Дискретная математика

Конспекты лекций М. Н. Вялого,
ПМИ ФКН ВШЭ, 1 курс, основной поток, 2020/21 уч.г.

Версия от 20 ноября 2020 г.

Файл пополняется по мере чтения лекций. Просьба о замеченных ошибках и неточностях сообщать автору (адрес `vyalyi`⟨стандартный суффикс gmail⟩).

Оглавление

Лекция 1

Алгебра логики

Для занятий математикой важно отличать осмысленные утверждения от бессмысленных, а среди осмысленных утверждений различать истинные и ложные.

Для первого математики дают ясные и недвусмысленные определения используемых в утверждениях слов. Каждый математический термин означает лишь то, что указано в его определении. Например, совершенное число равно сумме всех своих делителей, которые меньше самого числа (например, $6 = 1+2+3$). Никаких отсылок к смыслу слова «совершенный» в обыденном языке в математических рассуждениях о совершенных числах не допускается.

Для второго математики используют доказательства — рассуждения по правилам формальной логики, которые объясняют, почему из истинности одних утверждений следует истинность других утверждений.

Мы сейчас познакомимся с примерами доказательств и с самыми началами формализма, придуманного математиками для доказательств.

1.1 Булевы функции–1. Логические связки и доказательства

В элементарной алгебре очень много доказательств имеют вид вычислений.

Пример 1.1. Тождество $x^2 - y^2 = (x - y)(x + y)$ доказывается цепочкой равенств:

$$(x - y)(x + y) = (x - y)x + (x - y)y = x^2 - yx + xy - y^2 = x^2 - y^2$$

(на самом деле, часть равенств пропущена). Каждое равенство использует одно из основных свойств арифметических операций с числами. □

Аналогично этим доказательствам-вычислениям, можно строить «алгебраические» доказательства и в более общем случае так называемой алгебры высказываний.

Мы считаем, что высказывание обязательно либо истинно, либо ложно (в противном случае фраза не является высказыванием). Из высказываний можно строить составные высказывания, используя *логические связки*.

Значения составных высказываний определяются в зависимости от связки по таблицам истинности. Приведём таблицы истинности самых употребительных связок: конъюнкции $\wedge$ «A и B», дизъюнкции $\vee$ «A или B», импликации (логическое следование: «если A, то B», «из A следует B», обозначение $\to$) и равносильности $\equiv$ «A равносильно B».

A	B	$A \wedge B$	$A \vee B$	$A \to B$	$A \equiv B$
Л	Л	Л	Л	И	И
Л	И	Л	И	И	Л
И	Л	Л	И	Л	Л
И	И	И	И	И	И

Заметим, что аргументы в импликации не симметричны, в отличие от остальных связок. Им поэтому присвоены специальные названия: в импликации $A \to B$ высказывание A называется *посылкой*, а высказывание B — *заключением*.

Таблица истинности импликации требует комментариев. На впечатлительные умы производит сильное впечатление тот факт, что из лжи следует истина. Однако, более точно сказать, что из лжи следует что угодно, не только истина, но и ложь.

Таблица истинности импликации вполне согласуется с бытовым применением конструкции «если ..., то ...». Представим себе, что кто-то делает следующее заявление: «Если я завтра заболею, то не приду на занятия». Если на следующий день этот человек не заболел и пришёл на занятия, следует ли считать, что он соврал? А если он не заболел и не пришёл? И то, и другое было бы странно, ведь человек и вовсе ничего не говорил про этот случай. Нечто содержательное было сказано только для той ситуации, когда он заболел. Так что, если посылка импликации ложна, то и в обычной жизни утверждение считают истинным.

Приведём аналогичный пример из математики. Рассмотрим утверждение «если число n делится на 4, то n чётно». Это утверждение верно. И оно не перестанет быть верным, если вместо произвольного числа подставить какое-нибудь конкретное, например 6. Посылка утверждения становится ложной, 6 не делится на 4, но само утверждение остаётся истинным.

Ещё одна постоянно используемая связка: отрицание «не A» (обозначение $\neg$). Таблица отрицания очень простая: $\neg$Л = И, $\neg$И = Л.

Логические тождества выражают законы логики. Если истинно утверждение, выражающееся левой частью тождества, то истинно и утверждение, выражающееся правой частью тождества. И наоборот. Части логического тождества соединяют знаком $\equiv$ и называют *равносильными* утверждениями.

Давайте рассмотрим пример такого закона логики, который применяется во всех доказательствах. По таблицам истинности легко проверить, что

$$(A \wedge (A \to B)) \to B \equiv \text{И}. \tag{1.1}$$

Это тождество мы используем всякий раз, когда из истинности высказывания A и составного высказывания «если A, то B» мы заключаем, что истинно B. Это

логическое правило, на латыни называемое modus ponens, лежит в основе всех математических рассуждений.

Составные высказывания, которые истинны при любых значениях входящих в них элементарных высказываний, называются *тавтологиями*. Высказывание в левой части (1.1) — пример тавтологии.

Помимо механической проверки тождества по таблицам истинности можно применить такой приём доказательств, как *разбор случаев*. Тут важно не пропустить какой-нибудь случай, иначе доказательство будет неполным.

Доказательство тождества 1.1 разбором случаев. Пусть $B = \mathsf{И}$. Из таблицы импликации видим, что $X \to \mathsf{И} \equiv \mathsf{И}$. Поэтому левая часть истинна.

Пусть $B = \mathsf{Л}$. Из таблицы импликации видим, что $X \to \mathsf{Л} = \neg X$. Поэтому левая часть приобретает вид $(A \wedge \neg A) \to \mathsf{Л} = \neg(A \wedge \neg A)$. Поскольку любое высказывание либо истинно, либо ложно, $A \wedge \neg A = \mathsf{Л}$, а $\neg(A \wedge \neg A) = \mathsf{И}$. □

В этом доказательстве возникло тождественно ложное высказывание $A \wedge \neg A$, которое называется *противоречием*. Если мы имеем противоречие — два противоположных высказывания «A» и «не A», — то по modus ponens мы можем вывести ложь, так как $(A \wedge \neg A) \to \mathsf{Л} \equiv \mathsf{И}$. А из лжи мы уже выведем что угодно. Это объясняет, почему математики так беспокоятся об отсутствии противоречий. Любое противоречие позволяет утверждать, что истинно любое высказывание.

Одним из популярных приёмов доказательств являются *доказательства от противного*. Допустим, мы хотим доказать утверждение A. Для этого мы выводим из его отрицания $\neg A$ противоречие, то есть доказываем, что некоторое высказывание B одновременно истинно и ложно. Другими словами, мы доказываем истинность составного высказывания $\neg A \to (B \wedge \neg B)$. Заключение этой импликации ложно. Поскольку сама импликация истинна, то и её посылка ложна. То есть, A истинно, что и требовалось доказать.

Пример 1.2. Приведём простой пример доказательства от противного. Докажем такое утверждение[1)]: если $a_1 + \cdots + a_n > n$, то какое-то из этих чисел больше 1.

Действительно, пусть $a_i \leqslant 1$ для всех i. Складывая эти неравенства, получаем, что $a_1 + \cdots + a_n \leqslant n$. Пришли к противоречию. □

Одной из важнейших тавтологий является *транзитивность* импликации:

$$\big((A \to B) \wedge (B \to C)\big) \to (A \to C) \equiv \mathsf{И}. \tag{1.2}$$

Это логическое тождество позволяет строить длинные цепочки вывода, аналогичные вычислениям в примере 1.1. Однако во многих случаях структура математических доказательств сложнее, она нелинейная.

[1)] Утверждение кажется очевидным, но мы уже говорили, что математики панически боятся противоречий. Поэтому «очевидные» утверждения нуждаются в доказательствах. В какой-то момент придётся остановиться и признать некоторые утверждения истинными, не давая им доказательств. В данном случае мы принимаем без доказательств свойства арифметических операций и сравнений чисел.

Доказательство (1.2) *от противного.* Предположим ложность левой части (1.2). Из таблицы истинности импликации видим, что заключение $A \to C$ внешней импликации ложно, а посылка $(A \to B) \wedge (B \to C)$ истинна.

Из ложности $A \to C$ заключаем, что $A = \mathsf{И}$, $C = \mathsf{Л}$. Истинность конъюнкции означает, что истинны оба члена конъюнкции, в частности $B \to C = B \to \mathsf{Л} = \mathsf{И}$. Это возможно лишь при $B = \mathsf{Л}$. Но тогда $A \to B = \mathsf{И} \to \mathsf{Л} = \mathsf{Л}$, а мы уже установили, что $A \to B = \mathsf{И}$. Пришли к противоречию. □

Ещё один важный приём доказательств основан на тавтологии, которая называется *законом контрапозиции*:

$$A \to B \equiv \neg B \to \neg A. \tag{1.3}$$

Доказательство тождества 1.3. Левая часть ложна тогда и только тогда, когда $A = \mathsf{И}$, $B = \mathsf{Л}$.

Правая часть ложна тогда и только тогда, когда $\neg B = \mathsf{И}$, $\neg A = \mathsf{Л}$. Но это равносильно первым двум условиям. Поэтому значения левой и правой части всегда одинаковы. □

Контрапозиция используется как логический шаг в очень многих доказательствах, у нас дальше будет много таких примеров. Пока приведём один несложный пример.

Пример 1.3. Докажем такое утверждение: если неотрицательное число x иррациональное, то и $\sqrt{x}$ иррациональное.

Закон контрапозиции говорит, что это утверждение равносильно такому: если $\sqrt{x}$ рациональное, то и x рациональное. А это уже легко доказать: пусть $\sqrt{x} = n/m$, где числитель и знаменатель целые. Тогда

$$x = \sqrt{x} \cdot \sqrt{x} = \frac{n}{m} \cdot \frac{n}{m} = \frac{n^2}{m^2}$$

также рациональное. □

Важным примером тавтологий являются *законы де Моргана.* Они позволяют строить высказывания, равносильные отрицанию конъюнкции или дизъюнкции:

$$\neg(A \wedge B) \equiv \neg A \vee \neg B; \quad \neg(A \vee B) \equiv \neg A \wedge \neg B. \tag{1.4}$$

Доказательство тождеств (1.4). Первое. Отрицание конъюнкции ложно тогда и только тогда, когда конъюнкция истинна, то есть $A = B = \mathsf{И}$. Дизъюнкция ложна тогда и только тогда, когда каждый её член ложен, то есть $\neg A = \neg B = \mathsf{Л}$. Эти условия равносильны.

Второе. Отрицание дизъюнкции истинно тогда и только тогда, когда дизъюнкция ложна, то есть $A = B = \mathsf{Л}$. Конъюнкция истинна тогда и только тогда, когда каждый её член истинен, то есть $\neg A = \neg B = \mathsf{И}$. Эти условия равносильны. □

Для конъюнкции и дизъюнкции выполняется много тавтологий, напоминающих свойства обычных арифметических операций. Все они легко доказываются аналогично рассмотренным выше тавтологиям.

Коммутативность конъюнкции, дизъюнкции:

$$A \wedge B \equiv B \wedge A, \quad A \vee B \equiv B \wedge A.$$

Ассоциативность тех же связок:

$$(A \wedge B) \wedge C \equiv A \wedge (B \wedge C), \quad (A \vee B) \vee C \equiv A \vee (B \vee C).$$

Дистрибутивность (тут даже лучше, чем с числами — есть две тавтологии):

$$(A \wedge B) \vee C \equiv (A \vee C) \wedge (B \vee C), \quad (A \vee B) \wedge C \equiv (A \wedge C) \vee (B \wedge C).$$

Этими простыми логическими тождествами законы логики не исчерпываются. В математике нужны ещё законы логики, позволяющие оперировать с кванторами: *квантором всеобщности* $\forall x A(x)$ («для всех x истинно утверждение $A(x)$» и *квантором существования* $\exists x A(x)$ («существует такое x, что $A(x)$ истинно». Систематическое изучение логики с кванторами мы откладываем до второго курса.

Пока лишь скажем, что квантор $\forall$ — это в сущности конъюнкция (по возможным значениям x), а квантор $\exists$ — дизъюнкция. Законы де Моргана позволяют строить утверждения, равносильные отрицаниям утверждений с кванторами

$$\neg\forall x A(x) \equiv \exists x \neg A(x), \qquad \neg\exists x A(x) \equiv \forall \neg A(x).$$

Эти логические правила вам потребуются всюду в математике.

Лекция 2

Множества, индукция

2.1 Множества–1. Операции с множествами

Множества лежат в основе формального языка математики. Мы сейчас дадим краткие и неформальные объяснения свойств множеств и операций с ними. Таких неформальных объяснений будет достаточно почти для всех тем этого курса. Для лучшего понимания советуем прочитать более подробные книги о множествах. Хорошим введением в теорию множеств является книга Верещагина и Шеня «Начала теории множеств».

Множество — это совокупность каких-то *элементов*. Природа элементов неважна. Никакие взаимоотношения между элементами не важны. Единственное, что существенно — какие элементы в входят в множество, а какие — нет.

Множество полностью определяется своими элементами. Два множества A и B называются *равными*, если каждый элемент множества A является элементом множества B, а каждый элемент множества B является элементом множества A. Множество A является *подмножеством* множества B, если каждый элемент множества A принадлежит множеству B (обозначение $A \subseteq B$). Высказывание «элемент x *принадлежит* множеству A» (обозначение $x \in A$) истинно, если в A есть элемент x, и ложно в противном случае.

Пример 2.1 (Пустое множество)**.** Есть такое множество, которому не принадлежит ни один элемент. Оно называется *пустым множеством* и обозначается $\varnothing$. Высказывание $x \in \varnothing$ ложно для любого x.

Конечное множество можно задать списком его элементов. Хотя на письме мы вынуждены записывать множества в каком-то порядке, этот порядок не имеет значения, как и возможные повторения элементов. Принято заключать список элементов в фигурные скобки.

Пример 2.2. Множество чётных цифр может быть задано такими способами

$$\{0, 2, 4, 6, 8\} = \{4, 2, 0, 8, 6\} = \{2, 2, 4, 6, 8, 6, 0, 2\}.$$

Списки разные, но задают они одно и то же множество. □

Из уже имеющегося множества можно выделить подмножество, указав некоторое свойство элементов. При таком определении множеств обычно используется запись вида

$$\{x \in \mathbb{Z} \mid x = 2y,\ y \in \mathbb{Z}\}$$

или

$$\{x \in \mathbb{Z} : x = 2y,\ y \in \mathbb{Z}\}.$$

В этих формулах $\mathbb{Z}$ обозначает множество целых чисел. Обе формулы определяют множество чётных чисел.

Ещё один способ строить новые множества из уже имеющихся состоит в применении к множествам *операций*.

Перечислим основные операции с множествами.

Объединение множеств. Обозначение $A \cup B$. Это множество, состоящее в точности из тех элементов, которые принадлежат хотя бы одному из множеств A и B. В формальной записи это определение выглядит так:

$$A \cup B = \{x : (x \in A) \vee (x \in B)\}. \tag{2.1}$$

Пересечение множеств. Обозначение $A \cap B$. Это множество, состоящее в точности из тех элементов, которые принадлежат обоим множествам A и B. В формальной записи это определение выглядит так:

$$A \cap B = \{x : (x \in A) \wedge (x \in B)\}. \tag{2.2}$$

Разность множеств. Обозначение $A \setminus B$. Это множество, состоящее в точности из тех элементов, которые принадлежат множеству A, но не принадлежат множеству B. В формальной записи это определение выглядит так:

$$A \setminus B = \{x : (x \in A) \wedge \neg(x \in B)\}. \tag{2.3}$$

Симметрическая разность множеств. Обозначение $A \triangle B$. Это множество, состоящее в точности из тех элементов, которые принадлежат ровно одному из множеств: либо A, либо B. В формальной записи это определение выглядит так:

$$A \triangle B = \Big\{x : \big((x \in A) \wedge \neg(x \in B)\big) \vee \big(\neg(x \in A) \wedge (x \in B)\big)\Big\}. \tag{2.4}$$

Помимо словесных определений, приведённых выше, есть наглядный графический способ иллюстрировать операции с множествами: круги Венна (иногда говорят Эйлера–Венна). При этом способе множество изображается условным кругом (или другой геометрической фигурой) и предполагается, что внутренность круга изображает элементы множества.

На паре кругов легко изобразить объединение, пересечение, разность и симметрическую разность множеств, как это сделано на рисунке 2.1. Для этого результат применения операции выделяют штриховкой или цветом.

Есть ещё одна часто используемая операция с множествами — дополнение к множеству (обозначение $\bar{A}$) определяют обычно как те элементы, которые не входят в

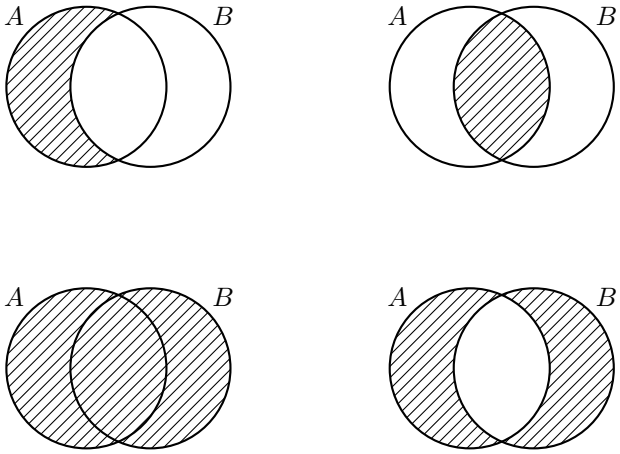


Рис. 2.1: Теоретико-множественные операции на кругах Венна

множество A. Однако буквально такое определение несодержательно. Операция дополнения всегда используется в рассуждениях о подмножествах одного множества U, которое будем называть *универсумом*. В таком контексте дополнение $\bar{A}$ даёт сокращённую запись для разности $U \setminus A$.

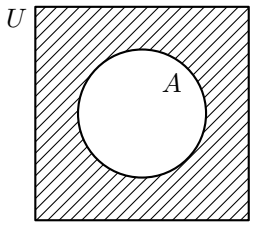


Рис. 2.2: Дополнение $\bar{A} = U \setminus A$ на рисунке заштриховано

2.2 Множества–2. Тавтологии и теоретико-множественные тождества

Между операциями с множествами и логическими связками есть соответствие. Предположим, что все рассматриваемые множества являются подножествами универсума U. Каждому множеству A и каждому элементу U сопоставляется высказывание $x \in A$. Это высказывание истинно для элементов A и ложно для остальных элементов универсума. Из формальных определений операций с множествами (2.1),

(2.2), (2.3) получаем такие эквивалентности

$$(x \in A \cup B) \equiv (x \in A) \vee (x \in B),$$
$$(x \in A \cap B) \equiv (x \in A) \wedge (x \in B),$$
$$(x \in A \setminus B) \equiv (x \in A) \wedge \neg(x \in B),$$
$$(x \in \bar{A}) \equiv \neg(x \in A).$$

Равенство множеств A и B, как уже говорилось, равносильно эквивалентности высказываний $x \in A$ и $x \in B$. Поэтому любой тавтологии взаимно однозначно отвечает некоторое теоретико-множественное тождество, то есть утверждение о том, что применение теоретико-множественных операций в разном порядке даёт одно и то же множество.

Пример 2.3. Докажем, что равенство

$$(A \cap B) \setminus C = (A \setminus C) \cap B$$

выполняется для любых множеств. Для этого запишем соответствующую логическую формулу:

$$(A \wedge B) \wedge \neg C \equiv (A \wedge \neg C) \wedge B.$$

Эта формула является тождеством, потому что конъюнкция коммутативна и ассоциативна. □

Что соответствует импликации на языке множеств? Посмотрев на таблицу значений, видим, что импликация истинна тогда и только тогда, когда элемент принадлежит второму множеству ИЛИ не принадлежит первому. То есть, теоретико-множественная операция, отвечающая импликации, записывается как $\bar{A} \cup B$.

У импликации есть ещё один важный смысл на языке множеств. Утверждение «если $x \in A$, то $x \in B$» (любой элемент A входит в B) выполняется для всех x тогда и только тогда, когда $A \subseteq B$, мы так определяли подмножества. Поэтому импликации соответствует включение множеств (а равносильности соответствует равенство множеств).

Пример 2.4. Что означает тавтология транзитивности импликации

$$(A \to B) \wedge (B \to C) \to (A \to C) \equiv \mathsf{И}$$

на языке множеств? Заменим часть импликаций на включение, получим утверждение «если A — подмножество B и B — подмножество C, то A — подмножество C», истинное для всех множеств.

Другой способ понимать эту тавтологию менее интересный: для любых подмножеств A, B, C множества U выполняется равенство

$$\overline{(\bar{A} \cup B) \cap (\bar{B} \cup C)} \cup (\bar{A} \cup C) = U.$$

Конечно, это равенство можно проверить, исходя из определений или на кругах Венна. □

2.3 Индукция–1

Одним из важнейших способов доказательства в дискретной математике являются доказательства по индукции. Это способ доказать *бесконечно много утверждений* одним рассуждением.

Рассмотрим простой пример.

Пример 2.5. Пусть нужно вычислить $1+2+\cdots+1000$. Неужели придётся выполнить 999 арифметических операций? Не обязательно, достаточно трёх операций:

$$1 + 2 + \cdots + 1000 = \frac{1000 \cdot (1000 + 1)}{2}\,.$$

Как убедиться, что правая часть даёт искомую сумму? Способов много. Все они так или иначе дают доказательство общей формулы

$$1 + 2 + \cdots + n = \sum_{i=1}^{n} i = \frac{n(n+1)}{2}\,. \tag{2.5}$$

Мы сейчас будем рассуждать так. Заметим, что формула (2.5) выполняется для первых нескольких сумм:

$$1 = 1 = \frac{1 \cdot 2}{2}\,,$$
$$1 + 2 = 3 = \frac{2 \cdot 3}{2}\,.$$

Теперь докажем *условное* утверждение: если формула (2.5) выполняется для n, то она выполняется и для $n+1$. Для этого делаем вычисления, как обычно в элементарной алгебре:

$$1 + 2 + \cdots + n + (n+1) = \Big(1 + 2 + \cdots + n\Big) + (n+1) =$$
$$= \frac{n(n+1)}{2} + (n+1) = \frac{n(n+1) + 2(n+1)}{2} = \frac{(n+1)(n+2)}{2}\,.$$

При переходе ко второй строчке мы используем формулу (2.5), которая по условию верна. В результате этого вычисления получаем, что формула (2.5) верна и для $n+1$.

И это всё! Завершает доказательство магическая фраза «по принципу математической индукции формула (2.5) верна для всех n». □

Обсудим суть этого принципа подробнее. Он основан на двух простых фактах. Во-первых, мы в прошлый раз обсуждали транзитивность импликации. Поэтому из сколь угодно длинной цепочки логических равенств

$$A_1 = \mathsf{И},$$
$$A_1 \to A_2 = \mathsf{И},$$
$$\cdots$$
$$A_n \to A_{n+1} = \mathsf{И}$$

следует, что $A_{n+1} = \mathsf{И}$.

Во-вторых, у целых положительных чисел есть такое свойство: прибавлением 1 можно получить любое целое положительное число. Отсюда и получается тот самый

> **Принцип математической индукции**. Пусть для последовательности утверждений
>
> $$A_1, A_2, A_3, \ldots, A_n, \ldots,$$
>
> занумерованных целыми положительными числами, верны утверждения
>
> **База индукции:** A_1 истинно.
>
> **Шаг индукции:** $A_n \to A_{n+1}$ истинно для любого n. Посылку импликации A_n называют *индуктивным предположением*.
>
> Тогда A_n истинно для любого n.

В примере 2.5 базой индукции является равенство $1 = 1 \cdot 2/2$, а шагом индукции — утверждение «для любого n, если (2.5) верна для n, то (2.5) верна и для $n+1$». Мы доказали оба эти утверждения. Значит, (2.5) выполняется для всех n.

Приведём ещё один простой пример доказательства по индукции.

Пример 2.6. Докажем, что для любых $q \neq 1$ и целого положительного n выполняется равенство

$$1 + q + q^2 + \cdots + q^n = \sum_{i=0}^{n} q^i = \frac{q^{n+1} - 1}{q - 1}\,. \tag{2.6}$$

База индукции (здесь первое число равно 0, так бывает и ничего не меняет в рассуждении, кроме номеров утверждений):

$$1 = \frac{q^{0+1} - 1}{q - 1}\,.$$

Тут и доказывать нечего, конечно, это верное равенство.

Индуктивный переход: «если (2.6) верно для n, то оно верно для $n+1$». Доказательство вычислением

$$\begin{aligned} &1 + q + \cdots + q^n + q^{n+1} = \left(1 + q + \cdots + q^n\right) + q^{n+1} = \\ =&\frac{q^{n+1} - 1}{q - 1} + q^{n+1} = \frac{q^{n+1} - 1 + q^{n+1}(q-1)}{q-1} = \\ =&\frac{q^{n+1} - 1 + q^{n+2} - q^{n+1}}{q-1} = \frac{q^{n+2} - 1}{q-1}\,. \end{aligned}$$

По принципу математической индукции формула (2.6) выполняется для всех целых неотрицательных n. □

Ещё один пример применения индукции: доказательство «принципа кроликов» или, как было раньше принято говорить в русской литературе, «принципа Дирихле».

Пример 2.7 (Принцип кроликов)**.** Если $k > n$ и k кроликов рассажены по n клеткам, то хотя бы в одной клетке сидит хотя бы два кролика.

Давайте запишем это утверждение в числах. Занумеруем клетки и пусть в клетку с номером i посажено r_i кроликов. Тогда принцип формулируется так: если $k > n$ и $r_1 + \cdots + r_n = k$, то для какого-то i выполняется неравенство $r_i > 1$.

Доказываем индукцией по n.

База: если $k > 1$ и $r_1 = k$, то $r_1 > 1$. Очевидно выполняется.

Индуктивный переход: пусть принцип кроликов верен для n. Докажем его для $n+1$. Пусть $k > n+1$ и $r_1 + \cdots + r_n + r_{n+1} = k$. Доказательство разбором случаев.

Если $r_{n+1} > 1$, то всё доказано: искомая клетка имеет номер $n+1$.

Если $r_{n+1} \leqslant 1$, то $r_1 + \cdots + r_n = k - r_{n+1} \geqslant k - 1 > n$. Значит, по принципу кроликов для n клеток найдётся такое i, что $r_i > 1$. □

Замечание 2.1. Принцип кроликов можно доказать иначе. Вспомним, что в прошлый раз мы доказали, что среднее не больше максимума. То есть из неравенства $r_1 + \cdots + r_n = k > n$ следует требуемое: для какого-то i выполняется $r_i > 1$.

У рассуждений, основанных на индукции, есть много вариантов. Вот поучительный пример.

Пример 2.8 (Числа Фибоначчи)**.** Рассмотрим *последовательность Фибоначчи*

$$1,\ 1,\ 2,\ 3,\ 5,\ 8,\ 13,\ 21,\ 34, \ldots,$$

в которой первые два числа равны единице, а каждое следующее равно сумме двух предыдущих. Обычный способ задания таких *рекуррентных* последовательностей выглядит так: $F_0 = 1$; $F_1 = 1$; $F_{n+2} = F_{n+1} + F_n$ для всех $n \geqslant 2$.

Докажем для чисел Фибоначчи формулу:

$$F_n = \frac{\varphi^{n+1} - \psi^{n+1}}{\sqrt{5}}, \quad \text{где} \quad \varphi = \frac{1+\sqrt{5}}{2}, \quad \psi = \frac{1-\sqrt{5}}{2}. \tag{2.7}$$

Эта формула верна для $n = 0$:

$$1 = F_0 = \frac{\varphi^{0+1} - \psi^{0+1}}{\sqrt{5}} = \frac{(1+\sqrt{5}) - (1-\sqrt{5})}{2\sqrt{5}}\,.$$

Верна она и для $n = 1$:

$$1 = F_1 = \frac{\varphi^{0+2} - \psi^{0+2}}{\sqrt{5}} = \frac{(\varphi-\psi)(\varphi+\psi)}{\sqrt{5}} = \frac{\sqrt{5}\cdot 1}{\sqrt{5}}\,.$$

Как доказать формулу (2.7) для всех n? Давайте для любого значения n докажем такое условное утверждение: если (2.7) верна для n и для $n+1$, то (2.7) верна для $n+2$.

Для этого заметим, что φ, ψ — корни квадратного уравнения $x^2 - x - 1 = 0$, то есть $\varphi^2 = \varphi + 1$ и $\psi^2 = \psi + 1$. Используя это наблюдение, получаем:

$$F_{n+2} = F_{n+1} + F_n = \frac{\varphi^{n+2} - \psi^{n+2}}{\sqrt{5}} + \frac{\varphi^{n+1} - \psi^{n+1}}{\sqrt{5}} =$$
$$= \frac{1}{\sqrt{5}}\Big(\varphi^{n+2} + \varphi^{n+1} - \psi^{n+2} - \psi^{n+1}\Big) = \frac{1}{\sqrt{5}}\Big(\varphi^{n+1}(\varphi+1) - \psi^{n+1}(\psi+1)\Big) =$$
$$= \frac{1}{\sqrt{5}}\big(\varphi^{n+3} - \psi^{n+3}\big).$$

Как теперь закончить рассуждение? Буквально принцип математической индукции не говорит о такой ситуации. Чтобы закончить рассуждение, обозначим через A_n высказывание «(2.7) верна для n» и рассмотрим серию составных высказываний $B_n = A_n \wedge A_{n+1} \to A_{n+2}$. Мы доказали истинность B_1 и для любого n истинность импликации $B_n \to A_{n+2}$. Но последняя равносильна импликации $B_n \to B_{n+1}$ (проверьте!). Значит, по принципу математической индукции все B_n истинные. Но тогда и все A_n истинные. То есть формула (2.7) верна для всех n. □

Мы будем использовать более общие формы индукции.

Принцип полной математической индукции. Пусть для последовательности утверждений

$$A_1, A_2, A_3, \ldots, A_n, \ldots,$$

занумерованных целыми положительными числами, истинны утверждения

База индукции: A_1 истинно.

Шаг индукции: $(A_1 \wedge \ldots \wedge A_n) \to A_{n+1}$ истинно для любого n.

Тогда A_n истинно для любого n.

Разница с обычным принципом математической индукции в том, что на шаге индукции предполагается, что все предыдущие утверждения истинны, а не только самое последнее.

Справедливость принципа полной математической индукции вытекает из справедливости обычного принципа математической индукции. Аккуратное доказательство этого факта оставляется в качестве упражнения. Удобно при этом использовать ещё одну равносильную формулировку принципа математической индукции.

Принцип наименьшего числа. Любое непустое подмножество натуральных чисел содержит наименьший элемент.

Лекция 3

Комбинаторика–1

В прошлый раз мы доказали формулу (2.5) для суммы первых n целых положительных чисел. Но мы не обсуждали, откуда эта формула берётся. Это общая проблема с доказательствами по индукции: если уже есть удачное утверждение, то его доказательство по индукции обычно не очень трудно провести. Но как догадаться до правильного утверждения?

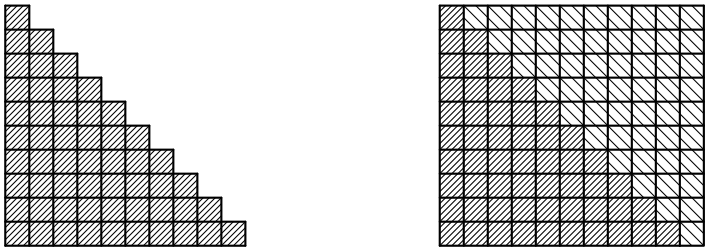
В случае формулы (2.5) есть несколько способов догадаться.

Группировка. Давайте запишем сумму двумя способами — как обычно и задом наперёд, — располагая слагаемые друг под другом:

$$\begin{array}{lll} 1+2 & + \cdots + & n \\ n+(n-1) & + \cdots + & 1 \end{array}$$

Видно, что соответственные слагаемые всегда дают в сумме $n+1$, а всего таких слагаемых n. Значит, удвоенное значение суммы равно $n(n+1)$.

Картинка. Есть наглядный способ нарисовать это рассуждение. Сумму $1+2+\cdots+n$ нарисуем в виде рядов квадратиков, поставленных один на другой. Получается «зубчатый треугольник», см. Рис. 3.1(a). Если приложить к этому треугольнику точно такой же, но повернутый треугольник, получится прямоугольник со сторонами n и $n+1$. В нём $n(n+1)$ клеточек и это ровно в два раза больше количества клеточек в треугольнике.



(a) (b)

Рис. 3.1: Дополнение треугольника до прямоугольника

Это простейший пример подсчётов, которыми занимается *перечислительная комбинаторика*. Мы сегодня разберём основные правила таких подсчётов и простые примеры их использования.

3.1 Правило произведения. Декартово произведение множеств

В примере выше использовано одно из главных правил перечислительной комбинаторики: *правило произведения*. Оно по сути говорит, что в клетчатом прямоугольнике со сторонами n и k ровно nk клеточек.

Во многих случаях нужно ещё увидеть прямоугольник среди данных задачи. Поэтому удобнее сформулировать это правило более общим образом. Для такой формулировки нам потребуется новая операция с множествами.

Декартово произведение множеств. Обозначение $A \times B$. Это множество, состоящее в точности из всех упорядоченных пар (a, b), где $a \in A$; $b \in B$.

Если множества конечны, то декартово произведение можно нарисовать в виде прямоугольника: столбцы — элементы A, строки — элементы B, на пересечении столбца a и строки b расположена пара $(a, b) \in A \times B$.

Отсюда получаем формулировку для правила произведения. Договоримся обозначать через $|A|$ количество элементов в множестве A, обычно оно называется *мощностью множества* (иногда — размером множества).

> **Правило произведения**. Для конечных множеств A, B выполняется равенство $|A \times B| = |A| \cdot |B|$.

Доказать правило произведения можно индукцией по мощности A.

База: $|A| = 0$, то есть $A = \varnothing$. По определению $\varnothing \times B = \varnothing$ (нет ни одной пары, первый член которой был бы элементом пустого множества). Поэтому $|\varnothing \times B| = |\varnothing| = 0 = |\varnothing| \cdot |B|$ — верное равенство.

Шаг индукции: пусть правило произведения справедливо для множеств мощности n. Рассмотрим пару A, B, где $|A| = n + 1$. Выделим в A какой-нибудь элемент a_{n+1} и обозначим через $A' = A \setminus \{a_{n+1}\}$ множество остальных элементов. Из каких пар состоит декартово произведение $A \times B$? Это либо пары вида (a, b), $a \in A'$, $b \in B$, либо пары (a_{n+1}, b), $b \in B$. Первых по предположению индукции $n \cdot |B|$ штук, а вторых — $|B|$ штук. Значит, всего в $A \times B$ входит $n \cdot |B| + |B| = (n+1) \cdot |B| = |A| \cdot |B|$ пар.

Шаг индукции доказан. По принципу математической индукции правило произведения выполняется для всех (конечных) множеств A, B.

3.2 Последовательности

В определении декартова произведения множеств появился новый объект, который будет постоянно возникать как в этом курсе, так и в других математических курсах.

Что такое упорядоченная пара? Это *последовательность* длины 2. Последовательности отличаются от множеств тем, что они образуют список своих элементов (ещё говорят, *членов* последовательности). Последовательности обозначают либо перечислением через запятую, либо, для наглядности, окружают их круглыми скобками. А иногда и попросту записывают элементы подряд, если можно отличить один от другого. Положение в списке важно: последовательности совпадают в том и только том случае, когда их длины (количество членов) равны и на каждом месте в обеих последовательностях стоит один и тот же элемент.

Пример 3.1. $(1,2) \neq (2,1)$; $(1,1,1) \neq (1,1)$. Последний пример показывает, что в последовательности элементы могут повторяться.

Важнейший для дискретной математики пример последовательностей: *слова в алфавите* A. Это произвольные последовательности конечной длины, члены которых принадлежат множеству A.

Всё множество слов в алфавите A обозначается A^*, а множество слов длины n обозначается A^n. В любом алфавите есть одно особое слово длины 0 — *пустое слово*, оно обычно обозначается ε. Это последовательность, в которой нет ни одного члена.

Теорема 3.1. *Количество слов длины n в конечном алфавите A равно $|A|^n$.*

Доказательство. Индукция по n.

База: $n = 0$. Пустое слово одно, $|A^0| = 1 = |A|^0$.

Шаг индукции. Пусть уже доказано, что $|A^n| = |A|^n$.

Рассмотрим слова длины $n+1$ и докажем, что они по сути совпадают с декартовым произведением $A \times A^n$.

Для любого слова α однозначно определены «голова» — первый член α_1 и «хвост» — остальные члены последовательности, они образуют последовательность длины на единицу меньше. Скажем, у слова 1012 головой является 1, а хвостом — 012.

И наоборот: по символу $a \in A$ и слову α однозначно получается слово $a\alpha$, длина которого на единицу больше: запишем слово α после символа a, то есть составим последовательность, первый член которой равен a, второй равен первому члену слова α и т.д.

Значит, мы можем представить слова длины $n+1$ как клеточки прямоугольника, строкам которого отвечают символы алфавита, а столбцам — слова длины n. Поэтому $|A^{n+1}| = |A \times A^n|$.

Применяя правило произведения и индуктивное предположение, получаем

$$|A^{n+1}| = |A| \cdot |A^n| = |A| \cdot |A|^n = |A|^{n+1},$$

что и требовалось доказать для шага индукции.

По принципу математической индукции количество слов длины n равно $|A|^n$ для любого n. □

3.3 Правило суммы

Всем ясно, что если в кошельке лежит 5 пятирублёвых монет и 6 десятирублёвых (и больше ничего), то всего в кошельке 11 монет.

Столь же ясно, что если в группе студентов 20 человек ездят на электричке и 20 человек подключены к Теле2, то это не означает, что в группе по крайней мере 40 человек. Может быть намного меньше.

Различать эти два случая при подсчётах важно. Сформулируем первый из них в виде правила.

> **Правило суммы**. Для конечных *непересекающихся* множеств A, B (то есть $A \cap B = \varnothing$) выполняется равенство $|A \cup B| = |A| + |B|$.

Заметим, что это правило мы неявно применили в доказательстве правила произведения, но не упомянули об этом.

Можно ли *доказать* правило суммы или нужно признать его исходным постулатом (аксиомой, как ещё говорят)? По существу ясно, что доказывать тут нечего: правило суммы фактически говорит о том, как *определяется* сложение целых неотрицательных чисел.

Правило суммы позволяет разделять подсчёт на случаи. Как и в доказательствах разбором случаев важно, чтобы все варианты были учтены. Но теперь не менее важно, чтобы каждый вариант учитывался ровно один раз.

3.4 Монотонные пути по прямой

Рассмотрим такую общую ситуацию. Есть клетчатая лента, по которой можно двигать фишку. Клетки пронумерованы целыми числами. В начале фишка находится в клетке 0. Далее её можно сдвигать вправо. Нужно подсчитать, сколько есть различных способов попасть в клетку с номером n.

Ответ зависит от того, какие ходы разрешены. Например, если разрешено сдвигать фишку только на одну клетку, то способ единственный. Для каждого набора разрешённых ходов получается своя задача подсчёта. Такие задачи в большинстве своём решаются однотипно. Правило суммы приводит к рекуррентному соотношению. Если угадать ответ, то доказать его можно методом математической индукции.

Пример 3.2. Пусть разрешены ходы на одну и на две клетки.

Задачу можно переформулировать на языке последовательностей целых чисел. А именно, нужно подсчитать количество монотонно возрастающих последовательностей целых чисел, первый член которых равен 0, последний равен n, а разность между двумя соседними принимает только значения 1 или 2. Действительно, такие последовательности — это протоколы движения фишки по клеточкам. Каждому способу движения отвечает ровно одна последовательность и по ней этот способ движения так же однозначно определяется.

Обозначим количество таких последовательностей F_n. Заметим, что $F_{n+2} = F_{n+1} + F_n$. Действительно, все последовательности, заканчивающиеся на $n+2$, разделяются на две непересекающиеся группы:

$$0, \ldots, n, n+2;$$
$$0, \ldots, n+1, n+2$$

(в клетку $n+2$ можно попасть либо с клетки n, либо с клетки $n+1$, на месте многоточий возможно вставить любую последовательность чисел, в которой разности между соседними числами равны 1 или 2).

Нетрудно подсчитать количество таких последовательностей при небольших n.

$\boldsymbol{n = 0}$**.** Единственная монотонная последовательность, начинающаяся и заканчивающаяся на 0: это 0. Поэтому $F_0 = 1$.

$\boldsymbol{n = 1}$**.** Единственная монотонная последовательность, начинающаяся на 0 и заканчивающаяся на 1: это 0,1. Поэтому $F_1 = 1$.

$\boldsymbol{n = 2}$**.** Монотонных последовательностей, начинающихся на 0 и заканчивающаяся на 2 уже две: это 0,1, 2 и 0, 2. Поэтому $F_2 = 2$.

Теперь становится понятно обозначение: мы получили рекурренту и начальные условия для чисел Фибоначчи. Для любого n количество способов попасть в n ходами длины 1 или 2 равно F_n.

Пример 3.3. Пусть разрешены ходы на любое количество клеток.

На языке последовательностей целых чисел мы хотим найти количество всех монотонно возрастающих последовательностей целых чисел, первый член которых равен 0, а последний равен n. Обозначим это количество $T(n)$.

Количество таких последовательностей при $n \leqslant 2$ такое же, как и в предыдущем примере: $T(0) = 1$; $T(1) = 1$; $T(1) = 2$. (Ограничения на длину шага выполняются в этих случаях для любой последовательности.)

При росте n количество вариантов растёт и уже легко ошибиться в подсчёте. Однако можно доказать общий факт:

$$T(n) = T(n-1) + T(n-2) + \cdots + T(0) \tag{3.1}$$

для любого n.

Обозначим множество всех последовательностей длины n через X. Разделим последовательности на группы, в зависимости от последнего хода. То есть группу X_i образуют те монотонные последовательности, которые имеют вид

$$0, \ldots, i, n.$$

Ясно, что каждая последовательность попала ровно в одну группу и группы не пересекаются (смотрим на последний ход или на предпоследний член последовательности). По правилу суммы получаем

$$|X| = |X_0| + |X_2| + \cdots + |X_{n-1}|.$$

Но, с другой стороны, $|X_i| = T(i)$ (монотонные последовательности, начинающиеся в 0 и заканчивающиеся в i). Отсюда и получается формула (3.1).

Используя формулу (3.1), докажем индукцией по n явную формулу для $T(n)$:

$$T(n) = 2^{n-1} \qquad \text{при } n \geqslant 1. \tag{3.2}$$

База уже доказана.

Индуктивный переход. Если равенство $T(n) = 2^{n-1}$ верно, то

$$\begin{aligned} T(n+1) &= T(n) + T(n-1) + T(n-2) + \cdots + T(0) = \\ &= T(n) + T(n) = 2^{n-1} + 2^{n-1} = 2^n = \\ &= 2^{(n+1)-1}. \end{aligned}$$

В первом равенстве использована формула (3.1), которая верна для всех n.

3.5 Формула включений–исключений

Теперь рассмотрим общую ситуацию, в которой варианты не взаимно исключающие. Другими словами, мы хотим определить мощность объединения множеств. В общем случае она не определяется однозначно размерами самих множеств.

Для случая двух множеств ответ такой.

Утверждение 3.2. $|A \cup B| = |A| + |B| - |A \cap B|$.

Доказательство. Пересчитаем все элементы A и все элементы B. Получим $|A|+|B|$. Элементы $|A \cap B|$, и только они, подсчитаны дважды. Значит, $|A \cup B|$ меньше $|A|+|B|$ на $|A \cap B|$. □

Для трёх множеств формула сложнее.

Утверждение 3.3. $|A \cup B \cup C| = |A|+|B|+|C|-|A \cap B|-|A \cap B|-|B \cap C|+|A \cap B \cap C|$.

Доказательство. Несколько раз применим формулу для объединения двух множеств.

Представим $A \cup B \cup C$ как $(A \cup B) \cup C$, получим

$$|A \cup B \cup C| = |A \cup B| + |C| - |(A \cup B) \cap C|. \tag{3.3}$$

Воспользуемся дистрибутивностью объединения и пересечения (дизъюнкции и конъюнкции): $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$. Применяем ещё раз формулу для объединения двух множеств:

$$|(A \cup B) \cap C| = |(A \cap C) \cup (B \cap C)| = |A \cap C| + |B \cap C| - |(A \cap C) \cap (B \cap C)|.$$

Легко увидеть, что $(A \cap C) \cap (B \cap C) = A \cap B \cap C$. Теперь подставляем полученное в (3.3) и получаем

$$|A \cup B \cup C| = |A \cup B| + |C| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$

Теперь применим ещё раз формулу для $|A \cup B|$ и получим искомое выражение. □

Формулы для двух и трёх множеств подсказывают общий вид формулы включений-исключений. Нужно взять сумму мощностей всех множеств. Некоторые элементы при этом посчитаны более одного раза. Поэтому нужно вычесть мощности попарных пересечений множеств, после чего некоторые элементы объединения вообще не будут посчитаны. Далее нужно последовательно прибавлять и вычитать мощности тройных, четверных и т.д. пересечений, включая их в итоговую сумму с чередующимися знаками.

Теорема 3.4 (Формула включений–исключений)**.**

$$\begin{aligned}|A_1 \cup A_2 \cup \ldots \cup A_n| = |A_1| + \ldots + |A_n| - \\ - |A_1 \cap A_2| - |A_1 \cap A_3| - \ldots \\ + |A_1 \cap A_2 \cap A_3| + |A_1 \cap A_2 \cap A_4| + \ldots \\ \ldots \\ + (-1)^{n+1}|A_1 \cap A_2 \cap \ldots \cap A_n|\end{aligned} \tag{3.4}$$

В первой строчке правой части равенства выписаны мощности всех множеств. Во второй — мощности всех попарных пересечений множеств (со знаком минус). Далее выписываем пересечения троек, четвёрок и т.д. множеств с чередующимися знаками.

Доказательство формулы включений-исключений. Индукция по количеству множеств. База: формула для двух множеств (да и для одного годится).

Шаг индукции в точности следует доказательству формулы для трёх множеств (и использует формулу для объединения двух множеств). Предполагаем, что (3.4) верна для любых n множеств. Рассмотрим набор из $n+1$ множеств: $A_1, \ldots, A_{n+1}$. Нам нужно доказать для этого набора равенство (3.4), что означает

$$\begin{aligned}|A_1 \cup A_2 \cup \ldots \cup A_n \cup A_{n+1}| = |A_1| + \ldots + |A_n| + |A_{n+1}| - \\ - |A_1 \cap A_2| - |A_1 \cap A_3| - \ldots - |A_n \cap A_{n+1}| \\ + |A_1 \cap A_2 \cap A_3| + |A_1 \cap A_2 \cap A_4| + \ldots \\ \ldots \\ (-1)^{n+2}|A_1 \cap A_2 \cap \ldots \cap A_n \cap A_{n+1}|.\end{aligned} \tag{3.5}$$

Запишем формулу для объединения двух множеств:

$$\begin{aligned}|A_1 \cup A_2 \cup \ldots \cup A_{n+1}| = |(A_1 \cup A_2 \cup \ldots \cup A_n) \cup A_{n+1}| = \\ = |(A_1 \cup A_2 \cup \ldots \cup A_n)| + |A_{n+1}| - |(A_1 \cup A_2 \cup \ldots \cup A_n) \cap A_{n+1}|.\end{aligned} \tag{3.6}$$

Применим формулу для объединения n множеств к первому слагаемому в (3.6). Получим те слагаемые из (3.5), в которые входят только множества $A_1, \ldots, A_n$.

Второе слагаемое в (3.6) равно $|A_{n+1}|$, такое же слагаемое есть и в (3.5).

Остальные слагаемые в (3.5) равны мощностям пересечения A_{n+1} с какими-то из множеств $A_1, \ldots, A_n$. Нужно убедиться, что третье слагаемое в (3.6) содержит те же слагаемые с теми же знаками.

В силу дистрибутивности пересечения и объединения множество в третьем слагаемом записывается как

$$(A_1 \cup A_2 \cup \ldots \cup A_n) \cap A_{n+1} = (A_1 \cap A_{n+1}) \cup (A_2 \cap A_{n+1}) \cup \cdots \cup (A_n \cup A_{n+1}).$$

Обозначим $B_i = A_i \cap A_{n+1}$. Тогда третье слагаемое в (3.6) равно $-|B_1 \cup \cdots \cup B_n|$. Применим индуктивное предположение (с учётом перемены знака) и получим

$$\begin{aligned} -|B_1 \cup B_2 \cup \ldots \cup B_n| = &-|B_1| - \ldots - |B_n| + \\ &+ |B_1 \cap B_2| + |B_1 \cap B_3| + \ldots + |B_{n-1} \cap B_n| - \\ &- |B_1 \cap B_2 \cap B_3| - |B_1 \cap B_2 \cap B_4| - \ldots \\ &\ldots \\ &- (-1)^{n+1} |B_1 \cap B_2 \cap \ldots \cap B_n|. \end{aligned} \tag{3.7}$$

Нам нужно ещё одно теоретико-множественное тождество

$$(A_1 \cap A_k) \cap (A_2 \cap A_k) \cap \cdots \cap (A_{k-1} \cup A_k) = A_1 \cap A_2 \cap \cdots \cap A_k,$$

которое легко проверяется раскрытием скобок и применением очевидного из определения равенства $A \cap A = A$.

В силу этого тождества в правой части (3.7) написаны пересечения каких-то множеств $A_1, \ldots, A_n$ и (обязательно) множества A_{n+1}. Это в точности те слагаемые, которых нам недоставало в равенстве (3.5).

Проверим, что они входят с правильными знаками.

Так как $B_{i_1} \cup \cdots \cup B_{i_s} = A_{i_1} \cup \cdots \cup A_{i_s} \cup A_{n+1}$, то мощность этого множества входит в (3.7) со знаком $-(-1)^{s+1}$, а в (3.5) — со знаком $(-1)^{(s+1)+1} = -(-1)^{s+1}$. Знаки совпадают. □

Лекция 4

Графы–1

4.1 Определения

Графы — один из важнейших математических объектов для дискретной математики. Есть много разных видов графов. Мы начнём с *неориентированных графов*. Наглядно такой граф можно изобразить набором точек («вершин»), соединённых линиями («рёбрами»). При этом важно, какие точки соединены, а как именно нарисована линия, соединяющая точки, не имеет значения. Примеры графов показаны на рисунках 4.1–4.3.

Рис. 4.1: Путь P_5

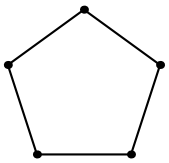


Рис. 4.2: Цикл C_5

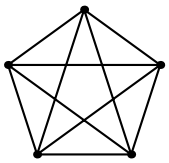


Рис. 4.3: Полный граф K_5

Наглядные картинки помогают понять рассуждения про графы, но для доказательств нужны более точные определения. Мы дадим сразу довольно много определений.

Простой неориентированный граф — это множество вершин V и множество рёбер E. Рёбрами являются 2-элементные подмножества множества V.

Ближайшие две лекции мы будем говорить только о простых неориентированных графах. Поэтому для краткости слова «простой неориентированный» будем пропускать.

Если $e = \{u, v\} \in E$, то вершины u, v называются *концами* ребра e. Концы ребра называются *смежными вершинами* или *соседями*.

Говорят также, что ребро $e = \{u, v\}$ *инцидентно* вершине u (как и вершине v). Ребра с общим концом также называются инцидентными.

Помимо картинок, с графами связаны две таблицы или, как принято говорить в математике, *матрицы*. Эти матрицы содержат только 0 или 1. Чтобы говорить о

матрице графа, нужно перенумеровать вершины и рёбра.

Матрица смежности графа: на пересечении i-й строки и j-го столбца стоит 1, если вершины i, j соседние; иначе там стоит 0.

Таким образом, матрица смежности — это квадратная матрица порядка n, где n — количество вершин графа.

Матрица инцидентности графа: на пересечении i-й строки и j-го столбца стоит 1, если вершина i инцидентна ребру j; иначе там стоит 0.

Таким образом, матрица инцидентности — это матрица размера $n \times m$, где n — количество вершин графа, m — количество рёбер графа.

4.2 Степени вершин

Количество соседей вершины v (оно же количество инцидентных её рёбер) называется *степенью* вершины, обозначать будем $d(v)$.

Теорема 4.1. *Сумма степеней всех вершин графа равна удвоенному числу его рёбер.*

Доказательство. Здесь применим *метод двойного подсчёта*. Под таким громким названием скрывается очень простой факт: если посчитать сумму элементов матрицы по строкам, то получится такое же число, как и при суммировании элементов матрицы по столбцам.

Давайте посчитаем количество 1 в матрице инцидентности графа. В строке i количество 1 равно количеству инцидентных вершине i рёбер, то есть степени этой вершины. Значит, сумма 1 по строкам равна сумме степеней вершин.

В каждом столбце матрицы инцидентности ровно две 1, так как у ребра ровно два конца. Значит, сумма 1 по столбцам равна удвоенному количеству рёбер.

Обе суммы равны общему количеству 1 в матрице инцидентности, а значит, равны между собой. □

Пример 4.1. Из этой теоремы получаются интересные следствия. Давайте докажем, что не существует графа, у которого 77 вершин, а степень каждой вершины равна 15.

Перебрать все возможные графы на 77 вершинах немыслимо.[1)] Однако это необязательно делать.

Доказательство от противного. Пусть такой граф существует. Заметим, что сумма степеней всех его вершин равна $77 \cdot 15$. Это нечётное число. С другой стороны, теорема утверждает, что эта сумма равна удвоенному количеству рёбер графа, то есть чётному числу. Противоречие.

Подсчёт сумм степеней вершин помогает и в более сложных ситуациях. Приведём пример.

Большие графы удобно задавать не матрицами и не рисунками, а точным определением множества вершин и рёбер.

[1)] Это множество конечно, но очень велико.

Пример 4.2 (Булев куб)**.** Вершины булева куба Q_n (булев куб размерности n) — двоичные слова длины n. Два слова u и v соседние в булевом кубе, если и только если одно можно получить из другого инвертированием бита ровно в одной позиции.

Скажем, 00010 и 01010 соседние в Q_5, а 00010 и 10000 — нет.

Как мы уже знаем, количество вершин в булевом кубе Q_n равно 2^n.

Степень каждой вершины равна n: есть ровно n позиций, инвертирование бита в каждой даёт соседа.

Подмножество I множества вершин графа называется *независимым*, если ни одна пара вершин в этом множестве не связана ребром.

Пример 4.3. В булевом кубе Q_n есть независимое множество размера 2^{n-1} (половина всех вершин).

Количество единиц в слове называется *(хэмминговым) весом* слова. При инвертировании бита в одной позиции количество единиц в слове изменяется ровно на 1. Поэтому концами каждого ребра являются слова, у которых чётность веса разная — у одного вес чётный, у другого — нечётный.

Значит, между словами чётного веса рёбер нет (как и между словами нечётного веса).

Как посчитать количество слов чётного и количество слов нечётного веса? Для этого опять применим двойной подсчёт. У каждого ребра один конец имеет чётный вес, а другой — нечётный. Значит, сумма степеней вершин чётного веса равна количеству рёбер и сумма степеней вершин нечётного веса равна количеству рёбер. Поскольку степени всех вершин булева куба одинаковы и равны n, получаем равенство $nV_{\text{odd}} = nV_{\text{even}}$. Поэтому $V_{\text{odd}} = V_{\text{even}} = 2^{n-1}$.

Пример 4.4. Докажем, что в булевом кубе Q_n нет независимого множества размера больше 2^{n-1}.

Обратите внимание, что предыдущего примера множеств вершин чётного и нечётного веса недостаточно. В независимое множество, вообще говоря, могут входить вершины с весами разной чётности.

Пусть I — независимое множество. Количество рёбер, инцидентных этому множеству, равно $n|I|$. Это число не больше общего количества рёбер $n2^{n-1}$. Отсюда и получаем неравенство $|I| \leqslant 2^{n-1}$.

4.3 Связность, компоненты связности

Путь по графу — это такая последовательность вершин $v_1, v_2, v_3, \ldots, v_k$, в которой стоящие рядом члены (вершины v_i и v_{i+1} при всех i) соединены ребром. Вершина v_1 называется *началом* пути, вершина v_k — его *концом*. *Длиной* пути называется число рёбер, то есть $k-1$. Мы будем разрешать также и пути длины 0, то есть последовательности из одной вершины. У такого пути начало совпадает с концом. Рёбер в таком пути нет, но вершина (одна) есть.

Вершины v и v' называются *связанными*, если существует путь с началом в v и концом v'. Граф называется *связным*, если любые две его вершины связаны.

Неформальное понимание связности графа: если представить вершины как города, а рёбра как дороги, то из любого города в любой можно проехать по дорогам.

Пример 4.5. Пример связного графа: *полный граф* K_n. В этом графе n вершин, и каждая пара вершин соединена ребром. Поэтому любая последовательность из двух вершин является путём в этом графе.

Пример 4.6. Пример несвязного графа: граф с n вершинами и 0 рёбер. В этом графе все пути имеют длину 0.

Если граф удачно нарисован, то увидеть его связность или несвязность легко.[2)] Но без картинки, только из определения или списка рёбер, это сделать уже труднее.

Пример 4.7. Вершины графа $Q_{n,3}$ — двоичные слова длины n. Два слова u и v соседние в этом графе, если и только если одно можно получить из другого инвертированием битов ровно в трёх позициях.

Связен ли граф $Q_{n,3}$? Ответ неочевиден и его обоснование требует некоторых усилий.

Для вершины v обозначим через $C(v)$ множество вершин, связанных с v. Будем называть это множество *областью достижимости вершины* v. Если граф связный, то для каждой вершины $C(v)$ совпадает со всем множеством вершин графа. В общем случае это не так. Но всегда выполняется несколько простых свойств для областей достижимости.

Лемма 4.2. *Для любого графа и любых его вершин v_1, v_2, v_3 выполняются следующие свойства:*

1. $v_1 \in C(v_1)$ *(вершина достижима из себя самой);*
2. $v_1 \in C(v_2)$ *равносильно* $v_2 \in C(v_1)$ *(если v_1 достижима из v_2, то v_2 достижима из v_1);*
3. *если* $v_1 \in C(v_2)$ *и* $v_2 \in C(v_3)$, *то* $v_1 \in C(v_3)$.

Доказательство. Эти свойства вполне очевидны из неформального представления о достижимости. Формальные их доказательства также очень просты.

v_1 — путь в любом графе, поэтому v_1 связанная с самой собой.

Если $v_1u_1 \dots u_sv_2$ — путь в графе, то $v_2u_s \dots u_1v_1$ — также путь. Поэтому достижимость v_2 из v_1 равносильная достижимости v_1 из v_2.

Наконец, если в графе есть пути $v_3u_1 \dots u_sv_2$ и $v_2w_1 \dots w_tv_1$ (то есть $v_1 \in C(v_2)$ и $v_2 \in C(v_3)$), то в это графе есть также и путь $v_3u_1 \dots u_sv_2w_1 \dots w_tv_1$, то есть v_1 достижима из v_3. □

[2)] Однако можно так нарисовать граф, что понять, связен ли он, трудно: это популярная разновидность головоломок.

На этой очевидной лемме основан важный способ доказательства связности графа. А именно, достаточно доказать, что из какой-то вершины достижимы все. Это эквивалентно в силу свойства 2 леммы 4.2, что из любой вершины достижима какая-то выделенная. А свойство 3 гарантирует, что года из каждой вершины достижима любая.

Утверждение 4.3. *Граф $Q_{n,3}$ связный при $n \geqslant 4$.*

Доказательство. Докажем, что любое слово длины $\geqslant 4$ последовательными инвертированиями битов в тройках позиций можно превратить в нулевое.

Первый шаг: если единиц в слове больше 2, уменьшаем их количество, инвертируя какие-нибудь три позиции, содержащие только единицы. Этот шаг заканчивается, когда в слове не больше 2 единиц.

Если единиц нет, то мы достигли требуемого — построили путь из начального слова в нулевое.

Если единица одна, то инвертируя позицию, в которой она стоит, и ещё две позиции (с нулями), получаем слово с двумя единицами ровно.

Если единиц две, то инвертируем позицию одной из них и ещё две позиции, содержащие нули (длина слова не меньше 4, так что позиций с нулями хотя бы две). Получаем слово ровно с тремя единицами. Инвертируя их, получаем нулевое слово. □

Лемма 4.4. *Если $w \in C(v_1) \cap C(v_2)$, то $C(v_1) = C(v_2)$. Области достижимости не пересекаются или совпадают.*

Доказательство. Поскольку w достижима из v_1 (определение), а v_2 достижима из w (свойство 2 леммы 4.2), то v_2 достижима из v_1 (свойство 3 леммы 4.2). Значит, и v_1 достижима из v_2 (свойство 2).

Пусть $x \in C(v_1)$. Тогда $x \in C(v_2)$, свидетельством тому путь из v_2 в v_1, продолженный путём из v_1 в x. Значит, $C(v_1) \subseteq C(v_2)$.

Верно и обратное: $C(v_2) \subseteq C(v_1)$ (поменяем индексы в рассуждении). Значит, $C(v_1) = C(v_2)$. □

Из свойства 1 леммы 4.2 следует

$$V = \bigcup_{v \in V} C(v).$$

Лемма 4.4 говорит, что области достижимости не пересекаются или совпадают. Таким образом, мы получаем *разбиение* множества вершин графа на подмножества. Каждое такое подмножество может быть представлено как область достижимости любого элемента из этого множества.

Удобно не упоминать этот случайно выбранный элемент. Поэтому используется такая терминология. *Компонента связности* графа — это область достижимости некоторой вершины этого графа. У связного графа одна компонента связности. Как мы обсудили выше, вершины графа разбиваются на компоненты связности.

У компонент связности есть другое описание. Для него нам потребуется новое понятие: *индуцированный подграф* графа. Пусть $U \subseteq V$ — подмножество вершин графа $G(V, E)$. Тогда $\langle U \rangle$ — это граф с множеством вершин U и множеством рёбер

$$E(\langle U \rangle) = \big\{\{x, y\} : \{x, y\} \in E(G),\ x, y \in U\big\}.$$

Теорема 4.5. *Компоненты связности — это в точности максимальные по включению множества вершин, индуцирующие связный граф.*

Условие теоремы означает фактически два утверждения: (а) любое множество, строго содержащее компоненту связности (все вершины компоненты и ещё какие-то, хотя бы одну), индуцирует несвязный граф; (б) любое множество, индуцирующее связный граф, содержится в какой-то компоненте связности.

Доказательство. Если $X \supset C(v)$ (этот знак обозначает строгое включение), то $\langle X \rangle$ несвязный: из вершины $x \in X \setminus C(v)$ недостижима v. Значит, компоненты связности — максимальные по включению множества, индуцирующие связные графы. Утверждение (а) доказано.

В обратную сторону. Пусть X — множество, индуцирующее связный граф, $v \in X$. Поскольку $\langle X \rangle$ связный, то $C(v) \supseteq X$ (вершины из X достижимы из v даже если запрещено выходить за пределы X). Утверждение (б) доказано. □

Лекция 5

Графы–2. Деревья

Мы охарактеризовали компоненты связности как максимальные по включению подмножества вершин графа, которые индуцируют связный граф.

Ясно, что добавление рёбер к связному графу сохраняет связность: путей становится только больше. И наоборот, выбрасывание рёбер из несвязного графа сохраняет несвязность: путей становится только меньше.

Сегодня рассмотрим *минимальные по включению рёбер* связные графы. Они называются *деревьями*. Примеры деревьев изображены на рисунке 5.1.

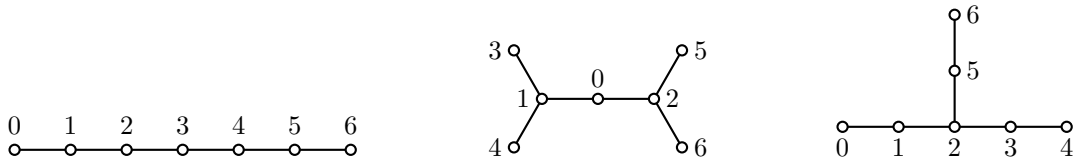


Рис. 5.1: Примеры деревьев

Точное определение дерева такое.

Определение 5.1. *Дерево* — такой связный граф, что выбрасывание любого ребра даёт несвязный граф.

Можно переформулировать это определение, используя понятие *моста*. Мост — это такое ребро в графе, что его удаление увеличивает количество компонент связности. Поэтому деревья — это связные графы, каждое ребро которых мост. А произвольные графы, у которых каждое ребро является мостом, называются *лесами*.

5.1 Простые пути и циклы

Глядя на рисунок 5.1, хочется сформулировать такое свойство деревьев: в них нет циклов. Однако мы ещё не определили, что такое цикл. К сожалению, в теории графов есть много путаницы в терминологии. В частности, слово «цикл» в разных

книгах может означать три разных понятия. Единственный выход: помнить об этом и внимательно следить за определениями, которые даются в книжках.

Мы называем *циклом* замкнутый путь по графу, то есть такой путь, у которого начало совпадает с концом. При таком определении сформулированное выше свойство неверно. Например, в левом графе на рисунке 5.1 есть цикл

$$(0, 1, 2, 3, 4, 5, 6, 5, 4, 3, 2, 1, 0).$$

То понятие, которое нужно для описания свойств деревьев, мы будем называть *простым циклом*. Это такой цикл, в котором все вершины различны (за исключением начала и конца, которые совпадают по определению цикла).

Однако и простые циклы бывают во всех графах, которые содержат хотя бы одно ребро. Если в графе G есть ребро $\{u, v\}$, то в этом графе есть цикл (u, v, u).

Мы докажем чуть позже, что в деревьях нет простых циклов длины больше 2.

Нам также будет нужно понятие *простого пути*: это такой путь, в котором все вершины различны. Когда мы говорим о связанности вершин, достаточно рассматривать только простые пути. Неформально это означает очень простое наблюдение: если вы едете из города A в город B, то можно так проехать, чтобы побывать в каждом промежуточном городе ровно один раз.

Утверждение 5.2. *Если две вершины x, y связаны в графе G, то в этом графе существует простой путь с началом x и концом y.*

Доказательство. Мы будем использовать принцип наименьшего числа. В соответствии с этим принципом если есть хотя бы один путь с началом x и концом y, то есть и путь наименьшей длины (нет ни одного пути короче).

Рассмотрим такой кратчайший путь $x = v_1, \ldots, v_k = y$ и докажем, что он простой. Для этого применим контрапозицию. Докажем, что если путь $x = u_1, \ldots, u_t = y$ не простой, то он не кратчайший (есть путь короче). Действительно, пусть $u_i = u_j$, $i < j$. Тогда последовательность $x = u_1, \ldots, u_i, u_{j+1}, u_t = y$ также является путём с началом x и концом y, а длина этого пути меньше. □

Замечание 5.1. В доказательстве есть одно тонкое место. Что если $j = t$? Тогда u_{j+1} не определена. В этом случае более короткий путь имеет вид $x = u_1, \ldots, u_i = u_t = y$.

5.2 Мосты, простые пути и простые циклы

Для деревьев и лесов есть несколько критериев (свойств, равносильных определению дерева). Два из них связаны с простыми циклами и простыми путями в графе.

Теорема 5.3. *Равносильны следующие свойства простых неориентированных графов:*

(1) *каждое ребро — мост;*

(2) *для любых связанных вершин u, v существует единственный простой путь из u в v;*

(3) *нет простых циклов длины больше* 2.

Свойства для деревьев получатся из этой теоремы, если потребовать связности графа.

Следствие 5.4. *Равносильны следующие свойства связных простых неориентированных графов:*

(1) *граф — дерево;*

(2) *для любых двух вершин u, v существует единственный простой путь из u в v;*

(3) *нет простых циклов длины больше* 2.

Будем доказывать утверждения теоремы 5.3 по очереди.

Доказательство (2) $\Rightarrow$ (3). Равносильно контрапозиции $\neg(3) \Rightarrow \neg(2)$. Пусть в графе G есть простой цикл $v_0, v_1, \ldots, v_\ell = v_0$, $\ell > 2$.

Вершины v_0 и v_1 связанные в этом графе, причём есть по крайней мере два разных пути с концами в этих вершинах: (v_0, v_1) (путь из одного ребра) и путь по остальным рёбрам цикла $(v_0 = v_\ell, v_{\ell-1}, \ldots, v_2, v_1)$ (здесь важно, что длина цикла больше 2). □

Доказательство (3) $\Rightarrow$ (1). Равносильно контрапозиции $\neg(1) \Rightarrow \neg(3)$.

Пусть ребро $e = \{v_0, v_1\}$ можно удалить из графа G и полученный граф $G - e$ остаётся связным. Это значит, что вершины v_0, v_1 связанные в G'. По утверждению 5.2 в графе G' есть простой путь $v_1, v_2, \ldots, v_\ell = v_0$. Все вершины этого пути различные.

Но тогда в графе G есть простой цикл $v_0, v_1, v_2, \ldots, v_\ell = v_0$ и, так как $v_0 \neq v_1$, длины этого цикла больше 2. □

Доказательство (1) $\Rightarrow$ (2). Равносильно контрапозиции $\neg(2) \Rightarrow \neg(1)$. Пусть между вершинами u и v есть два разных пути

$$u = u_0 u_1 \ldots u_s = v \quad \text{и} \quad u = v_0 v_1 \ldots v_t = v.$$

Начинаются эти пути в одной вершине, но полностью совпадать не могут. Выделим ребро, которое входит только в один из этих путей. Без ограничения общности это ребро $\{u_i, u_{i+1}\}$ на первом пути.

Докажем, что ребро $\{u_i, u_{i+1}\}$ — не мост. При удалении этого ребра из графа вершины u_i, u_{i+1} остаются в одной компоненте связности: они связаны (не обязательно простым) путём

$$u_i u_{i-1} \ldots u_0 = v_0 v_1 \ldots v_t = u_s u_{s-1} \ldots u_{i+1}.$$

Области достижимости вершин не из $C(u_i)$ не изменяются: пути из таких вершин не проходят через ребро $\{u_i, u_{i+1}\}$. □

Завершение доказательства теоремы 5.3. Поскольку мы доказали циклическую цепочку импликаций (2) ⇒ (1) ⇒ (3) ⇒ (2), все эти утверждения равносильны (если хотя бы одно истинно, остальные два тоже истинны). □

5.3 Размерность графа

Обозначим количество вершина графа G через n, количество рёбер через m, а количество компонент связности через c. *Размерностью* графа называется величина $\dim G = m - n + c$. Это и впрямь размерность некоторого векторного пространства. Мы ограничимся лишь комбинаторными свойствами этой размерности.

Теорема 5.5. *Графы, у которых размерность равна* 0, *— это в точности леса, то есть графы без мостов.*

Отсюда получаем ещё один критерий дерева:

Следствие 5.6. *Связный граф является деревом тогда и только тогда, когда число рёбер в нём на единицу меньше числа вершин.*

Доказательство теоремы основано на таком утверждении.

Утверждение 5.7. *Пусть граф $G' = G + e$ получается из графа G добавлением ребра $e = \{x, y\}$ к множеству рёбер, а вершины у него те же.*

Тогда $\dim G' = \dim G$, если концы ребра x, y лежат в разных компонентах связности графа G, и $\dim G' = \dim G + 1$, если x, y лежат в одной компоненте связности графа G.

Доказательство. Рассмотрим два случая, указанных в утверждении.

Вершины x, y лежат в одной компоненте связности C графа G. Тогда количество компонент связности не изменилось: для любой вершины x область достижимости в графе G' та же самая, что и в G (поскольку y достижима из x и в графе G). Количество рёбер увеличилось на 1, количество вершин не изменилось. Значит, и размерность увеличилась на 1.

Вершины x, y лежат в разных компонентах связности графа G. Тогда в графе G' в область достижимости вершины x добавляется $C(y)$, поскольку в G' вершина y достижима из x. Аналогично рассуждаем про y, получаем

$$C'(x) = C'(y) = C(v) \cup C(u),$$

то есть области достижимости x и y в графе G' равны объединению областей достижимости этих вершин в графе G. Области достижимости вершин из других компонент связности G остаются теми же самыми. Значит, количество компонент связности уменьшилось на 1. Количество рёбер увеличилось на 1, количество вершин не изменилось. Поэтому размерность не изменилась. □

Для доказательства теоремы 5.5 мы используем индукцию по числу рёбер графа. Базой индукции будут графы без рёбер (с произвольным количеством вершин). В таком графе размерность равна нулю: рёбер нет, каждая вершина является компонентой связности. И такой граф является лесом, так как каждое его ребро — мост (рёбер вообще нет, так что это утверждение верно).

Лемма 5.8. *Размерность графа неотрицательная.*

Доказательство. Индукция по количеству рёбер. База проверена выше.

Пусть для графа G размерность неотрицательная, то есть $m-n+c \geqslant 0$. Рассмотрим граф $G' = G + e$, $e = \{x, y\}$. По утверждению 5.7 его размерность не меньше размерности графа G, то есть неотрицательная. Шаг индукции доказан, лемма выполняется в силу принципа математической индукции. □

Доказательство теоремы 5.5. Пусть размерность графа G равна 0. Поскольку размерность любого графа неотрицательная, каждое ребро G обязано быть мостом, так как удаление не моста уменьшает размерность.

В другую сторону нужно доказать, что размерность всякого леса равна 0. Доказываем индукцией по количеству рёбер. Базой, как уже говорилось, являются графы без рёбер.

Шаг индукции. Предположим, что утверждение теоремы выполняется для графов с количеством рёбер меньше m. Рассмотрим лес G с m рёбрами, и граф $G' = G - e$, полученный из G удалением ребра $e = \{x, y\}$. Это ребро является мостом, так что размерность графа G' равна размерности графа G (утверждение 5.7).

В графе G' нет простых циклов длины больше 2, так как любой такой цикл был бы и простым циклом в лесу G. Значит, по теореме 5.3, граф G' — лес. По индуктивному предположению, его размерность равна 0. Поэтому и размерность леса G равна 0.

Шаг индукции доказан. По принципу математической индукции, размерность любого леса равна 0. □

5.4 Висячие вершины в деревьях

Вершины степени 0 называются *изолированными*, а вершины степени 1 — *висячими*. В дереве из одной вершины висячих вершин нет вообще, единственная вершина изолированная.

Теорема 5.9. *В дереве с хотя бы двумя вершинами есть по крайней мере две висячие вершины.*

Доказательство. Используем следствие (5.6). Пусть в дереве $n \geqslant 2$ вершин. Тогда в этом дереве $n - 1$ ребро.

Обозначим степени вершин дерева $d_1, \ldots, d_n$. Поскольку $n \geqslant 2$, изолированных вершин нет (каждая изолированная вершина является компонентой связности). Из

теоремы 4.1 получаем равенство

$$d_1 + \cdots + d_n = 2(n-1).$$

Перепишем его в виде

$$(d_1 - 2) + (d_2 - 2) + \cdots + (d_n - 2) = -2.$$

Так как $d_i > 0$, каждое слагаемое в левой части не меньше -1. Значит, хотя бы два должны равняться -1, они отвечают висячим вершинам, для которых $d_i - 2 = 1 - 2 = -1$. □

5.5 Остовные деревья

У нас уже появлялись подграфы, индуцированные подмножеством вершин. В общем случае *подграф* графа получается так: выбираем некоторое подмножество вершин и некоторое подмножество рёбер с концами в выбранных вершинах. Подграф называется *остовным*, если его множество вершин совпадает с множеством вершин самого графа. Из следствия 5.4. получаем такой важный факт.

Теорема 5.10. *В любом связном графе есть остовное дерево.*

Доказательство. Удаляем не мосты графа, пока это возможно. При удалении не моста связный граф остаётся связным. В итоге получится связный граф, в котором каждое ребро — мост, то есть дерево. Оно остовное — вершины те же самые, что в исходном графе. □

Сформулируем без доказательства замечательную теорему.

Теорема 5.11 (Кэли)**.** *Количество остовных деревьев в полном графе на n вершинах равно n^{n-2} при $n \geqslant 2$.*

Лекция 6

Графы–3. Ориентированные графы

Простой ориентированный граф (орграф) — это множество вершин V и множество рёбер E. Рёбрами являются упорядоченные пары вершин.

Если $e = (u, v) \in E$, то вершина u называется *началом* ребра e, а вершина v — *концом*. Говорят также, что ребро $e = (u, v)$ орграфа *выходит* из вершины u и *входит* в вершину v.

На рисунках ориентированные рёбра изображаются линиями со стрелками. Стрелка направлена от начала к концу ребра, см. рис. 6.1.

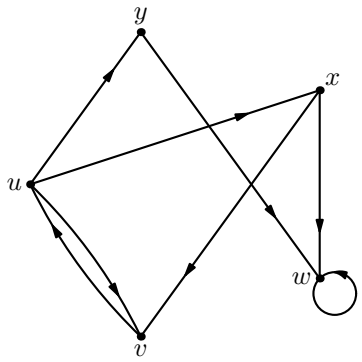


Рис. 6.1: Пример ориентированного графа

В случае неориентированных графов ребро $\{u, v\}$ однозначно определяется своими концами. В случае ориентированных графов между парой вершин u, v возможны два ребра: (u, v) и (v, u). В графе на рис. 6.1 есть оба таких ребра.

Кроме того, наше определение разрешает *петли* в орграфе. На рис. 6.1 есть пример петли: упорядоченная пара (w, w). У петли начало и конец совпадают.

Орграфы, как и обычные неориентированные графы, можно задавать матрицей смежности. Как и раньше, чтобы говорить о матрице смежности графа, нужно перенумеровать его вершины и рёбра.

Матрица смежности орграфа — квадратная матрица порядка n, где n — количество вершин графа. В этой матрице на пересечении i-й строки и j-го столбца

стоит 1, если в орграфе есть ребро (i, j); иначе там стоит 0. Матрица смежности орграфа уже не обязательно симметрическая: возможно, что $A_{ij} = 1$, $A_{ji} = 0$, $i \neq j$.

6.1 Степени вершин

В неориентированных графах степень вершины равна количеству инцидентных ей рёбер. В орграфах часть рёбер входит в вершину, часть — выходит. Их считают по отдельности. *Исходящая степень* вершин равна числу рёбер, выходящих из этой вершины. *Входящая степень* равна числу рёбер, входящих в вершину. Если в вершине v есть петля $e = (v, v)$, то вершина v является и началом и концом петли e. Поэтому петля даёт вклад 1 и в исходящую степень, и во входящую.

Для степеней вершин графа есть соотношение, аналогичное соотношению для суммы степеней вершин неориентированного графа.

Теорема 6.1. *Сумма исходящих степеней всех вершин равна сумме входящих степеней всех вершин: обе суммы равны числу рёбер графа.*

Доказательство. Каждое ребро имеет одно начало (выходит из какой-то вершины) и поэтому учитывается по разу, когда мы складываем исходящие степени всех вершин. Аналогично для концов рёбер. □

У каких орграфов и входящая, и исходящая степени каждой вершины равны 1? Пример такого графа изображён на рис. 6.2. Из этого рисунка легко догадаться, как устроены такие графы в общем случае. Они разбиваются на ориентированные циклы.

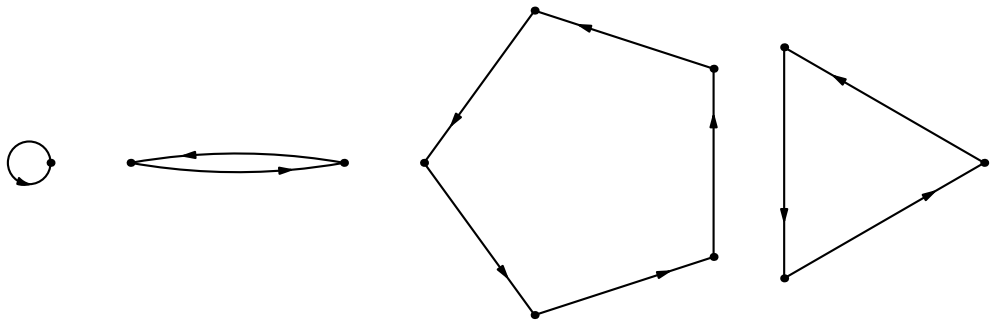


Рис. 6.2: Пример ориентированного графа с входящими и исходящими степенями 1 в каждой вершине

Определения путей и циклов для орграфов похожи на определения для обычных графов. *Путь* по орграфу — это такая последовательность вершин $v_1, v_2, v_3, \ldots, v_k$, в которой стоящие рядом члены (вершины v_i и v_{i+1} при всех i) соединены ребром, причём v_i — начало ребра, а v_{i+1} — его конец. Цикл — это путь, у которого первая и последняя вершины совпадают. Простые пути и циклы определяются точно так же, как в неориентированном случае: все вершины должны быть различны.

Ориентированным циклом называется множество рёбер любого простого цикла (обратите внимание на разницу: ориентированный цикл — множество рёбер, а цикл — последовательность вершин и рёбер).

Теорема 6.2. *Если в орграфе G каждая вершина имеет исходящую и входящую степень* 1*, то рёбра такого графа разбиваются на несколько ориентированных циклов: каждое ребро принадлежит в точности одному из этих циклов.*

Доказательство. Рассмотрим орграф G на множестве вершин V, который удовлетворяет условиям теоремы.

Выберем вершину $v = v_0$ и построим путь $v_0, v_1, \ldots, v_i, \ldots$ по орграфу G. Этот путь однозначно определён, так как из каждой вершины v_i выходит ровно одно ребро (v_i, v_{i+1}).

Построенный путь бесконечный, а вершин в графе конечное количество. Поэтому рано или поздно на этом пути какая-то вершина повторится. Выберем самое первое повторение: $v_i = v_\ell$, $i < \ell$; все вершины $v_0, \ldots, v_{\ell-1}$ различны.

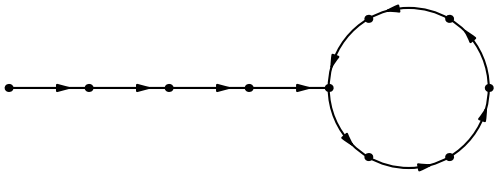


Рис. 6.3: Повтор не в начальной вершине противоречит входящей степени 1

Докажем от противного, что повторится именно вершина v_0. Пусть $i > 0$. Тогда в графе есть два ребра (v_{i-1}, v_i) и $(v_{\ell-1}, v_\ell)$, входящие в $v_i = v_\ell$. Поскольку входящая степень равна 1, то $v_{i-1} = v_{\ell-1}$. Это противоречит тому, что $v_i = v_\ell$ первое повторение. (Рис. 6.3.)

Получили простой цикл $C(v) = (v_0, v_1, \ldots, v_\ell = v_0)$. Из условий теоремы следует, что никакие другие рёбра не входят и не выходят из вершин v_i.

Различные циклы вида $C(v)$ не пересекаются, так как исходящие степени вершин равны 1. С другой стороны, каждая вершина v лежит на цикле $C(v)$. Значит, рёбра этих циклов и задают разбиение рёбер орграфа на ориентированные циклы. □

Теперь опишем графы, у которых исходящая степень в каждой вершине равна 1. Они не исчерпываются наборами ориентированных циклов, как показывает рис. 6.3. Оказывается, в этих графах помимо ориентированных циклов есть ещё *ориентированные деревья*. Определим формально, что это такое.

Иногда в дереве выделяют особую вершину — *корень*. В этом случае дерево называют корневым. (Заметим, что висячие вершины, отличные от корня, называют *листьями*.)

По любому простому неориентированному графу можно построить орграф, выбрав для каждого ребра одну из двух возможных ориентаций. Для любого корневого дерева есть две естественные ориентации: по направлению к корню и по направлению от корня.

Будем называть корневое дерево с корнем r *ориентированным к корню*, если каждое ребро (u, v) удовлетворяет такому условию: вершина v лежит на простом пути от u к r. (Напомним, что в дереве такой путь единственный.)

Аналогично определяется *ориентация от корня*: вершина u лежит на простом пути от v к r. Но нам она сейчас не понадобится.

Теорема 6.3. *Если в орграфе G каждая вершина имеет исходящую степень* 1*, то рёбра такого графа разбиваются на несколько ориентированных циклов и несколько ориентированных корневых деревьев, корень каждого такого дерева принадлежит одному из циклов.*

Доказательство. Как и доказательстве предыдущей теоремы, рассмотрим путь

$$v = v_0, v_1, \ldots, v_i, \ldots$$

по орграфу G, начинающийся в вершине v. Этот путь однозначно определён, вершины в нём обязаны повторяться.

Рассмотрим первое повторение $v_i = v_j$. Тогда $v_{i+1} = v_{j+1}$ и так далее. Поэтому, начиная с v_i, этот путь периодичен, и наименьший период является простым циклом. Обозначим этот цикл $C(v)$, а первую повторяющуюся вершину — $r(v)$.

Различные циклы вида $C(v)$ не пересекаются. Но теперь, в отличие от случая когда и все входящие степени равны 1, будут также и вершины, которые не лежат на этих циклах. (Поскольку теперь v необязательно лежит на цикле $C(v)$.

Пусть r лежит на одном из циклов. Рассмотрим граф, индуцированный множеством вершин $V_r = \{v : r = r(v)\}$ (за исключением возможной петли r, r). Докажем, что это ориентированное дерево с корнем r.

Заметим, что если убрать ориентации рёбер, то полученный неориентированный граф G_r является связным (из любой вершины достижима вершина r).

Обозначим через n количество вершин в графе G_r, а через m — количество рёбер. Из каждой вершины, кроме r выходит ровно одно ребро (ребро, выходящее из r лежит на цикле). Значит, $m = n - 1$. По следствию 5.6 из теоремы 5.5 граф G_r является деревом.

Осталось доказать, что всё ребра в дереве G_r ориентированы в исходном орграфе к корню. Действительно, из любой вершины $v \in V_r$ есть путь в $r(v)$, то есть корень дерева. Значит ребро (v, v') (единственное ребро, исходящее из v) ориентировано к корню. □

6.2 Сильная связность, компоненты сильной связности

Как и в случае неориентированных графов, обозначим через $R(u)$ множество тех вершин v, которые *достижимы* из u, то есть существует путь с началом u и концом v.

Будем говорить, что вершина u *сильно связана* с вершиной v, если v достижима из u и наоборот, то есть если есть путь из u в v, а также путь из v в u.

Через $C(u)$ обозначим множество тех вершин v, которые сильно связаны с u. Эти множества обладают теми же свойствами, что и компоненты связности обычного ориентированного графа и называются *компонентами сильной связности*.

Лемма 6.4. *Для любого графа и любых его вершин v_1, v_2, v_3 выполняются следующие свойства:*

1. $v_1 \in C(v_1)$ *(вершина сильно связана сама с собой);*
2. $v_1 \in C(v_2)$ *равносильно* $v_2 \in C(v_1)$*;*
3. *если* $v_1 \in C(v_2)$ *и* $v_2 \in C(v_3)$*, то* $v_1 \in C(v_3)$*.*

Доказательство. v_1 — путь в любом графе, поэтому v_1 сильно связана с самой собой.

Определение сильной связанности симметрично, отсюда свойство 2.

Наконец, если в графе есть пути из v_3 в v_2, из v_2 в v_3, из v_2 в v_1, из v_1 в v_2, то обязательно есть и пути из v_1 в v_3 (соединяем путь из v_1 в v_2 с путём из v_2 в v_3), а также из v_3 в v_1 (соединяем путь из v_3 в v_2 с путём из v_2 в v_1). Это доказывает свойство 3. □

Лемма 6.5. *Если $w \in C(v_1) \cap C(v_2)$, то $C(v_1) = C(v_2)$. Компоненты сильной связности не пересекаются или совпадают.*

Доказательство. Поскольку w сильно связана с v_1 и с v_2, то v_2 достижима из v_1 (путь из v_1 в w, соединённый с путём из w в v_2). Аналогично, v_1 достижима из v_2.

Значит, $C(v_2) \subseteq C(v_1)$ и $C(v_1) \subseteq C(v_2)$. То есть $C(v_1) = C(v_2)$. □

Из этих свойств, аналогично случаю неориентированных графов, следует, что компоненты сильной связности орграфа задают разбиение его вершин.

Если всё множество вершин орграфа образует компоненту сильной связности, такой орграф называется *сильно связным*. Примером сильно связного графа является ориентированный цикл.

6.3 Ациклические орграфы

Орграф называется *ациклическим*, если каждая компонента сильной связности состоит из одной вершины. Другими словами, никакие две различные вершины не являются сильно связанными. Название объясняется следующей теоремой. В ней мы требуем отсутствия петель в орграфе.

Теорема 6.6. *Следующие свойства ориентированного графа без петель равносильны:*

(1) *Каждая сильно связная компонента состоит из одной вершины.*

(2) *В орграфе нет циклов длины больше* 0*.*

(3) *Вершины орграфа можно пронумеровать натуральными числами таким образом, чтобы все рёбра вели «вверх»: из вершины с меньшим номером в вершину с бóльшим.*

Для доказательства этой теоремы нам понадобится такая полезная лемма.

Лемма 6.7. *В орграфе без циклов есть вершина, из которой не выходит ни одного ребра, а также есть вершина, в которую не входит ни одного ребра.*

Доказательство. От противного. Если из каждой вершины выходит хотя бы одно ребро, то оставим по одному ребру, исходящему из каждой вершины. Получаем граф, в котором исходящие степени вершин равны 1. Как мы уже доказали в теореме 6.3, в таком графе есть цикл.

Чтобы доказать второе утверждение, перейдём к графу, в котором ориентации всех рёбер изменены на противоположные. Если исходный граф был ациклическим, то граф с инвертированными ориентациями также будет ациклическим. Но исходящие и входящие степени вершин переставляются. □

Доказательство теоремы 6.6. (1) $\Rightarrow$ (2) равносильно контрапозиции $\neg(2) \Rightarrow \neg(1)$. Докажем вторую импликацию. Раз в орграфе нет петель, в нём нет циклов длины 1. Если в орграфе есть цикл с $n > 1$ вершинами, то вершины этого цикла сильно связаны (из любой можно попасть в любую по циклу).

(2) $\Rightarrow$ (1) равносильно контрапозиции $\neg(1) \Rightarrow \neg(2)$. Докажем вторую импликацию. Если вершины $a \neq b$ сильно связаны, то существуют пути из a в b и из b в a. Соединением этих путей получается цикл.

(3) $\Rightarrow$ (2): если возможна нумерация вершин, при которой все рёбра идут из меньшей вершины в бóльшую, то циклов нет: вдоль любого пути номера вершин строго возрастают, что невозможно при возвращении в исходную вершину.

(2) $\Rightarrow$ (3) докажем индукцией по числу вершин усиленный вариант: нумерация использует числа от 1 до n, где n — число вершин в орграфе.

База индукции: граф без петель на одной вершине. Он ациклический и требуемая нумерация существует (это очевидно, так как рёбер нет).

Шаг индукции: пусть (2) $\Rightarrow$ (3) выполняется для графов с $< n$ вершинами. Рассмотрим граф без циклов на n вершинах. Выберем вершину v_n исходящей степени 0, которая существует в таком орграфе по лемме 6.7. Ей присвоим номер n. Удалив v_n и все входящие в неё рёбра, получим граф без циклов. (Циклы в нём были бы циклами и в исходном графе.) По предположению индукции его вершины можно пронумеровать числами от 1 до $n-1$ с соблюдением условия. Объединяя эту нумерацию с номером n вершины v_n, получаем искомую нумерацию. Шаг индукции доказан. □

6.4 Эйлеровы (ор-)графы

Цикл (в неориентированном или ориентированном графе) называется *эйлеровым*, если он проходит по всем рёбрам графа по ровно одному разу (любое ребро входит

в цикл, и никакое ребро не входит дважды).

Граф называется *эйлеровым*, если в нём есть эйлеров цикл.

Есть простой критерий эйлеровости графов и орграфов. Прежде всего заметим, что добавление и удаление *изолированных вершин*, т.е. тех вершин, из которых не входит и в которые не выходит ни одно ребра, не изменяет свойство эйлеровости графа.

Теорема 6.8. *В ориентированном орграф без изолоированных вершин существует эйлеров цикл тогда и только тогда, когда граф сильно связен и у любой вершины входящая степень равна исходящей.*

Доказательство. Пусть эйлеров цикл в орграфе есть. Тогда он проходит через все вершины (поскольку они имеют ненулевую степень), и по нему можно дойти от любой вершины до любой. Значит, орграф сильно связен.

Возьмём какую-то вершину v, пусть она встречается в эйлеровом цикле k раз. Двигаясь по циклу, мы приходим в неё k раз и уходим k раз, значит, использовали k входящих и k исходящих рёбер. При этом, раз цикл эйлеров, других рёбер у этой вершины нет, так что в ориентированном графе её входящая и исходящая степени равны k.

В обратную сторону чуть сложнее. Пусть орграф сильно связен и в каждой вершине исходящая степень равна входящей. Рассмотрим пути, которые не проходят дважды по одному ребру. Выберем среди таких путей самый длинный (его длина не больше общего количества рёбер)

$$\tau = (v_1,\ v_2,\ v_3,\ \ldots,\ v_{t-1},\ v_t)$$

и докажем, что этот путь и является искомым циклом, то есть что $v_1 = v_t$ и этот путь содержит все рёбра орграфа.

В самом деле, если τ самый длинный, то добавить к нему ребро (v_t, v_{t+1}) невозможно. Это означает, что все выходящие из v_t рёбра уже входят в τ. Это возможно, лишь если $v_1 = v_t$: если вершина v_t встречалась только внутри пути (пусть она входит k раз внутри пути и ещё раз в конце пути), то мы использовали $k+1$ входящих рёбер и k выходящих, и больше выходящих нет. Это противоречит равенству входящей и исходящей степени.

Итак, мы имеем цикл, и осталось доказать, что в него входят все рёбра. В самом деле, если во всех вершинах цикла использованы все рёбра, то из вершин этого цикла нельзя попасть в вершины, не принадлежащие циклу, то есть использованы все вершины (так как орграф сильно связен) и, следовательно, все рёбра. С другой стороны, если из какой-то вершины v_i выходит ребро (v_i, v), то путь можно удлинить до

$$(v_{i+1},\ \ldots, v_t = v_1,\ \ldots,\ v_i,\ v)$$

вопреки нашему выбору самого длинного пути. Аналогично можно получить противоречие и для входящего ребра (v, v_i), добавив его в начало. □

Для неориентированных графов критерий аналогичен.

Теорема 6.9. *Неориентированный граф без вершин нулевой степени содержит эйлеров цикл тогда и только тогда, когда он связен и степени всех вершин чётны.*

Доказательство полностью аналогично доказательству в ориентированном случае. Кратко повторим его.

Пусть эйлеров цикл в графе есть. Он проходит по всем вершинам, так что граф связен. В каждую вершину эйлеров цикл k раз заходит и k раз выходит. Значит, степень вершины $k + k = 2k$ чётна.

В обратную сторону опять рассматриваем самый длинный путь, в котором каждое ребро встречается не больше одного раза. Это цикл, так как иначе есть вершина нечётной степени.

Этот цикл обязан содержать все рёбра графа, так как в противном случае его можно удлинить.

Лекция 7

Графы–4. Раскраски. Комбинаторика–2

7.1 Раскраски графов

Правильной раскраской вершин неориентированного графа $G(V, E)$ в k цветов называется такое присваивание вершинам графа чисел (цветов) от 1 до k, что присвоенные смежным вершинам числа различны. Если для графа существует хотя бы одна правильная раскраска в k цветов, граф называется *k-раскрашиваемым*.

Очень легко понять, какие графы 1-раскрашиваемые. Это в точности графы без рёбер. Действительно, если вершинам графа без рёбер присвоить одно и то же число (цвет), то условие правильной раскраски выполняется. И наоборот: если в графе есть ребро $\{u, v\}$, то в правильной раскраске вершинам u, v присвоены разные цвета, поэтому количество цветов хотя бы 2.

Случай правильных раскрасок в 2 цвета интереснее.

Теорема 7.1. *2-раскрашиваемые графы это в точности графы, в которых длины всех циклов чётные.*

Доказательство. Достаточно доказать утверждение для связных графов, так как несвязный граф 2-раскрашиваемый тогда и только тогда, когда все его компоненты связности 2-раскрашиваемые и то же самое верно для свойства «длины всех циклов чётные».

Если в графе есть цикл нечётной длины, то его нельзя правильно раскрасить в 2 цвета. Соседние вершины должны быть противоположных цветов, поэтому количество вершин одного цвета должно равняться количеству вершин другого цвета.

Теперь докажем обратное. Пусть в графе длины всех циклов чётные. Докажем, что тогда для любых двух вершин u, v длины путей из u в v имеют одинаковую чётность.

Если в графе есть путь $\alpha = (u, \ldots, v)$ с чётным числом вершин (нечётной длины), а также другой путь $\beta = (v, \ldots, u)$ с нечётным числом вершин (чётной длины), то соединение этих путей $\alpha\beta$ (идём по первому пути из u в v, затем по второму пути из v в u) даёт цикл с нечётным числом вершин (нечётной длины): вершины u и

v считаются дважды в путях α, β и по одному разу в цикле. Это противоречит сделанному предположению, что все циклы в графе имеют чётную длину.

Теперь укажем искомую правильную раскраску в 2 цвета. Выберем вершину u и раскрасим вершину x графа в цвет 0, если длины путей из u в x чётные; в цвет 1, если длины путей из u в x нечётные. Это правило корректно по доказанному выше утверждению про одинаковую чётность длин циклов в графе без нечётных циклов (вспомним также, что мы доказываем утверждение теоремы для связных графов).

Заметим, что смежные в графе вершины не могут быть покрашены в один цвет: если $\{x, y\}$ — ребро графа, то для каждого пути $(u, \ldots, x)$ существует путь в y противоположной чётности, а именно, $(u, \ldots, x, y)$. □

Пример 7.1. Докажем, что булев куб 2-раскрашиваемый. Вершинами булева куба Q_n являются двоичные слова длины n. Покрасим вершины с чётным количеством единиц в цвет 0; вершины с нечётным количеством единиц в цвет 1.

Ребро булева куба связывает вершины, которые отличаются ровно в одной позиции. Одна вершина на этой позиции содержит 0, другая — 1. Чётность количества единиц в таких вершинах разная, то есть они покрашены в разные цвета.

Замечание 7.1. Эта теорема обосновывает простой и эффективный алгоритм проверки 2-раскрашиваемости графа. Закрасим какую-нибудь вершину в цвет 0. Далее действуем так.

Если есть непокрашенная вершина u, соединённая с уже покрашенной v, красим u в цвет, противоположный v.

Если все непокрашенные вершины несмежны уже покрашенным, красим какую-нибудь из непокрашенных в цвет 0.

Если в процессе такой раскраски встретилась вершина, которая смежна с вершинами двух противоположных цветов, то объявляем, что граф не является 2-раскрашиваемым. В противном случае получаем правильную 2-раскраску.

Корректность алгоритма доказывается так: нужно индукцией по числу действий проверить, что в 0 красятся вершины, которые соединены с начальной путями чётной длины, а в 1 — те, которые соединены путями нечётной длины.

Вопрос о существовании правильной раскраски в 3 и более цветов гораздо сложнее. Простого способа проверить 3-раскрашиваемость нет и не предвидится.

7.2 Двудольные графы

Двудольным графом называется неориентированный граф, в котором вершины заранее разделены на две *доли — левую* и *правую*, и все рёбра соединяют вершины из разных долей (нет рёбер, соединяющих вершины одной доли). Другими словами, чтобы задать двудольный граф, надо указать два конечных множества L (левую долю) и R (правую долю) и указать, какие вершины левой доли соединены с какими вершинами правой доли.

Разделение вершин на левые и правые задаёт правильную раскраску двудольного графа. Таким образом, граф можно представить как двудольный, если в нём нет циклов нечётной длины.

Пример 7.2. *Паросочетанием* называется двудольный граф, у которого степени всех вершин не больше 1.

Пример паросочетания приведён на рис. 7.1. Здесь доли нарисованы как верхняя и нижняя. Ясно, что нет никакой проблемы объявить одну из них левой, а другую — правой.

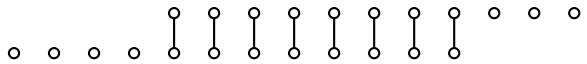


Рис. 7.1: Паросочетание

Такой граф устанавливает взаимно однозначное соответствие между частью вершин левой доли и частью вершин правой доли. В частности, если паросочетание *совершенное* (нет изолированных вершин, то есть вершин степени 0), то рёбра паросочетания устанавливают взаимно однозначное соответствие между вершинами левой и правой долей. Такое возможно, если размеры долей одинаковы.

Рассмотрим такую задачу. Дан двудольный граф G, нужно найти среди его рёбер максимальное по количеству рёбер паросочетание.

Размер максимального паросочетания не превосходит размера любой из долей. Однако бывают графы, в которых размер максимального паросочетания намного меньше, см. рис. 7.2.

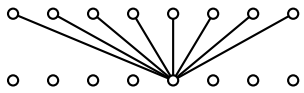


Рис. 7.2: Размер максимального паросочетания в таком графе равен 1

Для решения задачи о максимальном паросочетании есть эффективные алгоритмы. Нас больше интересуют теоремы, а не алгоритмы. Поэтому сформулируем и докажем критерий того, что размер максимального паросочетания достигает верхней границы, то есть совпадает с размером (меньшей) доли.

Без ограничения общности считаем, что в левой (нижней) доле вершин не больше, чем в правой (верхней). Для множества вершин $X \subseteq L$ левой доли обозначим $G(X) \subseteq R$ множество всех соседей этих вершин (они все лежат в правой доле, так как мы рассматриваем двудольные графы).

Теорема 7.2 (теорема Холла)**.** *Пусть для двудольного графа $G = (L \cup R, E)$ выполнено $|L| \leqslant |R|$.*

Если для каждого множества $X \subseteq L$ множество соседей $G(X) \subseteq R$ содержит не меньше вершин, чем X, то в графе G есть паросочетание размера $|L|$.

Доказательство. В доле L нет изолированных вершин, так как для изолированной вершины $v \in L$ нарушается условие теоремы: $1 = |\{v\}| > |G(\{v\})| = |\varnothing| = 0$. Поэтому паросочетание размера 1 точно есть.

Пусть имеется паросочетание P с концами в множестве $X \subset L$ и $Y \subset R$. Если оно не максимальное, то существует вершина $v \in L \setminus X$. Докажем, что тогда существует паросочетание с концами в левой доле $\{v\} \cup X$. Отсюда будет следовать утверждение теоремы.

Определим вспомогательный ориентированный граф $G' = (L \cup R, E')$ на том же множестве вершин. Его рёбра имеют вид

$$E' = \{(x,y) : \{x,y\} \in E(G),\ x \in L,\ y \in R; \quad \{y,x\} \in P,\ y \in R,\ x \in L\}.$$

Другими словами, мы разрешаем идти из левой доли в правую по любом ребру графа G, а из правой в левую — только по рёбрам паросочетания P.

Обозначим через $C(v) = L' \cup R'$, $L' \subseteq L$, $R' \subseteq R$, область достижимости вершины v в этом графе. Заметим, что $G(L') \subseteq R'$: ведь в правую долю разрешается идти по любым рёбрам G. Поэтому $|R'| \geqslant |G(L')|$.

В обратную сторону разрешается ходить по рёбрам P. Поэтому, если $y \in Y \cap R'$, то есть существует ребро $\{y,x\} \in P$, то $x \in L'$. Множество L' заведомо содержит вершину v, остальные вершины этого множества лежат в X (множество левых концов паросочетания P). По условию теоремы $|G(L')| \geqslant |L'|$. Значит, $|R'| \geqslant |L'|$. Так как $|L' \cap X| = |R' \cap Y|$, а $L' \setminus X = \{v\} \neq \varnothing$, то множество $R' \setminus Y$ непусто. Тут полезно посмотреть на рис. 7.3.

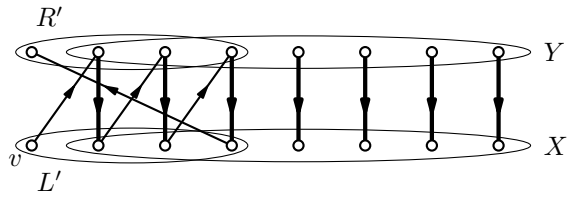


Рис. 7.3: Область достижимости «внешней» вершины v

Выберем в $R' \setminus Y$ вершину w. По определению области достижимости существует ориентированный путь из v в w, причём из правой доли в левую этот путь идёт по (ориентированным) рёбрам паросочетания P.

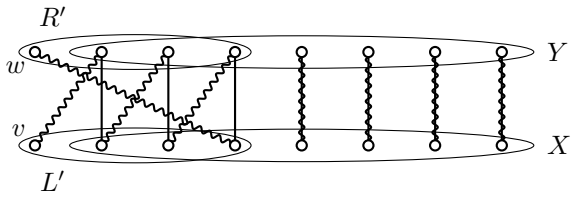


Рис. 7.4: Увеличение паросочетания

Рёбра этого пути разбиваются на две группы: «старые» рёбра из P и «новые» рёбра не из P (но эти рёбра являются рёбрами исходного графа G). Причём рёбра разных групп чередуются, а начало и конец пути инцидентны «новым рёбрам». Это означает, что новые рёбра образуют паросочетание в G, размер которого на 1 больше $|R' \cap Y|$. Заменяя «старые» рёбра, исходящие из $R' \cap Y$, на «новые», и добавляя остальные рёбра исходного паросочетания (с концами в $Y \setminus R'$) получаем паросочетание P', в котором рёбер на одно больше, чем в P (см. рис. 7.4, рёбра увеличенного паросочетания нарисованы волнистыми линиями). □

7.3 Возвращение к комбинаторике

7.3.1 Паросочетания и взаимно однозначные соответствия

Теперь вернёмся к перечислительной комбинаторике. Мы уже отмечали, что паросочетание задаёт взаимно однозначное соответствие между левыми и правыми концами рёбер. Поэтому, в частности, левых концов ровно столько же, сколько правых.

Это позволяет «сводить» одну комбинаторную задачу к другой, если построить паросочетание, в котором левые концы — это элементы множества, размер которого уже известен, а правые концы — элементы того множества, размер которого мы хотим найти.

Приведём пару простых примеров, в последующем таких примеров станет больше.

Пример 7.3. Рассмотрим все подмножества n-элементного множества. Обозначим семейство[1)] таких множеств через $\mathcal{P}(n)$. Сколько их?

Элементы n-элементного множества всегда возможно занумеровать числами от 1 до n и считать, что рассматриваем подмножества множества $[n] = \{1, 2, \ldots, n\}$.

Построим такой двудольный граф: вершины левой доли — двоичные слова длины n, вершины правой доли — подмножества из $\mathcal{P}(n)$. Рёбра этого графа соединяют пары $(w = w_1 w_2 \ldots w_n, S)$, где $i \in S$ тогда и только тогда, когда $w_i = 1$.

Этот граф — паросочетание: у каждого слова есть ровно один сосед в этом графе (множество тех позиций, на которых стоят единицы), и у каждого множества есть ровно один сосед (слово, в котором 1 стоит на тех позициях, номера которых входят в множество).

Значит, подмножеств n-элементного множества столько же, сколько двоичных слов длины n. А это число мы уже подсчитали, оно равно 2^n.

Пример 7.4. Мы уже подсчитывали количество монотонных путей из 0 в n (строго возрастающих последовательностей целых чисел, начинающихся с 0 и заканчивающихся n). При $n \geqslant 1$ оно равно 2^{n-1}. Мы получили его решением рекуррентного соотношения. А сейчас приведём «натуральное» доказательство этого факта.

[1)] Слово «семейство» используется как синоним слова «множество» для благозвучия.

Построим такой двудольный граф: вершины левой доли — подмножества $(n-1)$-элементного множества $[n-1] = \{1, \ldots, n-1\}$, вершины правой доли — монотонные пути из 0 в n. Ребра этого графа соединяют пары (S, τ), где промежуточные вершины пути τ — это в точности числа из множества S.

Есть ровно один монотонный путь, в котором множество промежуточных вершин совпадает с данным множеством S: из-за монотонности нужно сначала посетить минимальное в S число, затем следующее по величине и т.д. Поэтому степени вершин в левой доле равны 1.

У каждого монотонного пути однозначно определено множество промежуточных вершин. Поэтому степени вершин в правой доле также равны 1.

Значит, этот граф — паросочетание. Поэтому количество монотонных путей в точности равно количеству подмножеств $(n-1)$-элементного множества, то есть равно 2^{n-1}.

7.3.2 Комбинаторное «правило деления»

Двудольные графы дают перечислительной комбинаторике не только паросочетания. Рассмотрим более подробно метод двойного подсчёта, который мы уже применяли раньше.

Суть этого метода в том, что число рёбер в двудольном графе равно сумме степеней вершин левой доли (каждое ребро имеет ровно один конец в левой доле). Но оно же равно и сумме степеней вершин в правой доле. Получаем равенство, которое можно использовать для выражения одних величин через другие.

Для перечислительной комбинаторики особенно важен случай, когда степени вершин в каждой доле одинаковы. Пусть в левой доле L вершин, в правой — R; степень каждой вершины в левой доле равна d_1, а в правой — d_2. Тогда выполняется равенство

$$Ld_1 = Rd_2, \tag{7.1}$$

которое мы образно будем называть «правилом деления». С помощью этого правила можно найти R, если известны все три величины: $R = Ld_1/d_2$ (вот оно, деление). Мы использовали частный случай этого правила для паросочетаний ($d_1 = d_2 = 1$).

Теперь рассмотрим примеры, когда одна из степеней отлична от 1.

Те слова длины k в n-символьном алфавите, в которых все символы разные, называют *упорядоченными выборками* или *размещениями* из n по k. (Представьте, что в лототроне лежат шары, помеченные всеми символами B, мы по очереди достаём шары из лототрона и фиксируем порядок их появления.)

Количество размещений из n по k обозначим $A_{n,k}$. Для краткости обозначений используем то же обозначение и для самого множества размещений. Из контекста нужно понимать, идёт ли речь о множестве или о его мощности.

Ясно, что $A_{n,k} = 0$, если $k > n$ (принцип кроликов, сейчас мы «сажаем» позиции слова в клетки, которые являются символами алфавита). В общем случае выполняется рекуррентное соотношение.

Утверждение 7.3. $A_{n,k} = (n-k+1)A_{n,k-1}$, $1 \leqslant k \leqslant n$.

Доказательство. Построим двудольный граф с долями $A_{n,k}$ и $A_{n,k-1}$, рёбра этого графа имеют вид

$$(b_1 b_2 \dots b_{k-1} b_k,\ b_1 b_2 \dots b_{k-1}).$$

Другими словами, мы соединяем ребром размещение длины k с его началом длины $k-1$. Поэтому степень любой вершины левой доли равна 1.

Степень любой вершины правой доли равна $n-k+1$: продолжить размещение можно любым из ещё неиспользованных $n-k+1$ символов алфавита.

Равенство утверждения теперь становится частным случаем равенства (7.1). □

Теорема 7.4. $A_{n,k} = n(n-1)(n-2)\cdot\ldots\cdot(n-k+1)$.

Доказательство. Применяя последовательно утверждение 7.3, получаем

$$\begin{aligned} A_{n,k} &= (n-k+1)A_{n,k-1} = (n-k+1)(n-k+2)A_{n,k-2} = \dots \\ &= (n-k+1)\cdot\ldots\cdot(n-1)nA_{n,0}. \end{aligned}$$

А размещение длины 0 ровно одно. □

Формулу из теоремы 7.4 можно записать через факториалы. По определению $n! = 1\cdot 2\cdot\ldots\cdot n$, $0! = 1$ (последнее не вполне очевидно из общего случая). Поэтому

$$A_{n,k} = n(n-1)(n-2)\cdot\ldots\cdot(n-k+1) = \frac{n!}{(n-k)!}\,.$$

Важный частный случай размещений получается при $k=n$. Получаем последовательности чисел из $[n]$ длины n. Такие последовательности называются *перестановками*. Количество перестановок находится по теореме 7.4, оно равно

$$A_{n,n} = \frac{n!}{0!} = n!\,.$$

Теперь рассмотрим *сочетания* или *неупорядоченные выборки*. В примере с лототроном это означает, что нас интересует лишь то, какие шары были вытащены, а не порядок их появления.

На обычном математическом языке это означает, что нас интересует *подмножество* вытащенных шаров. Вот и будем называть сочетанием из n элементов по k подмножество n-элементного множества, в котором ровно k элементов. Количество сочетаний из n по k будем обозначать C_n^k (обратите внимание на порядок индексов).

Теорема 7.5. $C_n^k = \dfrac{n!}{k!(n-k)!}\,.$

Доказательство. Как нетрудно догадаться, чтобы доказать равенство, в котором используется деление, нужно применить комбинаторное правило деления.

Используя формулу для размещений, перепишем это равенство в другом виде:

$$C_n^k \cdot k! = A_{n,k}\,. \tag{7.2}$$

Построим двудольный граф. Вершины левой доли — сочетания из n по k, то есть k-элементные подмножества множества $[n]$; вершины правой доли — размещения $A_{n,k}$. Рёбра графа соединяют пары (S, w), где S — это множество символов, которые встречаются в размещении w.

Из определения ясно, что степени вершин правой доли равны 1 (по размещению множество символов определяется однозначно).

Найдём степень вершины левой доли. Сколько есть размещений длины k, которые используют ровно k заданных символов? Это $A_{k,k} = k!$, то есть количество перестановок k символов.

Подставляя полученные значения в (7.1), получаем (7.2). □

Комбинируя уже известный приём с паросочетаниями, отсюда можно получить решения многих перечислительных задач.

Пример 7.5. Найдём количество двоичных слов длины n, в которых ровно k единиц.

Для этого ограничим граф из примера 7.3 на слова, у которых ровно k единиц. Соседями в этом графе будут как раз k-элементные множества. Значит, количество таких двоичных слов равно C_n^k.

7.4 Биномиальные коэффициенты

Рассмотрим *бином* $(x + y)^n$. Как известно из алгебры, целое алгебраическое выражение можно записать в виде многочлена. Поэтому

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k = x^n + \binom{n}{1} x^{n-1} y + \cdots + \binom{n}{n-1} x y^{n-1} + y^n. \qquad (7.3)$$

Здесь $\binom{n}{k}$ — числа, которые называются *биномиальными коэффициентами*. (Обратите внимание на порядок индексов.) Оказывается, это в точности числа сочетаний из n по k.

Теорема 7.6. $\binom{n}{k} = C_n^k$.

Доказательство. Давайте переходить от левой части (7.3) к правой в два этапа. Сначала раскроем скобки. Получим сумму выражений вида $xyyx\ldots$, где всего сомножителей n, а каждый из них — это x или y. Количество таких сомножителей равно количеству слов длины n в алфавите $\{x, y\}$, то есть равно 2^n (от замены символов $0, 1$ на x, y количество слов не изменяется).

Теперь «приведём подобные». Мы знаем, что сложение коммутативно и ассоциативно. Поэтому все слагаемые с одинаковым количеством x и y равны $x^{n-k}y^k$, где k — количество символов y (а количество символов x равно $n-k$, потому что других символов в этих выражениях нет).

Итак, $\binom{n}{k}$ равен количеству слагаемых с k символами y и $n-k$ символами x, а это количество равно количеству двоичных слов с k единицами, то есть C_n^k (см. пример 7.5). □

Лекция 8

Комбинаторика–3. Биномиальные коэффициенты и их друзья

8.1 Монотонные пути в квадранте

Мы уже рассматривали задачу подсчёта монотонных путей на прямой. Если двигаться можно только на 1 вправо, то ответ в такой задаче тривиальный: для любого n есть ровно один способ попасть из 0 в n.

Задача становится интереснее, если рассматривать монотонные пути на плоскости. Теперь мы двигаем фишку по точкам плоскости с целыми координатами. За один шаг можно увеличить абсциссу на 1 или ординату на 1. Сколько есть различных монотонных путей из точки $(0,0)$ в точку (a,b)? Обозначим это количество $T(a,b)$. Из правила суммы следует рекуррентное соотношение

$$T(a,b) = T(a-1,b) + T(a,b-1). \tag{8.1}$$

Действительно, все пути в (a,b) разбиваются на две группы: те, в которых на последнем шаге увеличивалась абсцисса, и те, в которых на последнем шаге увеличивалась ордината. Это первое и второе слагаемое в (8.1) соответственно.

Одной формулы (8.1) недостаточно для вычисления числа монотонных путей. Нужны ещё «граничные условия»:

$$T(0,b) = T(a,0) = 1 \tag{8.2}$$

(если возможно изменять лишь одну координату, путь единственный).

Пользуясь (8.1) и (8.2), можно посчитать количество монотонных путей для заданной пары (a,b) (при этом придётся решить ту же задачу и для всех пар (x,y), $x \leqslant a$, $y \leqslant b$). Вот несколько первых значений:

1	5	15	35	70
1	4	10	20	35
1	3	6	10	15
1	2	3	4	5
1	1	1	1	1

Есть и обычная, нерекуррентная формула для $T(a,b)$.

Теорема 8.1. $T(a,b) = \binom{a+b}{a} = \dfrac{(a+b)!}{a!b!}$.

Доказательство. Построим, как мы уже не раз делали, двудольный граф. Вершины левой доли — двоичные слова в алфавите $\{x,y\}$ длины $a+b$, а вершины правой доли — монотонные пути из $(0,0)$ в (a,b). Рёбра графа соединяют слово с путём, в котором на i-м шаге увеличивается та координата, которая записана в слове на i-м месте.

Этот граф — паросочетание: слово однозначно определяет путь, путь однозначно определяет слово. Количество слов в двоичном алфавите длины $a+b$, в которых a букв одного вида (и b букв другого) мы уже подсчитали: это как раз биномиальный коэффициент из $a+b$ по a. □

Биномиальные коэффициенты часто записывают в виде *треугольника Паскаля*

$$\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 1 & & 1 & & & & \\
 & & & 1 & & 2 & & 1 & & & \\
 & & 1 & & 3 & & 3 & & 1 & & \\
 & 1 & & 4 & & 6 & & 4 & & 1 & \\
1 & & 5 & & 10 & & 10 & & 5 & & 1
\end{array}$$

Легко увидеть, что это те же числа, что мы писали для точек квадранта, только теперь квадрант повёрнут вверх ногами (точнее, на угол 135°).

8.2 Свойства биномиальных коэффициентов

У нас появилось несколько равносильных способов определять биномиальные коэффициенты (они же числа сочетаний, они же — количество монотонных путей в квадранте). Это даёт возможность доказывать свойства биномиальных коэффициентов разными способами: привлекая комбинаторику, алгебру и даже анализ.

Рассмотрим начальную серию таких примеров.

Утверждение 8.2. *Каждая строка треугольника Паскаля симметрична относительно середины.*

Доказательство. В n-й строке треугольника Паскаля записаны биномиальные коэффициенты $\binom{n}{0}, \binom{n}{1}, \ldots, \binom{n}{n}$.

Симметрия относительно середины означает равенство

$$\binom{n}{k} = \binom{n}{n-k}.$$

Проще всего это равенство увидеть из формулы для числа сочетаний

$$\binom{n}{k} = C_n^k = \frac{n!}{k!(n-k)!} = \binom{n}{n-k}$$

(переставим сомножители в знаменателе). □

Не сложнее «натуральное доказательство» этого утверждения, которое сопоставляет k-элементному подмножеству n-элементного множества его дополнение, в котором как раз $n-k$ элементов.

Утверждение 8.3. *В первой половине строки треугольника Паскаля числа возрастают.*

Доказательство. И здесь нетрудно воспользоваться формулой для числа сочетаний. Но даже легче использовать двойной подсчёт.

Построим двудольный граф. Вершины левой доли — k-элементные подмножества n-элементного множества $[n]$; вершины правой доли — $(k+1)$-элементные подмножества того же множества. Рёбра — это пары (A, B), для которых $A \subset B$.

Каждое k-элементное подмножество A возможно расширить до $(k+1)$-элементного подмножества $n-k$ способами (столько элементов не входят в A). Поэтому степени вершин левой доли равны $n-k$.

В каждом $(k+1)$-элементном подмножестве B есть $k+1$ подмножество размера k (чтобы получить такое нужно удалить один из элементов подмножества B, а их $k+1$). Значит,

$$\binom{n}{k} \cdot (n-k) = \binom{n}{k+1} \cdot (k+1),$$

что равносильно

$$\binom{n}{k} \Big/ \binom{n}{k+1} = \frac{k+1}{n-k} < 1$$

при $2k < n-1$.

Таким образом, биномиальные коэффициенты растут до тех пор, пока не выполнится неравенство $k \geqslant (n-1)/2$, а это случится как раз в середине строки треугольника Паскаля. □

Утверждение 8.4. *Каждое число в треугольнике Паскаля по крайней мере в* 2 *раза меньше, чем число, которое стоит под ним.*

Доказательство. Тут полезно представление биномиальных коэффициентов как числа монотонных путей в квадранте и рекуррентная формула для этого числа.

Под числом $\binom{n}{k}$ стоит число в $(n+2)$-й строке треугольника Паскаля, это биномиальный коэффициент $\binom{n+2}{k+1}$.

Первое число — $\binom{n}{k}$ — это количество монотонных путей из $(0,0)$ в $A = (k, n-k)$; второе — $\binom{n+2}{k+1}$ — из $(0,0)$ в $B = (k+1, n-k+1)$. Из точки A в точку B ведёт два монотонных пути (увеличиваем сначала абсциссу, а потом ординату или наоборот). Поэтому каждый путь в A продолжается двумя способами до пути в B (а есть ещё, конечно, пути в B, которые вообще не проходят через A). □

Утверждение 8.5. *Количество подмножеств n-элементного множества с нечётным количеством элементов равно количеству подмножеств n-элементного множества с чётным количеством элементов.*

Доказательство. Поскольку количество k-элементных подмножеств n-элементного множества равно биномиальному коэффициенту, по сути речь идёт о том, что знакочередующаяся сумма чисел в строке треугольника Паскаля равна 0.

Запишем формулу бинома

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$$

и подставим в неё $1 = x = -y$. В левой части получится 0. А в правой

$$\sum_{k=0}^{n} \binom{n}{k} 1^{n-k}(-1)^k = \sum_{k \text{ чётное}} \binom{n}{k} - \sum_{k \text{ нечётное}} \binom{n}{k},$$

т.е. как раз знакопеременная сумма чисел в строке треугольника Паскаля. □

8.3 Мультиномиальные коэффициенты

Вместо бинома рассмотрим n-ю степень суммы нескольких переменных. Она также раскладывается в сумму мономов. Но теперь это мономы от нескольких переменных. Записывать такие мономы сложнее. Мы используем следующую запись: моном $x_1^{a_1} x_2^{a_2} \dots x_k^{a_k}$ однозначно определяется последовательностью показателей $\alpha = (a_1, a_2, \dots, a_k)$, мы будем обозначать такой моном сокращённо как x^α. Разложение

$$(x_1 + x_2 + \dots + x_k)^n = \sum_{\alpha} \binom{n}{\alpha} x^\alpha \tag{8.3}$$

приводит сразу к двум интересным задачам перечислительной комбинаторики.

Первая состоит в нахождении формулы для *мультиномиальных коэффициентов*, т.е. коэффициентов в разложении 8.3. Приведём сразу ответ, а потом дадим два разных доказательства этой формулы.

Теорема 8.6. $\displaystyle\binom{n}{a_1, a_2, \dots, a_k} = \frac{n!}{a_1! a_2! \dots a_k!}$.

Эту теорему можно доказать двумя способами: алгебраическим и комбинаторным. Приведём сначала комбинаторное доказательство.

У мультиномиальных коэффициентов есть внятный комбинаторный смысл. Вспомним, как мы находили формулу для биномиальных коэффициентов. Мы раскладывали бином в два шага: сначала раскрывали скобки, а затем приводили подобные.

Что даёт раскрытие скобок в выражении (8.3)? Получаются слагаемые, каждое из которых имеет вид $x_1 x_2 x_2 \dots$. Это слово ξ в алфавите $\{x_1, \dots, x_k\}$, в котором n букв. После перестановок переменных из этого слова получается моном $x_1^{a_1} x_2^{a_2} \dots x_k^{a_k}$, где a_i — количество букв x_i в слове ξ.

Значит, мультиномиальный коэффициент $\binom{n}{a_1,\dots,a_n}$ равен количеству слов в алфавите $\{x_1, \dots, x_k\}$, длина которых равна n, а количество вхождений каждого символа задаётся числами $a_1, \dots, a_n$.

Комбинаторное доказательство теоремы 8.6. Построим двудольный граф. Вершины левой доли — слова в алфавите $\{x_1, \ldots, x_k\}$, в которых a_1 букв x_1, a_2 букв x_2, и т.д., $a_1 + \cdots + a_k = n$. Вершины правой доли — перестановки чисел от 1 до n.

Чтобы определить рёбра этого графа, разделим числа от 1 до n на k групп так, чтобы в j-й группе было ровно a_j чисел. Пусть первая группа состоит из чисел от 1 до a_1; вторая — от $a_1 + 1$ до $a_1 + a_2$; $\ldots$; k-я группа — числа от $a_1 + \cdots + a_{k-1} + 1$ до n.

Рёбрами в нашем графе будут пары (ξ, π), где слово ξ получается из перестановки $\pi = (\pi_1, \ldots, \pi_n)$ заменой каждого числа π_i на x_j, где j — номер группы, в которую входит это число.

Степень каждой вершины в правой доле этого графа равна 1 (по перестановке однозначно определяется смежное с ней слово).

Чтобы найти степень слова (вершины левой доли), обратим внимание на то, что если (ξ, π) — ребро графа, то вхождения буквы x_j в слово ξ заменяются в перестановке π на числа из j-й группы. Порядок этих чисел произвольный и каждое число должно быть использовано ровно один раз.

Всего есть $a_j!$ перестановок a_j чисел j-й группы, сохраняющих их места в перестановке π. По правилу произведения общее количество перестановок, связанных ребром со словом ξ равно $a_1!a_2! \ldots a_k!$. Подсчитывая число рёбер в построенном графе двумя способами, получаем равенство

$$\binom{n}{a_1 \ldots a_k}\big(a_1! \ldots a_k!\big) = n!\,,$$

что и требовалось. □

Теперь приведём доказательство, основанное на индукции по числу слагаемых в формуле 8.6.

Алгебраическое доказательство теоремы 8.6. Индукция по числу переменных k.

База индукции: $k = 2$. Это обычная формула для биномиальных коэффициентов, см. теорему 7.5. Поскольку $a_1 + a_2 = n$, то

$$\binom{n}{a_1, a_2} = C_n^{a_1} = \frac{n!}{a_1!(n - a_1)!} = \frac{n!}{a_1!a_2!}\ .$$

Шаг индукции. Предполагаем, что формула из теоремы 8.6 доказана для k. Представим $x_1 + \cdots + x_k + x_{k+1}$ как $(x_1 + \cdots + x_k) + x_{k+1}$ и запишем разложение n-й степени суммы $k + 1$ переменной как бинома от этих двух слагаемых:

$$(x_1 + x_2 + \cdots + x_k + x_{k+1})^n = \sum_{j=0}^{n} \binom{n}{j} (x_1 + x_2 + \cdots + x_k)^j x_{k+1}^{n-j}.$$

Теперь раскрываем скобки в множителях вида $(x_1+x_2+\cdots+x_k)^j$ и из индуктивного предположения получаем равенство

$$\binom{n}{a_1,\ldots,a_k,a_{k+1}} = \binom{n}{j}\binom{j}{a_1,\ldots,a_k} =$$
$$= \frac{n!}{j!(n-j)!}\cdot\frac{j!}{a_1!a_2!\ldots a_k!} = \frac{n!}{a_1!a_2!\ldots a_k!(n-j)!}\,.$$

Осталось заметить, что $n-j = n-a_1-\cdots-a_k = a_{k+1}$. □

Рассмотрим типичный пример применения формулы для мультиномиальных коэффициентов.

Пример 8.1. Три человека составляют график дежурств на 6 дней. Каждый день дежурит кто-то один, каждый должен дежурить ровно 2 дня. Сколько есть вариантов составления графика?

Обозначим людей А, Б, В. Каждый график дежурств представляется словом в алфавите $\{\text{А},\text{Б},\text{В}\}$: слово ААББВВ означает, что в первые два дня дежурит А, в следующий день — Б и т.д. Таким образом, вариантов составления графика столько же, сколько слов в 3-элементном алфавите длины 6, в которые каждая буква входит ровно два раза. Это и есть мультиномиальный коэффициент

$$\binom{6!}{2!2!2!} = 90.$$

8.4 Сочетания с повторениями

Вторая перечислительная задача, связанная с разложением степени суммы (8.3) состоит в подсчёте числа различных мономов в этом разложении. Степень монома — это сумма степеней переменных, в него входящих. Степень монома $x_1x_2x_3$ равна 3, степень монома $x_1^2x_2$ также равна 3. А сколько всего мономов от трёх переменных степени 3? На такой вопрос нетрудно ответить, выписав все нужные мономы:

$$x_1^3,\ x_2^3,\ x_3^3,\ x_1^2x_2,\ x_1^2x_3,\ x_1x_2^2,\ x_2^2x_3,\ x_1x_3^2,\ x_2x_3^2,\ x_1x_2x_3.$$

Но даже в этом случае нужно проверить, что мы ничего не пропустили и эти 10 мономов и есть все возможные варианты.

Сформулируем задачу точно. Моном $x_1^{a_1}x_2^{a_2}\ldots x_k^{a_k}$ имеет степень $a_1+\cdots+a_k$ и мономы совпадают тогда и только тогда, когда соответствующие последовательности показателей равны. Поэтому нам нужно найти количество решений уравнения

$$a_1+\cdots+a_k = n \tag{8.4}$$

в неотрицательных целых числах. Это число традиционно называется *числом сочетаний с повторениями* из n по k. Обозначим его

$$\left(\!\binom{n}{k}\!\right)\,.$$

Название можно объяснить примером с лототроном, который рассматривался выше. Теперь мы каждый раз возвращаем выпавший шар в лототрон, поэтому шары могут повторяться. Но нам неважно, как и раньше, в каком порядке выпадали эти шары.

Ещё одно популярное представление чисел с повторениями даётся в формулировке следующей задачи.

Задача 8.2. Сколько есть вариантов разделить n одинаковых монет между k людьми?

Это то же самое число сочетаний с повторениями из n по k. Действительно, каждый вариант делёжки задаётся указанием числа a_1 монет, которые получает первый человек, числа a_2 монет, которые получает второй и т.д.

Теорема 8.7. $\left(\!\binom{n}{k}\!\right) = \binom{n+k-1}{k-1}$.

Доказательство. Установим взаимно однозначное соответствие между решениями уравнения (8.4) и $(k-1)$-элементными подмножествами $(n+k-1)$-элементного множества. Будем делать это, используя терминологию задачи о разделе монет.

Выстроим монеты в ряд и разделим их перегородками, чтобы указать, кому какие монеты отходят. Первый получает монеты, которые расположены до первой перегородки, второй — те, которые лежат между первой и второй, и т.д. Например, на рисунке 8.1 показан раздел 7 монет между 7 людьми, при котором первому не

Рис. 8.1: $a_1 = 0$, $a_2 = 2$, $a_3 = 0$, $a_4 = 2$, $a_5 = 0$, $a_6 = 1$, $a_7 = 2$

достаётся ничего, второму — две монеты, третьему — ничего, четвёртому — две монеты, пятому — ничего, шестому — одна, а седьмому — две монеты.

Такой раздел отвечает решению уравнения (8.4), которое указано в подписи под рисунком.

Последний человек получает монеты, которые лежат после последней перегородки. Поэтому для 7 людей нужно всего 6 перегородок. А в общем случае, когда людей k, нужна $k-1$ перегородка.

Итак, у нас есть позиции, на каждую из которых можно поставить либо монету, либо перегородку. Всего позиций $n+k-1$, а перегородок — $k-1$. Любой выбор $(k-1)$-элементного подмножества позиций, на котором стоят перегородки, возможен, и каждому такому выбору отвечает ровно одно решение уравнения (8.4). Получаем искомое соответствие. □

Если монеты выглядят неубедительно, то можно использовать то же по сути рассуждение, но в другой комбинаторной ситуации.

Задача 8.3. Сколько есть монотонных путей длины k по прямой из 0 в n?

Решение. Монотонный путь длины k по прямой из 0 в n — это другое название такой строго возрастающей последовательности целых чисел $x_1 < \cdots < x_{k+1}$, что $x_1 = 0$, $x_{k+1} = n$ (длина пути — это количество шагов, оно на 1 меньше количества членов последовательности).

Такой монотонный путь однозначно задаётся выбором $k-1$ числа в интервале от 1 до $n-1$ (путь монотонный, поэтому эти числа он обязан проходить в порядке возрастания).

Поэтому число таких путей равно числу $(k-1)$-элементных подмножеств $(n-1)$-элементного множества, то есть $\binom{n-1}{k-1}$. □

А какое отношение имеют эти пути к нашей задаче о числе решений уравнения (8.4)? Заметим, что путь однозначно задаётся последовательностью длин ходов: $\ell_1 = x_2 - x_1 = x_2$, $\ldots \ell_k = x_{k+1} - x_k = n - x_k$. В сумме эти числа обязаны давать n:

$$\ell_1 + \cdots + \ell_k = n. \tag{8.5}$$

Получаем то же самое уравнение. Вот только ответ почему-то другой получился...

Разница между уравнениями (8.4) и (8.5) в том, какие решения мы подсчитываем. В первом случае мы искали решения в *неотрицательных целых* числах. А во втором нам нужны решения в *положительных целых* числах: ведь стоять на месте не разрешается, все длины ходов должны быть положительными.

Чтобы связать эти два числа, заметим, что если $a_1 + \cdots + a_k = n$ — решение уравнения (8.4) в неотрицательных числах, то ему однозначно соответствует решение уравнения

$$\ell_1 + \cdots + \ell_k = n + k \tag{8.6}$$

в положительных числах: $\ell_i = a_i + 1$. И наоборот, по решению $\ell_1, \ldots, \ell_k$ уравнения (8.6) в положительных целых числах однозначно строится решение уравнения (8.4) в неотрицательных целых числах: $a_i = \ell_i - 1$.

Из решения задачи 8.3 получаем ту же самую формулу

$$\left(\!\binom{n}{k}\!\right) = \binom{n+k-1}{k-1}$$

для числа сочетаний с повторениями.

8.5 Числа Каталана

Приведём ещё один пример перечислительной задачи, где в ответе возникают биномиальные коэффициенты.

Задача 8.4. Робот ходит по целочисленным точкам координатной плоскости, удовлетворяющим условиям $x \geqslant 0$, $y \geqslant 0$, $x \geqslant y$. На каждом шаге он может увеличить одну из координат на 1. Докажите, что количество способов, которыми можно переместить Робота из точки $(0,0)$ в точку (n,n), равно

$$\frac{1}{n+1}\binom{2n}{n}.$$

Числа, которые возникают в ответе этой задачи, называются *числами Каталана*. Это последовательность чисел является ответом в очень многих задачах перечислительной комбинаторики. Монотонные пути по треугольнику — не самая известная из них.

Подробнее про числа Каталана можно прочитать в учебнике «Лекции по дискретной математике» (М. Вялый, В. Подольский, А. Рубцов, Д. Шварц, А. Шень), раздел 2.10; черновой вариант доступен по ссылке
`publications.hse.ru/mirror/pubs/share/direct/393719078.pdf`.

Ещё больше различных комбинаторных представлений чисел Каталана (более 30) можно найти в материалах 14-й летней конференции международного математического Турнира городов, `olympiads.mccme.ru/lktg/2002/problem2.ru/index.htm`.

Но и этот список далеко не полный.

Лекция 9

Отношения и функции–1

9.1 Бинарные отношения

Язык двудольных графов не всегда удобен. Оказывается полезным ввести более общее понятие.

Определение 9.1. *Бинарным отношением на множествах A и B* называется любое подмножество R декартова произведения $A \times B$.

Двудольный граф на долях L и R задаёт бинарное отношение на множествах A и B. Но в общем случае множества A и B не обязаны быть дизъюнктными (без общих элементов). Во многих интересных случаях это попросту одно и то множество. Тогда говорим о бинарном отношении на множестве.

Пример 9.1. Рассмотрим множество пар действительных чисел (x, y), для которых $x < y$. Это множество по определению задаёт бинарное отношение «строго меньше» на действительных числах.

Пример 9.2. «x является родителем y» — это бинарное отношение на множестве людей.

«x является братом y» — это бинарное отношение на множестве мужчин и множестве людей. В данном случае множества не совпадают, но пересекаются.

Часто бинарные отношения обозначаются как $R(x, y)$ или даже как $x\ R\ y$. Эта запись указывает на утверждение «x и y находятся в отношении R» или, более формально, $(x, y) \in R$. В общем случае такое утверждение истинно для одних пар (x, y) и ложно для других.

Отношения на конечных множествах, как и графы, удобно задавать матрицами. Строки такой матрицы обычно отвечают первому множеству в отношении, а столбцы — второму. На пересечении строки a и столбца b стоит 1, если $(a, b) \in R$, и 0 в противном случае. Часто удобно считать, что это не числа, а логические значения: 1 отвечает истинности высказывания $(a, b) \in R$, а 0 — ложности.

Разумеется, нет принципиальной разницы между строками и столбцами. Если транспонировать матрицу отношения, получим *транспонированное отношение*: $R^T = \{(b,a) : (a,b) \in R\} \subseteq B \times A$.

Пример 9.3. «x является ребёнком y» — это бинарное отношение на множестве людей, которое транспонировано к отношению «x является родителем y».

Из одних отношений можно строить другие как с помощью теоретико-множественных операций, так и с помощью операции композиции.

Определение 9.2. Пусть даны два отношения $R \subset A \times B$ и $S \subset B \times C$. Их *композицией* называется отношение $S \circ R \subseteq A \times C$, определяемое так:

$$(x,z) \in S \circ R \Leftrightarrow \text{существует такой } y \in B, \text{ что } (x,y) \in R \text{ и } (y,z) \in S.$$

Обратите внимание, что (1) композиция определена не для всех отношений, необходимо совпадение второго множества в первом отношении и первого во втором; (2) порядок записи отношений в композиции важен, ниже станет ясно, почему выбран именно такой порядок.

Если задавать отношения на конечных множествах матрицами, композиция отношений задаётся формулой, напоминающей формулу произведения числовых матриц, но операции в этой формуле логические:

$$R(x,y) = \bigvee_{z \in B} \big(R(x,z) \wedge R(z,y)\big).$$

Как и умножение числовых матриц, композиция отношения обладает свойством ассоциативности.

Лемма 9.3. *Если $R \subset A \times B$, $S \subset B \times C$ и $T \subset C \times D$, то $(R \circ S) \circ T = R \circ (S \circ T)$.*

Доказательство. Обе части равенства задают отношение M, для которого $M(x,t)$ равносильно тому, что найдутся такие $y \in B$ и $z \in C$, что одновременно $R(x,y)$, $S(y,z)$ и $T(z,t)$:

$$M(x,t) \Leftrightarrow (\exists\, y \in B)(\exists\, z \in C)[R(x,y) \wedge S(y,z) \wedge T(z,t)].$$

Обе импликации непосредственно следуют из определения композиции. □

Рассмотрим несколько примеров.

Пример 9.4. Чему равна композиция отношения $P =$«x является родителем y» с самим собой? Это отношение «x является дедом или бабушкой y». Проверим это формально, исходя из определения.

$(x,y) \in P \circ P$ тогда и только тогда, когда найдётся такой z, что $(x,z) \in P$ и $(z,y) \in P$. Это означает, что x — родитель z, а z — родитель y. В обычном языке такое свойство выражается как раз словами «дед» или «бабушка», в зависимости от пола x.

Пример 9.5. Для отношения $x < y$ строгого сравнения действительных чисел выполняется $< \circ < = <$. Проверим это формально.

$(x, y) \in < \circ <$ тогда и только тогда, когда найдётся такой z, что $x < z$ и $z < y$. По свойству сравнения действительных чисел получаем $x < y$, откуда следует включение $< \circ < \subseteq <$.

Чтобы доказать равенство, нужно проверить обратное включение. Для этого нужно доказать, что если $x < y$, то найдется такой z, что $x < z$, $z < y$. В качестве числа z можно взять, например, полусумму $(x + y)/2$.

Пример 9.6. Композиция отношения $B =$«x является братом y» с самим собой не определена, поскольку это отношение на разных множествах. Но определена композиция $B \circ B^T$. Это отношение на множестве мужчин. Совпадает ли оно совпадает с отношением братства, если ограничить его на множество мужчин?

Будем обозначать такое ограниченное отношение той же буквой B. Легко видеть, что B *симмметрично*: $B^T = B$ (на множестве мужчин справедливо утверждение «если x брат y, то y — брат x»).

Легко видеть, что $B \circ B \subseteq B$. Если $(x, y) \in B \circ B$, то существует такой z, что x брат z, а z брат y. Но брат моего брата — мой брат[1)]. Поэтому $(x, y) \in B$.

Обратное включение может и не выполняться. Допустим x и y — братья, но других братьев у них нет. Тогда $(x, y) \in B$, но $(x, y) \notin B \circ B$. Здесь мы считаем, следуя смыслу слов в естественном языке, что отношение братства *антирефлексивно*: $(x, x) \notin B$ для любого x (я не считаю себя своим братом).

9.2 Более общие отношения

Мы рассмотрели бинарные отношения. Есть более общее понятие отношения R на нескольких множествах A_1, A_2,..., A_k. Это по определению подмножество декартова произведения $A_1 \times A_2 \times \cdots \times A_k$. Такое отношение называют k-арным или отношением валентностии k.

Наиболее важны *унарные* отношения, то есть подмножества множества и бинарные, которые мы рассмотрели выше. Однако встречаются и отношения большей арности, как в математике, так и в приложениях.

Пример 9.7. Тернарное отношение $S(x, y, z)$ на действительных числах — это множество таких троек (x, y, z), что $x = y + z$. Последняя запись уже может рассматриваться как задание отношения. Это равенство истинно или ложно для любой тройки чисел.

Аналогично можно рассматривать отношение «(x, y, z) — координаты точки на единичной сфере» и т.п.

Пример 9.8. Результаты проверки домашнего задания являются тернарным отношением «x получил за задачу y оценку z». на множествах `Студенты`, `Задачи`, `Оценки`.

[1)] Такое свойство отношений называется *транзитивностью*.

В реляционных базах данных аналогичным образом используются и отношения бóльшей арности.

Мы не будем подробно разбираться с отношениями большой арности. Ограничимся несколькими важными классами бинарных отношений.

9.3 Функции

Важнейшее для математики понятие функции естественно определяется в терминах бинарных отношений.

Неформально под функцией мы понимаем соответствие: элементам одного множества сопоставляются элементы другого множества, причём каждому элементу ставится в соответствие не более одного элемента второго множества.

Дадим формальные определения понятий, связанных с функциями.

Определение 9.4. *Функцией* f из множества A в множество B (обозначение $f\colon A \to B$) называется такое бинарное отношение $f \subseteq A \times B$, что для каждого $a \in A$ есть не более одной пары $(a, b) \in \Gamma_f$. Если такая пара существует, используется также обозначение $b = f(a)$.

Элементы множества A называются *аргументами* функции, элементы множества B — значениями функции.

Область определения $\mathrm{Dom}\, f$ функции из A в B — это множество тех a, для которых существует такой b, что $(a, b) \in f$. Формальная запись этого определения:

$$\mathrm{Dom}(f) = \{x \in A \mid \exists y \in B\colon y = f(x)\}.$$

Если $\mathrm{Dom}(f) = A$, то функция называется *тотальной* (всюду определённой). Нетотальные функции называют *частичными*.

Область значений $\mathrm{Range}\, f$ — это множество тех b, для которых существует такой a, что $(a, b) \in \Gamma_f$. Формальная запись этого определения:

$$\mathrm{Range}(f) = \{y \in B \mid \exists x \in A\colon y = f(x)\}.$$

Замечание 9.1. Отношение f называют ещё *графиком функции* и иногда обозначают Γ_f, чтобы различать график и саму функцию. При нашем определении функция и график — это одно и то же. Но в рассуждениях о функциях исторически принято использовать оба термина.

Неформально, мы говорим о функции, если речь идёт о соответствии («значение функции от данного аргумента»), и о графике, если речь идёт об отношении целиком («график линейной функции — прямая»).

Замечание 9.2. Тотальные функции мы будем также называть *отображениями*. Функция и отображение, в сущности, синонимы, но в разных областях математики преимущественно употребляется тот или иной термин.

Замечание 9.3. Если применить операцию композиции к функциям, то получится функция. В привычных обозначениях значение композиции $(f \circ g)(x)$ равно $f\big(g(x)\big)$ (и требуется, чтобы $x \in \operatorname{Dom} g$, а $g(x) \in \operatorname{Dom} f$. Наш выбор порядка отношений в композиции согласован с обозначением $f\big(g(x)\big)$.

С функцией из A в B можно связать двудольный граф с долями A и B. Ребро такого графа связывает a и $f(a)$. Двудольные графы, отвечающие функциям, и только они обладают таким свойством: из каждой вершины доли A выходит не более одного ребра.

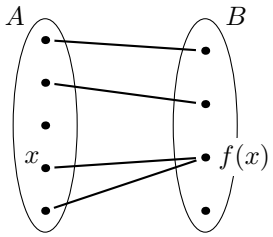


Рис. 9.1: функция

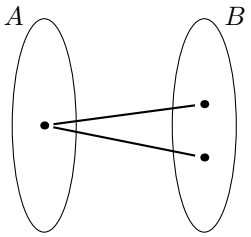


Рис. 9.2: не функция

Эта конструкция корректна, если A и B — непересекающиеся множества. Если у них есть общие элементы при построении графа нужно мысленно «дублировать» общие элементы A и B, отправляя один в левую долю, а другой — в правую. Именно поэтому удобнее использовать язык бинарных отношений.

С функциями из A в A (множество аргументов и значений совпадают) можно также связать ориентированный граф, рёбрами которого являются пары $(x, y) \in f$. Исходящая степень вершины в таком графе не больше 1.

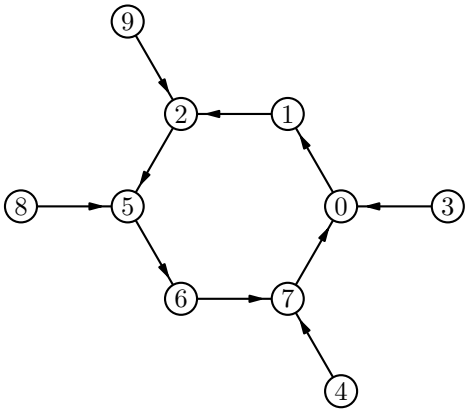


Рис. 9.3: Ориентированный граф функции

9.4 Сюръекции, инъекции, биекции

Из тотальных функций $A \to B$ выделяются некоторые функции с особыми свойствами.

Транспонированное к графику отношение не является в общем случае функцией. Если $y = f(x_1) = f(x_2)$ и $x_1 \neq x_2$, то $(x_1, y) \in \Gamma_f$, $(x_2, y) \in f$. Поэтому $(y, f_1) \in f^T$ и $(y, f_2) \in f^T$, что противоречит определению (графика) функции.

Тотальная функция $f\colon A \to B$ называется *инъекцией*, если транспонированное отношение f^T также является функцией. Другими словами, значения инъекции в различных точках различны. Пересказывая определения функции и транспонированного отношения, получаем такое равносильное определение: f — инъекция, если $x_1 \neq x_2$ влечёт $f(x_1) \neq f(x_2)$. (Или контрапозиция: f — инъекция, если $f(x_1) = f(x_2)$ влечёт $x_1 = x_2$.)

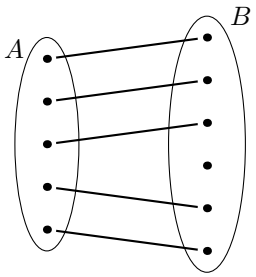


Рис. 9.4: инъекция

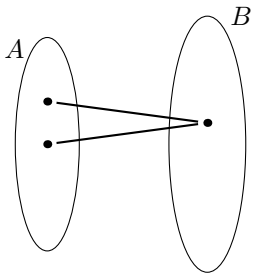


Рис. 9.5: не инъекция

Тотальная функция $f\colon A \to B$ называется *сюръекцией*, если область значений совпадает со всем множеством B, то есть если для всякого элемента $y \in B$ найдётся элемент $x \in A$, для которого $f(x) = y$.

Пример сюръекции изображён на рис. 9.6. Примеры не сюръекций изображены на рисунке 9.7 (а также на рисунке 9.4): для сюръективной функции не должно быть точек справа, в которые не ведёт ни одного ребра.

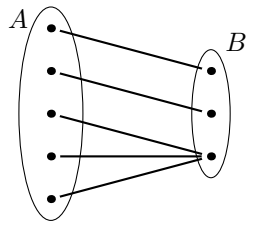


Рис. 9.6: сюръекция

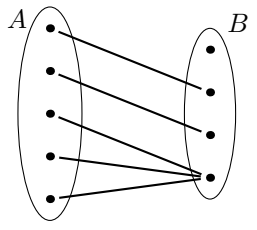


Рис. 9.7: не сюръекция

Наконец, тотальная функция $f\colon A \to B$ называется *биекцией*, если она одновременно является и инъекцией, и сюръекцией. Другими словами, функция является

биекцией, если всякому элементу из B соответствует ровно один элемент из A.

Лемма 9.5. *Для тотальных функций из конечного множества в конечное выполняются такие свойства:*

1. *если $f\colon A \to B$ сюръекция, то $|A| \geqslant |B|$;*
2. *если $f\colon A \to B$ инъекция, то $|A| \leqslant |B|$;*
3. *если $f\colon A \to B$ биекция, то $|A| = |B|$.*

Доказательство. Первый факт утверждает неформально, что если рассадить кроликов по клеткам и в каждой клетке есть хотя бы один кролик, то кроликов не меньше, чем клеток.

Формально: обозначим через a_i, $i \in B$, количество тех элементов $a \in A$, для которых $f(a) = i$ (размер *полного прообраза* множества $\{i\}$). Для сюръекции $a_i \geqslant 1$ для любого i. Поэтому

$$|A| = \sum_i a_i \geqslant \sum_i 1 = |B|.$$

Первое равенство выполняется потому, что a_i подсчитывают элементы в непересекающихся подмножествах A (функция сопоставляет каждому элементу A только один элемент B).

Второй факт означает неформально, что если в комнате есть люди и стулья, и каждый человек сел на стул, то людей не больше, чем стульев.

Формальное доказательство получается из выражения свойства инъекции в виде $a_i \leqslant 1$ для любого i. Тогда

$$|A| = \sum_i a_i \leqslant \sum_i 1 = |B|.$$

Третий факт непосредственно следует из первых двух. □

Когда мы строили взаимно однозначные соответствия, мы фактически задавали биекции. В отличие от двудольных графов, в общем случае нет нужды следить за тем, чтобы множества, между которыми строится биекция, не пересекались. Они даже могут совпадать.

Что такое биекция множества A на себя? Посмотрим на ориентированный граф такой функции. Исходящая степень каждой вершины равна 1 (функция тотальная) и входящая степень каждой вершины равна 1 (сюръективна и инъективна). Мы такие графы полностью расклассифицировали: это объединения ориентированных циклов.

Если $A = [n]$, то биекциям $[n] \to [n]$ взаимно однозначно соответствуют перестановки. Биекции $f\colon [n] \to [n]$ сопоставляем перестановку $f(1)f(2)\dots f(n)$ (каждое число использовано и ровно по одному разу). Поэтому биекции $[n] \to [n]$ часто также называют перестановками. Ориентированный граф такой перестановки называется *цикловым разложением.*

9.5 Индикаторные функции

Если множество значений функции — действительные числа, с такими функциями можно выполнять арифметические действия «поточечно»:

$$(f+g)(x) = f(x) + g(x), \quad (fg)(x) = f(x)g(x).$$

Приведём один важный пример. *Индикаторная функция* $\chi_S \colon X \to \mathbb{R}$ подмножества S множества X опредедяется как

$$\chi_S(x) = \begin{cases} 1, & \text{если } x \in S, \\ 0 & \text{в противном случае.} \end{cases}$$

Индикаторные функции χ_{S_1} и χ_{S_2} равны тогда и только тогда, когда подмножества S_1 и S_2 равны. Таким образом, индикаторные функции и подмножества — это два способа говорить об одном и том же.

Покажем, как на языке индикаторных функций доказывается формула включений-исключений. Будем считать, что все рассматриваемые множества лежат в каком-то объемлющем множестве (*универсуме*), например, в объединении всех множеств, для которых доказывается формула.

Теоретико-множественные операции выражаются через индикаторные функции. Для пересечения

$$\chi_{A\cap B}(x) = \chi_A(x) \cdot \chi_B(x)$$

(x принадлежит пересечению тогда и только тогда, когда $x \in A$ и $x \in B$). Для дополнения получаем

$$\chi_{\overline{A}}(x) = 1 - \chi_A(x),$$

для разности

$$\chi_{A\setminus B}(x) = \chi_A(x) \cdot \big(1 - \chi_B(x)\big),$$

для объединения

$$\chi_{A\cup B}(x) = 1 - \big(1 - \chi_A(x)\big)\big(1 - \chi_B(x)\big). \tag{9.1}$$

Доказать последнюю формулу можно как разбором случаев, так и с помощью логических формул де Моргана: $A \cup B = \overline{\overline{A} \cap \overline{B}}$. Формула (9.1) получается из предыдущих заменой левой части формулы де Моргана на правую.

Аналогично можно выразить и объединение нескольких множеств через дополнения и переесечения:

$$\bigcup_{i=1}^{n} A_i = \overline{\bigcap_{i=1}^{n} \overline{A}_i} \tag{9.2}$$

(в объединение множеств A_i входят в точности те элементы, которые не входят в пересечение всех дополнений).

Обозначим $A = \bigcup_{i=1}^{n} A_i$. Для индикаторных функций из (9.2) получаем

$$\chi_A(x) = 1 - \big(1 - \chi_{A_1}(x)\big)\big(1 - \chi_{A_2}(x)\big) \ldots \big(1 - \chi_{A_n}(x)\big). \tag{9.3}$$

Раскроем скобки в (9.3) и заменим произведения индикаторных функций на индикаторные функции пересечений. Для удобства записи через A_S обозначим пересечение всех множеств, входящих в семейство S, то есть

$$A_S = \bigcap_{i \in S} A_i.$$

Получаем

$$\chi_A(x) = \sum_{S \neq \varnothing} (-1)^{|S|+1} \chi_{A_S}(x)$$

(перед произведением стоит минус, в каждой скобке стоит минус; поэтому коэффициент при произведении k множителей равен $(-1)^{k+1}$).

Количество элементов в множестве выражается как сумма индикаторной функции по всему универсуму:

$$|A| = \sum_u \chi_A(u)$$

(каждый элемент множества даёт вклад 1 в сумму, остальные элемементы дают вклад 0).

Поэтому для размера объединения получается формула

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \sum_{S \neq \varnothing} (-1)^{|S|+1} |A_S|,$$

это и есть формула включений-исключений.

Лекция 10

Отношения и функции–2

10.1 Композиции функций

Функции мы определяем как особый вид отношений. Ограничение операции композиции отношений на функции даёт операцию *композиции функций*.

Разворачивая определения функции и композиции отношений, получаем: для функции f из множества A в множество B и функции g из множества B в множество C *композицией* $g \circ f$ этих функций является такая функция из A в C, которая определена на тех x из области определения функции f, для которых $f(x)$ принадлежит области определения функции g, и равна $g(f(x))$. Это действительно функция, а не более общее отношение, так как каждое значение $x \in A$ аргумента находится в отношении не более чем с одним элементом из C.

Отсюда становится понятным порядок записи отношений в композиции. Мы хотим, чтобы он был согласован с порядком записи функций в привычном обозначении $g(f(x))$.

Как и в общем случае, композиция функций ассоциативна:

$$(f \circ g) \circ h = f \circ (g \circ h).$$

10.2 Обратная функция

Тождественной функцией на множестве A (или тождественным отображением множества A в себя) называется функция $\mathrm{id}_A \colon A \to A$, которая отображает всякий элемент $x \in A$ в себя: $\mathrm{id}_A(x) = x$. При композиции тождественные функции ведут себя, как единица при умножении: для любого отображения $f \colon A \to B$ выполнены равенства

$$\mathrm{id}_B \circ f = f \circ \mathrm{id}_A = f.$$

(Обратите внимание, что здесь две тождественные функции — одна на A, другая на B, иначе композицию нельзя определить.)

Для биекции $f \colon A \to B$ (взаимно однозначного отображения) определена *обратная функция* (или обратное отображение) f^{-1}: если f отображает x в y, то обратная

функция f^{-1} отображает y в x. Инъективность f гарантирует, что это действительно функция, а сюръективность f гарантирует, что эта функция определена на всём B.

Заметим, что определение обратной функции симметрично: если g обратна к f, то и f обратна к g.

Свойство биективности может быть выражено алгебраическими средствами.

Теорема 10.1. *Если для отображений $f\colon A \to B$ и $g\colon B \to A$ выполнены два равенства $g \circ f = \mathrm{id}_A$ и $f \circ g = \mathrm{id}_B$, то функция f является биекцией и g обратна к f.*

Доказательство. Пусть $f(x_1) = f(x_2)$. Тогда из первого условия на композиции получаем:

$$x_1 = (g \circ f)(x_1) = g(f(x_1)) = g(f(x_2)) = (g \circ f)(x_2) = x_2.$$

Значит, функция f инъективна.

Для любого $y \in B$ из второго условия на композиции следует, что $y = f(g(y))$, то есть y принадлежит множеству значений f. Значит, функция f сюръективна.

Итак, f биекция.

Если $y = f(x)$, то из первого условия на композиции получаем $g(y) = g(f(x)) = x$. Значит, g обратна к f. □

Выполнения одного условия $g \circ f = \mathrm{id}_A$ недостаточно, чтобы утверждать, что f биекция.

Пример 10.1. Определим две функции на множестве неотрицательных целых чисел: $f\colon x \mapsto 2x$ и $g\colon x \mapsto \lfloor x/2 \rfloor$. Композиция $g \circ f$ — тождественное отображение:

$$x \xrightarrow{f} 2x \xrightarrow{g} x$$

для любого x. Однако f не биекция: у числа 1 нет прообраза.

Аналогичное замечание справедливо и для второго условия $f \circ g = \mathrm{id}_B$.

Ещё один важный факт: композиции сохраняют биекции. Другими словами,

Теорема 10.2. *Если отображения $f\colon A \to B$ и $g\colon B \to C$ — биекции, то и их композиция $g \circ f\colon A \to C$ является биекцией.*

Доказательство. Разные элементы A переходят в разные элементы B, потому что f инъекция, и эти разные элементы B переходят в разные элементы C, потому что g инъекция. Таким образом, при $a \neq a'$ получаем $f(a) \neq f(a')$ и затем $g(f(a)) \neq g(f(a'))$, так что $g \circ f$ — инъекция. Ещё надо проверить, что $g \circ f$ — сюръекция, то есть что в каждый элемент $c \in C$ что-то переходит. Но мы знаем, что g — сюръекция, так что $c = g(b)$ для некоторого $b \in B$; поскольку f — сюръекция, то $b = g(a)$ для некоторого $a \in A$, так что $c = g(b) = g(f(a)) = (g \circ f)(a)$. □

10.3 Подсчёты числа функций

Пример 10.2. Сколько есть тотальных функций из k-элементного множества в n-элементное?

Ответ: ровно столько же, сколько есть слов длины k в алфавите из n символов.

Пусть $|A| = k$, $|B| = n$. Занумеруем элементы A: $a_1, a_2, \ldots, a_k$.

Теперь сопоставим тотальной функции $f\colon A \to B$ слово $\beta(f) = b_1 b_2 \ldots b_k$ длины k в алфавите B по правилу: $b_i = f(a_i)$. Это инъекция: разным функциям сопоставлены разные слова, так как из $f(a_j) \neq g(a_j)$ следует, что $\beta(f)_j \neq \beta(g)_j$.

Но это и сюръекция: по слову $b = b_1 b_2 \ldots b_k$ однозначно определяется такая функция f, что $\beta(f) = b$. Нужно положить $f(a_j) = b_j$.

Значит, количество тотальных функций из A в B равно количеству слов длины k в алфавите из n символов и равно n^k.

Заметим, что множество тотальных функций из A в B обозначается B^A для любых множеств. Этот пример показывает причину такого обозначения.

Пример 10.3. Сколько есть всех функций из k-элементного множества в n-элементное?

Ответ теперь другой, поскольку нужно посчитать и частичные функции. Это нетрудно сделать. Давайте добавим элемент `void` $\notin B$.

Тотальные функции из A в $B \cup \{\texttt{void}\}$ находятся во очевидном взаимно однозначном соответствии с функциями из A в B: значение `void` мы рассматриваем как указание на то, что функция из A в B не определена.

Ответ: $(n+1)^k$.

Пример 10.4. Сколько есть *инъекций* из k-элементного множества в n-элементное?

Достаточно рассмотреть случай $A = [k]$, $B = [n]$.

Сопоставим инъекции $f\colon A \to B$ слово в алфавите B длины k: $f(1)f(2)\ldots f(k)$. Поскольку f — инъекция, все символы в этом слове разные. Это соответствие взаимно однозначно. Поэтому искомое количество инъекций равно числу размещений $A_{n,k} = n!/(n-k)!$.

Пример 10.5. Сколько есть *биекций* из n-элементного множества в n-элементное? Уже обсуждалось, что их столько же, сколько перестановок, то есть $n!$.

Труднее подсчитать количество сюръекций.

Теорема 10.3. *Количество сюръекций k-элементного множества в n-элементное при $k \geqslant n$ равно*

$$\sum_{p=0}^{n} (-1)^p \binom{n}{p} (n-p)^k = n^k - \sum_{p=1}^{n} (-1)^{p+1} \binom{n}{p} (n-p)^k$$

и равно нулю при $m < n$.

Доказательство. Воспользоваться формулой включений и исключений. Для этого удобно выделить первое слагаемое суммы. Получаем правую часть равенства теоремы. Чтобы найти количество сюръекций, нужно из всего количества тотальных функций, их n^k, вычесть количество не-сюръекций.

Пусть B состоит из n элементов $b_1, \ldots, b_n$. Не-сюръекции $A \to B$ — это те тотальные функции, область значений которых не содержит одного из элементов $b_1, \ldots, b_n$, то есть объединение множеств

$$A(b_1) \cup A(b_2) \cup \ldots \cup A(b_n),$$

где через $A(b)$ обозначается множество тех функций, которые не принимают значения b.

Все множества $A(b)$ имеют размер $(n-1)^k$ (мы выбросили одно из возможных значений функции, поэтому количество таких функций равно количеству тотальных функций из k-элементного множества в $(n-1)$-элементное).

Для формулы включений и исключений нужно ещё подсчитать размер пересечений таких множеств. Рассмотрим пересечение p множеств вида $A(b)$. Это функции, которые не принимают некоторые p значений. Таких функций столько же, сколько тотальных функций из k-элементного множества в $(n-p)$-элементное.

А всего разных наборов из p множеств вида $A(b)$ столько же, сколько p-элементных подмножеств n-элементного множества, то есть $\binom{n}{p}$. Поэтому формула включений и исключений для данного семейства множеств приобретает вид, указанный в теореме. □

10.4 Отношения эквивалентности

Определение 10.4. Отношение R на некотором множестве A, которое одновременно *рефлексивно*: xRx для всех $x \in A$, *симметрично*: если xRy, то yRx для всех $x, y \in A$ и *транзитивно*: если xRy и yRz, то xRz для всех $x, y, z \in A$, называют *отношением эквивалентности.*

Пример 10.6. Отношение $x \in C(v)$, где $C(v)$ — область достижимости вершины v простого неориентированного графа, является отношением эквивалентности на множестве вершин графа. Это мы уже проверяли.

Пример 10.7. Отношение, состоящее из пар (u, v) сильно связанных вершин в орграфе, также является отношением эквивалентности. Это мы уже проверяли.

Пример 10.8. Отношение, состоящее из пар (x, x), $x \in A$, является отношением эквивалентности. Рефлексивность, симметричность и транзитивность очевидны.

Последний пример — отношение *равенства* — является прототипом всех отношений эквивалентности. Его можно обобщить.

Пример 10.9. Пусть A разбито в дизъюнктное объединение семейства множеств A_i:

$$A = \bigcup_i A_i, \qquad A_j \cap A_j = \varnothing \text{ если } i \neq j.$$

Тогда пары (x, y), для которых выполняется условие $x \in A_i$, $y \in A_i$ (то есть эти элементы лежат в одном множестве разбиения), образуют отношение эквивалентности.

Рефлексивность и симметричность очевидны из определения. Транзитивность легко проверяется. Пусть $x, y \in A_i$; $y, z \in A_j$. Так как $A_i \cap A_j \supseteq \{y\} \neq \varnothing$, то $A_i = A_j$. Значит (x, z) также находится в отношении.

Последний пример исчерпывает все возможные отношения эквивалентности.

Теорема 10.5. *Любое отношение R, являющееся отношением эквивалентности на множестве A, делит A на классы эквивалентности — непересекающиеся подмножества множества X, при этом любые два элемента одного класса находятся в отношении R, а любые два элемента разных классов не находятся в отношении R.*

Доказательство. По сути мы повторим в общем виде доказательство аналогичного утверждения для случая компонент связности.

Для каждого $x \in A$ рассмотрим множество $C(x) = \{y : xRy\}$ тех y, для которых верно xRy. Это и есть обещанные классы эквивалентности. Чтобы это доказать, нужно проверить три условия:

1. Объединение всех множеств вида $C(x)$ совпадает с множеством A.
2. Два множества $C(x)$ и $C(y)$ либо не пересекаются, либо совпадают;
3. $C(x) = C(y)$ в том и только том случае, когда xRy (то есть R совпадает с отношением «принадлежать одному классу», как в примере 10.9).

1. В силу рефлексивности множество $C(x)$ содержит x в качестве своего элемента: $x \in C(x)$, поскольку xRx. Отсюда следует, что объединение всех этих множеств совпадает с A.

2. Пусть $z \in C(x) \cap C(y)$, то есть верно xRz и yRz. Симметричность даёт zRy. Теперь применим транзитивность к xRz и zRy, заключаем, что xRy и по симметричности yRx.

Пусть $t \in C(y)$, то есть yRt. Применим транзитивность к xRy и yRt, заключаем, что xRt, то есть $t \in C(x)$. Значит, $C(y) \subseteq C(x)$. Аналогично доказывается, что $C(x) \subseteq C(y)$, так что $C(x) = C(y)$.

3. Если для каких-то x, y верно xRy, то x и y оба лежат в одном классе, а именно, в $C(x)$. Обратно, если x и y лежат в каком-то $C(z)$, то по определению имеем zRx и zRy. Симметричность даёт xRz, после чего транзитивность даёт xRy. □

10.5 Изоморфизм графов

Отношения эквивалентности встречаются повсюду в математике. Очень часто они имеют вид отношений «изоморфизма», когда две структуры объявляются «по сути одинаковыми, с точностью до переобозначений».

Давайте рассмотрим пример такого отношения из теории графов.

Посмотрим на рис. 10.1. Там изображены два связных графа. Одинаковы ли они? Рисунки выглядят совершенно по-разному, но с точки зрения теории графов геометрия неважна, важны лишь связи между вершинами. С этой точки зрения оба графа выглядят одинаково: их рёбра являются рёбрами простого цикла длины 7 и других рёбер в этих графах нет.

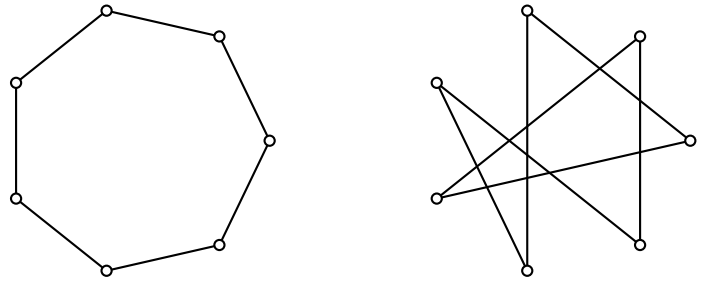


Рис. 10.1: Одинаковы ли эти графы?

Эта «похожесть» фиксируется определением отношения изоморфизма.

Определение 10.6. Графы $G_1 = (V_1, E_1)$ и $G_2 = (V_2, E_2)$ называются *изоморфными* (обозначение $G_1 \cong G_2$), если существует такая биекция $\pi\colon V_1 \to V_2$ на множествах их вершин, которая переводит множество рёбер первого графа в множество рёбер второго графа, т.е. $\{u, v\} \in E_1$ равносильно $\{\pi(u), \pi(v)\} \in E_2$.

Неформально это определение можно пересказать так: графы изоморфны, если можно так отождествить их вершины, чтобы рёбра этих графов совпали.

Пример 10.10. Зададим изоморфизм графов на рисунке 10.1. Для этого нужно как-то обозначить их вершины. Занумеруем их как на рис. 10.2.

Один из возможных изоморфизмов левого графа на правый задаётся как

i	0	1	2	3	4	5	6
$\pi(i)$	0	2	5	3	6	1	4

Заметим, что в верхней строки вершины выписаны в порядке прохождения цикла длины 7 в левом графе, а к нижней строке — в порядке прохождения цикла длины 7 в правом графе. Поэтому рёбра левого графа переходят при таком отображении в рёбра правого графа.

Утверждение 10.7. *Отношение изоморфизма — отношение эквивалентности.*

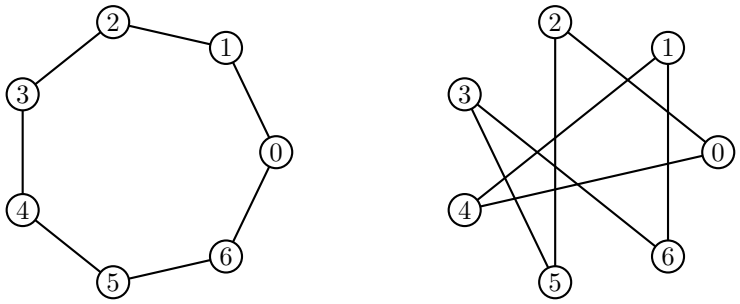


Рис. 10.2: Нумерация вершин графов

Доказательство. Рефлексивность: тождественное отображение задаёт изоморфизм графа с самим собой.

Симметричность. Докажем, что если $\pi\colon V_1 \to V_2$ — изоморфизм, то $\pi^{-1}\colon V_2 \to V_1$ — также изоморфизм. По определению нужно проверить, что $\{u, v\} \in E_2$ равносильно $\{\pi^{-1}(u), \pi^{-1}(v)\} \in E_1$. Так как π — изоморфизм (V_1, E_1) на (V_2, E_2), второе равносильно $\{\pi \circ \pi^{-1}(u), \pi \circ \pi^{-1}(v)\} \in E_2$, что равносильно $\{u, v\} \in E_2$, так как $\pi \circ \pi^{-1} = \mathrm{id}_{V_2}$.

Транзитивность. Пусть $\pi_1\colon V_1 \to V_2$ — изоморфизм (V_1, E_1) на (V_2, E_2); а $\pi_2\colon V_2 \to V_3$ — изоморфизм (V_2, E_2) на (V_3, E_3). Докажем, что тогда $\pi = \pi_2 \circ \pi_1$ — изоморфизм (V_1, E_1) на (V_3, E_3). Условие $\{u, v\} \in E_1$ равносильно $\{\pi_1(u), \pi_1(v)\} \in E_2$, так как π_1 — изоморфизм, а это условие в свою очередь равносильно $\{\pi_2 \circ \pi_1(u), \pi_2 \circ \pi_1(v)\} \in E_3$. Осталось применить транзитивность импликации. □

Изоморфизм сохраняет все свойства графов, которые выражаются в терминах связей между вершинами и рёбрами и не ссылаются на конкретные имена вершин. Такие свойства называются *инвариантами изоморфизма*.

Для доказательства неизоморфности графов достаточно указать какое-нибудь инвариантное свойство, которое есть у одного графа и которого нет у другого графа.

Например, число вершин в графе — инвариант изоморфизма, так как биекция возможна лишь между множествами одинакового размера.

Число рёбер в графе также является инвариантом изоморфизма, так как изоморфизм устанавливает взаимно однозначное соответствие между рёбрами.

Степень вершины сама по себе инвариантом изоморфизма не является. Но степень вершины сохраняется при изоморфизме: соседей у v ровно столько же, сколько у $\pi(v)$: соседи вершины обязаны переходить в соседей её образа.

Отсюда следует, что если в графе G_1 есть вершина v степени 5, а в графе G_2 все вершины имеют степень отличную от 5, то такие графы неизоморфны: при любой биекции π степень вершины $\pi(v)$ будет отличаться от 5.

Поэтому множества степеней вершин в графах должны совпадать. Но есть и более сильное условие. Если в графе G_1 есть ровно две вершины степени 5, а в графе G_2 таких вершин три, то графы неизоморфны: при любой биекции π в одну из вершин степени 5 в графе G_2 перейдёт вершина другой степени и условие изоморфизма

будет нарушено.

Значит, должны совпадать *наборы степеней*. Что это такое? Это множество таких пар (d, k), что в графе есть ровно k вершин степени d. Обычно набор степеней задают, записывая степени всех вершин графа в невозрастающем порядке.

Однако и совпадения наборов степеней недостаточно для изоморфизма.

Пример 10.11. Два графа на рис. 10.3 неизоморфны. Оба графа — деревья, наборы

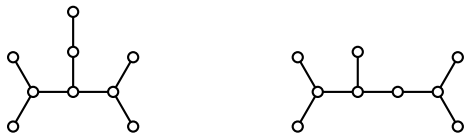


Рис. 10.3: два неизоморфных дерева

степеней вершин которых одинаковы и равны $(3, 3, 3, 2, 1, 1, 1, 1, 1)$. Однако соседи у вершины степени 2 в правом графе имеют степени 3, 3, а в левом — 3, 1. Изоморфизм должен сохранять степени вершин, поэтому вершина степени 2 перейдёт при изоморфизме в вершину степени 2. Её соседи также должны перейти в соседей образа, а это невозможно.

В общем случае проверка изоморфизма графов является трудной задачей, требующей перебора многих вариантов. Прямолинейный подход, основанный на определении, требует перебора $n!$ возможных биекций, если речь идёт об изоморфизме n-вершинных графов. Есть более изощрённые алгоритмы проверки изоморфизма, которым работают за время $n^{\log^k n}$, здесь k — некоторая константа.

Лекция 11

Отношения–3. Частичные порядки

11.1 Определения отношений частичного порядка

Определение 11.1. Бинарное отношение R на множестве X является *строгим частичным порядком*, если выполнены такие свойства:

- если aRb и bRc, то aRc (*транзитивность*);
- aRa всегда ложно (*антирефлексивность*).

Утверждение 11.2 (антисимметричность строгого порядка)**.** *Если R — строгий частичный порядок, то aRb влечёт ложность bRa.*

Доказательство. Пусть одновременно истинны aRb и bRa. Тогда по транзитивности истинно aRa, противоречие. □

Примером порядка является сравнение чисел по величине: $x < y$ обозначает, что число x меньше числа y. В дальнейшем для наглядности мы часто используем в качестве имени отношения строго порядка знак «<», обозначая им не только сравнение чисел. Для сравнения чисел выполняется дополнительное свойство *линейности* порядка: для любых $a \neq b$ истинно одно из двух: aRb или bRa. Но так бывает не всегда (отсюда слово «частичный» в названии).

Пример 11.1 (порядок по включению подмножеств)**.** На множестве $\mathcal{P}(n)$ всех подмножеств n-элементного множества определим порядок $X \subset Y$, включая в него те пары подмножеств (X, Y), для которых все элементы подмножества X содержатся в Y и есть хотя бы один элемент в Y, который не содержится в X.

Это отношение строгого частичного порядка. При этом свойство линейности порядка не выполняется: одновременно $\{1\} \not\subset \{2\}$ и $\{2\} \not\subset \{1\}$. (Перечёркнутый знак отношения означает, что пара не находится в отношении.)

Для чисел помимо отношения строго сравнения используется также отношение $\leqslant$ («меньше или равно») и часто оно удобнее строгого порядка.

То же самое верно и для частичных порядков.

Определение 11.3. Бинарное отношение $\leqslant$ на множестве X является *нестрогим частичным порядком*, если выполнены такие свойства:

- $a \leqslant a$ (*рефлексивность*);
- $(a \leqslant b)$ и $(b \leqslant a)$ влечёт $(a = b)$ (*антисимметричность*);
- $(a \leqslant b)$ и $(b \leqslant c)$ влечёт $(a \leqslant c)$ (*транзитивность*).

Между отношениями строго и нестрого порядка есть очевидная связь.

Утверждение 11.4. *Пусть $<$ — отношение строгого частичного порядка. Тогда отношение*

$$a \leqslant b \text{ равносильно } (a < b) \vee (a = b)$$

является отношением нестрогого частичного порядка.

Доказательство. Рефлексивность записана в определении.

Антисимметричность: предположим, что $a \leqslant b$, $b \leqslant a$, но $a \neq b$. Тогда по построению должно быть $a < b$ и $b < a$, что невозможно (см. утв. 11.2).

Транзитивность доказывается разбором случаев: если $a = b$ или $b = c$, то транзитивность очевидно выполняется, а если $a < b$ и $b < c$, применяем транзитивность для исходного отношения строгого частичного порядка. □

Утверждение 11.5. *Пусть $\leqslant$ — отношение нестрогого частичного порядка. Тогда отношение*

$$a < b \text{ равносильно } (a \leqslant b) \wedge (a \neq b)$$

является отношением строгого частичного порядка.

Доказательство. Антирефлексивность ясна по построению. Надо проверить транзитивность: пусть $a < b$ и $b < c$, то есть (согласно определению порядка $<$) $a \leqslant b$, $a \neq b$, $b \leqslant c$, $b \neq c$. Надо получить $a \leqslant c$ и $a \neq c$. Первое сразу следует из транзитивности отношения $\leqslant$. Докажем второе: если $a = c$, то получаем $a \leqslant b$ и $b \leqslant a$, откуда следует $a = b$ (антисимметричность порядка $\leqslant$) в противоречии с предположением. □

Таким образом, имеется взаимно однозначное соответствие между строгими и нестрогими порядками: один получается из другого выбрасыванием (или добавлением) *диагонального множества* $\{(a, a) : a \in X\}$.

В силу этих утверждений мы будем пользоваться и одним, и другим видом отношений частичного порядка, выбирая тот, который удобнее.

Частично упорядоченным множеством $(X, <)$ называется множество X с отношением частичного порядка $<$ на нём. Для краткости такое множество часто называют частичным порядком или даже просто порядком. Если отношение на записи часто опускают, если оно ясно из контекста.

11.2 Частичные порядки и ориентированные графы

Пример 11.2. На множестве чисел $\{0, 1, 2, \ldots, 8, 9\}$ рассмотрим обычное отношение порядка. Изобразим это упорядоченное множество, помещая меньшие элементы левее бóльших, см. рис. 11.1. Это линейный порядок: любые два числа сравнимы.

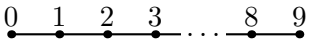


Рис. 11.1: Линейный порядок на $\{0, 1, 2, \ldots, 8, 9\}$, сравнение по величине

Аналогично можно рисовать и другие порядки.

Пример 11.3. Порядок по включению на подмножествах 2-элементного множества изображён на рис. 11.2.

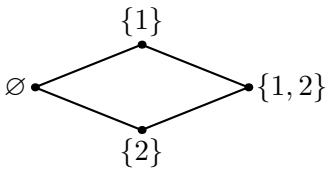


Рис. 11.2: $(\mathcal{P}(2), \subset)$

Этот порядок, как уже обсуждалось, частичный. Подмножества $\{0\}$ и $\{1\}$ несравнимы. Поэтому между ними нет линии. Но и между $\varnothing$ и $\{0, 1\}$ нет линии, хотя они сравнимы. Мы предполагаем при таком изображении, что одно множество меньше другого, если на рисунке из первого можно пройти во второе, двигаясь по линиям вправо.

Соблюдать такое соглашение не всегда легко. Поэтому лучше проводить проводить стрелки на рёбрах в направлении возрастания. Таким образом, частичный порядок удобнее изображать ориентированным графом. Разберём подробнее соответствие между ориентированными графами и частичными порядками.

Во-первых, заметим, что любой частичный порядок на множестве V задаёт ориентированный граф, рёбра которого — это в точности те пары (x, y), для которых $x < y$. Видно, что на риунках выше изображены какие-то другие графы: рёбер на рисунках меньше, чем пар сравнимых элементов.

Говорят, что элементы x, y частично упорядоченного множества $(X, <)$ *соседние*, элемент x *непосредственно предшествует* y, элемент y *непосредственно следует за* x, если $x < y$ и нет такого z, что $x < z < y$.[1)]

По частичному порядку $<$ на множестве X построим ориентированный граф $N(<)$ с множеством вершин X и множеством рёбер

$$E = \{(u, v) : u \text{ непосредственно предшествует } v\}.$$

[1)] Это три названия для одного и того же.

Утверждение 11.6. *Для всякого частичного порядка $<$ граф $N(<)$ ациклический.*

Доказательство. Если в $N(<)$ есть цикл $(a_1 a_2 \dots a_n a_1)$, то по определению графа $N(<)$ выполняются сравнения:

$$a_1 < a_2 < \dots < a_n < a_1$$

(соседние в цикле непосредственно предшествуют в порядке). По транзитивности получаем $a_1 < a_1$ и приходим к противоречию с антирефлексивностью. □

В другую сторону. Любой ациклический граф $G = (V, E)$ задаёт на множестве вершин V частичный порядок по следующему правилу:

$$u \leqslant_G v \text{ равносильно } v \in R(u),$$

где $R(u)$ обозначает область достижимости вершины u.

Утверждение 11.7. *Для любого ациклического графа отношение $\leqslant_G$ является отношением нестрогого частичного порядка.*

Доказательство. Проверим свойства частичного порядка для отношения $\leqslant_G$. Рефлексивность и транзитивность мы уже проверяли, когда рассматривали ориентированные графы.

Если $u \leqslant_G v$ и $v \leqslant_G u$, то по определению $v \in R(u)$ и $u \in R(v)$, то есть вершины u, v сильно связаны. Но в ациклическом графе каждая компонента сильной связности состоит из одной вершины. Поэтому $u = v$. □

Обратите внимание, что построенное соответствие не взаимно однозначно.

Пример 11.4. В порядке $(\mathbb{R}, <)$ на действительных числах соседних пар нет вообще. Это называется свойством *плотности* порядка: между любыми двумя различными числами $a < b$ есть хотя бы одно число, которое больше a и меньше b (например, полусумма $(a + b)/2$).

Поэтому граф $N(<)$ не содержит рёбер. Но такой граф задаёт тривиальный частичный порядок, в котором нет ни одной пары сравнимых элементов.

11.3 Операции с порядками

Пример 11.5. На множестве векторов $\mathbb{R}^n$ определено отношение *покоординатного порядка*:

$$x = (x_1, \dots, x_n) \leqslant (y_1, \dots, y_n) = y \quad \Leftrightarrow \quad x_i \leqslant y_i \text{ для всех } i.$$

Числа в правой части сравниваются обычным способом.

Свойства частичного порядка легко проверяются (упражнение для самостоятельной работы).

Этот порядок частичный. Например, векторы $(0, 2)$ и $(1, 1)$ несравнимы.

Этот пример — частный случай операции *покоординатного произведения частичных порядков*. Пусть P, Q — два частичных порядка. Тогда покоординатный порядок на декартовом произведении $P \times Q$ задается правилом:

$$(p_1, q_1) \leqslant (p_2, q_2) \text{ по определению означает } p_1 \leqslant_P p_2 \text{ и } \ q_1 \leqslant_Q q_2.$$

Свойства частичного порядка для такого отношения также легко проверяются, их доказательство оставляется для самостоятельной работы.

Как мы видели в примере 11.5, покоординатное произведение линейных порядков не всегда линейно. Есть другие операции с порядками, которые сохраняют свойство линейности.

Определение 11.8. Пусть P, Q — два частичных порядка. *Лексикографический порядок* на $P \times Q$ задаётся правилом:

$(p_1, q_1) \leqslant (p_2, q_2)$ по определению означает, что $(p_1 <_P p_2)$ или $\ (p_1 = p_2)$ и $(q_1 \leqslant_Q q_2)$.

Лемма 11.9. *Лексикографический порядок на $P \times Q$ является отношением частичного порядка. Если P и Q — линейные порядки, то лексикографический порядок также линейный.*

Доказательство. Рефлексивность сразу следует из определения и рефлексивности порядка Q.

Антисимметричность. Пусть $(p_1, q_1) \leqslant (p_2, q_2)$ и $(p_2, q_2) \leqslant (p_1, q_1)$. Случай $p_1 \neq p_2$ невозможен, так как тогда $p_1 < p_2 < p_1$ в порядке P, что противоречит антирефлексивности строгого порядка. Если же $p_1 = p_2$, то получаем из определения $q_1 \leqslant q_2 \leqslant q_1$, то есть $q_1 = q_2$ в силу антисимметричности порядка Q.

Транзитивность. $(p_1, q_1) \leqslant (p_2, q_2)$ и $(p_2, q_2) \leqslant (p_3, q_3)$. Из определения лексикографического порядка видим, что $p_1 \leqslant p_2 \leqslant p_3$. Если $p_1 < p_2 < p_3$, то $p_1 < p_3$ по транзитивности порядка P и потому $(p_1, q_1) < (p_3, q_3)$. Если $p_1 = p_2 < p_3$ или $p_1 < p_2 = p_3$, то также $p_1 < p_3$ и $(p_1, q_1) < (p_3, q_3)$. Если же $p_1 = p_2 = p_3$, то из определения лексикографического порядка получаем $q_1 \leqslant q_2 \leqslant q_3$, в силу транзитивности порядка Q и определения лексикографического порядка получаем $(p_1, q_1) \leqslant (p_3, q_3)$.

Последнее свойство очевидно из определения. □

Определение 11.10 (неудачное)**.** Пусть P, Q — два частичных порядка, $P \cap Q = \varnothing$. *Суммой* $P + Q$ называется порядок на $P \cup Q$, в котором все элементы P меньше всех элементов Q.

Легко проверить (оставляется в качестве самостоятельного упражнения), что сумма частичных порядков является частичным порядком и сумма линейных порядков является линейным порядком.

Обратите внимание, что сумма порядков некоммутативна. Порядки $\mathbb{N} + \mathbb{Z}$ и $\mathbb{Z} + \mathbb{N}$ — существенно разные порядки. Но что это утверждение означает? Ведь $\mathbb{N} \subset \mathbb{Z}$, а в данном выше определении суммы порядков такое запрещено. Определение нужно поправить.

11.4 Изоморфизм порядков

Определение 11.11. Порядки P и Q называются *изоморфными* (обозначение $P \cong Q$), если есть такая биекция $\varphi\colon P \to Q$, что $x \leqslant y$ равносильно $\varphi(x) \leqslant \varphi(y)$ для всех пар x, y.

Пример 11.6. Рассмотрим два порядка: порядок $(\mathcal{P}_n, \subset)$ на подмножествах n-элементного множества по включению и покоординатный порядок на двоичных словах длины n. Это два разных отношения, заданные на разных множествах.

Изоморфизм между ними устанавливает стандартная биекция: подмножеству S сопоставляется слово x_S, в котором на i-й позиции стоит 1 тогда и только тогда, когда $i \in S$.

Если $S \subseteq T$, то на всех позициях, в которых в слове x_S стоит 1, в слове x_T также стоит 1.

Теперь уже ясно, как определить сумму порядков в общем случае.

Определение 11.10 (окончательное)**.** Пусть P, Q — два частичных порядка, $P' \cong P$, $Q' \cong Q$, $P' \cap Q' = \varnothing$. *Суммой* $P + Q$ называется порядок на $P' \cup Q'$, в котором все элементы P' меньше всех элементов Q'.

Как и в случае изоморфизма графов, проще устанавливать неизоморфизм порядков, указывая различающее их *инвариантное свойство*, то есть свойство, которое не изменяется при изоморфизме. Такими свойствами являются любые свойства, которые выражаются в терминах сравнения элементов без отсылок к конкретным именам элементов.

Пример 11.7. Докажем, что $\mathbb{N} + \mathbb{Z}$ и $\mathbb{Z} + \mathbb{N}$ неизоморфны. Чтобы перейти к непересекающимся множествам, рассмотрим обычные целые числа и «штрихованные натуральные»: числа вида $0', 1', \ldots$. Сравниваются эти числа так же, как нештрихованные. Но теперь множества не пересекаются (штрих либо есть, либо его нет).

В $\mathbb{N}+\mathbb{Z}$ есть *наименьший элемент* — $0'$ меньше всех остальных элементов суммы порядков. А в $\mathbb{Z} + \mathbb{N}$ такого элемента нет (для каждого целого числа есть меньшее его).

Из этого примера можно заключить, что на бесконечном множестве существуют неизоморфные линейные порядки. Для конечных множеств это не так, если в множестве одинаковое количество элементов.

Теорема 11.12. *Пусть $(X, \leqslant)$ и $(Y, \leqslant)$ — два линейных порядка на конечных множествах и $|X| = |Y|$. Тогда эти порядки изоморфны.*

Сначала докажем лемму.

Лемма 11.13. *В конечном линейном порядке есть наибольший и наименьший элементы.*

Доказательство. Рассмотрим *убывающие цепи*: последовательности элементов порядка $x_1 > x_2 > \ldots$, в которой каждый следующий элемент меньше предыдущего. Будем дополнять убывающую цепь новыми элементами, пока это возможно. Поскольку всего элементов конечное число, процесс рано или поздно остановится. Последний элемент такой убывающей цепи обязан быть наименьшим: в противном случае её можно было бы продолжить.

Аналогичное рассуждение с *возрастающими цепями* показывает существование наибольшего элемента. □

Доказательство теоремы 11.12. Индукция по числу элементов. База — один элемент в порядке — очевидна.

Индуктивный переход. Предположим, что все линейные порядки с n элементами изоморфны. Рассмотрим два линейных порядка P и Q с $n+1$ элементом. Выделим в них наименьшие элементы p_0, q_0. Порядки на оставшихся элементах изоморфны по предположению индукции. Продолжая этот изоморфизм соответствием $p_0 \mapsto q_0$, получаем искомый изоморфизм порядков P и Q. □

11.5 Цепи и антицепи

Среди частичных порядков на конечном множестве есть два крайних случая. Первый: линейный порядок (каждая пара элементов сравнима). Второй: пустой порядок (никакая пара различных элементов несравнима).

В остальных случаях можно выделять подмножества частично упорядоченного множества, которые образуют эти два крайних случая при ограничении исходного частичного порядка на это подмножество. *Цепь* — это такое подмножество частично упорядоченного множества, которое образует линейный порядок. *Антицепь* — это такое подмножество, в котором элементы попарно несравнимы.

Пример 11.8. Рассмотрим порядок $(\mathcal{P}_3, \subset)$ на подмножествах 3-элементного мно-

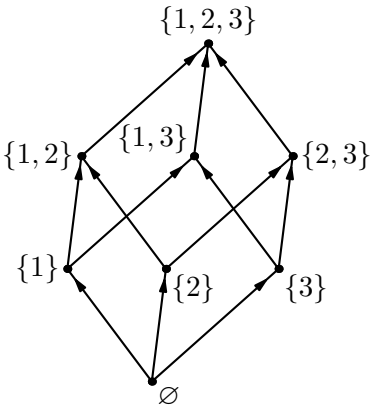


Рис. 11.3: $(\mathcal{P}(3), \subset)$

жества, упорядоченных по включению. Он изображён на рис. 11.3. Легко увидеть антицепь размера 3: $\{\{1\},\{2\},\{3\}\}$. Антицепей большего размера в этом порядке нет. Но как это доказать? Перебор вариантов кажется очень трудоёмким.

Разобьём элементы этого порядка на три цепи: $\varnothing \subset \{1\} \subset \{1,2\} \subset \{1,2,3\}$; $\{2\} \subset \{2,3\}$; $\{3\} \subset \{1,3\}$.

Любая антицепь пересекает цепь не более чем по одному элементу (любая пара сравнима в цепи и несравнима в антицепи). Значит, любая антицепь в этом порядке содержит не более трёх элементов.

Оказывается, это соотношение точное.

Теорема 11.14 (Дилуорс)**.** *Наибольший размер антицепи в порядке равен наименьшему количеству цепей в разбиениях порядка на непересекающиеся цепи.*

Известно много доказательств этой теоремы. Приведём свежее.

Доказательство Фёдора Куянова, ФКН ВШЭ, 1 *курс.* В одну сторону нужно повторить рассуждение из примера 11.8: если порядок разбит на k непересекающихся цепей, то любая антицепь пересекается с каждой из цепей не более чем по одному элементу и в антицепи не больше k элементов.

Теперь предположим, что в частично упорядоченном множестве P размер максимальной антицепи равен k. Нужно доказать, что найдётся разбиение P на k цепей.

Добавим к этому множеству k несравнимых между собой элементов, которые больше всех остальных элементов порядка (k дополнительных максимумов) и k несравнимых между собой минимумов, которые меньше всех остальных элементов порядка (включая добавленные максимумы). Получаем новый порядок G. Размер максимальной антицепи не изменился: антицепь в G либо содержит только добавленные элементы (причём либо максимумы, либо минимумы), либо только элементы порядка P.

Разбиение порядка G на антицепи урезается до разбиения P на антицепи выбрасыванием добавленных элементов. Поэтому достаточно доказать, что существует разбиение G на k антицепей. Для этого применим теорему Холла.

Рассмотрим двудольный граф $F = (L, R, E)$, в котором L — множество элементов G без добавленных минимумов, R — множество элементов G без добавленных максимумов, а множество рёбер $E = \{(a,b) : a > b\}$ (сравнение в порядке G). Из построения видно, что $|L| = |R|$. В таком графе элементы исходного порядка P входят в обе доли. Но мы хотим рассматривать этот граф как двудольный. Нужно себе представить, что сделаны две копии P', P'' порядка P, одна отправлена в левую (верхнюю на рисунке 11.4) долю, вторая — в правую (нижнюю).

Как видно из рисунка 11.4, цепям в порядке G отвечают паросочетания в графе F. Совершенному паросочетанию в F будет соответствовать разбиение порядка G на цепи (на рисунке выделена одна из таких цепей, остальные строятся из других вершин области maxima).

Осталось доказать, что в графе F существует совершенное паросочетание. Проверим выполнение условия теоремы Холла. Нужно доказать $|G(S')| \geqslant |S'|$ для любого $S' \subseteq L$. Здесь $G(S')$ обозначает множество вершин доли R, соединённых ребром

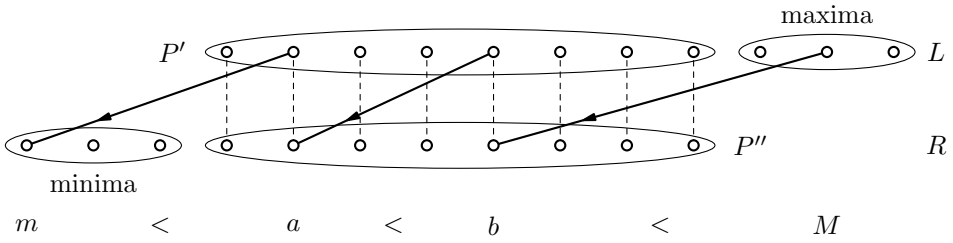


Рис. 11.4: Цепи превращаются в паросочетания во вспомогательном графе

хотя бы с одной вершиной множества S'. Заметим, что в $G(S')$ входят все минимумы, их k штук. Обозначим A' подмножество S', состоящее из тех вершин, копии которых не принадлежат $G(S')$ или которые являются максимумами. Это антицепь, так как из $x > y$ и $x' \in S'$ следует, что $y'' \in G(S')$. Поэтому $|A'| \leqslant k$. Но тогда

$$|G(S')| \geqslant k + |S' \setminus A'| \geqslant k + |S'| - k = |S'|,$$

что и требовалось доказать. Первое слагаемое в первом неравенстве отвечает минимумам в правой доле, второе — тем вершинам S', копии которых в правой доле лежат в $G(S')$. □