} = \{2, j_0(x), x + j_0(x) + J_1(x) + J_{k-1}(x), \min(x,y)\}$.

   □ *Решение.* Утверждается, что для $D = \{0,1\}\{2,\ldots,k-1\}$ система $\mathscr{A} \subseteq U(D)$. Действительно, константа 2 сохраняет любое разбиение, функция минимума сохраняет любое монотонное разбиение, а D монотонно, то есть все элементы одного блока находятся в одном и том же отношении порядка со всеми элементами другого. И, наконец, обозначив $f(x) = x + j_0(x) + J_1(x) + J_{k-1}(x)$, имеем $1 = f(0) \sim f(1) = 0 \pmod D$ $f(a) \sim f(b) \pmod D$ $\forall a,b \in \{2,\ldots,k-1\} : f(a), f(b) \in \{2,\ldots,k-2\}$. Следовательно, при $k \geqslant 3$ система не полна. При $k=2$ рассматривать систему не имеет смысла, так как она содержит константу 2. ■

   (d) $\mathscr{A} = \{J_2(x), x + j_0(x), x + j_0(x) + J_1(x), \max(x,y)\}$.

   □ *Решение.* Утверждается, что для $\mathscr{E} = \{0,1\}$ система $\mathscr{A} \subseteq T(\mathscr{E})$. Действительно, $J_2(0) = J_2(1) = 0$, $0 + j_0(0) = 1$, $1 + j_0(1) = 1$, $0 + j_0(0) + J_1(0) = 1 + j_0(1) + J_1(1) = 1$, а функция максимума сохраняет любое множество. Следовательно, при $k \geqslant 3$ система не полна. При $k=2$ рассматривать систему не имеет смысла, так как она содержит функцию $J_2(x)$. ■

(e) $\mathscr{A} = \{k-1, J_0(x), x \dot{-} y, x \cdot y \cdot z\}$.

□ *Решение.* Утверждается, что для $\mathscr{E} = \{0, k-1\}$ система $\mathscr{A} \subseteq T(\mathscr{E})$. Действительно, константа сохраняет любое множество, содержащее ее как элемент, $J_0(0) = k-1$, $J_0(k-1) = 0$, $0 \dot{-} 0 = 0 \dot{-} (k-1) = (k-1) \dot{-} (k-1) = 0$, $(k-1) \dot{-} 0 = k-1, 0 \cdot 0 \cdot 0 = 0 \cdot 0 \cdot (k-1) = 0 \cdot (k-1) \cdot 0 = 0 \cdot (k-1) \cdot (k-1) = (k-1) \cdot 0 \cdot 0 = (k-1) \cdot 0 \cdot (k-1) = (k-1) \cdot (k-1) \cdot 0 = 0$, $(k-1) \cdot (k-1) \cdot (k-1) = k-1$. Следовательно, при $k \geqslant 3$ система не полна. При $k = 2$ легко видеть, что система полна, так как первая функция — константа 1 — не сохраняет ноль и не является самодвойственной, вторая функция превращается в отрицание, которое не монотонно и не сохраняет единицу, а четвертая функция не линейная. ■

(f) $\mathscr{A} = \left\{2x^3, 2x+y, x^2y, xJ_0(y), \overline{x}^2 + (\sim y)\right\}$.

□ *Решение.* Утверждается, что для $\mathscr{E} = \{0\}$ система $\mathscr{A} \subseteq T(\mathscr{E})$. Действительно, $2 \cdot 0^3 = 0$, $2 \cdot 0 + 0 = 0$, $0^2 \cdot 0 = 0, 0 \cdot J_0(0) = 0, \overline{0}^2 + (\sim 0) = 0$. Следовательно, при $k \geqslant 2$ система не полна. ■

(g) $\mathscr{A} = \{x \cdot y, \max(x,y) - z + 1\}$.

□ *Решение.* Утверждается, что для $\mathscr{E} = \{1\}$ система $\mathscr{A} \subseteq T(\mathscr{E})$. Действительно, $1 \cdot 1 = 1$, $\max(1,1) - 1 + 1 = 1$. Следовательно, при $k \geqslant 2$ система не полна. ■

(h) $\mathscr{A} = \left\{-x^2, \max(x,y) + \overline{z}\right\}$.

□ *Решение.* Утверждается, что для $\mathscr{E} = \{k-1\}$ система $\mathscr{A} \subseteq T(\mathscr{E})$. Действительно,

$$-(k-1)^2 = k-1, \ \max(k-1, k-1) + \overline{k-1} = k-1.$$

Следовательно, при $k \geqslant 2$ система не полна. ■

(i) $\mathscr{A} = \left\{1, -x \cdot y, \overline{x^2 \dot{-} y}\right\}$.

□ *Решение.* Утверждается, что для $\mathscr{E} = \{1, k-1\}$ система $\mathscr{A} \subseteq T(\mathscr{E})$. Действительно, константа единица сохраняет это множество, $-1 \cdot 1 = -(k-1) \cdot (k-1) = k-1$, $-1 \cdot (k-1) = -(k-1) \cdot 1 = 1$, $\overline{1^2 \dot{-} 1} = \overline{1^2 \dot{-} (k-1)} = \overline{(k-1)^2 \dot{-} 1} = \overline{(k-1)^2 \dot{-} (k-1)} = 1$. Следовательно, при $k \geqslant 2$ система не полна. ■

(j) $\mathscr{A} = \{2, \max(x,y), x \dot{-} y\}$.

□ *Решение.* Утверждается, что для $\mathscr{E} = \{0, 2\}$ система $\mathscr{A} \subseteq T(\mathscr{E})$. Действительно, константа 2 сохраняет это множество, функция максимума сохраняет любое множество, а $0 \dot{-} 0 = 0 \dot{-} 2 = 2 \dot{-} 2 = 0$, $2 \dot{-} 0 = 2$. Следовательно, при $k \geqslant 3$ система не полна. При $k = 2$ рассматривать систему не имеет смысла, так как она содержит константу 2. ■

(k) $\mathscr{A} = \{k-2, \sim j_{k-2}(x), \max(x,y), \overline{x} + \overline{y}\}$.

□ *Решение.* Утверждается, что для $\mathscr{E} = \{k-2\}$ система $\mathscr{A} \subseteq T(\mathscr{E})$. Действительно, константа $k-2$ сохраняет это множество, функция максимума сохраняет любое множество, а $\sim j_{k-2}(k-2) = k-2$, $\overline{k-2} + \overline{k-2} = k-2$. Следовательно, при $k \geqslant 2$ система не полна. ■

(l) $\mathscr{A} = \{j_2(x), x + j_0(x) + J_1(x), x \cdot y, x \dot{-} y\}$.

□ *Решение.* Утверждается, что для $\mathscr{E} = \{0, 1\}$ система $\mathscr{A} \subseteq T(\mathscr{E})$. Действительно, $j_2(0) = j_2(1) = 0$, $0 + j_0(0) + J_1(0) = 1$, $1 + j_0(1) + J_1(1) = 0$, $0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0$, $1 \cdot 1 = 1$, $0 \dot{-} 0 = 0 \dot{-} 1 = 1 \dot{-} 1 = 0$, $1 \dot{-} 0 = 1$. Следовательно, для $k \geqslant 3$ система не полна. При $k = 2$ рассматривать систему не имеет смысла, так как она содержит функцию $j_2(x)$. ■

(m) $\mathscr{A} = \{1, J_0(x), \overline{x} + j_{k-1}(x), \min(x,y), \max(x,y)\}$.

□ *Решение.* Утверждается, что для $D = \{0\}\{1, \ldots, k-1\}$ система $\mathscr{A} \subseteq U(D)$. Действительно, константа сохраняет любое разбиение, функции минимума и максимума сохраняют любое монотонное разбиение, а D в данном случае — монотонное, функция $J_0(x)$ сохраняет D очевидным образом: при $x \neq 0$ все значения J_0 равны 0, то есть попадают в один блок, а блок, состоящий из одного элемента сохраняет любая функция. Обозначив третью функцию через $f(x)$, имеем $f(a) \in \{1, \ldots, k-1\}$ $\forall a \in \{1, \ldots, k-1\}$. Следовательно, для $k \geqslant 3$ система не полна. При $k = 2$ система, очевидно, полна, так как вторая функция превратится в отрицание, а четвертая в конъюнкцию. ■

(n) $\mathscr{A} = \{1, 2, \ldots, k-1, x + j_0(x), j_2(x) + 1, \max(x,y)\}$

□ *Решение.* Утверждается, что для $D = \{0,1\}\{2\}\{3,\ldots,k-1\}$ система $\mathscr{A} \subseteq U(D)$. Действительно, константы сохраняют любое разбиение, функция максимума сохраняет данное разбиение в силу его монотонности, функция $x + j_0(x)$ переставляет элементы в первом блоке, а остальные оставляет неподвижными, функция $j_2(x) + 1$ отображает элементы первого блока в единицу, второй блок оставляет неподвижным, а элементы третьего блока отображает в единицу. Следовательно, при $k \geqslant 3$ система не полна. При $k = 2$ рассматривать систему не имеет смысла, так как она содержит функцию $j_2(x) + 1$. ■

(o) $\mathscr{A} = \left\{1, \sim x, \overline{x \dot{-} y}, \min(x,y)\right\}$

□ *Решение.* Утверждается, что для $\mathscr{E} = \{1, k-2\}$ система $\mathscr{A} \subseteq T(\mathscr{E})$. Действительно, константа, отрицание Лукасевича и минимум тривиально сохраняют это множество. Также $\overline{1 \dot{-} 1} = \overline{1 \dot{-} (k-2)} = \overline{(k-2) \dot{-} (k-2)} = 1$, $\overline{(k-2) \dot{-} 1} = k-2$. Следовательно, при $k \geqslant 3$ система не полна. При $k = 2$ система, тривиально, полна, потому что отрицание Лукасевича, тривиально, перейдет в простое отрицание, а минимум — в конъюнкцию. ■

(p) $\mathscr{A} = \{\sim x, J_0(x), J_1(x), \ldots, J_{k-1}(x), \min(x,y) + (j_0(x) + j_0(y)) \cdot (x+y)\}$

□ *Решение.* Утверждается, что для $D = \{0, k-1\}\{1,\ldots,k-2\}$ система $\mathscr{A} \subseteq U(\mathscr{D})$. Действительно, образы отрицания Лукасевича и всех J_i совпадает с первым блоком. Обозначим последнюю функцию через $f(x,y)$. Если и x, и y принимают значение из второго блока, то и $f(x,y)$ примет значение также из второго блока (второе слагаемое обнулится, а минимум не выводит за пределы одного блока). Далее, $f(0,0) = 0$, $f(0,k-1) = f(k-1,0) = f(k-1,k-1) = k-1$, то есть первый блок переходит посредством $f(x,y)$ в первый блок. Пусть теперь a из второго блока. Легко видеть, что $f(0,a) = f(k-1,a) = a$, а также, $f(x,y) = f(y,x)$, откуда следует, что наборы со значениями из разных блоков отображаются все во второй блок. Следовательно, при $k \geqslant 3$ система не полна. При $k = 2$ система полна, так как отрицание Лукасевича перейдет в простое отрицание, которое не сохраняет константы и не монотонно, а последняя функция станет равна $xy \oplus x \oplus y$, при этом являясь нелинейной и несамодвойственной. ■

3. Пусть $\mathscr{E}$ — непустое подмножество из E_k, отличное от всего E_k, и $D = \{\mathscr{E}, E_k \setminus \mathscr{E}\}$. Подсчитать число функций в P_k, зависящих от переменных $x_1, x_2, \ldots, x_n$ $(n \geqslant 0)$ и содержащихся в множестве:

   (a) $T(\mathscr{E}) \setminus U(D)$;

   (b) $U(D) \setminus T(\mathscr{E})$;

   (c) $T(\mathscr{E}) \cup U(D)$.

□ *Решение.* Для начала найдем $|U(D)|^{\langle n \rangle}$. Типом набора $\widetilde{\alpha}^n$ назовем вектор из нулей и единиц $(\delta_1, \ldots, \delta_n)$, где $\delta_i = 0 \Leftrightarrow \alpha_i \in \mathscr{E}$. Все множество наборов разобьем на классы эквивалентности: два набора $\widetilde{\alpha}^n$ и $\widetilde{\beta}^n$ назовем эквивалентными, если они имеют одинаковый тип. Весом набора $\|\widetilde{\alpha}^n\|$ назовем число единиц в его типе $\left\|\widetilde{\delta}^n\right\|$. Всего классов эквивалентности — 2^n. В одном классе эквивалентности с весом l содержится $(k-m)^l m^{n-l}$ различных наборов. Каждому такому набору внутри одного класса эквивалентности функцией, сохраняющей разбиение, ставится в соответствие либо одно из m значений из $\mathscr{E}$, либо одно из $k-m$ значений из $E_k \setminus \mathscr{E}$, причем эти возможности несовместны. Итак, число функций, сохраняющих разбиение внутри класса эквивалентности веса l равно $m^{m^{n-l}(k-m)^l} + (k-m)^{m^{n-l}(k-m)^l}$. Поскольку классы эквивалентности не пересекаются, всего разных функций, зависящих от одних и тех же n переменных, сохраняющих данное разбиение —

$$\prod_{\tilde{t} \in \mathbb{B}^n} \left(m^{m^{n-\|\tilde{t}\|}(k-m)^{\|\tilde{t}\|}} + (k-m)^{m^{n-\|\tilde{t}\|}(k-m)^{\|\tilde{t}\|}} \right) = \prod_{t=0}^{n} \left(m^{m^{n-t}(k-m)^t} + (k-m)^{m^{n-t}(k-m)^t} \right)^{\binom{n}{t}}.$$

Теперь легко сказать, сколько функций содержится в пересечении: если в наборе все переменные из $\mathscr{E}$, то им ставятся в соответствие значения только из $\mathscr{E}$, то есть при $t = 0$ второе слагаемое пропадает:

$$|T(\mathscr{E}) \cap U(D)|^{\langle n \rangle} = m^{m^n} \cdot \prod_{t=1}^{n} \left(m^{m^{n-t}(k-m)^t} + (k-m)^{m^{n-t}(k-m)^t} \right)^{\binom{n}{t}}.$$

Для того, чтобы ответить на поставленные вопросы осталось вспомнить, что $|T(\mathscr{E})|^{\langle n \rangle} = m^{m^n} k^{k^n - m^n}$. Таким образом,

(a)

$$\begin{aligned}|T(\mathscr{E})\setminus U(D)|^{\langle n\rangle} &= |T(\mathscr{E})|^{\langle n\rangle} - |T(\mathscr{E})\cap U(D)|^{\langle n\rangle}\\ &= m^{m^n}\cdot k^{k^n-m^n} - m^{m^n}\cdot\prod_{t=1}^{n}\left(m^{m^{n-t}(k-m)^t} + (k-m)^{m^{n-t}(k-m)^t}\right)^{\binom{n}{t}}\\ &= m^{m^n}\cdot\left(k^{k^n-m^n} - \prod_{t=1}^{n}\left(m^{m^{n-t}(k-m)^t} + (k-m)^{m^{n-t}(k-m)^t}\right)^{\binom{n}{t}}\right),\end{aligned}$$

(b)

$$\begin{aligned}|U(D)\setminus T(\mathscr{E})|^{\langle n\rangle} &= |U(D)|^{\langle n\rangle} - |T(\mathscr{E})\cap U(D)|^{\langle n\rangle}\\ &= \prod_{t=0}^{n}\left(m^{m^{n-t}(k-m)^t} + (k-m)^{m^{n-t}(k-m)^t}\right)^{\binom{n}{t}}\\ &\quad - m^{m^n}\cdot\prod_{t=1}^{n}\left(m^{m^{n-t}(k-m)^t} + (k-m)^{m^{n-t}(k-m)^t}\right)^{\binom{n}{t}}\\ &= (k-m)^{m^n}\cdot\prod_{t=1}^{n}\left(m^{m^{n-t}(k-m)^t} + (k-m)^{m^{n-t}(k-m)^t}\right)^{\binom{n}{t}},\end{aligned}$$

(c)

$$\begin{aligned}|T(\mathscr{E})\cup U(D)|^{\langle n\rangle} &= |T(\mathscr{E})|^{\langle n\rangle} + |U(D)|^{\langle n\rangle} - |T(\mathscr{E})\cap U(D)|^{\langle n\rangle}\\ &= m^{m^n}k^{k^n-m^n} + \prod_{t=0}^{n}\left(m^{m^{n-t}(k-m)^t} + (k-m)^{m^{n-t}(k-m)^t}\right)^{\binom{n}{t}}\\ &\quad - m^{m^n}\cdot\prod_{t=1}^{n}\left(m^{m^{n-t}(k-m)^t} + (k-m)^{m^{n-t}(k-m)^t}\right)^{\binom{n}{t}}\\ &= m^{m^n}k^{k^n-m^n} + (k-m)^{m^n}\cdot\prod_{t=1}^{n}\left(m^{m^{n-t}(k-m)^t} + (k-m)^{m^{n-t}(k-m)^t}\right)^{\binom{n}{t}}.\end{aligned}$$

■

4. Исследовать на полноту в P_k следующие системы:

(a) $\{k-1, x+2, \max(x,y)\}$.

□ *Решение.* Возможны два случая:

i. $k \geqslant 3$ — нечетное. Тогда $x + \underbrace{2+\cdots+2}_{\frac{k+1}{2}\text{ раз}} = x+1 = \overline{x}$, и исходная система содержит систему Поста, которая является полной в P_k.

ii. $k \geqslant 4$ — четное. В этом случае утверждается, что для $\mathscr{E} = \{1,3,\ldots,k-1\}$ исходная система содержится в $T(\mathscr{E})$, то есть сохраняет нечетное множество и является неполной.

Рассматривать систему при $k=2$ не имеет смысла, так как она содержит функцию $x+2$. ■

(b) $\left\{1, x, \overline{\dot{x-y}}\right\}$.

□ *Решение.* Утверждается, что для $\mathscr{E} = \{1,2\}$ исходная система содержится в $T(\mathscr{E})$. Действительно, константы сохраняют это множество, и $\overline{\dot{1-1}} = \overline{\dot{1-2}} = \overline{\dot{2-2}} = 1$, $\overline{\dot{2-1}} = 2$. Следовательно, для $k \geqslant 3$ система не полна. Рассматривать систему при $k=2$ не имеет смысла, так как она содержит константу 2. ■

(c) $\{k-2, x+y, \min(x,y)\}$.

□ *Решение.* Возможны два случая:

i. $k \geqslant 2$ — четное. В этом случае, подобно 4(a)ii, система сохраняет четное множество.

ii. $k \geqslant 3$ — нечетное. Тогда $x + \underbrace{(k-2)+\cdots+(k-2)}_{\frac{k-1}{2}\text{ раз}} = \overline{x}$, и исходная система содержит систему Поста, которая является полной в P_k.

■

(d) $\left\{1, k-1, x \dot{-} \left\lfloor \frac{k}{2} \right\rfloor, \min(x,y)\right\}$.

□ *Решение.* Утверждается, что для $D = \left\{0,\ldots,\left\lfloor \frac{k}{2} \right\rfloor\right\}\left\{\left\lfloor \frac{k}{2} \right\rfloor+1,\ldots,k-1\right\}$ исходная система содержится в $U(D)$. Действительно, константы сохраняют любое разбиение, минимум сохраняет любое монотонное разбиение, а D — монотонное. Далее, третья функция отображает первый блок в 0, а второй блок в первый. Следовательно, при $k \geqslant 3$ система не полна. При $k = 2$ система также не полна, так как целиком содержится в классе монотонных функций (в случае $k = 2$ она превратится в $\{0, 1, x \cdot y\}$). ■

5. Выделить базис из полной в P_k системы $\mathscr{A}$:

(a) $\mathscr{A} = \{k-1, j_0(x), j_1(x), \ldots, j_{k-1}(x), x \cdot y, x \dot{-} y\}$.

□ *Решение.* Рассмотрим подсистему $\mathscr{B} = \{k-1, x \dot{-} y, j_{k-1}(x)\} \subset \mathscr{A}$. Она является полной, так как $j_{k-1}(k-1) \equiv 1$ и система сводится к полной системе 6. Докажем, что если убрать из нее любую функцию, она перестанет быть полной. Действительно, $\mathscr{A} \setminus \{k-1\} \subseteq T(\{0\})$, $\mathscr{A} \setminus \{x \dot{-} y\} \subseteq P_k^{(1)}$, $\mathscr{C} = \mathscr{A} \setminus \{j_{k-1}(x)\} \subseteq T(\{0, k-1\})$. Последнее равенство, однако, не доказывает неполноту в случае $k = 2$. При $k = 2$ $\mathscr{A} \setminus \{j_{k-1}(x)\}$ является и полной системой, и базисом, так как $k-1 = 1$ — не сохраняет 0 и не самодвойственная, а вторая — $x \dot{-} y = xy \oplus x$ — нелинейная, не сохраняет единицу и не монотонная. Следовательно, при $k \geqslant 3$ базисом является система $\mathscr{B}$, а при $k = 2$ — система $\mathscr{C}$. ■

(b) $\mathscr{A} = \left\{x-2, J_0(x), \max(x,y), x \dot{-} y^2, x^2 \cdot y\right\}$.

□ *Решение.* Рассмотрим подсистему $\mathscr{B} = \left\{J_0(x), x \dot{-} y^2\right\}$. Покажем, что она полная. Действительно, $(\ldots(J_0(x) \underbrace{\dot{-} J_0^2(x)) \dot{-} \cdots \dot{-} J_0^2(x))}_{k-1 \text{ раз}} \dot{-} J_0^2(x) \equiv 0$, $J_0(0) = k-1$, $x \dot{-} (k-1)^2 \equiv x \dot{-} 1$, $(k-1) \dot{-} 1 = k-2$, $(k-2) \dot{-} 1 = k-3$, …, $2 \dot{-} 1 = 1$. Таким образом получены все константы и функции вида $x \dot{-} m$ для любого $m = \overline{1, k-1}$. Используя тот факт, что $J_0(x \dot{-} m) = \begin{cases} k-1 & x \leqslant m, \\ 0 & x > m, \end{cases}$ получим теперь все J_m для $0 \leqslant m \leqslant k-1$:

$$J_m(x) = (\ldots(J_0(x \dot{-} m) \underbrace{\dot{-} J_0^2(x \dot{-} (m-1))) \dot{-} \cdots \dot{-} J_0^2(x \dot{-} (m-1))}_{k-1 \text{ раз}} \dot{-} J_0^2(x \dot{-} (m-1)).$$

Далее заметим, что

$$x \dot{-} y \equiv (\ldots(x \dot{-} J_1^2(y)) \dot{-} J_2^2(y)) \dot{-} J_2^2(y)) \dot{-} \cdots) \underbrace{\dot{-} J_i^2(y)) \dot{-} J_i^2(y)) \dot{-} \cdots) \dot{-}}_{i \text{ раз}} J_i^2(y)) \dot{-} \cdots) \underbrace{\dot{-} J_{k-1}^2(y)) \dot{-} \cdots) \dot{-}}_{k-1 \text{ раз}} J_{k-1}^2(y)$$

Действительно, при $y = i$ только квадраты соответствующих J_i будут равны единицам, остальные же будут нулями. Следовательно, из x при $y = i$ будет усеченно вычитаться как раз i. Таким образом, система $\mathscr{A}$ сведена к системе 6: получены усеченная разность и константы 0 и $k-1$. Базисность этой системы при условии полноты очевидна: первая функция существенно зависит только от одной переменной, а вторая сохраняет, например, ноль. ■

(c) $\mathscr{A} = \left\{2, j_0(x,), x + y^2, x^2 \dot{-} y, x \cdot y \cdot z\right\}$

□ *Решение.* Рассмотрим подсистему $\mathscr{B} = \left\{j_0(x), x + y^2\right\}$. Докажем ее полноту. Заметим, что $j_0(j_0(x)) + j_0^2(x) \equiv 1$, $x + 1^2 = \bar{x}$. Имея отрицание Поста и j_0 можно получить все j_i для $0 \leqslant i \leqslant k-1$. Далее, используя тот же прием, что и в примере 5b, получим $x + y = x + j_1^2(y) + j_2^2(y) + j_2^2(y) + \cdots + \underbrace{j_i^2(y) + \cdots + j_i^2(y)}_{i \text{ раз}} + \cdots + \underbrace{j_{k-1}^2(y) + \cdots + j_{k-1}^2(y)}_{k-1 \text{ раз}}$. Таким образом, система $\mathscr{B}$ сводится к системе 7, которая полна при $k \geqslant 3$. При $k = 2$ система $\mathscr{B}$ теряет смысл, так как содержит константу 2. Базисность $\mathscr{B}$ очевидна: как и в 5b одна из функций существенно зависит только от одной переменной, а вторая — сохраняет ноль. ■

Упражнения.

1. Используя метод сведения к заведомо полным системам, доказать полноту в P_k следующих систем:
   (a) $\{\bar{x}, \min(x,y)\}$;
   (b) $\{\min(x,y)-1\}$;
   (c) $\{J_0(x), x+y, x\cdot y^2\}$;
   (d) $\{1, x^2+y, x^2\dot{-}y\}$;
   (e) $\{J_0(x), x+y, x\cdot y^2\}$;
   (f) $\{k-2, x\dot{y}+1, (\sim x)\dot{-}y\}$;
   (g) $\{k-1, x^2-y, x^2\dot{-}y\}$;
   (h) $\{1, 2\cdot x+y, x\dot{-}y\}$;
   (i) $\{1, x^2-y, \min(x,y)\}$;
   (j) $\{1, x+y+2, x^2\dot{-}y\}$;
   (k) $\{\bar{x}\cdot j_0(y), \min(x,y)\}$.

2. Подобрав подходящий класс типа $T(\mathscr{E})$ или $U(D)$, доказать, что система
$$\mathscr{A} = \{1-x, j_0(x), j_1(x), \ldots, j_{k-1}(x), x\cdot y, x\dot{-}y, \min(x,\bar{y})\}$$
не полна в P_k.

3. Как известно (см. теорему 2.2), система
$$\mathscr{A} = \{0, 1, \ldots, k-1, j_0(x), j_1(x), \ldots, j_{k-1}(x), x+y, x\cdot y\}$$
полна в P_k.
   (a) Доказать, что из системы $\mathscr{A}$ можно выделить полную в P_k подсистему, состоящую из двух функций.
   (b) Показать, что любая подсистема системы $\mathscr{A}$, состоящая из одной функции, не полна в P_k.

4. Система Россера-Туркетта
$$\mathscr{A}_1 = \{0, 1, \ldots, k-1, J_0(x), J_1(x), \ldots, J_{k-1}(x), \min(x,y), \max(x,y)\},$$
как известно, полна в P_k (см. теорему 2.1).
   (a) Проверить, что, удаляя из $\mathscr{A}_1$ любую константу, отличную от 0 и $k-1$, получаем подсистему, содержащуюся в некотором классе типа $T(\mathscr{E})$, где $\varnothing \neq \mathscr{E} \neq E_k$ (и, значит, неполную в P_k).
   (b) Выделить из системы $\mathscr{A}_1$ полную в P_k подсистему, состоящую из $2k-2$ функций.

5. Для заданных k исследовать на полноту следующие подсистемы системы Россера-Туркетта:
   (a) $k=3$, $\{1, J_0(x), J_2(x), \min(x,y), \max(x,y)\}$;
   (b) $k=3$, $\{1, 2, J_2(x), \min(x,y), \max(x,y)\}$;
   (c) $k=4$, $\{1, 2, J_0(x), J_1(x), \min(x,y), \max(x,y)\}$;
   (d) $k=4$, $\{1, 2, J_0(x), J_3(x), \min(x,y), \max(x,y)\}$.

6. (a) Для $k=3,4$ и 5 подсчитать число различных замкнутых классов в P_k, являющихся классами сохранения разбиений.
   (b) Пусть $D=\{\mathscr{E}_1, \ldots, \mathscr{E}_s\}$ — разбиение множества E_k. Подсчитать число функций в P_k, содержащихся в классе $U(D)$ и зависящих от переменных $x_1, x_2, \ldots, x_n$ ($n \geqslant 0$).

7. Исследовать на полноту в P_k следующие системы:
   (a) $\{0, 1, \bar{x}\dot{-}(\sim y)\}$;
   (b) $\{2, 2x+y, x^2\dot{-}y\}$;
   (c) $\{1, 2, \max(\bar{x}, y)\}$;
   (d) $\{2\dot{-}x, x\cdot y, \max(x,y)\}$;
   (e) $\{k-2, 2x+y, x\dot{-}y\}$;

(f) $\{\sim x, -x\cdot y, \min(x,y)\}$;

(g) $\{2, x+y, x\dot{-}y\}$;

(h) $\{\sim x, 2j_0(x), J_1(x), x\dot{-}y\}$;

(i) $\{1, \sim x, J_0(x)+J_1(x), \max(x.y)\}$;

(j) $\{0, 1, \sim x, 2-j_0(x)-2j_1(x), \min(x,y)\}$;

(k) $\{k-2, \sim x, x\dot{-}y\}$;

2.2 Теоремы о функциональной полноте

Теорема об алгоритмической разрешимости проблемы распознавания полноты в k-значной логике. Рассмотрим конечную систему функций $\mathscr{A} = \{f_1, \ldots, f_m\}$, зависящих от одних и тех же n переменных $x_1, \ldots, x_n$. Обозначим $g_m^n(x_1, \ldots, x_n) = x_m$ — *селекторную функцию* для $1 \leqslant m \leqslant n$. Используем две из них: $g_1^2(x_1, x_2) = x_1$, $g_2^2(x_1, x_2) = x_2$.

Теорема 2.4. *Существует алгоритм, распознающий в P_k при $k \geqslant 2$ полноту любой конечной системы.*

□ *Док-во.* Построим последовательность вложенных друг в друга множеств

$$\mathfrak{N}_0 = \varnothing : \mathfrak{N}_0 \subsetneq \mathfrak{N}_1 \subsetneq \mathfrak{N}_2 \subsetneq \cdots \subsetneq \mathfrak{N}_r \subsetneq \mathfrak{N}_{r+1} \subsetneq \cdots \subsetneq \mathfrak{N}_{r^*} = \mathfrak{N}_{r^*+1} = \cdots$$

по следующим индуктивным правилам: $\mathfrak{N}_1$ — множество всех функций двух переменных, реализуемых формулами вида $f(H_1(x_1,x_2), H_2(x_1,x_2), \ldots, H_n(x_1,x_2))$, где $H_i(x_1,x_2) = \begin{bmatrix} g_1^2 \\ g_2^2 \end{bmatrix}$. Заметим, что $|\mathfrak{N}_1| \leqslant m \cdot 2^n$ (поскольку всего функций в $\mathscr{A}$ — m, все зависят от n переменных, на месте каждой из которых стоит одна из двух функций). Пусть уже построены все классы, до r-го включительно, и $|\mathfrak{N}_r| = s_r$. Тогда класс $\mathfrak{N}_{r+1}$ — это множество всех функций двух переменных, реализуемых формулами вида $f(H_1(x_1,x_2), H_2(x_1,x_2), \ldots, H_n(x_1,x_2))$, где $H_i(x_1,x_2) = \begin{bmatrix} g_1^2 \\ g_2^2 \\ h_i \in \mathfrak{N}_r \end{bmatrix}$. Очевидно, что $|\mathfrak{N}_{r+1}| \leqslant m \cdot (s_r+2)^n$. Это следует из того, что любая функция из $\mathfrak{N}_{r+1}$ реализуется формулой над $\mathfrak{N}_{r+1}$. Все функции из $\mathfrak{N}_r$ зависят от двух переменных. Поскольку всего функций от двух переменных k^{k^2}, не более, чем за $k^{k^2}+2$ шагов возникнет ситуация, $\mathfrak{N}_{r^*} = \mathfrak{N}_{r^*+1} = \cdots$. Как только построен последний уникальный класс, мы проверяем наличие в нем функции Вебба. Если она в нем есть, то мы свели систему к функции Вебба, следовательно, система полна. Если же функция Вебба не содержится в последнем уникальном классе, то система не полна в силу следующих рассуждений. Выделяем из замыкания исходной системы функций $\mathscr{A}$ функции, зависящие только от x_1, x_2 — множество $[\mathscr{A}]_{x_1,x_2}$. Очевидно, $[\mathscr{A}]_{x_1,x_2} = \mathfrak{N}_{r^*}$. В то же время, если бы $\mathscr{A}$ была бы полна, то она содержала бы функцию Вебба $V_k(x_1,x_2)$. Следовательно, в этом случае система не полна. ■

Теорема Кузнецова о функциональной полноте. В этом пункте мы покажем существование системы 2.5 в P_k для любого k. Рассмотрим $\mathfrak{N}$ — некоторое множество функций k-значной логики, зависящих от переменных $y_1, \ldots, y_m$. Для удобства будем считать, что сами переменные в это множество включены: $y_i = g_i^m(y_1, \ldots, y_m) \in \mathfrak{N}$.

Определение. Функция k-значной логики $f(x_1, \ldots, x_n)$ *сохраняет* $\mathfrak{N}$, если для любых $h_1, \ldots, h_n \in \mathfrak{N}$ суперпозиция $f(h_1, \ldots, h_n) \in \mathfrak{N}$. Множество функций $\mathfrak{M}$ с*сохраняет* $\mathfrak{N}$, если все функции, сохраняющие $\mathfrak{N}$, заключены в $\mathfrak{M}$.

Пример. Пусть $m=1$, $\mathfrak{N}: f(\sim y) = \sim f(y)$. Множество $\mathfrak{N}$ содержит, например, тождественную функцию, само отрицание Лукасевича. Множество функций, сохраняющих данное $\mathfrak{N}$, является множеством всех самодвойственных функций: $\mathfrak{M}: \sim g(\sim x_1, \ldots, \sim x_n) = g(x_1, \ldots, x_n)$. Действительно, для любых $h_1(y), \ldots, h_n(y) \in \mathfrak{N} \Rightarrow F(y) = f(h_1(y), \ldots, h_n(y)) = f(\sim h_1(\sim y), \ldots, \sim h_n(\sim y)) \in \mathfrak{N}$, то есть $F(\sim y) = \sim F(y) \Leftrightarrow \sim f(\sim x_1, \ldots, \sim x_n) = f(x_1, \ldots, x_n)$. Заметим, что сами функции $f(y)$ входят в $\mathfrak{M}$.

Лемма 2.2.1. *Пусть $\mathfrak{N}$ — множество функций, зависящих от переменных $y_1, \ldots, y_m$, содержащее тождественные функции g_i^m, а $\mathfrak{M}$ — множество функций, сохраняющих $\mathfrak{N}$. Тогда $\mathfrak{M}$ замкнуто.*

□ *Док-во.* Так как тождественные функции сохраняют $\mathfrak{N}$, достаточно доказать, что суперпозиция сохраняющих $\mathfrak{N}$ функций также сохраняет $\mathfrak{N}$. Пусть $f(z_1, \ldots, z_l), f_i(x_1, \ldots, x_n) \in \mathfrak{M}$, $i = \overline{1,l}$, то есть для любых $h_1, \ldots, h_n \in \mathfrak{N}$ выполняется $f_i(h_1, \ldots, h_n) \in \mathfrak{N}$. Рассмотрим суперпозицию $F(x_1, \ldots, x_n) = f(f_1, \ldots, f_l)$. Для любых $h_1, \ldots, h_n \in \mathfrak{N} \Rightarrow H_i = f_i(h_1, \ldots, h_n) \in \mathfrak{N}$ для всех $i = \overline{1,l}$. Но тогда и $F(h_1, \ldots, h_n) = f(H_1, \ldots, H_l) \in \mathfrak{N}$. ■

Лемма 2.2.2. *Пусть $\mathfrak{N}$ — множество функций, зависящих от переменных $y_1, \ldots, y_m$, содержащее тождественные функции g_i^m и $[\mathfrak{N}]_{y_1,\ldots,y_m} = \mathfrak{N}$. Тогда для $\mathfrak{M}$, сохраняющего $\mathfrak{N}$, выполнено $\mathfrak{M}_{y_1,\ldots,y_m} = \mathfrak{N}$.*

□ *Док-во.* Рассмотрим любую функцию $f(y_1,\dots,y_m) \in \mathfrak{N}$. Для любых $h_1,\dots,h_n \in \mathfrak{N}$ по условию теоремы $f(h_1,\dots,h_m) \in [\mathfrak{N}]_{y_1,\dots,y_m} = \mathfrak{N} \Rightarrow f \in \mathfrak{M}$, и при этом она зависит от $y_1,\dots,y_m$, то есть $f \in \mathfrak{M}_{y_1,\dots,y_m}$. Таким образом, $\mathfrak{N} \subseteq \mathfrak{M}_{y_1,\dots,y_m}$.

Обратно: для любой функции $f \in \mathfrak{M}_{y_1,\dots,y_m} \Rightarrow f(y_1,\dots,y_m) = f(g_1^m,\dots,g_m^m) \in \mathfrak{N}$ в силу замкнутости $\mathfrak{N}$ по переменным $y_1,\dots,y_m$. Следовательно, $\mathfrak{M}_{y_1,\dots,y_m} \subseteq \mathfrak{N}$.

Из доказанного немедленно вытекает, что $\mathfrak{N} = \mathfrak{M}_{y_1,\dots,y_m}$. ■

Теорема 2.5 (А.В. Кузнецов). *Для любого $k \geqslant 2$ существует система, называемая критериальной, $\mathfrak{M}_1,\dots,\mathfrak{M}_s$ замкнутых классов, попарно не содержащих друг друга, таких, что любой класс функций $\mathscr{A} \subseteq P_k$ полон тогда и только тогда, когда $\mathscr{A}$ целиком не лежит ни в одном из классов $\mathfrak{M}_1,\dots,\mathfrak{M}_s$.*

□ *Док-во.* Построим эти классы. Рассмотрим множество всех функций $P_{k_{x_1,x_2}}$, зависящих от переменных x_1 и x_2 — всего их k^{k^2}. Это множество имеет 2^{k^2} подмножеств, из которых мы выбираем все подмножества $\mathfrak{N}_i$, $i = \overline{1,s'}$, удовлетворяющие следующим трем условиям:

1. $\mathfrak{N}_i$ не пусто и не совпадает с $P_{k_{x_1,x_2}}$ для любого $i = \overline{1,s'}$,
2. $\mathfrak{N}_i$ содержит тождественные функции $g_1^2(x_1,x_2)$ и $g_2^2(x_1,x_2)$ для любого $i = \overline{1,s'}$ и
3. $\mathfrak{N}_i$ замкнуты по переменным x_1,x_2 для любого $i = \overline{1,s'}$.

Для каждого $\mathfrak{N}_i$ строится замкнутый класс $\mathfrak{M}_i'$ функций, сохраняющих $\mathfrak{N}_i$. Всего $\mathfrak{M}_i'$ — конечное число. Упорядочим их по включению. Как легко проверить, это будет являться частичным порядком. В построенном частично упорядоченном множестве возьмем систему максимальных элементов $\mathfrak{M}_1,\dots,\mathfrak{M}_s$ $(s < s')$, заметив, что $\mathfrak{M}_i \neq P_k\ \forall i = \overline{1,s}$. Последнее вытекает из того, что если бы какой-то из них совпадал со всем P_k, то он в силу замкнутости содержал бы функцию Вебба переменных x_1,x_2. Но тогда в силу замкнутости соответствующего $\mathfrak{N}_l$ по лемме 2.2.2, $\mathfrak{N}_l$ также совпадало бы со всем P_k, что противоречит построению. Далее, любой класс $\mathfrak{M}_i'$ содержится в одном из классов этой системы. Очевидно, что если $\mathscr{A} \subseteq \mathfrak{M}_i$, то $\mathscr{A}$ не полна: $[\mathscr{A}] \subseteq M_i \subsetneq P_k$.

Обратно, пусть $\mathscr{A}$ не лежит ни в одном из классов $\mathfrak{M}_i$, $i = \overline{1,s}$. Тогда рассмотрим систему $\mathfrak{M} = \left[\mathscr{A} \cup \left\{g_1^2(x_1,x_2), g_2^2(x_1,x_2)\right\}\right] \supseteq \mathscr{A}$. Очевидно, что $\mathscr{A}$ и $\mathfrak{M}$ полны или не полны одновременно. Предположим, что $\mathfrak{M}$ неполная. Тогда в $\mathfrak{M}_{x_1,x_2}$ не содержится $V_k(x_1,x_2)$. По лемме 2.2.2 существует такое j, что $\mathfrak{M}_{x_1,x_2} = \mathfrak{N}_j$. Но тогда $\mathfrak{M} \subseteq \mathfrak{M}_j' \subseteq \mathfrak{M}_k$, где $\mathfrak{M}_j'$ — класс функций, сохраняющих $\mathfrak{N}_j$, что противоречит тому, что $\mathscr{A}$ не лежит ни в одном из классов $\mathfrak{M}_i$. ■

Можно тривиально оценить снизу число функций критериальной системы числом функций, сохраняющих множества: $s \geqslant 2^k - 2$.

2.3 Существенные функции

Определение. Функция k-значной логики f называется *существенной*, если она существенно зависит не менее, чем от двух переменных.

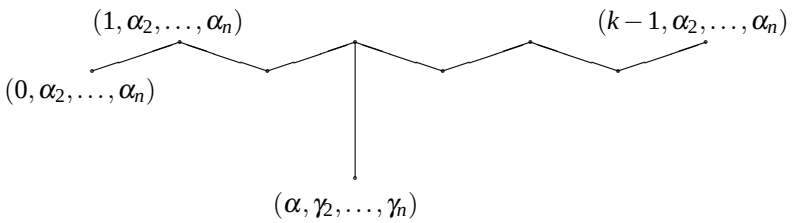
Леммы о существенных функциях.

Лемма 2.3.1 (о трех наборах). *Пусть функция $f(x_1,\dots,x_n)$ — существенная (x_1 — ее существенная переменная) и принимает $l \geqslant 3$ различных значений. Тогда существует три набора вида*

$$(\alpha,\alpha_2,\dots,\alpha_n),$$
$$(\beta,\alpha_2,\dots,\alpha_n),$$
$$(\alpha,\gamma_2,\dots,\gamma_n),$$

на которых функция принимает три различных значения.

□ *Док-во.* По предположению теоремы x_1 — существенная переменная функции f. Это означает, что существуют такие константы $\alpha_1,\dots,\alpha_n$, что $f(x_1,\alpha_1,\dots,\alpha_n) \not\equiv \text{const}$. Рассмотрим цепочку



Возможны два случая:

1. На этой цепочке функция принимает не все l значений. Тогда существует набор $(\alpha, \gamma_2, \ldots, \gamma_n)$, на котором функция принимает оставшееся значение. Берем также проекцию этого набора на цепь $(\alpha, \gamma_2, \ldots, \gamma_n)$ и какой-то другой набор с цепи $(\beta, \alpha_2, \ldots, \alpha_n)$. На полученных трех наборах функция принимает три разных значения.

2. На цепи принимаются все значения. Но у f есть по крайней мере еще одна существенная переменная, то есть существуют такие $\alpha, \gamma_2, \ldots, \gamma_n$, что $f(\alpha, \alpha_2, \ldots, \alpha_n)$ и $f(\alpha, \gamma_2, \ldots, \gamma_n)$ различны. Кроме этих двух значений берем еще одно с цепи.

■

Лемма 2.3.2 (Основная). *Пусть f — существенная функция, принимающая $l \geqslant 3$ различных значений, и x_1 — ее существенная переменная. Тогда существуют множества $Q_i \subseteq E_k$, $i = \overline{1,n} : |Q_i| \leqslant l-1$ такие, что на $Q_1 \times Q_2 \times \cdots \times Q_n$ функция f принимает все свои l значений.*

□ *Док-во.* Дополним три набора из леммы 2.3.1 $l-3$-мя наборами так, чтобы получилось l наборов, на которых функция принимает все свои значения:

$$\begin{array}{cccc}
(\alpha\,, & \alpha_2, & \ldots, & \alpha_n) \\
(\beta\,, & \alpha_2, & \ldots, & \alpha_n) \\
(\alpha\,, & \gamma_2, & \ldots, & \gamma_n) \\
(\alpha_1^4\,, & \alpha_2^4, & \ldots, & \alpha_n^4) \\
\ldots & \ldots & \ldots & \ldots \\
(\alpha_1^{l-3}\,, & \alpha_2^{l-3}, & \ldots, & \alpha_n^{l-3}) \\
Q_1 & Q_2 & \ldots & Q_n
\end{array}$$

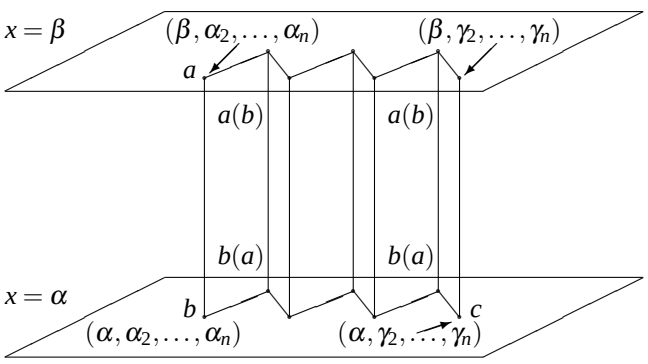
Множество первых разрядов обозначим Q_1, его мощность благодаря равенству первых разрядов первого и третьего наборов не превосходит $l-1$; множество i-ых разрядов обозначим Q_i для $i = \overline{2,n}$, его мощность благодаря равенству i-ых разрядов для $i = \overline{2,n}$ также не превзойдет $l-1$. По построению наборов, на их декартовом произведении функция примет все свои значения. ■

Лемма 2.3.3 (о квадрате). *Пусть f — существенная функция, принимающая $l \geqslant 3$ различных значений, и x_1 — ее существенная переменная. Тогда существует четверка наборов, называемая квадратом, вида*

$$\begin{array}{l}
(\alpha_1, \ldots, \alpha_{i-1}, \alpha, \alpha_{i+1}, \ldots, \alpha_{j-1}, \gamma, \alpha_{j+1}, \ldots, \alpha_n) \\
(\alpha_1, \ldots, \alpha_{i-1}, \alpha, \alpha_{i+1}, \ldots, \alpha_{j-1}, \delta, \alpha_{j+1}, \ldots, \alpha_n) \\
(\alpha_1, \ldots, \alpha_{i-1}, \beta, \alpha_{i+1}, \ldots, \alpha_{j-1}, \gamma, \alpha_{j+1}, \ldots, \alpha_n) \\
(\alpha_1, \ldots, \alpha_{i-1}, \beta, \alpha_{i+1}, \ldots, \alpha_{j-1}, \delta, \alpha_{j+1}, \ldots, \alpha_n)
\end{array},$$

на вершинах которого функция либо принимает не менее трех различных значений, либо принимает два значения, но одно из них только на одной вершине. Иными словами, одна из вершин квадрата является уникальной.

□ *Док-во.* Согласно лемме 2.3.1 найдутся три набора указанного вида такие, что функция на них принимает три различных значения a, b и c. Два набора находятся в одной гиперплоскости, а третий — в другой, но является проекцией первого. Рассмотрим первый квадрат, две вершины которого равны соответственно a и b. Если среди оставшихся двух вершин есть одна, значение на которой отлично от значений на первых двух или значения на них равны, то лемма доказана.



В противном случае, если на одной вершине значение равно a, а на другой — b, то перейдем к рассмотрению следующего квадрата. Для него повторим все эти рассуждения. Если мы таким образом дойдем до последнего квадрата, что будет означать, что во всех предыдущих квадратах на одних двух вершинах принимается значение a, а на других двух — b, то утверждение леммы выполнится потому, что в последнем квадрате будет три различных значения. ■

Теоремы о существенных функциях.

Теорема 2.6 (С.В. Яблонский). *Система функций, содержащая все одноместные функции, принимающие не более $k-1$ различных значений (CS_k) полна тогда и только тогда, когда она содержит существенную функцию, принимающую все k значений.*

□ *Док-во.* Необходимость доказывается от противного. Возможны два варианта.

1. Система вообще не содержит существенных функций. В этом случае она, очевидно, не полна, так как содержится в классе $P_k^{(1)}$.

2. Система содержит существенную функцию, но она принимает (не ограничивая общности) $k-1$ значение. Но тогда подстановкой на места переменных этой функции других функций системы нельзя получить существенную функцию двух переменных, принимающую все k значений, например, $x+y$.

Таким образом, в этом случае система не полна.

Достаточность. Пусть система содержит CS_k и существенную функцию, принимающую все k значений. В этом случае, очевидно, все константы принадлежат системе. Докажем достаточность системы по индукции.

Базис индукции. Построим все функции, принимающие не более двух значений. Для функции f справедлива лемма 2.3.3, то есть существует квадрат, на одной из вершин которого принимается уникальное значение a: $f(\alpha_1,\dots,\alpha_{i-1},x,\alpha_{i+1},\dots,\alpha_{j-1},y,\alpha_{j+1},\dots,\alpha_n)$ равно a при $x=\alpha$ и $y=\beta$. Рассмотрим функции, существенно зависящие от одной переменной, и принимающие не более $k-1$ значения, заведомо содержащиеся в исходной системе

$$t_1(x)=\begin{cases}\alpha & x=0,\\ \beta & x\neq 0,\end{cases}\qquad t_2(y)=\begin{cases}\beta & y=0,\\ \alpha & y\neq 0,\end{cases}\qquad t(z)=\begin{cases}0 & z=a,\\ 1 & z\neq a.\end{cases}$$

и возьмем третью от f, на местах переменных x и y у которой стоят первые две:

$$t\left(f\left(\alpha_1,\dots,\alpha_{i-1},t_1(x),\alpha_{i+1},\dots,\alpha_{j-1},t_2(y),\alpha_{j+1},\dots,\alpha_n\right)\right)=\vee_{0,1}(x,y).$$

Эту функцию назовем дизъюнкцией x и y. По аналогии построим конъюнкцию:

$$\&_{0,1}(x,y)=j_0\left(\vee_{0,1}\left(j_0(x),j_0(y)\right)\right).$$

Для функции произвольной $f(\tilde{x}^n)\not\equiv\text{const}$, принимающей только значения 0 и 1, построим формулу, ее реализующую:

$$f(\tilde{x}^n)=\bigvee_{\substack{(\alpha_1,\dots,\alpha_n)\\ f(\alpha_1,\dots,\alpha_n)=1}} j_{\alpha_1}(x_1)\cdot j_{\alpha_2}(x_2)\cdots j_{\alpha_n}(x_n).$$

Теперь можно реализовать и любую функцию, принимающую *любые* два значения: если $f(\tilde{x}^n)$ принимает два значения σ_1 и σ_2, то, используя функцию $h(x)=\begin{cases}\sigma_1 & x=0,\\ \sigma_2 & x\neq 0\end{cases}\in CS_k$, можно реализовать f формулой

$$h\left(\bigvee_{\substack{(\alpha_1,\dots,\alpha_n)\\ f(\alpha_1,\dots,\alpha_n)=1}} j_{\alpha_1}(x_1)\cdot j_{\alpha_2}(x_2)\cdots j_{\alpha_n}(x_n)\right).$$

Предположение индукции. Пусть реализованы все $f\in P_k$, принимающие не более $l-1$ различных значений.

Индуктивный переход. Реализуем произвольную функцию $g(\tilde{y}^m)$, принимающую l различных значений $\tau_1,\dots,\tau_l$. Разделим два случая.

1. $l-1\leqslant k-2$. Реализуем существенную функцию, принимающую $l\leqslant k-1$ различных значений. По основной лемме найдутся наборы

$$l\left\{\begin{array}{rlll} 3\left\{\begin{array}{llll}(\alpha,\alpha_2,\dots,\alpha_n) & \widetilde{\beta}_1 & \delta_1\\ (\beta,\alpha_2,\dots,\alpha_n) & \widetilde{\beta}_2 & \delta_2\\ (\alpha,\gamma_2,\dots,\gamma_n) & \widetilde{\beta}_3 & \delta_3\end{array}\right.\\ l-3\left\{\begin{array}{llll}(\beta_1^4,\beta_2^4,\dots,\beta_n^4) & \widetilde{\beta}_4 & \delta_4\\ \dots\dots\dots\dots\dots & & \\ \dots\dots\dots\dots & \widetilde{\beta}_l & \delta_l\end{array}\right.\end{array}\right.,$$

на которых функция f принимает l различных значений. Далее $s_i(\tilde{y}^m)$ — функции, принимающие $l-1$ значение.

$y_1,\ldots,y_m$	g	$s_1(\tilde{y}^m)\,s_2(\tilde{y}^m)\ldots s_n(\tilde{y}^m)$	$f(s_1,\ldots,s_n)$	$n(f(\tilde{s}))$
…	τ_1	$\widetilde{\beta}_1$	δ_1	τ_1
…	τ_2	$\widetilde{\beta}_2$	δ_2	τ_2
…	$\vdots$	$\vdots$	$\vdots$	$\vdots$
…	τ_l	$\widetilde{\beta}_l$	δ_l	τ_l

Таким образом, во всех столбцах, составленных из i-х разрядов наборов $\widetilde{\beta}_i$, находится не более, чем $l-1$ значение. Применим к различным значениям δ_i функцию $n(x)=\begin{pmatrix}\delta_1 & \delta_2 & \ldots & \delta_l\\ \tau_1 & \tau_2 & \ldots & \tau_l\end{pmatrix}$, принадлежащую классу CS_k, следовательно, находящуюся в исходной системе.

2. $l=k$. В этом случае последнего шага не нужно:

$y_1,\ldots,y_m$	g	$s_1(\tilde{y}^m)\,s_2(\tilde{y}^m)\ldots s_n(\tilde{y}^m)$	$f(s_1,\ldots,s_n)$
…	0	$\widetilde{\beta}_1$	0
…	1	$\widetilde{\beta}_2$	1
…	$\vdots$	$\vdots$	$\vdots$
…	$k-1$	$\widetilde{\beta}_l$	$k-1$

Действительно, если все значения различны, и принадлежат множеству $\{0,1,\ldots,k-1\}$, то каждое из них принимается ровно по одному разу, и все наборы $\widetilde{\beta}_i$ можно упорядочить так, чтобы получить желаемый порядок в последнем столбце.

■

В качестве следствия теоремы 2.6 можно привести более слабый критерий полноты:

Теорема 2.7 (И. Слупецкий). *Система функций, содержащая все одноместные функции) полна тогда и только тогда, когда она содержит существенную функцию, принимающую все k значений.*

Обозначим через $h_{i,j}(x)$ перестановку значений i и j. Очевидно, $h_{0,1}(x)=x+j_0(x)+J_1(x)$. Легко проверить справедливость следующего утверждения:

Теорема 2.8 (С. Пикар). *Следующие системы полны в $P_k^{(1)}$:*

1. $\{\bar{x},h_{0,1}(x),x+j_0(x)\}$,
2. $\{h_{0,1}(x),h_{0,2}(x),\ldots,h_{0,k-1}(x),x+j_0(x)\}$.

Теорема 2.9 (критерий шефферовости). *Функция f является шефферовой тогда и только тогда, когда из нее можно получить все функции от одной переменной, принимающие не более $k-1$ значения (класс CS_k).*

□ *Док-во.* Необходимость в данном случае очевидна. Покажем достаточность. Поскольку все константы принадлежат CS_k, функция принимает все k значений. Докажем, что она существенная от противного: пусть она не является существенной. Возможны два случая:

1. у f вообще нет существенных переменных, следовательно, она константа, что невозможно;
2. у f ровно одна существенная переменная, следовательно, она является перестановкой, то есть $f\in S_k\Rightarrow[f]\subseteq S_k$ и из нее нельзя получить константы.

Таким образом, f существенная и по теореме 2.6 система $\{f\}$ полна. ■

Примеры. Используя критерий Слупецкого, доказать полноту в P_k нижеприводимых систем:

1. $\{k-1,x-y+2,x^2\dot{-}y\}$

□ *Решение.* Очевидно, что $x-y+2$ — существенная функция, принимающая все k значений. Далее, $(k-1)^2\dot{-}(k-1)=0$, $(k-1)^2\dot{-}0=1$, $x-1+2=x+1=\bar{x}$, $0+1=1$, $1^2-x=j_0(x)$. Также есть все константы и все j_i, $x-(y+2)+2=x-y$, $x-\underbrace{y-\cdots-y}_{k-1}=x+y\Rightarrow\underbrace{j_1(x)+\cdots+j_1(x)}_{k-1}=J_1(x)$, $h_{0,1}(x)=x+j_0(x)+J_1(x)$, также имеется $x+j_0(x)$. Следовательно, исходная система содержит систему Софи Пикар 1 и является полной по теореме 2.7. ■

2. $\{(1\dot{-}x)\cdot y+\bar{x}\cdot(1\dot{-}y)\}$

□ *Решение.* Обозначим $f(x,y)=(1\dot{-}x)\cdot y+\bar{x}\cdot(1\dot{-}y)$.

$$f(x,x)=j_0(x),\ f(x,j_0(x))=\bar{x},\ j_0(f(j_0(x),x))=0,$$
$$f(0,x)=x+j_0(x),\ f(j_1(x),x)=h_{0,1}(x),$$

получена система Софи Пикар 1. В то же время функция существенно зависит от обеих переменных и принимает все k значений, следовательно, является шефферовой по теореме 2.7. ■

3. $\{j_2(x),x+y^2,x\cdot y+1\}$

□ *Решение.* Функция $x\cdot y+1$ — существенная и принимает все k значений. Далее, $j_2(j_2(x))=0$, $0\cdot 0+1=1$, $x+1^2=\bar{x}$, откуда можно получить все $j_i(x)$, $x+j_0^2(x)=x+j_0(x)$, $x+\underbrace{j_1^2(x)+\cdots+j_1^2(x)}_{k-1}+j_0(x)=h_{0,1}(x)$. Следовательно, исходная система содержит систему Софи Пикар 1 и является полной по теореме 2.7. ■

4. $\{x\dot{-}y,(\sim x)-y\}$

□ *Решение.* Усеченная разность является существенной функцией, принимающей все k значений. Далее, $x\dot{-}x\equiv 0$, $(\sim 0)-0=k-1$, $(k-1)-y=\sim y$, $(\sim(\sim x))-y=x-y$, $x-\underbrace{y-\cdots-y}_{k-1}=x+y$, $(\ldots(x\dot{-}\underbrace{1)\dot{-}\cdots)\dot{-}1}_{k-2}=j_{k-1}(x)$, $0-(k-1)=1$, $x+1=\bar{x}$, следовательно есть все $j_i(x)$, а, следовательно, есть и $x+j_0(x)$, и $h_{0,1}(x)=x+j_0(x)+\underbrace{j_1(x)+\cdots+j_1(x)}_{k-1}$. Следовательно, исходная система содержит систему Софи Пикар 1 и является полной по теореме 2.7. ■

5. $\{j_1(x),\bar{x}-y,x^2-y\}$

□ *Решение.* Функция $\bar{x}-y$ является существенной и принимает все k значений. Далее, $\bar{x}-x\equiv 1$, $1^2-1=0$, $\bar{x}-0=\bar{x}$, следовательно, получены все константы, суммы вида $x+i$ и $j_i(x)$, $x-\underbrace{y-\cdots-y}_{k-1}=x+y$, $h_{0,1}(x)=x+j_0(x)+\underbrace{j_1(x)+\cdots+j_1(x)}_{k-1}$. Следовательно, исходная система содержит систему Софи Пикар 1 и является полной по теореме 2.7. ■

6. $\{\bar{x},j_0(x),x\cdot y\}$

□ *Решение.* Произведение является существенной функцией, принимающей все k значений. $x\cdot j_0(x)\equiv 0$, следовательно, есть все константы и все $j_i(x)$. Далее рассмотрим функцию

$$f(x)=(1+(x-1)\,j_1(x))\,(1+(x-1)\,j_2(x))\cdots(1+(x-1)\,j_{k-1}(x))$$

и заметим, что она равна как раз $x+j_0(x)$. Осталось увидеть, что $h_{0,1}(x)=f(x)\cdot j_0(j_1(x))$. Следовательно, исходная система содержит систему Софи Пикар 1 и является полной по теореме 2.7. ■

Упражнения. Используя критерий Слупецкого, доказать полноту в P_k нижеприводимых систем:

1. $\{x-1,(x+j_0(x))\cdot(1\dot{-}y)+(1\dot{-}x)\cdot(y-j_1(x))\}$;
2. $\{\bar{x}\cdot j_0(x-y)+(x-j_1(x))\cdot j_0(y)+y\cdot j_0(x)\}$;
3. $\{j_0(x-y)+x\cdot j_0(y)+(\bar{x}-j_1(x))\cdot j_1(y)\}$;
4. $\{x\cdot j_0(y)+j_0(x)\cdot(y+j_0(y)-j_1(y))+j_1(x)\cdot(\bar{y}-j_0(y))\}$;
5. $\{\bar{y}\cdot j_0(x)+j_1(x)\cdot(y+j_0(y))+j_1(y)\cdot(j_2(x)-j_1(x))\}$.

2.4 Особенности многозначных логик

Представление функции k-значной логики полиномами. Рассматриваются функции k-значной логики при $k \geqslant 3$ и исследуется вопрос об их представимости полиномами. Известно, что если $f(\tilde{x}^n) \not\equiv 0$, то ее можно представить во второй форме:

$$f(\tilde{x}^n) = \sum_{\substack{(\alpha_1,\ldots,\alpha_n) \\ f(\alpha_1,\ldots,\alpha_n)\neq 0}} f(\alpha_1,\ldots,\alpha_n)\cdot j_{\alpha_1}(x_1)\cdot j_{\alpha_2}(x_2)\cdots j_{\alpha_n}(x_n).$$

Из этого следует, что если все j_i представить полиномами, то $f(\tilde{x}^n)$ также представится полиномом. Очевидно, справедливо и обратное, то есть $\forall f \in \mathbf{Pol} \Leftrightarrow \forall j_i(x) \in \mathbf{Pol}$, а поскольку $j_i(x) = j_0(x-i)$, то задача представимости полиномом любой функции сводится к задаче представимости j_0. Полином функции одного переменного $f(x) = a_0 + a_1 x + \cdots + a_{k-1}x^{k-1}$ можно пытаться найти методом неопределенных коэффициентов:

$$\begin{cases} a_0 & = f(0), \\ a_0 + a_1 + a_2 + \cdots + a_{k-1} & = f(1), \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & \\ a_0 + a_1 s + a_2 s^2 + \cdots + a_{k-1}s^{k-1} & = f(s), \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & \\ a_0 + a_1(k-1) + a_2(k-1)^2 + \cdots + a_{k-1}(k-1)^{k-1} & = f(k-1). \end{cases}$$

Это — линейная система k уравнений с k неизвестными, матрица которой является матрицей Вандермонда:

$$\begin{pmatrix} 1 & 1^2 & \ldots & 1^{k-1} \\ 2 & 2^2 & \ldots & 2^{k-1} \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots \\ k-1 & (k-1)^2 & \ldots & (k-1)^{k-1} \end{pmatrix}$$

Определитель этой матрицы равен $\prod\limits_{0\leqslant j<i\leqslant k-1}(i-j) \pmod k$ и отличен от нуля при простых k. Получим $j_0(x)$ при простых k.

Теорема 2.10 (П. Ферма, малая). *Пусть p — простое. Тогда для любого a такого, что $1 \leqslant a \leqslant p-1$ выполняется $a^{p-1} \equiv 1 \pmod p$.*

□ *Док-во.* Все равенства в дальнейшем подразумеваются по модулю p. Пусть a удовлетворяет условию теоремы. Рассмотрим набор чисел вида $a\cdot 1, a\cdot 2, \ldots, a\cdot(p-1)$. Очевидно, они все различны и не равны нулю. В то же время среди них содержатся в каком-то порядке все числа $1,2,\ldots,p-1$ (по модулю p). Перемножим их всех и получим $a^{p-1}(p-1)! = (p-1)! \pmod p \Rightarrow a^{p-1} \equiv 1 \pmod p$. ■

По теореме 2.10 нетрудно сообразить, как при простых значениях $k = p$ будет выглядеть полином для функции $j_0(x)$: $j_0(x) = 1 - x^{p-1}$. Таким образом, получено, что при простых значениях k любая функция представима полиномом.

Пусть теперь k — составное. Докажем результат от противного: пусть $j_0(x) = a_0 + a_1 x + \cdots + a_s x^s$. Тогда $j_0(0) = 1 \Rightarrow a_0 = 1$. Пусть $0 \neq k_1 \mid k \Rightarrow j_0(k_1) = 1 + a_1 k_1 + \cdots + a_s k_1^s = 0 \Rightarrow a_1 k_1 + \cdots + a_s k_1^s = k-1 \Rightarrow k_1 \mid k-1$, чего не может быть при $k \geqslant 3$. Объединить два полученных выше результата можно в следующей теореме.

Теорема 2.11. *Класс функций, представимых полиномами полон тогда и только тогда, когда k — простое.*

Теоремы о замкнутых классах в P_k при $k \geqslant 3$. В P_2 любой замкнутый класс имеет конечный базис, следовательно, замкнутых классов в P_2 — счетное множество. В P_k при $k \geqslant 3$ ситуация совершенно другая.

Теорема 2.12 (Янов). *В P_k при $k \geqslant 3$ существует замкнутый класс, не имеющий базиса.*

□ *Док-во.* Построим этот класс. Определим последовательность функций следующим образом: $f_0 = 0$, для $i = \overline{1,\infty}$

$$f_i = f_i(x_1,\ldots,x_i) = \begin{cases} 1 & x_1 = x_2 = \cdots = x_i = 2, \\ 0 & \text{иначе.} \end{cases}$$

$\mathscr{F} = \{f_0, f_1, \ldots, f_m, \ldots\}$. Рассмотрим все функции, получаемые из этих переименованием переменных без отождествления, это множество обозначим $\mathscr{M}$. Докажем по индукции, что класс $\mathscr{M}$ замкнут. Для $i = 1$ это очевидно. Пусть теперь это верно для $i \leqslant n$, докажем для $i = n+1$. Рассмотрим $f(\mathfrak{A}_1,\ldots,\mathfrak{A}_i)$. Если среди $\mathfrak{A}_1,\ldots,\mathfrak{A}_i$ есть хотя бы одна формула, то функция является тождественным нулем и принадлежит $\mathscr{M}$. Если же все $\mathfrak{A}_j$ различные переменные, то функция получается из некоторой функции $\mathscr{F}$ переименованием переменных без отождествления, то есть принадлежит $\mathscr{M}$.

Предположим, что у $\mathscr{M}$ существует базис. Тогда в нем существует функция $f(y_1,\ldots,y_{n_0})$, имеющая наименьшее число существенных переменных n_0 среди всех функций базиса. Тогда возможны два различных случая.

1. Существует еще одна функция $f(u_1,\dots,u_n)$, зависящая от $n \geqslant n_0$ существенных переменных. Тогда первую функцию можно получить из этой переименованием переменных с отождествлением.

2. В базисе одна функция. Если это константа 0, то это не базис, следовательно, она должна иметь существенные переменные. В этом случае любая суперпозиция $f(\mathfrak{A}_1,\dots,\mathfrak{A}_n)$, содержащая формулы на местах переменных, реализует тождественный ноль, а не содержащая формулы, зависит не более, чем от n переменных, то есть суперпозициями нельзя получить функцию f_m, существенно зависящую от $m > n$ переменных.

■

Теорема 2.13 (Мучник). *В P_k при $k \geqslant 3$ существует замкнутый класс со счетным базисом.*

□ *Док-во.* Построим этот класс. Пусть $\mathscr{F} = \{f_2, f_3, \dots, f_i, \dots\}$, где

$$f_i(x_1,\dots,x_i) = \begin{cases} 1 & x_1 = x_2 = \dots = x_{j-1} = x_{j+1} = \dots = x_i = 2,\ x_j = 1, j = \overline{1,i} \\ 0 & \text{иначе.} \end{cases}$$

Рассмотрим замыкание $\mathscr{M} = [\mathscr{F}]$. Докажем, что $\mathscr{F}$ — базис. Действительно, $\mathscr{F}$ полна в $\mathscr{M}$. Покажем, что из $\mathscr{F}$ нельзя удалить ни одну из функций. Пусть для $m \neq n$ существует $f_n(x_1,\dots,x_n) = f_m(\mathfrak{A}_1,\dots,\mathfrak{A}_m)$. Возможны три случая:

1. Среди $\mathfrak{A}_i$ есть хотя бы две формулы. Тогда они обе принимают значения 0 и 1 и

$$f_m(\mathfrak{A}_1,\dots,\mathfrak{A}_m) \equiv 0$$

), но $f_n(x_1,\dots,x_n) \not\equiv 0$. Противоречие.

2. Среди $\mathfrak{A}_i$ есть ровно одна формула. Тогда при $m \geqslant 2$ существует место, где есть символ переменной x_l, $1 \leqslant l \leqslant n$. Тогда на наборе $x_l = 1, x_i = 2\ (l \neq l)$ $f_n = 1, f_m = 0$. Противоречие.

3. Все $\mathfrak{A}_i$ суть символы переменных. Тогда для $m > n$ ввиду существенности каждой переменной f_n неизбежны повторы, и есть два места с x_l. На наборе $x_l = 1, x_i = 2\ (i \neq l)$ $f_n = 1, f_m = 0$. Противоречие.

■

Построенный в теореме 2.13 замкнутый класс не имеет конечных базисов. Из хода доказательства видно, что если взять бесконечную систему $\mathscr{F}' = \{f_{i_1}, f_{i_2}, \dots, f_{i_s}, \dots\}$, то замкнутый класс $\mathscr{M}' = [\mathscr{F}']$ будет иметь также счетный базис $\mathscr{F}'$, то есть разные подпоследовательности $\mathscr{F}$ порождают разные замкнутые классы. Таким образом, справедливо следующее утверждение.

Следствие 2.4.1 (из теоремы 2.13). *Число замкнутых классов в P_k при $k \geqslant 3$ равно континуум.*

Примеры.

1. Разложить в полином по модулю k функцию f из P_k:

   (a) $f = 2x \dot{-} x^2, k = 5$

   □ *Решение.* Эта функция задает подстановку $\begin{pmatrix} 0 & 1 & 2 & 2 & 4 \\ 0 & 1 & 0 & 0 & 2 \end{pmatrix}$. Представим ее во второй форме: $2x \dot{-} x^2 = j_1(x) + 2j_4(x) = j_0(x-1) + 2j_0(x-4) = j_0(x-1) + 2j_0(x+1) = 1 - (x-1)^4 + 2 - 2(x-4)^4 = 3 - x^4 + 4x^3 - 6x^2 + 4x - 1 - 2x^4 - 8x^3 - 12x^2 - 8x - 2 = 2x^4 + x^3 + 2x^2 + x.$ ■

   (b) $f = \max(2x \dot{-} y, x \cdot y), k = 3$

   □ *Решение.* Таблица этой функции имеет следующий вид:

x \ y	0	1	2
0	0	0	0
1	2	1	2
2	1	2	1

   Теперь легко видеть, что эта функция просто равна $xy + 2xj_0(y) = xy + 2x(1 - y^2) = xy^2 + xy + 2x$. ■

   (c) $f = \min(x^2, y), k = 3$

□ *Решение.* Таблица этой функции имеет следующий вид:

x \ y	0	1	2
0	0	0	0
1	0	1	1
2	0	1	1

Теперь легко видеть, что эта функция просто равна x^2y^2. ■

2. Выяснить, представима ли полиномом по модулю k функция f из P_k, если:

(a) $f = 2(J_1(x) + J_4(x)), k = 6$

□ *Решение.* Эта функция задает подстановку $\begin{pmatrix} 0 & 1 & 2 & 2 & 4 & 5 \\ 0 & 4 & 0 & 0 & 4 & 0 \end{pmatrix}$. Выпишем табличку степеней по модулю 6 с тем, чтобы ограничить степень искомого полинома:

x	0	1	2	3	4	5
x^0	1	1	1	1	1	1
x^1	0	1	2	3	4	5
x^2	0	1	4	3	4	1
x^3	0	1	2	3	4	5

Легко видеть, что начиная с кубов все степени повторяют стоящие на две строки выше. Следовательно, достаточно ограничиться квадратами. Поскольку функция сохраняет ноль, искать ее полином будем в виде $ax^2 + bx$. Решим соответствующую систему линейных уравнений:

$$\left.\begin{array}{cc|c} 1 & 1 & 4 \\ 2 & 4 & 0 \\ 3 & 3 & 0 \\ 4 & 4 & 4 \\ 5 & 0 & 0 \end{array}\right. \sim \left.\begin{array}{cc|c} 1 & 1 & 4 \\ 0 & 2 & 4 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 2 & 4 \end{array}\right. \sim \left.\begin{array}{cc|c} 1 & 1 & 4 \\ 0 & 2 & 4 \end{array}\right. \Rightarrow \left[\begin{array}{l} a = 2, b = 2; \\ a = 5, b = 5. \end{array}\right.$$

Таким образом, $f(x) = 2x^2 + 2x = 5x^2 + 5x$ при $k = 6$. ■

(b) $f = (\max(x,y) - \min(x,y))^2, k = 4$

□ *Решение.* Если $x > y$, то выражение в скобках равно $x - y$, иначе оно равно $y - x$, но в любом случае его квадрат равен $(x-y)^2 = x^2 - 2xy + y^2 = x^2 + (k-2)xy + y^2$, при $k = 4$: $x^2 + 2xy + y^2$. Заметим, что данная функция представима полиномом при любом значении k. ■

(c) $f = 3j_0(x), k = 6$

□ *Решение.* Эта функция задает подстановку $\begin{pmatrix} 0 & 1 & 2 & 2 & 4 & 5 \\ 0 & 4 & 0 & 0 & 4 & 0 \end{pmatrix}$. Как было показано в примере 2a, достаточно ограничиться квадратами. Также, поскольку $f(0) = 3$, полином имеет смысл искать в виде $3 + ax + bx^2$. Решим соответствующую систему линейных уравнений:

$$\left.\begin{array}{cc|c} 1 & 1 & 3 \\ 2 & 4 & 0 \\ 3 & 3 & 0 \\ 4 & 4 & 0 \\ 5 & 0 & 0 \end{array}\right. \sim \left.\begin{array}{cc|c} 1 & 1 & 3 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \\ 0 & 0 & 0 \\ 0 & 2 & 3 \end{array}\right.$$

Третья строчка показывает, что решений нет. ■

3. Доказать, что приводимые ниже системы полны в P_k тогда и только тогда, когда k — простое число:

(a) $\{1, x+y+x\cdot z\}$

□ *Решение.* Очевидно, что при составных k система не полна, так как состоит из полиномов. При $k = 2$ система сохраняет единицу, так что в дальнейшем k — простое и нечетное. Имеем $1 + y + 1 \cdot 1 = y + 2$, $x + \underbrace{2 + \cdots + 2}_{\frac{p+1}{2}} = x + 1$. Из этого можно получить все константы, $x + y + x \cdot 0 = x + y$, $x + 0 + x \cdot y = x(y+1)$, $x(y + (k-1) + 1) = xz$. Получен базис системы полиномов — умножение, сложение и константа 1, следовательно, при простых k система полна. ■

(b) $\{x-y+1, x^2-y, x\cdot y^2\}$

□ *Решение.* Поскольку все представленные в системе функции — полиномы, она не полна при составных значениях k. При $k=2$ система полна, так как первая функция не сохраняет ноль, не самодвойственная и не монотонная, вторая не сохраняет единицу, а третья нелинейная, так что в дальнейшем k простое и нечетное. Имеем $x-x+1\equiv 1$, $1^2-1=0$, $x-0+1=x+1$, следовательно, есть все константы и все функции вида $x+i$. Теперь получаем функцию $x+\underbrace{(k-1)y+1+\cdots+(k-1)y+1}_{k-1}=x+y+k-1$, откуда $x+y+1+k-1=x+y$. Далее, $1\cdot x^2=x^2$, $(x+y)^2-\left(x^2+y^2\right)=2xy$, $\underbrace{2xy+\cdots+2xy}_{\frac{k+1}{2}}=xy$. Получен базис системы полиномов — умножение, сложение и константа 1, следовательно, при простых k система полна. ■

(c) $\{1+x_1-x_2+x_1\cdot x_2\cdots x_k\}$

□ *Решение.* Поскольку все представленные в системе функции — полиномы, она не полна при составных значениях k. В дальнейшем k простое. Имеем, $1+x-x+x^k=x+1$, $1+x-\bar{x}+x\cdot\bar{\bar{x}}\cdots(x+(k-1))\equiv 0$, $1+x_1-x_2+x_1x_2\cdot 0\cdots 0=1+x_1-x_2$, $1+x_1-(x_2+1)=x_1-x_2$, $x_1-\underbrace{x_2-\cdots-x_2}_{k-1}=x_1+x_2$, $1+x_1-1+x_1\cdot 1\cdots 1\cdot x_2=x_1+x_1x_2$, $x_1+x_1x_2-x_1=x_1x_2$. Получен базис системы полиномов — умножение, сложение и константа 1, следовательно, при простых k система полна. ■

Упражнения.

1. Разложить в полином по модулю k функцию f из P_k:
   (a) $f=\min\left(x^2,x^3\right),k=5$;
   (b) $f=\max\left(2x\dot{-}1,x^2\right),k=5$;
   (c) $f=3x\dot{-}\left(x\dot{-}2x\right),k=7$;
   (d) $f=\max\left(\left(x\dot{-}1\right)^2,x^3\right),k=7$;
   (e) $f=x\dot{-}y,k=3$;
   (f) $f=J_{k-2}(x),k$ — произвольное простое число;
   (g) $f=j_2\left(x-x^2\right),k$ — произвольное простое число.
2. Выяснить, представима ли полиномом по модулю k функция f из P_k, если:
   (a) $f=3x\dot{-}2x^2,k=4$;
   (b) $f=(x\dot{-}y)\dot{-}y,k=4$.
3. Доказать, что приводимые ниже системы полны в P_k тогда и только тогда, когда k — простое число:
   (a) $\{x-1,x+y,x^2\cdot y\}$;
   (b) $\{k-1,x\cdot y+x-y+z\}$;
   (c) $\{k-2,x+2y,x\cdot y^2\}$;
   (d) $\{\sim x,x-y,x^2\cdot y\}$;
   (e) $\{x-2,x+2y+1,x\cdot y-x-y\}$;
   (f) $\{1,2x+y,x\cdot y^2-x+y\}$;
   (g) $\{x+y+1,x\cdot y-x^2\}$;
   (h) $\{x-2y,x\cdot y+x+1\}$.