Алгебра логики, комбинаторика и теория графов: семинары

Бутаков И. Д.

2021

Содержание

Предисловие

Перед вами сборник всех семинаров по АЛКТГ за авторством Бутакова И. Д. Автор выражает благодарность Маланчук Софии Владимировне за помощь в составлении материалов.

1 Алгебра логики

Математика — это общий язык для многих сфер деятельности человека, позволяющий формализовать объекты, которыми оперирует наш разум. Одним из важнейших разделов математики считается ***математическая логика***, так как именно она является фундаментом математических суждений, исследует природу математического доказательства в целом. Поэтому не зря курс дискретного анализа начинается именно с ***алгебры логики*** — объекта математической логики, хоть и сравнительно простого, но важного и полезного.

1.1 Булева алгебра

Алгебра логики изучает логические операции над высказываниями. При этом в простейшем случае считается, что высказывания могут быть только истинными (обозначается «1») или ложными (обозначается «0»);

Определение 1.1. Переменные, принимающие значения только 0 или 1, называются ***булевыми переменными***. Аналогично, функции от булевых переменных, принимающие только значения 0 или 1 — ***булевы функции***, или ***логические операции***, ***связки***. ***Высказываниям*** ставится в соответствие либо булева переменная с фиксированным значением, либо значение булевой функции на фиксированных аргументах.

Примеры логических операций: «НЕ» (обозначается «$\neg$»), «И» (обозначается «$\wedge$»), «ИЛИ» (обозначается «$\vee$»), исключающее «ИЛИ» (обозначается «$\oplus$»), импликация (обозначается «$\rightarrow$»), эквивалентность (обозначается «$\leftrightarrow$»).

Заметим, что как и любые другие функции с конечной областью определения, булевы функции можно задать таблицей, просто перечислив их значения на всех возможных значениях аргументов. Данные таблицы называются ***таблицами истинности***.

A	B	$\neg A$	$A \wedge B$	$A \vee B$	$A \oplus B$	$A \rightarrow B$	$A \leftrightarrow B$
0	0	1	0	0	0	1	1
0	1	1	0	1	1	1	0
1	0	0	0	1	1	0	0
1	1	0	1	1	0	1	1

Таблица 1.1: задание логических связок таблицами истинности

Заметим сразу, что запись таблицы истинности можно сократить, если изначально условиться, в каком порядке перечисляются возможные значения аргументов, и оставить только столбец значений функции; этот столбец тогда будет являться ***булевым вектором*** (***вектором значений***), задающим функцию. Стандартный порядок перечисления значений аргументов таков, чтобы они образовывали двоичную запись номера строки (см. таблицу 1.1).

Пример 1.2. Операция «НЕ» задаётся булевым вектором 10, а, например, импликация — 1101.

Булевы функции можно также задавать при помощи формул, «собирая» из других связок. Формально, формула является деревом, задающим порядок применения составляющих формулу связок к аргументам и к значениям других связок. Однако такой взгляд на вещи полностью эквивалентен стандартному написанию математических формул, если задать приоритет операций, или просто использовать скобки. Приоритет изученных

связок указан в таблице 1.2, пример формулы и соответствующего ей дерева — на рис. 1.1.

Связка	Приоритет	Краткое название	Название	Смысл
$\neg$	1	«НЕ»	отрицание	«не A»
$\wedge$	2	«И»	конъюнкция	«A и B»
$\vee$	3	«ИЛИ»	дизъюнкциця	«A или B»
$\oplus$	3	«ИСКЛИЛИ», «XOR»	исключающее или	«либо A, либо B»
$\to$	4	–	импликация	«если A, то B»
$\leftrightarrow$	5	–	эквивалентность	«A равносильно B»

Таблица 1.2: информация о логических связках

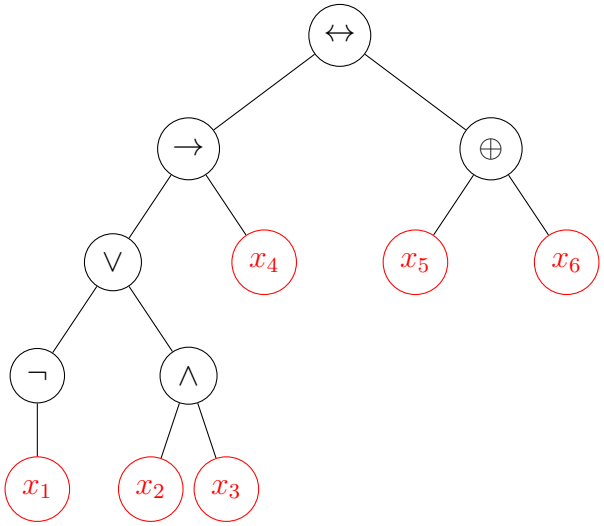


Рис. 1.1: дерево формулы $\neg x_1 \vee x_2 \wedge x_3 \to x_4 \leftrightarrow x_5 \oplus x_6$ (или, что то же самое, $(((\neg x_1) \vee (x_2 \wedge x_3)) \to x_4) \leftrightarrow (x_5 \oplus x_6)$)

1.2 Логические законы

Логический закон (***тождество***) — равенство двух булевых функций, заданных разными формулами. Равенство булевых функций определяется так же, как и равенство любых других функций: требуется равенство областей определений функций и равенство значений функций в любой точке области определения. Равенство формул и области определения, очевидно, влечет равенство функций; обратное неверно. Принято также считать, что если аргументы в формуле пронумерованы, то число аргументов равно максимальному индексу («нет пропусков»).

Пример 1.3.

- С точки зрения правил школьной математики, функции $\sqrt[3]{x}$ и $(x)^{1/3}$ не равны.
- Формула, задающая функцию трёх аргументов: $x_1 \wedge x_3$.
- Две формулы, задающие одну и ту же функцию: $x_1 \to x_2$ и $\neg x_1 \vee x_2$.
- Равенство областей определения **существенно**: пусть

$$f(A, B, C) = A \vee B, \quad g(A, B) = A \vee B$$

Данные две функции заданы одной и той же формулой, но $f \neq g$.

В случае булевых функций определение равенства можно записать иначе, если воспользоваться понятием ***тавтологии***.

Определение 1.4. Функция g называется ***тавтологией*** $\overset{\triangle}{\Longleftrightarrow}$ она тождественна равна единице на всей области определения.

Замечание 1.5. Для булевых функций f и g их равенство эквивалентно равенству областей определений и тавтологичности $f \leftrightarrow g$.

Пользуясь определением связок из таблицы 1.1, можно доказать множество логических законов. Самые тривиальные законы — *коммутативность* и *ассоциативность* операций $\wedge$, $\vee$ и $\oplus$:

$$x_1 \wedge x_2 = x_2 \wedge x_1, \qquad x_1 \vee x_2 = x_2 \vee x_1, \qquad x_1 \oplus x_2 = x_2 \oplus x_1$$

$$x_1 \wedge (x_2 \wedge x_3) = (x_1 \wedge x_2) \wedge x_3, \qquad x_1 \vee (x_2 \vee x_3) = (x_1 \vee x_2) \vee x_3, \qquad x_1 \oplus (x_2 \oplus x_3) = (x_1 \oplus x_2) \oplus x_3$$

Также имеет смысл выписать некоторые *дистрибутивные* законы:

$$x_1 \wedge (x_2 \vee x_3) = (x_1 \wedge x_2) \vee (x_1 \wedge x_3)$$

$$x_1 \vee (x_2 \wedge x_3) = (x_1 \vee x_2) \wedge (x_1 \vee x_3)$$

Другие полезные законы:

1) $x_1 \vee (x_1 \wedge x_2) = x_1; \quad x_1 \wedge (x_1 \vee x_2) = x_1$ *(законы поглощения)*
2) $\neg(x_1 \wedge x_2) = \neg x_1 \vee \neg x_2; \quad \neg(x_1 \vee x_2) = \neg x_1 \wedge \neg x_2$ *(законы де Моргана)*
3) $x_1 \to x_2 = \neg x_2 \to \neg x_1$ *(закон контрапозиции)*
4) $x_1 \leftrightarrow x_2 = \neg(x_1 \oplus x_2) = (x_1 \to x_2) \wedge (x_2 \to x_1)$
5) $x_1 \to x_2 = \neg x_1 \vee x_2$

Остальные законы и свойства можно найти в конспекте лекций Александра Александровича.

Задача 1

Докажите равенство функций

$$(x_1 \to x_2) \wedge (x_2 \to x_3) \wedge \ldots \wedge (x_{k-1} \to x_k) \wedge (x_k \to x_1) = \left(\bigwedge_{i=1}^{k-1} (x_i \to x_{i+1}) \right) \wedge (x_k \to x_1)$$

и

$$x_1 \leftrightarrow x_2 \leftrightarrow x_3 \leftrightarrow \ldots \leftrightarrow x_k$$

Решение задачи 1

Несложно заметить, что если $\forall i, j \; x_i = x_j$, то оба высказывания истинны. Если же $\exists i, j : x_i \neq x_j$, то второе высказывание ложно. Но что насчёт первого? Понятно, что раз $\exists i, j : x_i \neq x_j$, то и $\exists m : \; x_m = 1 \neq 0 = x_{m+1}$ (считаем, что $x_{k+1} = x_1$). Но тогда и первое высказывание ложно.

1.3 Преобразование и упрощение формул

В последнем пункте примера 1.3 видно, что значение f не зависит от значения C. В этом случае говорится, что C — ***несущественная*** или ***фиктивная переменная***.

Определение 1.6. x_i — ***фиктивная переменная*** функции $f(x_1, \ldots, x_k) \overset{\triangle}{\iff} f\big|_{x_i=0}$ и $f\big|_{x_i=1}$ равны как функции, то есть

$$\forall x_1, \ldots, x_{i-1}, x_{i+1}, \ldots x_k \quad f(x_1, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_k) = f(x_1, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_k)$$

Все нефиктивные переменные называются ***существенными***.

Задача 2

Найдите все фиктивные переменные функции f, заданной формулой

$$f(x_1, \ldots, x_6) = (0 \wedge x_1) \vee \neg(1 \vee x_2) \vee \neg(0 \to x_3) \vee (x_4 \wedge x_5) \vee (x_4 \wedge (x_6 \to x_5) \wedge \neg x_6)$$

Решение задачи 2

Первые три дизъюнкта, очевидно, равны нулю, поэтому x_1, x_2 и x_3 — несущественные переменные, и формула упрощается:

$$f(x_1, \ldots, x_6) = (x_4 \wedge x_5) \vee (x_4 \wedge (x_6 \to x_5) \wedge \neg x_6)$$

Заметим, что второй дизъюнкт в новой формуле принимает истинное значение только тогда, когда $x_4 = 1$ и $x_5 = 1$, то есть, только тогда, когда первый дизъюнкт принимает истинное значение. Но тогда формула упрощается еще сильнее:

$$f(x_1, \ldots, x_6) = x_4 \wedge x_5$$

Отсюда x_6 — еще одна несущественная переменная; все остальные переменные существенны.

Из решения задачи выше можно извлечь и обобщить одну важную идею, позволяющую упрощать логические формулы

Лемма 1.7 (Обобщённые правила поглощения). Пусть f и g — булевы функции, определённые на общем наборе аргументов. Тогда

1) Если $g = 1$ только на тех значениях аргументов, на которых $f = 1$, то функции $f \vee g$ и f равны.
2) Если $g = 0$ только на тех значениях аргументов, на которых $f = 0$, то функции $f \wedge g$ и f равны.
3) Если $g = 1$ только на тех значениях аргументов, на которых $f = 0$, то функции $f \to g$ и f равны.

Доказательство. Докажем только первый пункт, так остальные делаются аналогично. Требуется доказать тавтологичность высказывания

$$(g \to f) \to ((g \vee f) \leftrightarrow f)$$

Перепишем формулу, используя только $\neg$, $\wedge$ и $\vee$:

$$\neg(\neg g \vee f) \vee ((\neg(g \vee f) \vee f) \wedge ((g \vee f) \vee \neg f))$$

Применим правила де Моргана:

$$(g \wedge \neg f) \vee (((\neg g \wedge \neg f) \vee f) \wedge ((g \vee f) \vee \neg f))$$

Используя тавтологичность $f \vee \neg f$, упрощаем формулу:

$$(g \wedge \neg f) \vee (\neg g \wedge \neg f) \vee f$$

Воспользовавшись дистрибутивностью, получаем

$$(\neg f \wedge (g \vee \neg g)) \vee f$$

$$(\neg f \wedge 1) \vee f$$

$$\neg f \vee f$$

Действительно, имеем тавтологию. □

Упрощение формул — важная задача, так как оно облегчает проверку некоторых свойств задаваемой формулой функции, например, тавтологичность или ***выполнимость*** (истинность хотя бы на каком-то наборе значений аргументов). «Трюки» по упрощению формул активно используются в SAT-солверах — программах, проверяющих указанные выше свойства.

Здесь открывается еще одна важная сторона логики: возможность записать какие-то утверждения формально влечет возможность их алгоритмической проверки. Например, можно написать программу, проверяющую верность теоремы, или по набору ограничений находящую верные утверждения.

Задача 3

Во время полуночного бала в поместье де Моргана произошло убийство. Убийца не оставил после себя никаких существенных улик, однако точно известно, что в момент преступления он был с жертвой наедине. В поместье есть две комнаты, доступные гостям: зал и библиотека. Гостями в ту ночь были Алиса, Боря, Вася, Гоша и Дима.

Ниже приведены утверждения, в которых полиция уверена точно:

1. Жертвой стал Дима.
2. Тело нашли в библиотеке.
3. В зале в полночь точно была Алиса или Боря или Гоша.
4. Неверно, что либо Гоша, либо Боря были в библиотеке.
5. Если Алиса была в зале, то и Боря тоже.
6. Боря был в зале, или Вася был в библиотеке.
7. Неверно, что Вася был в библиотеке, а Гоша был в зале.
8. Алиса и Вася были в разных комнатах.

Решение задачи 3

Пусть x_i — утверждение, что i-ый гость был в библиотеке в момент убийства. Требуется найти аргументы, при которых истинно выражение

$$x_5 \wedge (\neg x_1 \vee \neg x_2 \vee \neg x_4) \wedge \neg(x_2 \oplus x_4) \wedge (\neg x_1 \to \neg x_2) \wedge (\neg x_2 \vee x_3) \wedge \neg(x_3 \wedge \neg x_4) \wedge (x_1 \oplus x_3)$$

Пользуясь тем, что $\neg(a \oplus b) = a \leftrightarrow b = (a \to b) \wedge (b \to a)$, а также законами де Моргана и контрапозиции, получаем эквивалентную формулу:

$$x_5 \wedge (\neg x_1 \vee \neg x_2 \vee \neg x_4) \wedge (x_2 \leftrightarrow x_4) \wedge (x_2 \to x_1) \wedge (x_2 \to x_3) \wedge (x_3 \to x_4) \wedge (x_1 \oplus x_3)$$

Из задачи 1 получаем следующую эквивалентную формулу:

$$x_5 \wedge (\neg x_1 \vee \neg x_2 \vee \neg x_4) \wedge (x_2 \leftrightarrow x_3 \leftrightarrow x_4) \wedge (x_2 \to x_1) \wedge (x_1 \oplus x_3)$$

Ей, в свою очередь, эквивалентна формула

$$x_5 \wedge (\neg x_1 \vee \neg x_2) \wedge (x_2 \leftrightarrow x_3 \leftrightarrow x_4) \wedge (x_2 \to x_1) \wedge (x_1 \oplus x_2)$$

Два последних дизъюнкта истинны только при $x_2 = 0$, $x_1 = 1$. Отсюда следующее упрощение:

$$x_1 \wedge \neg x_2 \wedge x_5(\neg x_1 \vee \neg x_2) \wedge (x_2 \leftrightarrow x_3 \leftrightarrow x_4)$$

$$x_1 \wedge \neg x_2 \wedge \neg x_3 \wedge \neg x_4 \wedge x_5$$

То есть, убийцей оказалась Алиса.

2 Множества и логика

Множество — ещё один низкоуровневый объект математики, который трудно определить строго. Формально, в наше время множеством называют объект, удовлетворяющий определённой системе аксиом[1]. Однако в ходе этого курса так глубоко копать не придётся: нам будет достаточно лишь сравнительно неформального определения множества.

2.1 Теория множеств

Определение 2.1. ***Множеством*** называют совокупность неповторяющихся объектов без указания отношения между ними.

Для краткости утверждение «элемент x принадлежит множеству A» обозначают как $x \in A$. Аксиоматически полагается существование ***пустого множества*** (то есть, множества, которому не принадлежит ни один элемент), которое обозначают $\varnothing$.

Множества можно задавать различными способами:

1) Перечислением всех элементов: $A = \{1, 2, 4\}$.
2) Перечисление посредством правила:

$$\mathbb{N}_0 = \{0, 1, 2, \ldots\}, \qquad \mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\} = \{0, 1, -1, 2, -2, \ldots\}$$

Понятно, что данный способ неприменим, если из перечисления читателю угадать правило невозможно.

3) Задание условием:

$$\{x \mid f(x)\} = \text{«множество всех } x\text{, для которых верно высказывание } f(x)\text{»}$$

Пример:

$$[0; 1) = \{x \mid (x \geqslant 0) \wedge (x < 1)\} \tag{2.1}$$
$$\mathbb{Q} = \left\{ \frac{m}{n} \,\middle|\, m \in Z,\ n \in \mathbb{N} \right\}$$

Последний способ вызвает некоторые вопросы; в частности, какие x «пойдут на вход» условию $f(x)$. Верно ли, например, что $\sqrt{2} \in \{x \mid \text{«}x \text{ не делится на } 2\text{»}\}$? А то, что “стул” $\in \{x \mid \text{«}x \text{ не делится на } 2\text{»}\}$? Для того, чтобы обойти эти трудности, вводится понятие множества всех элементов, или полного множества, или ***юнивёрсума***, которое обычно обозначают U.

Определение 2.2. ***Юнивёрсум*** — множество всех элементов, на которых происходит проверка условия при соответствующем задании некоторого множества.

Очевидно, что изначально нет никаких ограничений в выборе юнивёрсума; этот выбор обусловлен лишь постановкой задачи. Поэтому требуется оговаривать заранее, что такое множество U, или хотя бы упоминать его при каждом задании множества условием:

$$\{x \in U \mid f(x)\} \qquad (\text{например, } [0; 1) = \{x \in \mathbb{R} \mid (x \geqslant 0) \wedge (x < 1)\})$$

Множество — настолько фундаментальный объект, что с его помощью даже пытались описать всю математику.

[1] Аксиоматическая теория множеств, система аксиом ZF.

Пример 2.3. С помощью множеств можно определить, что такое упорядоченная пара:

$$(x, y) = \{x, \{y\}\}$$

Или что такое натуральные числа:

$$\varnothing,\ \{\varnothing\},\ \{\varnothing, \{\varnothing\}\},\ \{\varnothing, \{\varnothing, \{\varnothing\}\}\}, \ldots$$

Однако камнем, на который нашла коса теории множеств, оказался, по сути, всё тот же юнивёрсум.

Пример 2.4 (Парадокс Рассела). Назовём некоторое множество «обычным», если оно не содержит себя в качестве элемента. Пусть U_0 — множество всех «обычных» множеств. Можно проверить, что не выполнено как $U_0 \in U_0$, так и $U_0 \notin U_0$, что является парадоксом.

Заметим, что запрет на существование «необычных» множеств сильно обедняет теорию, ведь тогда не будет существовать юнивёрсум всех множеств.

Данный парадокс можно решить, лишь отказавшись от теории множеств в пользу более фундаментальной теории — теории типов, но это уже совсем другая история.

2.2 Множества и логика

Исследуя базовые понятия теории множеств, мы совсем не рассматривали операции, которые можно над множествами совершать. В этом разделе мы убьём сразу двух зайцев: исследуем связь алгебры логики и теории множеств, а также наконец определим упомянутые операции.

Вернёмся к определению множества посредством задания условия. Понятно, что если юнивёрсум — $\{0, 1\}$, то $f(x)$ в пункте 3) — булева функция. В более общем случае говорят, что $f(x)$ — ***унарный предикат***.

Определение 2.5. ***Предикатом*** арности n называют булевозначную функцию от n аргументов из U.

Аналогично булевым функциям, сложные предикаты можно конструировать из простых при помощи формул и логических связок (см. (2.1)). Однако наличие юнивёрсума позволяет использовать при построении предикатов ещё более мощный инструмент — ***кванторы***. Ограничимся лишь неформальным их определением:

$$\begin{aligned} \forall \text{ (всеобщности)}: &\quad \forall x\, P(x) = \text{«для любого } x \in U \text{ истеннен предикат } P(x)\text{»} \\ \exists \text{ (существования)}: &\quad \exists x\, P(x) = \text{«существует } x \in U \text{ такой, что истеннен предикат } P(x)\text{»} \end{aligned}$$

Замечание 2.6. В случае, когда юнивёрсум конечный, любую формулу с кванторами можно заменить эквивалентной формулой без них, используя связки $\wedge$, $\vee$ и $\neg$. В общем случае это не так.

Замечание 2.7 (Обобщённый закон де Моргана). Справедливо равенство

$$\forall x\, P(x) = \neg\left(\exists x\, \neg P(x)\right)$$

Наконец, можно установить соответствие между любым множеством и некоторым предикатом:

$$A = \{x \mid f(x)\} \qquad \Longleftrightarrow \qquad f(x) = \text{«}x \in A\text{»} \tag{2.2}$$

Предикат, соответствующий согласно равенству (2.2) некоторому множеству A, будем называть ***индикаторной функцией*** A и обозначать $\mathbb{I}_A(x)$. Используя индикаторные функции и алгебру логики, можно определить все привычные и непривычные вам теоретико-множественные операции (таблица 2.1) и отношения (таблица 2.2). Заметим, что пустое множество является подмножеством любого множества!

Название	Обозначение	Описание	Формула
Пересечение	$A \cap B$	Элементы, входящие как в A, так и в B	$\mathbb{I}_{A\cap B}(x) = \mathbb{I}_A(x) \wedge \mathbb{I}_B(x)$
Объединение	$A \cup B$	Элементы, входящие в A или B	$\mathbb{I}_{A\cup B}(x) = \mathbb{I}_A(x) \vee \mathbb{I}_B(x)$
Разность	$A \setminus B$	Элементы, входящие в A, но не в B	$\mathbb{I}_{A\setminus B}(x) = \mathbb{I}_A(x) \wedge \neg\mathbb{I}_B(x)$
Симметрическая разность	$A \triangle B$	Элементы, входящие либо в A, либо в B	$\mathbb{I}_{A\triangle B}(x) = \mathbb{I}_A(x) \oplus \mathbb{I}_B(x)$
Дополнение	A^c, $U \setminus A$	Элементы юнивёрсума, не входящие в A	$\mathbb{I}_{A^c}(x) = \neg\mathbb{I}_A(x)$

Таблица 2.1: теоретико-множественные операции

Название	Обозначение	Описание	Формула
Равенство	$A = B$	Все элементы A являются элементами B, и наоборот	$\mathbb{I}_A(x) \leftrightarrow \mathbb{I}_B(x)$
Подмножество	$A \subseteq B$	Все элементы A являются элементами B	$\mathbb{I}_A(x) \rightarrow \mathbb{I}_B(x)$
Собственное подмножество	$A \subset B$, $A \subsetneq B$	Все элементы A являются элементами B, но $A \neq B$	$(\mathbb{I}_A(x) \rightarrow \mathbb{I}_B(x)) \wedge$ $\wedge\neg(\mathbb{I}_B(x) \rightarrow \mathbb{I}_A(x))$

Таблица 2.2: теоретико-множественные отношения

Множества, отношения и операции с ними часто бывает удобно схематично изображать в виде диаграмм Эйлера-Венна. В общем случае это набор геометрических фигур, пересечения, вложения и прочие отношения между которыми обозначают те же отношения между соответствующими исходными множествами.

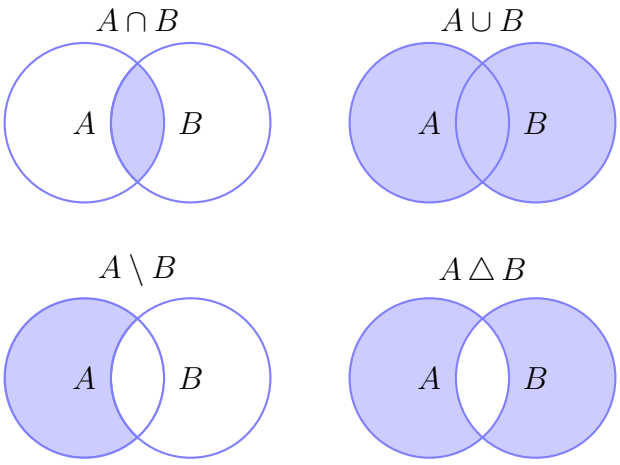


Рис. 2.1: диаграммы Эйлера-Венна для двух пересекающихся множеств и результатов базовых операций с ними

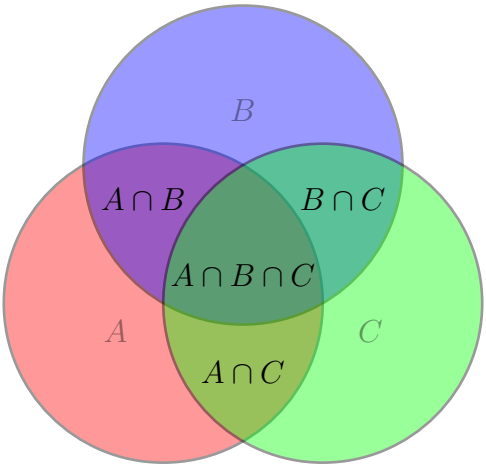


Рис. 2.2: диаграмма Эйлера-Венна для трёх множеств

Замечание 2.8. Интересно, что невозможно нарисовать диаграмму Эйлера-Венна, состоящую из окружностей (пусть и произвольного размера), для всех вариантов отношений между четырьмя и более множествами.

Наконец, введём последнее обозначение, необходимое в этом разделе.

Определение 2.9. ***Множеством всех подмножеств*** (или ***булеаном***) некоторого множества A называется множество $\mathcal{P}(A) = 2^A = \{x \mid x \subseteq A\}$.

Задача 1

Задайте формально следующие множества:

1) Множество простых чисел.
2) Множество всех отрезков на числовой прямой.
3) Множество всех действительных корней всевозможных нетривиальных квадратных многочленов с целыми коэффициентами. Что изменится, если убрать условие на коэффициенты?

Решение задачи 1

1) $\mathbb{P} = \{x \in \mathbb{N} \mid \neg\,(\exists a \exists b\,(x = a \cdot b) \wedge (a \neq 1) \wedge (a \neq x)) \wedge (x \neq 1)\}$
2) $S = \left\{x \in 2^{\mathbb{R}} \mid \exists a \exists b\,(a \in \mathbb{R}) \wedge (b \in \mathbb{R}) \wedge (\forall c\,(a \leqslant c \leqslant b) \leftrightarrow (c \in x))\right\}$
3) $R = \{x \in \mathbb{R} \mid \exists a \exists b \exists c\,(a \in \mathbb{Z}) \wedge (b \in \mathbb{Z}) \wedge (c \in \mathbb{Z}) \wedge (a^2 + b^2 + c^2 \neq 0) \wedge (ax^2 + bx + c = 0)\}$. Если коэффициенты сделать произвольными, то, очевидно, получится $\mathbb{R}$, так как любое число a является корнем $x - a = 0$.

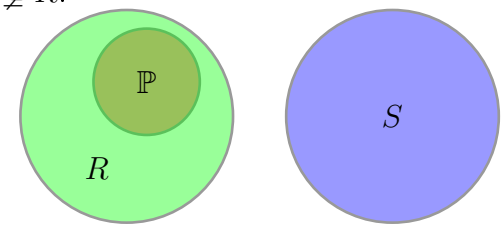
Задача 2

Нарисуйте диаграмму Эйлера-Венна для трёх множеств из предыдущей задачи.

Решение задачи 2

Очевидно, S никак не пересекается с $\mathbb{P}$ и R в силу разной природы объектов. Также понятно, что для любого простого числа p можно построить многочлен $x - p$ с целыми

коэффициентами, корнем которого p и будет являться; также, например, $\sqrt{2} \in R$. Итого, $\mathbb{P} \subsetneq R$.



Задача 3

Верно ли, что если $B \subseteq A$, то $A \setminus B = A \triangle B$?

Решение задачи 3

Если $B \subseteq A$, то

$$\mathbb{I}_{A \triangle B}(x) = \underbrace{(\mathbb{I}_A(x) \vee \mathbb{I}_B(x))}_{\mathbb{I}_A(x),\ \text{т.к. } \forall x\, \mathbb{I}_B(x) \to \mathbb{I}_A(x)} \wedge \underbrace{\neg(\mathbb{I}_A(x) \wedge \mathbb{I}_B(x))}_{\neg\mathbb{I}_B(x),\ \text{т.к. } \forall x\, \mathbb{I}_B(x) \to \mathbb{I}_A(x)} = \mathbb{I}_A(x) \wedge \neg\mathbb{I}_B(x) = \mathbb{I}_{A \setminus B}(x)$$

Аналогичное доказательство в теоретико-множественных обозначениях:

$$A \triangle B = \underbrace{(A \cup B)}_{A} \setminus \underbrace{(A \cap B)}_{B} = A \setminus B$$

Задача 4

Используя только операции $\triangle$ и $\cap$, выразите $A \cup B \cup C$

Решение задачи 4

Докажем, что

$$A \cup B \cup C = U \triangle A \triangle B \triangle C \triangle A \cap B \triangle A \cap C \triangle B \cap C \triangle A \cap B \cap C$$

Действительно, если это переписать в терминах индикаторных функций, то получим

$$1 \oplus a \oplus b \oplus c \oplus a \wedge b \oplus a \wedge c \oplus b \wedge c \oplus a \wedge b \wedge c$$

где $a = \mathbb{I}_A(x)$, $b = \mathbb{I}_B(x)$, $c = \mathbb{I}(x)$.

Видно, что если $a = b = c = 0$, то выражение ложно. Также заметим, что если $a = 1$, а $b = c = 0$, то выражение истинно. Далее можно заметить, что до тех пор, пока есть хотя бы одна истинная переменная, формула не меняет своего значения при изменении любой другой переменной: свои значения всегда будет менять чётное число слагаемых. Но тогда из всего вышесказанного следует, что формула задаёт функцию $a \vee b \vee c$. Возвращаясь к множествам, получаем, что исходное тождество доказано.

Кратко упомянем и иное доказательство: достаточно проверить равенство только в случаях $(a, b, c) = (0, 0, 0)$, $(1, 0, 0)$, $(1, 1, 0)$ и $(1, 1, 1)$, а потом воспользоваться симметричностью формулы.

3 Математические определения, утверждения и доказательства

В предыдущих разделах мы ввели внушительный математический аппарат, более-менее строго описывающий базовые математические объекты и связи между ними. Настало время применить этот аппарат и для формального описания более сложных объектов.

Определение 3.1. ***Определением*** называется некоторый унарный предикат; он является индикаторной функцией множества объектов, удовлетворяющих определению.

Определение 3.2. ***Математическим утверждением*** называется формула, не имеющая свободных переменных (параметров), а потому либо истинная, либо ложная. Иногда утверждением также называется предикат арности, большей нуля; в таком случае подразумевается, что перед ним стоят кванторы всеобщности по всем свободным переменным.

Определение 3.3. ***Теоремой***, ***леммой***, ***предложением*** или ***утверждением*** называется истинное математическое утверждение. Выбор конкретного названия обусловлен лишь ролью утверждения в математическом тексте.

Определение 3.4. ***Критерием*** называется истинное математическое утверждение вида

$$\forall x\ (A(x) \leftrightarrow B(x))$$

Определим также несколько вспомогательных терминов, возникающих при рассмотрении математических утверждений определённого вида.

Определение 3.5. Пусть имеется математическое утверждение вида

$$\forall x\ (A(x) \to B(x))$$

Тогда говорится, что условие $B(x)$ ***необходимо*** для выполнения $A(x)$, а условие $A(x)$ ***достаточно*** для выполнения $B(x)$. Или, по-другому, условие $A(x)$ более ***сильное***, чем $B(x)$, а $B(x)$ — более ***слабое***, чем $A(x)$.

Если также имеются математические утверждения вида

$$\forall x\ (A(x) \to C(x))\,, \qquad \forall x\ (B(x) \to C(x))\,,$$

то второе из них считается более ***сильным***, так как в нём $C(x)$ следует из более слабого математического утверждения $B(x)$.

3.1 Доказательства

Наверняка вы заметили, как просто было доказать тавтологичность формул в алгебре логики: если совсем никак не получается это сделать преобразованием формул, верный ответ всегда даст таблица истинности. Проблемы начинаются при первой же попытке перейти к чему-то более сложному. Реальные теоремы простым перебором всех аргументов предикатов не докажешь, ведь юнивёрсум может быть бесконечным. Остаются только преобразования формул.

Во многом, формальная логика — это наука о переписывании формул. В основу формальной системы ложатся некоторые аксиомы, тавтологичность которых постулируется, и некоторые правила вывода. Основным правилом является ***modus ponens***:

$$\frac{A \to B, \quad A}{B}$$

Данная запись, по существу, означает, что если истинно как утверждение A, так и $A \to B$, то истинно и B. На его основе можно сконструировать и более сложные правила, некоторые из которых даже имеют своё название.

Пример 3.6.

1. Несколько безымянных правил вывода:

$$\frac{A \vee B, \quad \neg A}{B} \qquad \frac{A_1, \quad \ldots, \quad A_{n-1}, \quad \neg\left(\bigwedge_{k=1}^{n} A_k\right)}{\neg A_n} \qquad \frac{A \wedge B}{A} \qquad \frac{B}{A \to B}$$

2. Правило контрапозиции:

$$\frac{A \to B}{\neg B \to \neg A}$$

   (то есть, $(A \to B) \leftrightarrow (\neg B \to \neg A)$ — тавтология, как уже было показано в разделе про алгебру логики).

3. «От противного»:

$$\frac{A \to B, \quad \neg B}{\neg A}$$

Замечание 3.7. В общем случае запись $\dfrac{A_1, \quad \ldots, \quad A_n}{B}$ эквивалентна тавтологичности формулы $\left(\bigwedge_{k=1}^{n} A\right) \to B$.

Доказательство теоремы сводится либо к упрощению при помощи правил вывода входной формулы до уровня, когда тавтологичность проверяется легко, либо к выводу из исходного утверждения и аксиом некоторого противоречия, которое будет говорить о том, что исходное утверждение ложно. В нашем курсе, конечно, не придётся опускаться до таких формальностей, чтобы даже самые простые утверждения доказывать исключительно итеративным явным применением правил вывода.

Отдельно отметим правило вывода, не сводящееся к modus ponens: ***математическую индукцию***. Формальная запись:

$$\frac{A(0), \quad \forall n \ (A(n) \to A(n+1))}{\forall n \, A(n)}$$

Данное правило либо постулируется, либо выводится из некоторых других аксиом.

Задача 1

Получите формально правило

$$\frac{A \oplus B, \quad B}{\neg A}$$

из modus ponens, правил в примере 3.6, правил преобразования к связкам $\neg$ и $\to$, а также тавтологичности $A \to (B \to A)$.

Решение задачи 1

Перейдём к отрицаниям и импликациям:

$$A \oplus B = \neg(A \leftrightarrow B) = \neg\left[(A \to B) \wedge (B \to A)\right] = \\ = \neg(A \to B) \vee \neg(B \to A) = (A \to B) \to \neg(B \to A)$$

Из правила в примере имеем

$$\frac{B}{A \to B}$$

Применяя modus ponens к исходному утверждению и полученной формуле, получаем

$$\frac{A \to B, \quad (A \to B) \to \neg(B \to A)}{\neg(B \to A)}$$

Правило «от противного»:

$$\frac{A \to (B \to A)}{\neg(B \to A) \to \neg A}$$

Наконец,

$$\frac{\neg(B \to A) \to \neg A, \quad \neg(B \to A)}{\neg A}$$

Еще раз акцентируем внимание на том, что **не требуется излишне формализовывать процесс доказательства, если в этом нет необходимости!** Изложенная выше теория должна помочь вам понять общую структуру процесса доказательства, увидеть некоторую его модульность, переиспользование каких-то распространённых схем вывода как самостоятельных правил.

3.2 Примеры

Рассмотрим несколько примеров использования изученных в предыдущем разделе методов доказательства.

Задача 2

Пусть A, B, C — множества. Верно ли, что если $A \cap B$ не является подмножеством C, то или $A \not\subseteq C$, или $B \not\subseteq C$?

Решение задачи 2

Требуется проверить тавтологичность

$$\neg(A \cap B \subseteq C) \to [\neg(A \subseteq C) \wedge \neg(B \subseteq C)]$$

Сделаем это, применив правило контрапозиции.

$$[(A \subseteq C) \vee (B \subseteq C)] \to (A \cap B \subseteq C)$$

Можно «добить» это выражение формальными преобразованиями, но, в принципе, уже понятно, что если хотя бы одно множество полностью лежит в C, то и пересечение тоже.

Для тренировки упростим формулу до конца, введя стандартные обозначения для индикаторных функций и перейдя к алгебре логики:

$$[(a \to c) \vee (b \to c)] \to (a \wedge b \to c)$$

Раскроем все импликации:

$$\neg\left[(\neg a \vee c) \vee (\neg b \vee c)\right] \vee (\neg(a \wedge b) \vee c)$$

$$\neg[\neg a \vee \neg b \vee c] \vee (\neg a \vee \neg b \vee c)$$

Тавтологичность доказана.

Задача 3

Докажите, что если у числоой последовательности есть предел, то он единственнен.

Решение задачи 3

Характерный пример доказательство от противного. Предположим, что $a \neq b$ — два предела $\{x_n\}_{n=1}^{\infty}$. Определение предела:

$$\forall \varepsilon > 0 \;\; \exists N : \; \forall n > N \;\; |x_n - a\,(b)| < \varepsilon$$

Возьмём $\varepsilon_0 = |b-a|/3 > 0$. Тогда

$$\exists N_a : \; \forall n > N_a \;\; |x_n - a| < \varepsilon_0 \qquad \exists N_b : \; \forall n > N_b \;\; |x_n - b| < \varepsilon_0$$

Обозначим $x' = x_{\max\{N_a, N_b\}+1}$. Тогда $3\varepsilon_0 = |a-b| = |a - x' + x' - b| \leqslant |a-x'| + |x'-b| < \varepsilon_0 + \varepsilon_0 < 3\varepsilon_0$. Противоречие Значит, либо $a = b$, либо $\{x_n\}_{n=1}^{\infty}$ не имеет предела.

Задача 4

Пусть последовательность $\{x_n\}_{n=0}^{\infty}$ задана рекуррентным соотношением $x_{n+1} = ax_n + b$, $a \neq 1$. Докажите, что

$$x_n = x_0 \cdot a^n + b \cdot \frac{a^n - 1}{a - 1} \tag{3.1}$$

Решение задачи 4

Докажем методом математической индукции.
База: $x_0 = x_0 \cdot 1 + b \cdot 0 = x_0$.
Шаг: пусть для некоторого n верно (3.1). Тогда

$$x_{n+1} = ax_n + b = x_0 \cdot a \cdot a^n + b \cdot \left[1 + a \cdot \frac{a^n - 1}{a - 1}\right] = x_0 \cdot a^{n+1} + b \cdot \frac{a^{n+1} - 1}{a - 1}$$

Итого, по индукции доказано.

4 Неориентированные графы

Графы — это математические объекты, довольно часто встречающиеся в реальных задачах (логистика, интернет, социальные связи), но при этом достаточно простые, чтобы без труда формально определить их при помощи изученного нами математического аппарата. Неформально говоря, граф — это абстракция, применимая к множеству любой природы, в случае, когда интересны только парные связи между его элементами.

Граф часто представляется в виде изображения следующего формата: точки или кружки (элементы множества, ***вершины***) соединены линиями или стрелками (***рёбрами***), изображающими связи между элементами. Вершины и рёбра могут иметь некоторые ***атрибуты*** (числа, строки, любые другие объекты).

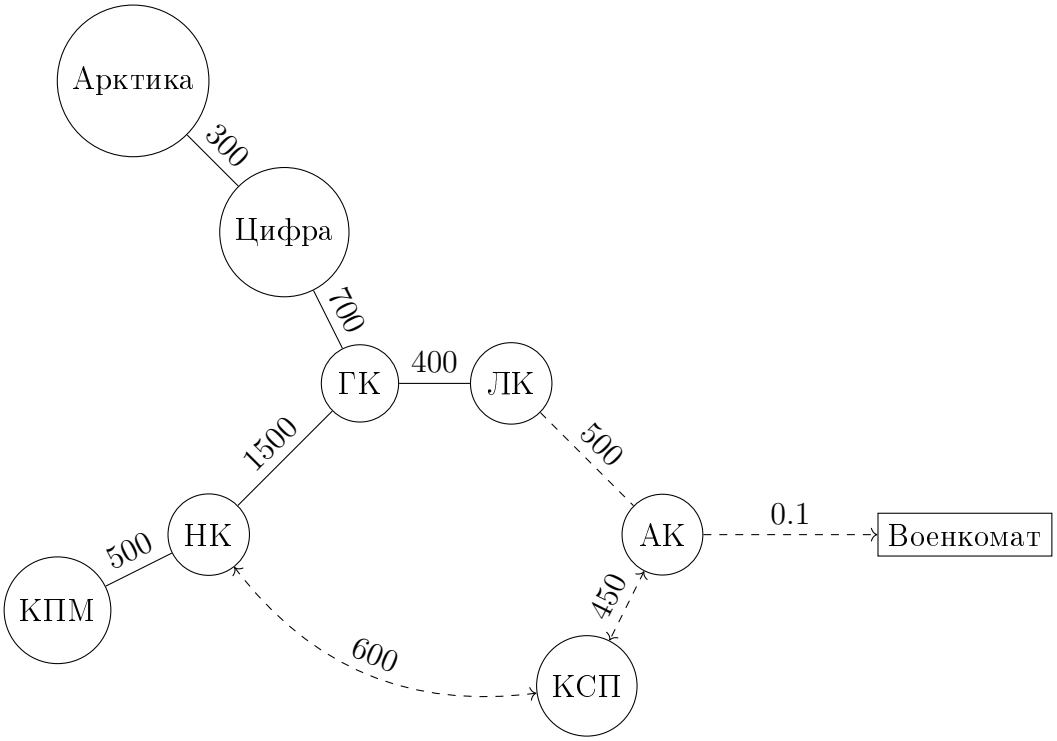


Рис. 4.1: граф ежедневного перемещения людей между некоторыми связанными с Физтехом зданиями. Рёбра обозначают тип и направление перехода, а также ежедневный поток студентов.

Изучение графов мы начнём с самых простых их разновидностей, постепенно усложняя конструкцию. Но перед этим потребуется ввести пару вспомогательных определений.

Определение 4.1. ***Множеством всех подмножеств мощности*** k некоторого множества A будем называть множество

$$\binom{A}{k} = \{B \mid (B \subseteq A) \wedge (|B| = k)\}$$

Определение 4.2. ***Множеством всех неупорядоченных пар*** некоторого множества A будем называть множество $\binom{A}{2}$.

Замечание 4.3. Если $|A| = n < +\infty$, и $0 \leqslant k \leqslant n$, то

$$\left|\binom{A}{k}\right| = \frac{n!}{k!(n-k)!} \triangleq \binom{n}{k} \triangleq C_n^k$$

4.1 Простые неориентированные графы

Начнём с самой простой конструкции графа, для построения которой достаточно понятия неупорядоченной пары.

Определение 4.4. ***(Простой неориентированный) граф*** — это упорядоченная пара (V, E) множества ***вершин*** V и ***рёбер*** $E \subseteq \binom{V}{2}$. Введём также следующие обозначения, если V и E фиксированы:

$$G = (V, E) \text{ — граф} \qquad \Longrightarrow \qquad G(V, E) \triangleq (V, E),\ V(G) \triangleq V,\ E(G) \triangleq E$$

«Простой» означает, что в графе нет ***петель*** (рёбер вида $\{v,\ v\} = \{v\}$) и ***кратных рёбер*** (каждое ребро входит в E единожды). ***«Неориентированный»*** означает, что ребро является неупорядоченной парой.

Зафиксируем граф $G = G(V, E)$.

Определение 4.5. Вершины u и v называются ***смежными*** или ***соседями***, если они образуют ребро: $\{u, v\} \in E$. Рёбра e и f называются ***смежными***, если они имеют общую вершину: $e \cap f \neq \varnothing$. Вершина v ***инцидента*** ребру e, если $u \in e$. Вершины u и v, инцидентные ребру e, называются его ***концами***; говорят, что e ***соединяет*** u и v.
Рёбра часто записывают сокращённо: uv вместо $\{u, v\}$.

Определение 4.6. ***Степенью*** вершины v называется число $d(v)$ смежных с v рёбер.

Теорема 4.7 (о рукопожатиях). $\sum\limits_{v \in V} d(V) = 2|E|$

Доказательство. $\sum\limits_{v \in V} d(V) = \sum\limits_{v \in V} \sum\limits_{\substack{e \in E, \\ v \in e}} 1 = \sum\limits_{e \in E} \sum\limits_{\substack{v \in V, \\ v \in e}} 1 = \sum\limits_{e \in E} 2 = 2|E|$ □

Определим отдельно несколько частных случаев простого неориентированного графа.

Определение 4.8.

1) ***Граф-путь*** P_n, $n \geqslant 0$ — граф вида

$$V(P_n) = \{v_1, \ldots, v_n\}, \qquad E(P_n) = \{\{v_0, v_1\}, \{v_1, v_2\}, \ldots, \{v_{n-1}, v_n\}\}$$

Вершины v_1 и v_n называются ***концами пути***, а $n = |E|$ — ***длиной***. *Ещё раз акцентируем внимание на том, что $n \geqslant 0$, а вершины нумеруются с нуля.*

2) ***Граф-цикл*** C_n, $n \geqslant 3$ — граф вида

$$V(G) = \{v_1, \ldots, v_n\}, \qquad E(G) = \{\{v_1, v_2\}, \{v_2, v_3\}, \ldots, \{v_{n-1}, v_n\}, \{v_n, v_1\}\}$$

Ещё раз акцентируем внимание на том, что $n \geqslant 3$.

3) ***Полный граф*** (или ***граф-клика***) $K_n(V, E)$, $n \geqslant 1$ — это граф, заданный равенством

$$K_n(V, E) = \left(V, \binom{V}{2}\right),\ n = |V| \qquad \left(\text{ то есть } E = \binom{V}{2}\right)$$

4) ***Граф-звезда*** S_n, $n \geqslant 0$ — граф вида

$$V(S_n) = \{v_0, v_1, \ldots, v_n\} \qquad E(S_n) = \{\{v_0, v_1\}, \{v_0, v_2\}, \ldots, \{v_0, v_n\}\}$$

Ещё раз акцентируем внимание на том, что $n \geqslant 0$, а вершины нумеруются с нуля.

5) ***Пустой граф*** — граф, у которого $V = E = \varnothing$. Его принято обозначать тоже $\varnothing$, хотя, формально, это $(\varnothing, \varnothing) \neq \varnothing$.

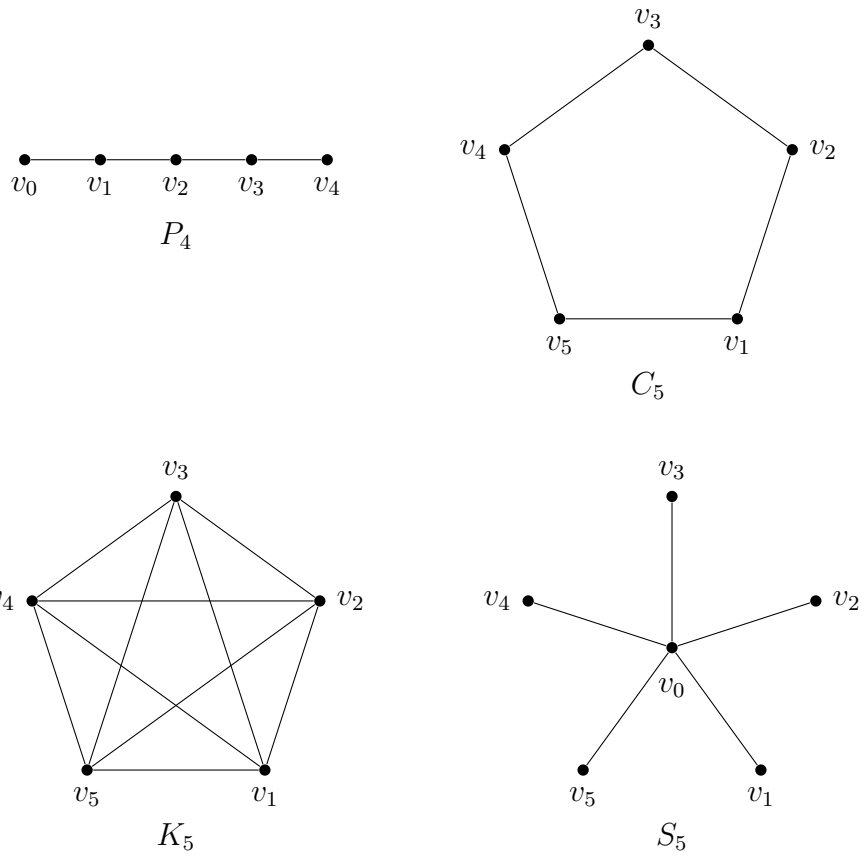


Рис. 4.2: базовые графы

4.2 Теоретико-множественные операции с графами

Известные нам теоретико-множественные операции можно обобщить на графы.

Определение 4.9. Пусть $G(V, E)$ и $H(W, I)$ — графы. Тогда ***объединение***, ***персечение*** G и H, а также ***дополнение*** G определяются как, соответственно,

$$G \cup H = (V \cup W, E \cup I), \quad G \cap H = (V \cap W, E \cap I), \quad G^c = \left(V, \binom{V}{2} \setminus E\right)$$

Множество $\binom{V}{2} \setminus E$ называется множеством ***нерёбер*** графа $G(V, E)$.

Замечание 4.10. $G \cup G^c = K_{|V(G)|}$.

Задача 1

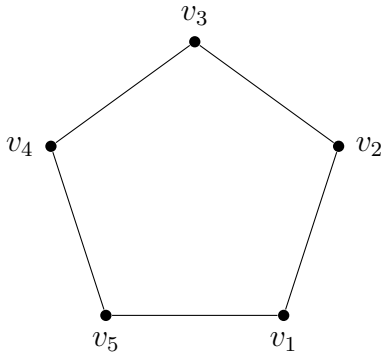
Существует ли такой граф-цикл, дополнение которого тоже является графом-циклом?

Решение задачи 1

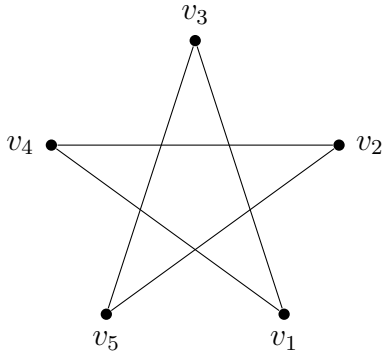
Так как при дополнении число вершин не меняется, если такой граф и есть, то, в силу 4.3 и 4.10, выполено равенство

$$|V(C_n)| = n = \frac{n(n-1)}{2} - n = |V(K_n)| - |V(C_n)|, \qquad n \geqslant 1$$

Отсюда $n = 5$. Тогда легко привести единственный пример такого графа:



C_5



$C_5^c = C_5'$

4.3 Подграфы

Иногда бывает интересно исследовать какую-то часть графа как отдельный граф. Это может понадобиться как при решении реальных задач, так и при доказательстве вспомогательных фактов.

Определение 4.11. Граф $H(W, I)$ является ***(рёберным) подграфом*** графа $G(V, E)$ $\overset{\triangle}{\iff} W \subseteq V$ и $I \subseteq E$. Это обозначается как $H \subseteq G$. Случай, когда $H \subseteq G$ и $H \neq G$, обозначается как $H \subsetneq G$. Если при этом ещё и $H \neq \varnothing$, $H \neq G$, то подграф называется ***несобственным***.

Определение 4.12. Пусть $G(V, E)$ — граф, $U \subseteq V$. Будем называть ***индуцированным (множеством U) подграфом*** граф $\left(U, \binom{U}{2} \cap E\right)$. Индуцированный подграф обозначается $H[U]$.

Неформально, индуцированный множеством U подграф — это подграф на вершинах U, в ктором провели все возможные рёбра, которые есть в исходном графе.

Определение 4.13. Множество $U \subseteq V$ называется ***независимым*** множеством вершин графа $G(V, E) \overset{\triangle}{\iff} H[U]$ не содержит рёбер.

Определение 4.14. ***Подграфом-путём/циклом/кликой/звездой*** некоторого графа G называется подграф G, являющийся путём/циклом/полным графом/звездой соответственно.

Данное определение естественным образом обобщается и на любые другие именные частные случаи графов.

Определение 4.15. Пусть предикат $P(x)$ определён на множестве графов (он задаёт некоторое свойство/определение, см. 3.1). Обозначим $P_G = \{x \subseteq G \mid P(x)\}$ множество всех подграфов графа G, удовлетворяющих свойству $P(x)$.
Подграф $H \in P_G$ является ***максимальным*** среди подграфов со свойством $P \overset{\triangle}{\iff} \forall H' \in P_G \ \ (H \subseteq H') \to (H = H')$.

Задача 2

Верно ли, что определение максимального подграфа со свойством P эквивалентно следующему: $H \in P_G$ — максимальный подграф графа G со свойством $P \overset{\triangle}{\iff} \forall H' \in P_G \;\; H' \subseteq H$?

Решение задачи 2

Нет, неверно. В частности, если рассмотреть $G = P_2 \sqcup P_1'$[2], то максимальным подграфом-путём в нём будет P_2, но определению из условия задачи он удовлетворять не будет, так как $P_1' \not\subseteq P_2$.

4.4 Связность

Граф, полученный в решении задачи 2, состоит как бы из двух «независимых», или ***несвязных*** подграфов P_2 и P_1'. В реальных задачах часто требуется обнаружить подобные случаи (например, чтобы определить недостижимые части страны по карте дорог, или отдельные социальные группы по графу связей).

Определение 4.16. Вершина u в графе G является ***достижимой*** из вершины $v \overset{\triangle}{\iff}$ существует подграф-путь графа G, концами которого являются вершины u и v. Это обозначается как $u \rightsquigarrow v$.

Замечание 4.17. В случае неориентированного графа $(u \rightsquigarrow v) \leftrightarrow (v \rightsquigarrow u)$ (***симметричность*** достижимости).
Также $u \rightsquigarrow u$ (***рефлексивность***) и $[(u \rightsquigarrow v) \wedge (v \rightsquigarrow w)] \to (u \rightsquigarrow w)$ (***транзитивность***).

Определение 4.18. ***Компонентой связности*** графа $G(V, E)$ будем называть подграф G, индуцированный на некотором непустом множестве $U \subseteq V$, удовлетворяющем свойству $\forall u, v \in U \; (u \rightsquigarrow v)$ и являющемся максимальным относительно него.
Компонента связности, состоящая из одной вершины, называется ***изолированной вершиной***.
Граф, являющийся компонентой связности самого себя, называется ***связным***.

Замечание 4.19. Позже будет доказано, что из замечания 4.17 следует, что любой граф разбивается на компоненты связности, причём единственным образом:

$$G = H_1 \sqcup H_2 \sqcup \ldots \sqcup H_k$$

Задача 3

Пусть G и H — простые графы, причём $G \cap H = \varnothing$. Определим граф $G \times H$ следующим образом:

$$V(G \times H) = \{\{u, v\} \mid u \in V(G), v \in V(H)\}$$

$$E(G \times H) = \left\{ \{\{u_1, v\}, \{u_2, v\}\} \;\middle|\; (\{u_1, u_2\} \in E(G)) \wedge (v \in V(H)) \right\} \cup \\ \cup \left\{ \{\{u, v_1\}, \{u, v_2\}\} \;\middle|\; (\{v_1, v_2\} \in E(H)) \wedge (u \in V(G)) \right\}$$

Пусть G имеет n компонент связности, а H — m. Сколько компонент связности имеет $G \times H$? Как они устроены?

[2]Операция $\sqcup$ означает то же самое, что и $\cup$, просто с такой записью уточняется, что объединяемые множества не пересекаются.

Решение задачи 3

Заметим, что $\{u_1, v_1\} \rightsquigarrow \{u_2, v_2\} \iff (u_1 \rightsquigarrow u_2) \wedge (v_1 \rightsquigarrow v_2)$.
Действительно,

$\Leftarrow$ Если $u_1 \rightsquigarrow u_k$ и $v_1 \rightsquigarrow v_l$, то существуют пути P_G и P_H из u_1 в u_k и из v_1 в v_l соответственно (нумерация введена уже для вершин путей).

Заметим, что все рёбра вида $\big\{\{u_i, v_j\}, \{u_{i+1}, v_j\}\big\}$ и $\big\{\{u_i, v_j\}, \{u_i, v_{j+1}\}\big\}$, где $\{u_i, u_{i+1}\} \in E(P_G)$ и $\{v_j, v_{j+1}\} \in E(P_H)$, лежат в $E(G \times H)$ по построению.

Но тогда в $G \times H$ есть путь вида

$$\{u_1, v_1\} \to \{u_2, v_1\} \to \ldots \to \{u_k, v_1\} \to \{u_k, v_2\} \to \ldots \to \{u_k, v_l\}$$

То есть $\{u_1, v_1\} \rightsquigarrow \{u_k, v_l\}$.

$\Rightarrow$ Если $\{u_1, v_1\} \rightsquigarrow \{u_k, v_l\}$, то существует путь $P_{G\times H}$ из $\{u_1, v_1\}$ в $\{u_k, v_l\}$.

Из определения $G \times H$ следует, можно перенумеровать u_i и u_j так, что путь $P_{G\times H}$ имеет рёбра только вида $\big\{\{u_i, v_j\}, \{u_{i+1}, v_j\}\big\}$ или $\big\{\{u_i, v_j\}, \{u_i, v_{j+1}\}\big\}$.

Но тогда в G и H есть пути $u_1 \to u_2 \to \ldots \to u_k$ и $v_1 \to v_2 \to \ldots \to v_l$ соответственно. То есть $u_1 \rightsquigarrow u_k$ и $v_1 \rightsquigarrow v_l$.

Но тогда получаем, что все компоненты связности графа $G \times H$ будут иметь вид $G_i \times H_j$, где G_i и H_j — компоненты связности графов G и H соответственно. Тогда ответ: $n \cdot m$.

4.5 Деревья

Часто бывает удобно исследовать, в некотором смысле, ***минимальные*** по числу рёбер связные графы. Такие графы называются ***деревьями*** и обладают множеством полезных свойств.

Определение 4.20. ***Деревом*** назовём ***минимально связный граф***, то есть граф, теряющий свойство связности при удалении любого ребра.

Если подходить к деревьям именно со стороны минимальности, то кажется осмысленным сначала привести некоторую оценку, насколько вообще можно сделать «малым» граф, сохраняя его связность.

Теорема 4.21. Пусть $\#\mathrm{KC}(G)$ обозначает число компонент связности некоторого графа $G(V, E)$. Тогда $\forall G \ \#\mathrm{KC}(G) \geqslant |V(G)| - |E(G)|$.

Доказательство. По индукции для фиксированного $|V|$ по числу рёбер от 0 до $|V|$. $\square$

Следствие 4.22. Если граф связный, то $|E| \geqslant |V| - 1$.

Из следствия очевидным образом можно получить эквивалентное определение дерева. На самом деле, этим множество эквивалентных определения дерева не ограничивается.

Теорема 4.23. Следующие свойства эквивалентны:

(1) Граф $G(V, E)$ минимально связный.

(2) Граф $G(V, E)$ связный и $|E| = |V| - 1$.

(3) Граф $G(V, E)$ связный и ***ациклический*** (не имеет подграфов-циклов).

(4) В графе $G(V, E)$ из любой вершины в любую есть путь, причём единственный.

В ходе доказательства теоремы выше обычно используется следующая (полезная и в отдельности) лемма:

Лемма 4.24. Если между некоторыми вершинами графа есть два различных пути, то граф содержит цикл.

Также стоит отметить следующее утверждение:

Следствие 4.25. В любом дереве более чем с одной вершиной есть хотя бы две вершины степени 1.

Доказательство. Следует из теоремы 4.7 и пункта (2) теоремы 4.23. □

4.6 Расстояние между вершинами. Диаметр графа

Поскольку графы часто используются для моделирования транспортных сетей, имеет смысл ввести некоторое «расстояние» между двумя вершинами, а также характеристики, связанные с ним.

Определение 4.26. Пусть G — связный граф, $u, v \in V(G)$. Тогда ***расстоянием*** между вершинами u и v называется длина кратчайшего пути между ними:

$$\rho(u, v) = \min_{P_{u \rightsquigarrow v} \subseteq G} |E(P_{u \rightsquigarrow v})|,$$

где $P_{u \rightsquigarrow v}$ — подграф-путь из u в v.[3]

Определение 4.27. ***Диаметром*** графа G называется наибольшее растояние между какими-то двумя его вершинами:

$$\operatorname{diam} G = \max_{u,v \in V(G)} \rho(u, v)$$

Определение 4.28. ***Центром*** графа G называется вершина, наименее удалённая от всех остальных, то есть

$$c(G) = \arg\min_{u \in V(G)} \max_{v \in V(G)} \rho(u, v)$$

На самом деле, таких вершин может быть несколько. Тогда, в зависимости от соглашения, под $c(G)$ понимают либо их множество, либо любую из них.
Максимальное расстояние от центра графа до какой-либо вершины называется ***радиусом*** графа G:

$$\operatorname{rad} G = \max_{v \in V(G)} \rho\left(c(G), v\right)$$

4.7 Правильные раскраски

При исследовании графов часто возникает задача разбиения вершин на некоторое количество групп (задача ***раскраски***). Иногда также получается, что какая-то задача из совершенно другой области математики может быть проинтерпретированна как задача раскраски некоторого графа. Поэтому так важен вопрос построения ***раскрасок***, обладающих определёнными свойствами.

[3] Это исключительно авторское обозначение. Не рекомендуется использовать без определения.

Определение 4.29. ***Раскраской*** (***k-раскраской***) графа G назывется функция f, принимающая в качестве аргумента $v \in V(G)$, и выдающая число из $\{1, \ldots, k\}$. То есть, $f : V(G) \to \{1, \ldots, k\}$.

Определение 4.30. Раскраска f графа G является ***правильной*** $\overset{\triangle}{\iff}$ никакие две смежные вершины не окрашены в один цвет, то есть

$$\forall u, v \in V(G) \;\; (\{u, v\} \in E(G)) \to (f(u) \neq f(v))$$

Определение 4.31. Граф G является k***-раскрашиваемым*** $\overset{\triangle}{\iff}$ для G существует правильная раскраска из k цветов.
Хроматическим числом графа G называется число $\chi(G)$, равное минимальному k такому, что G k-раскрашиваемый.

Задача проверки 2-раскрашиваемости (двураскрашиваемости) графа является сравнительно «лёгкой». Полного перебора позволяет избежать следующий критерий:

Теорема 4.32. Граф G является двураскрашиваемым тогда и только тогда, когда в нём нет циклов нечётной длины.

Следствие 4.33. Дерево двураскрашиваемо.

Доказательство. Раз в дереве нет циклов, то нет и циклов нечётной длины. □

Общая задача — задача определения $\chi(G)$ в случае, когда оно заведомо больше двух — является уже гораздо более «сложной»: на такущий момент уровень развития науки человеческой цивилизации не позволяет придумать неперебоpный алгоритм. Казалось бы, и что с того? Задача, с виду, не очень практически важная. На самом деле, важная, это иллюстрирует следующая задача:

Задача 4

Пусть имеется система вида

$$\begin{cases} x_{k_1} \oplus x_{l_1} = 1 \\ \ldots \\ x_{x_n} \oplus x_{l_n} = 1 \end{cases}$$

Как можно проверить, имеет ли она решение?

Решение задачи 4

Построим граф, вершинами в котором будут x_i. Проведём в графе рёбра между всеми парами вершин, которые фигурируют в системе уравнений из условия. Тогда нетрудно проверить, что система имеет решение тогда и только тогда, когда полученный граф двураскрашиваем: достаточно интерпретировать цвета как значения x_i.

Это довольно игрушечная задача, но, оказывается, аналогичные ***сводимости*** можно построить и для исследования решений более сложных уравнений в алгебре логики. Таким образом, умение эффективно раскрашивать граф в три или более цвета, или хотя бы определять, можно ли это сделать, позволяет эффективно решать многие задачи алгебры логики (на самом деле, даже задачи математической логики вообще).

4.8 Эйлеровы маршруты

Путь в графе — это довольно узкое понятие. Путь, например, не может иметь самопересечений, что сильно ограничивает область использования данного термина. В этой связи вводится следующее определение:

Определение 4.34. ***Маршрутом*** длины $n \geqslant 0$ в графе G называется последовательность вершин $v_0, v_1, \ldots, v_n$ такая, что $\forall i \in \{0, \ldots, n-1\}$ $(\{v_i, v_{i+1}\} \in E(G))$.
Число n называется ***длиной маршрута***.
Отметим отдельно, что одна вершина тоже является маршрутом длины 0.

Вершины v_0 и v_n называются ***концами*** маршрута; говорится, что маршрут ***соединяет*** v_0 и v_n. В случае $v_0 = v_n$ маршрут является ***замкнутым***.
Говорят, что ребро $\{x, y\} \in E(G)$ ***лежит*** на маршруте, если $\exists i : \ \{x, y\} = \{v_i, v_{i+1}\}$.

Утверждение 4.35. В графе есть путь между вершинами u и v тогда и только тогда, когда между ними есть и маршрут.

Определение 4.36. Маршрут является ***эйлеровым*** $\overset{\triangle}{\iff}$ каждое ребро графа лежит на маршруте, причём вхождение единственно.

Теорема 4.37. Связный граф G содержит замкнутый эйлеров маршрут тогда итолько тогда, когда степень каждой вершины чётна.

4.9 Многодольные графы и паросочетания

На k-раскрашиваемые графы иногда бывает полезно посмотреть с других позиций: раз ни у какого ребра концы не покрашены в один цвет, все вершины графа можно разбить на ***доли*** согласно их цвету, причём рёбра в графе будут только между вершинами из разных долей. Это разбиение может являться отражением более сложной природы моделируемых объектов (например, если граф отображает связи между работниками и их задачами).

Определение 4.38. Будем называть ***k-дольным графом*** такой граф G, для которого $\exists H_1, \ldots, H_k$: $V(G) = H_1 \sqcup \ldots \sqcup H_k$ и $\forall e \in E(G)\ \forall i \in \{1, \ldots, k\}\ |e \cap H_i| \leqslant 1$. То есть, рёбра проведены только между различными ***долями*** H_i.

Замечание 4.39. Граф k-дольный тогда и только тогда, когда он k-раскрашиваемый.

Определение 4.40. ***Полным*** k-дольным графом называется граф вида

$$K_{|H_1|,\ldots,|H_k|} = \left(H_1 \sqcup \ldots \sqcup H_k,\ \bigcup_{\substack{i,j=1 \\ i \neq j}}^{k} \{\{u, v\} \mid u \in H_i, v \in H_j\} \right)$$

То есть это k-дольный граф, в котором проведены все возможные рёбра между его долями.

Также может возникнуть задача построения разбиения другого вида: разбиения вершин на непересекающиеся пары, или ***паросочетания***.

Определение 4.41. ***Паросочетание (на графе G)*** — это множество рёбер $M \subseteq E(G)$, в котором ни одна пара (рёбер) не имеет общего конца.

Определение 4.42. Вершинами графа G, ***покрытыми*** паросочетанием M, назовём множество $V_M = \{v \in V(G) \mid \exists e \in M : v \in e\}$ (множество вершин, смежных с рёбрами из M).
Паросочетание M назовём ***совершенным*** в случае $V_M = V(G)$ (все вершины покрыты).

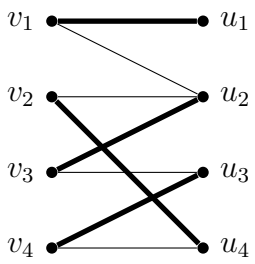


Рис. 4.3: пример совершенного паросочетания на двудольном графе

В случае двудольных графов задача построения паросочетаний и, в частности, совершенных паросочетаний может быть мотивирована желанием построить взаимнооднозначное соответствие для как можно большего числа вершин из разных долей (возвращаясь к примеру с работниками и задачами, построение совершенного паросочетания означает наиболее оптимальное распределение задач по работникам).

В этой связи формулируется теорема, гарантирующая существование совершенного паросочетания в двудольном графе при выполнении определённого условия. Для строгой формулировки этого условия придётся ввести некоторые вспомогательные понятия.

Определение 4.43. ***Множеством соседей (окрестностью) вершины*** v графа G будем называть множество $N(v) = \{u \mid \{u, v\} \in E(G)\}$
Множеством соседей подмножества вершин $U \subseteq V(G)$ графа G будем называть множество $N(U) = \left(\bigcup_{u \in U} N(u)\right) \setminus U$.

Теорема 4.44 (Холла о свадьбах). В двудольном графе с долями L и R существует совершенное паросочетание тогда и только тогда, когда $|L| = |R|$ и для любого подмножества $S \subseteq L$ справедливо $|N(S)| \geqslant |S|$.

Задача 5

Пусть G связный граф, $v_0 \in V(G)$. Пусть $S_0 = \{v_0\}$, $S_{k+1} = N(S_k) \cup S_k$. Задайте множества S_k явно в терминах расстояний в графе.

Решение задачи 5

По индукции докажем, что $S_k = \{u \in V(G) \mid \rho(v_0, u) \leqslant k\}$.
База: $S_0 = \{v_0\} = \{u \mid \rho(v_0, u) \leqslant 0\}$ по определению.
Шаг: Пусть для k утверждение истинно. Рассмотрим $k+1$. Пусть $\rho(v_0, u) \leqslant k$. Тогда $u \in S_k \subseteq S_{k+1}$. Пусть теперь $\rho(v_0, u) = k+1$. Кратчайший путь из v_0 в u содержит вершину u', смежную с u и такую, что $\rho(v_0, u') = k$. Тогда $u' \in S_k$, из чего следует, что $u \in N(S_k) \subseteq S_{k+1}$. Наконец, пусть $\rho(v_0, u) > k+1$. По предположению индукции $u \notin S_k$. Также $u \notin N(S_k)$, иначе был бы путь из v_0 в u длины $k+1$. Значит, $u \notin S_{k+1}$.
По индукции доказано.

Задача 6

Используя задачу 5, постройте алгоритм поиска кратчайших путей из заданной вершины во все остальные в простом неориентированном графе.

5 Ориентированные графы

Ориентированные графы — естественное обобщение неориентированных. Они получаеются простой заменой неупорядоченной пары на упорядоченную в определении ребра:

Определение 5.1. ***Ориентированный граф (возможно, с петлями)*** — это упорядоченная пара (V, E) множества ***вершин*** V и ***рёбер*** $E \subseteq V^2$. В дальнейшем будет подразумеваться, что в ориентированном графе петель нет, то есть $E \cap \{(v, v) \mid v \in V\} = \varnothing$.

Определения, введённые нами для неориентированных графов, с поправками переносятся на ориентированные.

Определение 5.2. ***Исходящей степенью*** $d_+(v)$ вершины v называется число рёбер, началом которых является v, то есть $d_+(v) = |\{(v, u) \mid u \in V\}|$. Симметрично вводится понятие ***входящей степени*** $d_-(v)$ вершины v: $d_-(v) = |\{(u, v) \mid u \in V\}|$.

Для ориентированного графа есть утверждение, аналогичное теореме 4.7 о рукопожатиях:

Утверждение 5.3. $\sum\limits_{v \in V} d_+(v) = \sum\limits_{v \in V} d_-(v) = |E|$

Определим отдельно несколько частных случаев простого неориентированного графа.

Определение 5.4.

1) ***Ориентированный граф-путь*** P_n, $n \geqslant 0$ — граф вида

$$V(P_n) = \{v_1, \ldots, v_n\}, \qquad E(P_n) = \{(v_0, v_1), (v_1, v_2), \ldots, (v_{n-1}, v_n)\}$$

Вершины v_1 и v_n называются ***концами пути***, а $n = |E|$ — ***длиной***. *Ещё раз акцентируем внимание на том, что $n \geqslant 0$, а вершины нумеруются с нуля.*

2) ***Ориентированный граф-цикл*** C_n, $n \geqslant 2$ — граф вида

$$V(G) = \{v_1, \ldots, v_n\}, \qquad E(G) = \{(v_1, v_2), (v_2, v_3), \ldots, (v_{n-1}, v_n), (v_n, v_1)\}$$

Ещё раз акцентируем внимание на том, что в отличие от неориентированного графа-цикла, $n \geqslant 2$.

Без изменений вводится понятие подграфа ориентированного графа, а также индуцированного графа.

Определение 5.5. Ориентированный граф, в котором нет подграфов-циклов, является ***ациклическим***.

Определение 5.6. Вершина u в ориентированном графе G является ***достижимой*** из вершины $v \overset{\triangle}{\iff}$ существует подграф-путь графа G, концами которого являются вершины u и v. Это обозначается как $u \rightsquigarrow v$.

Из свойств, описанных в замечании 4.17, для ориентированного сохраняются только *рефлексивность* и *транзитивность*; симметричности в общем случае нет. Однако понятие достижимости для ориентированного графа можно симметризовать:

Определение 5.7. Вершины u и v являются ***двусторонне достижимыми*** $\overset{\triangle}{\iff}$ $(u \rightsquigarrow v) \wedge (v \rightsquigarrow u)$. Это обозначается как $u \leftrightsquigarrow v$.

Для отношения двусторонней достижимости можно ввести понятие ***компонент сильной связности***, аналогичное 4.18:

Определение 5.8. ***Компонентой сильной связности*** ориентированного графа $G(V, E)$ будем называть подграф G, индуцированный на некотором непустом множестве $U \subseteq V$, удовлетворяющем свойству $\forall u, v \in U\ (u \leftrightsquigarrow v)$ и являющемся максимальным относительно него.

Определение 5.9. ***Маршрутом*** длины $n \geqslant 0$ в ориентированном графе G называется последовательность вершин $v_0, v_1, \ldots, v_n$ такая, что $\forall i \in \{0, \ldots, n-1\}\ \ ((v_i, v_{i+1}) \in E(G))$.
Число n называется ***длиной маршрута***.
Отметим отдельно, что одна вершина тоже является маршрутом длины 0.

Вершины v_0 и v_n называются ***концами*** маршрута; говорится, что маршрут ***соединяет*** v_0 и v_n. В случае $v_0 = v_n$ маршрут является ***замкнутым***.
Говорят, что ребро $(x, y) \in E(G)$ ***лежит*** на маршруте, если $\exists i :\ (x, y) = (v_i, v_{i+1})$.

С учётом введённых определений утверждение 4.35 справедливо и для ориентированного графа. Также можно сформулировать замечание, аналогичное 4.19.

Введём теперь новое определение, которое можно обобщить и на случай неориентированного графа:

Определение 5.10. Два графа $G(V, E)$ и $G'(V', E')$ называются ***изоморфными*** $\overset{\triangle}{\iff}$ существует биекция $f : V \to V'$ такая, что $\forall (u, v) \in E\ [(f(u), f(v)) \in E']$.

6 Функции

Понятие функции уже встречалось нам ранее. Например, оно фигурировало при определении *булевой функции*, а также *раскраски графа*. Неформально, ***функция*** — это некоторое правило, в одностороннем порядке сопостовляющая каждому объекту из одного множества некоторый объект из другого множества. Сопоставляемый объект не обязан быть уникальным, однако не может быть ситуации, когда одному элементу сопоставляются два и более.

Например, если некоторому действительному числу мы сопоставляем его квадрат, то это правило сопоставления — функция. Если же мы попытаемся каждому положительному действительному числу y сопоставить решние уравнения $x^2 = y$, то натолкнёмся на проблему неоднозначности: функции не получается.

6.1 Формальное определение

На лекции вам давалось определение функции через понятие ориентированного двудольного графа. В рамках семинара мы дадим другое, эквивалентное, но более часто используемое определение. Для этого нам потребуется ввести некоторые вспомогательные обозначения.

Определение 6.1. ***Декартовым произведением*** множеств A и B называется множество всех ***упорядоченных пар***, где первый элемент взят из A, а второй — из B:

$$A \times B = \{(a, b) \mid a \in A,\ b \in B\}$$

Напомним, что один из вариантов строгого определения упорядоченной пары давался в разделе 2.1.

Определение легко обобщается и на случай множественного произведения: вместо пар будут использоваться ***кортежи***. Также заметим, что $A \times A$ обозначают как A^2.

Определение 6.2. ***Функцией (частичной функцией)***, принимающей аргументы из множества X и значения во множестве Y, называется подмножество $f \subseteq X \times Y$ такое, что ни у каких двух пар из f первый элемент не совпадает.
Если $x \in X$ и $\exists y \in Y : (x, y) \in f$, то говорят, что функция f ***определена*** в точке x, и $f(x) = y$.

Пример 6.3. Рассмотрим пару примеров функций и не функций.

1. $X = \{0, 1\}$, $Y = \{x, y\}$. Тогда $X \times Y = \{(0, x), (0, y), (1, x), (1, y)\}$.
   $f = \{(0, y), (1, y)\}$ является функцией, в то время как $g = \{(0, x), (0, y), (1, x)\}$ — нет, хотя и $g \subseteq X \times Y$.
2. $X = \mathbb{R}_+$, $Y = \mathbb{R}$.
   $f = \{(x, x^2) \mid x \in X\}$ является функцией, в то время как $g = \{(x, y) \mid x \in X,\ y \in B,\ y^2 = x\}$ — нет, хотя и $g \subseteq X \times Y$.

Понятно, что каждый раз излишне формально определять функцию как множество пар не стоит. Достаточно записать непосредственно правило, по которому одному элементу ставится в соответствие другой: $f : x \mapsto f(x)$. Например, $\exp : x \mapsto e^x$, или просто $\exp(x) = e^x$.

Заметим, что функция не должна быть определена в каждой точке множества аргументов. Например, функцию $f(x) = 1/|x|$ можно рассматривать в контексте $X = Y = \mathbb{R}$,

хотя она и не определена в точке $x = 0$. Эта же самая функция также принимает не все возможные значения из Y. В этой связи полезно ввести следующие определения:

Определение 6.4. ***Областью определения*** функции $f \subseteq X \times Y$ называется множество

$$\mathrm{dom}(f) = \{x \in X \mid \exists y \in Y : f(x) = y\}$$

Областью значений функции $f \subseteq X \times Y$ называется множество

$$\mathrm{range}(f) = \{y \in Y \mid \exists x \in X : f(x) = y\}$$

Определение 6.5. Если $f(x) = y$, то y называется ***образом*** элемента x, а x — ***прообразом*** элемента y

Также нас будет интересовать то, как функция отображает целое множество, а не только один элемент. Для этого вводятся следующие определения:

Определение 6.6. ***Образом*** некоторого подмножества $A \subseteq X$ называется множество

$$f(A) = \{y \in Y \mid \exists x \in X : f(x) = y\}$$

Полным прообразом некоторого подмножества $B \subseteq Y$ называется множество

$$f^{-1}(B) = \{x \in X \mid \exists y \in Y : f(x) = y\}$$

Полным прообразом некоторого элемента $y \in Y$ называется полный прообраз множества $\{y\}$.

Замечание 6.7. $f(X) = f(\mathrm{dom}(f)) = \mathrm{range}(f)$, $f^{-1}(Y) = f^{-1}(\mathrm{range}(f)) = \mathrm{dom}(f)$.

6.2 Отображения

Отдельно рассматривается случай, когда функция определена в любой точке из множества аргументов. В этом случае говорится, что функция является ***отображением***, или ***всюду определённой функцией***.

Определение 6.8. Функция $f \subseteq X \times Y$ называется ***отображением*** в случае $\mathrm{dom}(f) = X$. При этом пишут $f : X \to Y$.

Замечание 6.9. Любая функция становится отображением при сужении множества аргументов до области определения: $f : \mathrm{dom}(f) \to Y$.

Определение 6.10. В случае $f : X \to X$ отображение f называют ***преобразованием***

Среди отображений выделяют следующие три важных вида:

Определение 6.11. Отображение $f : X \to Y$ называется ***инъекцией*** $\overset{\triangle}{\iff} \forall x_1, x_2 \in X \ (x_1 \neq x_2) \to (f(x_1) \neq f(x_2))$. То есть, из неравенства аргументов следует неравенство значений отображения.

Определение 6.12. Отображение $f : X \to Y$ называется ***сюръекцией*** $\overset{\triangle}{\iff} \mathrm{range}(f) = Y$. То есть, у любого элемента из Y существует прообраз.

Определение 6.13. Отображение $f : X \to Y$ называется ***биекцией*** в случае, когда оно и инъекция, и сюръекция.

Замечание 6.14. Биекция является правилом, взаимнооднозначно сопостовляющим каждому элементу из X некоторый элемент из Y и наоборот.

Следствие 6.15. Каждое биективное отображение ***обратимо***, то есть если $f : X \to Y$ — биекция, то

$$g = f^{-1} \triangleq \{(y, x) \in Y \times X \mid (x, y) \in f\}$$

является отображением, причём биекцией.

Пример 6.16.

1. Пусть $f : \mathbb{R}^2 \to \mathbb{R}^3$ — отображение, ставящее в соответствие паре чисел (x_1, x_2) коэффициенты (a, b, c) квадратного уравнения, корнями которого являются (x_1, x_2), причём $a = 1$.

   Это **инъекция**, так как $(a, b, c) = (1, -x_1 - x_2, x_1 x_2)$, и равенство всех значений невозможно при $(x_1', x_2') \neq (x_1'', x_2'')$. С другой стороны, это **не сюръекция**, так как у троек с $a \neq 1$ нет прообразов.

2. Пусть X — множество многочленов степени не выше $m + 1$, а Y — многочленов степени не выше m.

   Рассмотрим операцию взятия производной $\frac{d}{dx} : X \to Y$, то есть $\frac{d}{dx} : p(x) \mapsto p'(x)$.

   Это **сюръекция**, но **не инъекция**: для каждого многочлена из Y есть прообраз в X — его интеграл, но при этом любой константный многочлен отображается в ноль.

3. Пусть $f : [0; 1] \to [0; 1]$ непрерывна и монотонно возрастает. Тогда по теореме об обратной функции это **биекция**.

Задача 1

Пусть $f : X \to X$ — сюръективное преобразование. Верно ли, что f инъективно?

Решение задачи 1

Нет. Приведём контрпример: пусть X — множество всех многочленов, а $f = \frac{d}{dx}$. Аналогично рассуждениям в примере 6.16 получаем, что f — сюръекция, но не инъекция.

Заметим однако, что если X конечно, то утверждение в условии верно. Предлагаю вам самим это проверить.

Задача 2

Приведите пример сюръективного преобразования $f : \mathbb{N} \to \mathbb{N}$ такого, что полный прообраз каждого элемента $\mathbb{N}$ бесконечен.

Решение задачи 2

Выпишем подряд все элементы $\mathbb{N}$. Вычеркнем все числа, стоящие на нечётных позициях. Для оставшихся чисел повторим операцию, и так далее.

Пусть теперь f сопоставляет числу номер шага, на котором его вычеркнули. Это действительно отображение, так как после каждого шага минимум среди невычеркнутых чисел растёт, из чего следует, что любое число будет вычеркнуто на каком-то шаге. Это действительно сюръекция, так как на любом шаге остаётся бесконечное число чисел —

процесс никогда не прекратится. И, наконец, полным прообразом каждого элемента $\mathbb{N}$ будет бесконечное множество, так как на каждом шаге вычёркивается бесконечное множество чисел.

6.3 Функции и мощность множества

Изученные нами понятия также играют важную роль и в теории множеств. Помимо состава множеств и взаимоотношений между ними нас часто будет интересовать то, насколько некоторое множество «велико». Легко определить «размер» множества в случае, когда оно конечно: это просто число элементов. Но что делать, если множество содержит бесконечно много элементов? Хочется сказать, что если два множества бесконечны, то они «равновелики». Однако это противоречит интуитивным представлениям о том, что, например, 2^A содержит элементов больше, чем A.

Оказывается, эти интуитивные представления можно формализовать, если по-другому взглянуть на размер конечных множеств. Если множества A и B конечны, то можно сказать, что они равновелики, если в них одинаковое число элементов. По сути, это эквивалентно тому, что можно задать взаимнооднозначное правило соответствия — *биекцию* — между каждым элементом A и B.

Утверждение 6.17. Если A и B — конечные множества, то они содержат одинаковое число элементов тогда и только тогда, когда существует биекция из одного множества в другое.

Формальное доказательство утверждения становится очевидным, если любым способом пронумеровать элементы множеств.

Данное утверждение позволяет по-иному формально определить размер, или ***мощность*** множества, и обобщить это определение на все множества вообще.

Определение 6.18. Множества A и B называются ***равномощными*** в том и только том случае, если существует биекция между элементами множеств.

Стоит обратить внимание, что требуемая биекция не обязана быть единственной.

Определение 6.19. Множество A называется ***счётным*** $\overset{\triangle}{\iff}$ A равномощно $\mathbb{N}_0$.

Пример 6.20.

1. Множества $\{1, 2\}$ и $\{a, x\}$ равномощны, причём можно построить две биекции между ними:
$$1 \sim a,\ 2 \sim x \qquad \text{или} \qquad 1 \sim x,\ 2 \sim a$$
2. Множества $\mathbb{N}_0$ и $E = \{x \in \mathbb{N}_0 \mid \exists k\,(x = 2k)\}$ равномощны, биекция задаётся, например, правилом $E \ni x = 2 \cdot k$, где k — любой элемент $\mathbb{N}_0$.
3. Множества $\mathbb{Q}$ и $\mathbb{N}_0$ равномощны. Идея доказательства: $\mathbb{Q}$ можно задать бесконечной таблицей, номер строки и столбца в которой — числитель и знаменатель. А все ячейки таблицы можно пронумеровать, идя «змейкой» (при этом сократимые дроби не нумеруются).

Может создасться впечатление, что все бесконечные множества счётны. Однако это неверно.

Теорема 6.21 (Кантора). Для любого A множества A и 2^A неравномощны.

Утверждение 6.22. Множество $\mathbb{R}$ несчётно.

Доказательство данного утверждения обычно приводят в курсе математического анализа.

Задача 3

Счётно ли множество всех корректных программ, написанных на языке C++?

Решение задачи 3

Да, оно счётно. Для доказательства этого заметим, что можно построить следующую таблицу: номер строки равен длине программы в символах, а номер столбца — лексикографическому порядковому номеру программы среди всех программ заданной длины. Обходя таблицу «змейкой», получаем взаимнооднозначную нумерацию всех программ.

На текущий момент мы формально определили лишь случай равенства мощностей двух бесконечных множеств. Можно пойти дальше и определить оставшиеся операции сравнения. Нетрудно проверить, что утверждение 6.17 можно обобщить в виде следующей леммы:

Лемма 6.23. Пусть A и B — конечные множества. Тогда

1. $|A| = |B| \iff$ существует биекция между A и B.
2. $|A| \leqslant |B| \iff$ существует инъекция из A в B.
3. $|A| \geqslant |B| \iff$ существует сюръекция из A в B.

Обобщим эту лемму на случай произвольных множеств, определив соответствующим образом операции сравнения.

Определение 6.24. В случае существования инъекции $f : A \to B$ говорят, что B ***не менее мощно, чем*** A. Это обозначается как $|A| \leqslant |B|$.
При этом по определению полагают $(|A| < |B|) \overset{\triangle}{\iff} (|A| \leqslant |B|) \wedge (|A| \neq |B|)$.

Утверждение 6.25. Множество B не менее мощно, чем множество A, тогда и только тогда, когда существует сюръекция $g : B \to A$.

Доказательство.

$\Rightarrow$ По определению, существует инъекция $f : A \to B$. Заметим тогда, что $g' = \{(y, x) \in B \times A \mid (x, y) \in f\}$ является частичной функцией. Действительно, раз f — инъекция, ни у каких двух (разных) пар из f не совпадают вторые элементы. Значит, ни у каких двух (разных) пар из g' не совпадают первые элементы.

Заметим также, что $g' : \mathrm{dom}(g') \to A$ — сюръекция. Действительно, так как f — отображение, любой элемент A является первым элементом хотя бы какой-то пары из f. Но тогда он же является и вторым элементом некоторой пары из g'.

Тогда построим g как произвольное доопределение g' на B. Таким образом, получена сюръекция $g : B \to A$.

$\Leftarrow$ Аналогично.

□

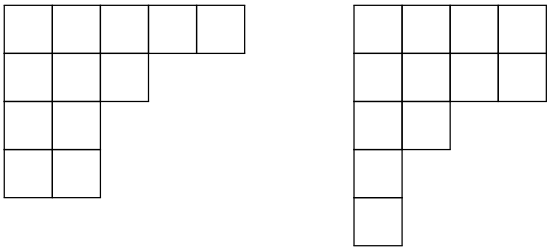
Из данного утверждения следует, что лемма 6.23 обобщается и на случай бесконечных множеств при использовании определения 6.24.

7 Комбинаторика

В предыдущем разделе мы подробно изучили инструментарий для сравнения мощностей множеств. Кажется, что полученные результаты полезны, скорее, при работе с бесконечными множествами, так как в ином случае достаточно сравнивать мощности как обычные числа. Однако это неверно: изученные методы оказываются хорошим подспорьем и в задачах, например, определения точного числа элементов в некотором множестве, или хотя бы в деле построения верхних и нижних оценок на это число. Данными задачами занимается ***комбинаторика***.

Пример 7.1. Чего больше: разбиений числа n на k слагаемых, или разбиений N на слагаемые, не превосходящие k?

Оказывается, в обоих случаях разбиений одно и то же число, ведь между данными множествами можно построить биекцию. Легче всего построить биекцию путём рассмотрения *диаграмм Юнга* для разбиений. Пример таких диаграмм для двух разбиений числа $N = 11$: $N = 5 + 3 + 2 + 2$ и $N = 4 + 4 + 2 + 1 + 1$.



Видно, что одно разбиение получается из другого транспонированием диаграммы. Также видно, что в первом случае имеется разбиение на k слагаемых, а во втором — на слагаемые, не превосходящие k. Детали биекции предлагаю вам додумать самостоятельно.

Таким образом, получаем *важный факт*: если требуется определить число элементов в некотором множестве, можно попробовать сначала доказать, что элементов в нём столько же, сколько и в некотором другом множестве (возможно, с более понятным составом), а потом уже пересчитать элементы второго множества. Данное правило очевидным образом обобщается и на случаи, когда требуется оценить мощность множества сверху или снизу.

7.1 Базовые комбинаторные задачи

Составим джентльменский набор базовых задач комбинаторики, к которым впоследствии можно будет сводить другие задачи посредством построения биекции.

7.1.1 Правило суммы

Начнём с задачи подсчёта числа элементов в множестве вида $A = A_1 \cup A_2 \cup \ldots \cup A_n$. Понятно, что если $\forall i \neq j \;\; A_i \cap A_j = \varnothing$, то $|A| = |A_1| + |A_1| + \ldots + |A_n|$. Для строгого доказательства этого факта нам потребуется следующее утверждение:

Утверждение 7.2. Если A конечно, то $|A| = \sum\limits_{x \in U} \mathbb{I}_A(x)$.

Доказательство. $|A|$ равно числу элементов, которые лежат в A. Но заметим, что каждый такой элемент добавляет единицу в сумму $\sum\limits_{x \in U} \mathbb{I}_A(x)$, причём никакие другие элементы на сумму не влияют, так как $\mathbb{I}_A$ принимает на них значение 0. □

Следствие 7.3. Если $A = A_1 \sqcup A_2 \sqcup \ldots \sqcup A_n$, то $|A| = |A_1| + |A_2| + \ldots + |A_n|$.

Доказательство. Раз $\forall i \neq j \;\; A_i \cap A_j = \varnothing$, то $\mathbb{I}_A(x) = \mathbb{I}_{A_1}(x) + \mathbb{I}_{A_2}(x) + \ldots + \mathbb{I}_{A_n}(x)$. Отсюда по утверждению 7.2 получаем требуемое. □

Но что делать, если множества пересекаются? Для случая двух множеств можно заметить, что $\mathbb{I}_{A\cup B}(x) = \mathbb{I}_A(x) + \mathbb{I}_B(x) - \mathbb{I}_{A\cap B}(x)$. Но тогда по утверждению 7.2 имеем $|A \cup B| = |A| + |B| - |A \cap B|$. Данная формула называется ***формулой включений-исключений***. Она обобщается и на случай с n множествами.

Лемма 7.4. Если $A = \bigcup\limits_{i=1}^{n} A_i$, то

$$|A| = \sum_{k=1}^{n} (-1)^{k+1} \left(\sum_{S \in \mathcal{C}_k} \left| \bigcap_{A \in S} A \right| \right), \qquad \mathcal{C}_k = \binom{\{A_1, A_2, \ldots, A_n\}}{k}$$

Доказательство. Можно доказать как по индукции, так и просто аккуратно записав $\mathbb{I}_A(x)$ через обычные математические операции и воспользовавшись утверждением 7.2. □

Задача 1

В группе 40 туристов. Из них 20 человек говорят по-английски, 15 — по-французски, 11 — по-испански. Английский и французский знают семь человек, английский и испанский — пятеро, французский и испанский — трое. Два туриста говорят на всех трёх языках. Сколько человек группы не знают ни одного из этих языков?

Решение задачи 1

По формуле включений-исключений имеем

$$N = 40 - (20 + 15 + 11 - 7 - 5 - 3 + 2) = 40 - 33 = 7$$

7.1.2 Правило произведения

Рассмотрим задачу подсчёта числа возможных путей из вершины так называемого ***дерева последовательного выбора*** в любой его лист.

Определение 7.5. ***Деревом последовательного выбора*** называется дерево, у которого можно выделить вершину (***корень***) так, чтобы все остальные вершины, расположенные на одном и том же расстоянии от выделенной, имели одинаковую степень.

Пример дерева последовательного выбора можно видеть на рис. 7.1.2. На каждой вершине отмечена её степень за вычетом родительского ребра. Слева от каждого уровня дерева выписано число путей с началом из корня и с концом на данном уровне.

Утверждение 7.6. Расстояние от корня дерева последовательного выбора до любого из листьев одинаково.

Определение 7.7. Расстояние от корня дерева последовательного выбора до любого из листьев называется ***высотой дерева*** (или ***числом выборов***) и обозначается h.
Степень каждой вершины (на расстоянии $m-1$ от корня) за вычетом родительского ребра

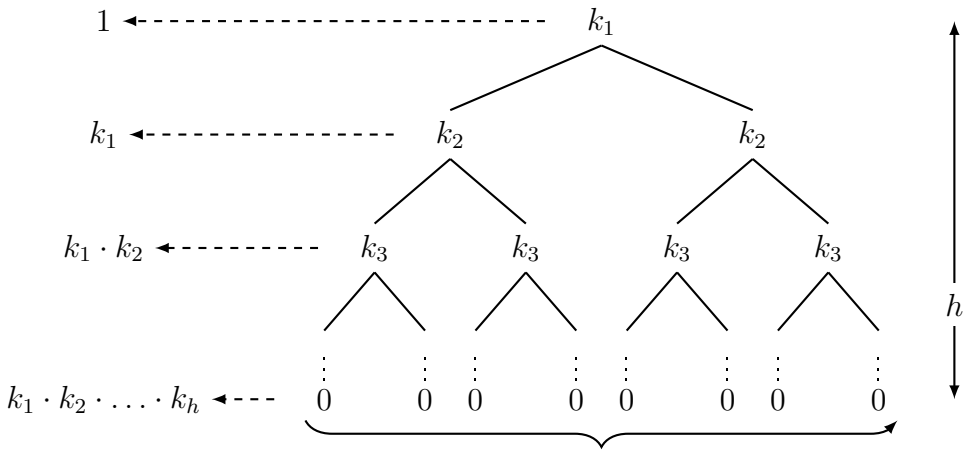


Рис. 7.1: дерево последовательного выбора (схематично)

называется ***мощностью выбора (на шаге m)*** и обозначается k_m.
Путь из корня в лист называется ***решающим путём***.

Утверждение 7.8. Пусть дерево последовательного выбора характеризуется высотой h и мощностями выборов $k_1, k_2, \ldots, k_h$. Тогда число путей из корня в любой лист равно $k_1 \cdot k_2 \cdot \ldots \cdot k_h$.

Доказательство. По индукции, проведите сами. □

Задача 2

На одном этаже семёрки живёт 100 человек. Среди них требуется выбрать двух ответственных за южную и северную кухни, одного ответственного за умывальники и санузел, а также его заместителя. Сколькими способами это можно сделать?

Решение задачи 2

Можно построить биекцию из множества способов выбрать ответственных в множество путей от корня к листьям в дереве последовательного выбора высоты $h = 4$ и с мощностями выборов $k_1 = 100$, $k_2 = 100 - 1$, $k_3 = 100 - 2$ и $k_4 = 100 - 3$. Действительно, движение от корня к листьям пусть будет соответствовать последовательному выбору ответственных. Тогда переход по первому ребру соответствует выбору ответственного за южную кухную из 100 студентов, переход по второму — выбору ответственного за северную кухню из оставшихся 99 студентов и так далее. Тогда всего способов — $100 \cdot 99 \cdot 98 \cdot 97$.

Мы рассмотрели очень частный случай, когда мощность очередного выбора на единицу меньше мощности предыдущего. Это не всегда так, и ниже будет рассмотрены две задачи другого типа. Однако и такой специальный случай встречается настолько часто, что для обозначения соответствующего ответа ввели специальное число:

$$A_n^k = n \cdot (n-1) \cdot \ldots \cdot (n-k) = \frac{n!}{(n-k)!}$$

Это число называется ***числом расстановок***. Связь названия и класса задач довольно очевидна: действительно, в задаче 2 мы «расставили» $n = 100$ студентов по $k = 4$ должностям.

Задача 3

Сколькими способами можно выбрать два числа разной чётности из множеств $\{1, \ldots, 4\}$ и $\{11, \ldots, 16\}$?

Решение задачи 3

На первом шаге можно четырьмя способами выбрать число из первого диапазона, на втором шаге мы будем выбирать из $6/2 = 3$ элементов (так как чётность фиксирована). В итоге имеем $4 \cdot 3 = 12$ способов.

Задача 4

Сколькими способами можно выбрать два числа из диапазона $\{1, \ldots, 9\}$, дающие разный остаток при делении на три?

По аналогии с прошлой задачей в голову сразу приходит ответ $9 \cdot (9 \cdot 2/3) = 54$. Однако если честно пересчитать все варианты, получится число в два раза меньшее. В чём же проблема?

Дело в том, что в предыдущей задаче на каждом шаге числа выбирались из разных множеств, что позволяло однозначно сопоставить каждому решающему пути число из первого множества и число из второго. В случае текущей задачи уже двум решающим путям будет соответствовать одна и та же пара чисел, просто выбранная в разном порядке (например, $\{1, 3\}$ и $\{3, 1\}$). Понятно, что учёт возможной перемены местами выбранных чисел как раз и уменьшает ответ в два раза, но как это отражается в построении биекции?

Если оставаться в рамках модели деревьев последовательного выбора, то данная проблема обычно решается введением дополнительных ограничений, позволяющих зафиксировать порядок получения результатов выбора. Например, в случае нашей задачи можно потребовать, чтобы второй выбор совершался не среди двух оставшихся классов, а только среди того класса, что соответствует следующему остатку по модулю три. То есть, например, если мы выбрали число с остатком 0, то второе число обязано иметь остаток 1, если выбрали число с остатком 1, то второе — с остатком 2 и так далее. То, что построена биекция между множеством из задачи и решающими путями в дереве с мощностями выборов 9 и 3, проверьте сами.

7.1.3 Подсчёт подмножеств

Из возникшей проблемы понятно, что одним правилом произведения сыт не будешь. Далеко не всегда ясно, какое ограничение надо ввести, чтобы получить биекцию. Пойдём дальше и рассмотрим другую базовую задачу, к которой уже будет легко свести проблемное упражнение из предыдущего пункта.

Пусть A — конечное множество мощности $|A| = n$. Тогда чему равно

$$\left| \binom{A}{k} \right|,$$

где $k \in \{1, \ldots, n\}$? Ответ уже давался в замечании 4.3, настало время его строго обосновать.

Доказательство замечания 4.3. Задача подсчёта числа расстановок n объектов по k позициям уже решена: их A_n^k. Осталось понять, чем это отличается от числа подмножеств мощности k.

Заметим, что каждой последовательности элементов A длины k соответствует подмножество A мощности k. Но каждому подмножеству A мощности k соответствует $A_k^k = k!$

последовательностей элементов этого множества. Но тогда имеем, что мощность множества подмножеств A мощности k равна

$$\frac{A_n^k}{k!} = \frac{n!}{k!(n-k)!} \triangleq \binom{n}{k} \triangleq C_n^k \tag{7.1}$$

Полученное число называется ***числом сочетаний***. □

Решение задачи 4

Выберем два разных класса из трёх классов чисел по остатку по модулю три. Из каждого класса затем можно тремя способами выбрать по экземпляру. В итоге имеем $C_3^2 \cdot 3 \cdot 3 = 27$ вариантов.

7.2 Комбинированные задачи

Разберём некоторые другие примеры, которые разбиваются на несколько базовых комбинаторных задач.

Задача 5

Сколькими способами можно выбрать два подмножества A и B множества $\{1, \ldots, 10\}$ так, чтобы $|A| = 2$, $|B| = 5$ и $A \subseteq B$?

Решение задачи 5

Выберем C_{10}^2 способами множество A. Далее выберем C_8^3 способами множество $B \setminus A$. В итоге, $N = C_{10}^2 \cdot C_8^3$.

Задача 6

Сколькими способами можно разбить $\{1, \ldots, 10\}$ на два непустых подмножества, а затем упорядочить элементы в одном из блоков любым образом?

Решение задачи 6

Если размер любого блока фиксирован и равен k, то число способов — $N_k = C_{10}^k \cdot (k! + (10-k)!) = A_{10}^k + A_{10}^{10-k}$. Осталось просуммировать по всем возможным значениям размера меньшего блока: $k \in \{1, \ldots, 5\}$.

$$N = \sum_{k=1}^{5} N_k = \sum_{k=1}^{5} A_{10}^k + A_{10}^{10-k}$$

Задача 7

В русском алфавите 33 буквы, 10 из них — гласные. Сколько всего можно составить слов длины 10, в которых есть три различные гласные, а согласные идут в строго возрастающем алфавитном порядке?

Решение задачи 7

Для начала C_{10}^3 способами выберем три различные гласные для нашего слова. Далее C_{23}^7 способами выберем согласные (так как в слове они должны идти в строго возрастающем алфавитном порядке, они все должны быть различные). Выбранные буквы расставим 10!

способами. Но порядок согласных фиксирован, а потому на каждое подходящее слово приходится еще $7! - 1$ неподходящих. Тогда ответ —

$$N = \frac{C_{10}^3 \cdot C_{23}^7 \cdot 10!}{7!} = C_{10}^3 \cdot C_{23}^7 \cdot A_{10}^3$$

Задача 8

В группе студентов есть один, который знает C++, Java, Python, Haskell. Каждые три из этих языков знают два студента. Каждые два — 6 студентов. Каждый из этих языков знают по 15 студентов. Каково наименьшее количество студентов в такой группе?

Решение задачи 8

Наименьшее число достигается тогда и только тогда, когда нет студентов, не знающих ни один из языков. Тогда по формуле включений-исключений имеем

$$N = C_4^1 \cdot 15 - C_4^2 \cdot 6 + C_4^3 \cdot 2 - C_4^4 \cdot 1 = 4 \cdot 15 - 6 \cdot 6 + 4 \cdot 2 - 1 \cdot 1 = 31$$

7.3 Биномиальные коэффициенты

Число сочетаний также называется ***биномиальным коэффициентом***. Это вызвано его появлением в следующей задаче:

Задача 9

Найдите коэффициент при $a^k b^{n-k}$ после раскрытия скобок в выражении $(a+b)^n$.

Решение задачи 9

Перепишем выражение в виде длинного произведения:

$$(a+b)^n = \underbrace{(a+b) \cdot (a+b) \cdot \ldots \cdot (a+b)}_{n \text{ раз}}$$

Любое слагаемое вида $a^k b^{n-k}$ после раскрытия получается только при выборе из некоторых k скобок числа a, а из оставшихся $n-k$ скобок — числа b. То есть таких слагаемых будет ровно столько, сколькими способами можно выбрать из n указанных скобок некоторые k, то есть C_n^k. Таким образом,

Утверждение 7.9.

$$(a+b)^n = \sum_{k=0}^{n} C_n^k \cdot a^k b^{n-k} \qquad \textbf{\textit{(Бином Ньютона)}}$$

Из связи числа сочетаний с биномом Ньютона очевидным образом следует, что $C_n^k = C_n^{n-k}$, хотя это было понятно и из формулы (7.1).

Замечание 7.10. $\sum\limits_{k=0}^{n} C_n^k = 2^n; \quad \sum\limits_{k=0}^{n} (-1)^k C_n^k = 0$

Доказательство. $2^n = (1+1)^n = \sum\limits_{k=0}^{n} C_n^k \cdot 1^k 1^{n-k}; \quad 0 = (-1+1)^n = \sum\limits_{k=0}^{n} C_n^k \cdot (-1)^k 1^{n-k}.$ $\square$

Есть и много других подобных замечанию 7.10 фактов касательно суммы биномиальных коэффициентов. Разберём задачу на эту тему:

Задача 10

Докажите справедливость формул (желательно найти комбинаторное доказательство):

1. $\sum\limits_{j=0}^{k} \binom{r}{j}\binom{s}{k-j} = \binom{r+s}{k}$; 2. $\sum\limits_{j=0}^{n} \binom{j}{k} = \binom{n+1}{k+1}$; 3. $\sum\limits_{j=0}^{k} \binom{n+j}{j} = \binom{n+k+1}{k}$;

Решение задачи 10

Под комбинаторным доказательством понимается доказательство, использующее построение биекции между некоторыми двумя множествами, мощность первого из которых равна левой части, а второго — правой. Такие доказательства обычно красивее и понятнее доказательств сугубо подсчётных (например, использующих формулу (7.1)).

1. $\sum\limits_{j=0}^{k} \binom{r}{j}\binom{s}{k-j} = \binom{r+s}{k}$.

   В правой части записано число способов выбрать из $(r+s)$-элементного множества подмножество размера k. Заметим, что и в левой части записано то же число.

   Действительно, разобьём условно исходное множество на два подмножества размера r и s. Пусть после выбора подмножества размера k в первом подмножестве оказалось j элементов (во втором тогда $k-j$). Всего имеем $C_r^j \cdot C_s^{k-j}$ способов получить подмножество, удовлетворяющее указанному свойству. Просуммировав по всем возможным j (от 0 до k), покроем все возможные исходы, причём без повторений. Что и требовалось доказать.

2. $\sum\limits_{j=0}^{n} \binom{j}{k} = \binom{n+1}{k+1}$.

   В правой части записано число способов выбрать из $(n+1)$-элементного множества подмножество размера $k-1$. Заметим, что и в левой части записано то же число.

   Действительно, упорядочим произвольным образом исходное множество. Пусть после выбора подмножества размера $k+1$ оказалось, что наибольший из индексов его элементов равен $j+1$. Всего имеем C_k^j способов получить подмножество, удовлетворяющее указанному свойству: оставшиеся k элементов выбираются среди первых j исходного множества. Просуммировав по всем возможным j (от 0 до n), покроем все возможные исходы, причём без повторений. Что и требовалось доказать.

3. $\sum\limits_{j=0}^{k} \binom{n+j}{j} = \binom{n+k+1}{k}$.

   Задача похожа на предыдущую. Воспользовавшись симметричностью биномиальных коэффициентов, получаем

   $$\sum_{j=0}^{k} \binom{n+j}{n} = \binom{n+k+1}{n+1}$$

   В правой части записано число способов выбрать из $(n+k+1)$-элементного множества подмножество размера $n+1$. Заметим, что и в левой части записано то же число.

Действительно, аналогично предыдущей задаче, упорядочим произвольным образом исходное множество. Пусть после выбора подмножества размера $n+1$ оказалось, что наибольший из индексов его элементов равен $n+j+1$. Всего имеем C_{n+j}^{j} способов получить подмножество, удовлетворяющее указанному свойству. Просуммировав по всем возможным j (от 0 до k), покроем все возможные исходы, причём без повторений. Что и требовалось доказать.

Задача 11

Сколькими способами среди n солдат можно выбрать командира и набрать ему в подчинение отряд произвольного размера?

Решение задачи 11

С одной стороны, можно n способами выбрать командира и каждого оставшегося солдата либо взять в отряд, либо нет. По правилу произведения имеем следующее число вариантов: $n \cdot 2^{n-1}$. С другой стороны, можно для всех возможных k сначала C_n^k способами выбрать отряд размера k, а затем в нём k способами выбрать командира.

В итоге имеем два тождественно равных ответа:

$$n \cdot 2^{n-1} = \sum_{k=1}^{n} k \cdot C_n^k$$

У полученного в предыдущей задаче тождества есть еще одно красивое доказательство, которое мы получим ближе к концу курса. А пока докажем полезное рекуррентное соотношение на биномиальные коэффициенты, которое полезно при построении *треугольником Паскаля*.

Утверждение 7.11. $C_n^k = C_{n-1}^k + C_{n-1}^{k-1}$.

Доказательство. Рассмотрим задачу выбора подмножества мощности k из множества мощности n. Зафиксируем в исходном множестве некоторый элемент. Тогда при выборе k-элементного подмножества мы можем либо включить данный элемент, либо не включить. В первом случае имеем C_{n-1}^{k-1} вариантов выбора, а во втором — C_{n-1}^k. □

Рассмотрим еще одну классическую задачу, в которой возникают биномиальные коэффициенты.

Задача 12

Найдите число решений уравнения $x_1 + x_2 + \ldots + x_k = n$ в неотрицательных целых числах.

Решение задачи 12

Решим задачу *методом точек и перегородок*. Заметим, что число решений равно числу способов разделить n неразличимых точек $(k-1)$-ой неразличимой перегородкой. Действительно, будем интерпретировать число точек в каждой секции как значение соответствующей переменной x_i. Таким образом, имеем биекцию.

Число способов так разделить n точек можно найти следующим образом: «свалим» в общую кучу точки и перегородки, перемешаем их $(n+k-1)!$ способами, а затем разделим на $n!$ и $(k-1)!$, учтя тем самым неразличимость точек и перегородок между собой. Итоговый ответ:

$$N_{\text{решений}} = \binom{n+k-1}{k-1} \qquad \textbf{\textit{(формула Муавра)}}$$

7.4 Мультиномиальные коэффициенты

Утверждение 7.9 сформулировано только для случая возведения в n-ую степень суммы *двух* слагаемых. Получим общую формулу:

Утверждение 7.12.

$$(x_1 + x_2 + \ldots + x_m)^n = \sum_{k_1+k_2+\ldots+k_m=n} \binom{n}{k_1,\ k_2,\ \ldots, k_m} x_1^{k_1} x_2^{k_2} \ldots x_m^{k_m},$$

где

$$\binom{n}{k_1,\ k_2,\ \ldots, k_m} = \binom{n}{k_1} \cdot \binom{n-k_1}{k_2} \cdot \ldots \cdot \binom{n-k_1-\ldots-k_m}{k_m} = \frac{n!}{k_1! k_2! \ldots k_m!}$$

— ***мультиномиальный коэффициент***.

Доказательство. Аналогично доказательству утверждения 7.9: для получения монома вида $x_1^{k_1} x_2^{k_2} \ldots x_m^{k_m}$ при раскрытии скобок мы $C_n^{k_1}$ способами выбираем скобки, из которых берём x_1, $C_{n-k_1}^{k_2}$ способами — скобки, из которых берём x_2, и так далее. □

Задача 13

Сколько различных слов (не обязательно осмысленных) можно получить, переставляя буквы в словах

а) «КОМПЬЮТЕР»; **б)** «ЛИНИЯ»; **в)** «ПАРАБОЛА»;

г) «ОБОРОНОСПОСОБНОСТЬ»?

Решение задачи 13

а) Всё девять букв различны, поэтому достаточно переставить их произвольным образом: $N = 9!$.

б) Среди пяти букв повторяется только «И», причём два раза. Сначала 5! способами расставим буквы из предположения, что они все различимы, а затем разделим на 2!, учтя тем самым, что две буквы неразличимы, а потому их перестановка ничего не изменит: $N = 5!/2!$.

в) Среди восьми букв повторяется только «А», причём три раза. Аналогично, $N = 8!/3!$.

г) Среди восемнадцати букв «О» повторяется семь раз, буква «С» — три, «Б» и «Н» — два, остальные буквы встречаются по одному разу. Тогда $N = \dfrac{18!}{7!3!2!2!}$.

Замечание 7.13. Пусть имеется m букв в количествах k_1, k_2, …, k_m соответственно ($k_1 + k_2 + \ldots + k_m = n$). Тогда число различных (не обязательно осмысленных) слов, которые можно из данных букв составить — $\binom{n}{k_1,\ k_2,\ \ldots,\ k_m}$.

8 Бинарные отношения

В данном разделе мы поговорим о некоторого рода обобщении понятия «функция» — о ***бинарном отношении***. Напомним, что согласно определению 6.2 функция f — это подмножество некоторого декартового произведения $X \times Y$, обладающее свойством ***функциональности***:

$$[(x, y) \in f \wedge (x, y') \in f] \to (y = y')$$

Иначе говоря, любому элементу из X ставится в соответствее не более одного элемента из Y. Однако это довольно сильное ограничение. Из-за него, например, функциями невозможно описать отношения между некоторыми студентами и их увлечениями; действительно, любой студент вполне может иметь несколько интересных ему занятий. В этой связи в математике отдельно рассматриваются и подмножества $X \times Y$, не обязательно обладающие свойством функциональности — ***бинарные отношения***.

Определение 8.1. ***Бинарным отношением*** между двумя множествами A и B называется любое множество $R \subseteq A \times B$. Если $A = B$, то $R \subseteq A^2$ и говорят, что бинарное отношение задано на множестве A.
Принадлежность $(a, b) \in R$ кратко записывают как aRb.

Замечание 8.2. Заметим, что определение 8.1 обобщается и на случай произвольного (пусть n) числа множителей в декартовом произведении. В таком случае говорят об ***отношении арности*** n. В нашем курсе мы подробно изучать их не будем.

Помимо свойства функциональности бинарное отношение может обладать целым набором других интересных свойств. Перечислим наиболее важные из них:

Определение 8.3. Пусть $R \subseteq A \times B$. Отношение R называется

1. ***функциональным*** в случае $\forall a \in A \ \ \forall b, b' \in B \ \ [aRb \wedge aRb'] \to (b = b')$.
2. ***(левым) тотальным*** в случае $\forall a \in A \ \ \exists b \in B : \ aRb$.
3. ***инъективным*** в случае $\forall a, a' \in A \ \ \forall b \in B \ \ [aRb \wedge a'Rb] \to (a = a')$.
4. ***сюръективным*** в случае $\forall b \in B \ \ \exists a \in A : \ aRb$.

Используя 8.3, легко дать определение, например, инъекции, как функционального тотального инъективного бинарного отношения.

Еще большим числом особых свойств могут обладать бинарные отношения, заданные на некотором множестве.

Определение 8.4. Пусть $R \subseteq A^2$. Отношение R называется

1. ***рефлексивным*** в случае $\forall a \in A \ \ aRa$.
2. ***антирефлексивным*** в случае $\forall a \in A \ \ \neg(aRa)$.
3. ***симметричным*** в случае $\forall a, b \in A \ \ \ (aRb \to bRa)$.
4. ***антисимметричным*** в случае $\forall a, b \in A \ \ \ [aRb \wedge bRa \to (a = b)]$.
5. ***асимметричным*** в случае $\forall a, b \in A \ \ \ [aRb \to \neg(bRa)]$.
6. ***транзитивным*** в случае $\forall a, b, c \in A \ \ \ [aRb \wedge bRc \to aRc]$.

Замечание 8.5. Любое рефлексивное (как и антирефлексивное) бинарное отношение по определению является тотальным и сюръективным.

Множество уже известных вам математических объектов и операций по сути являются бинарными отношениями. Например, операции сравнения: $\{(a,b) \mid a\,(*)\,b\} \subseteq \mathbb{R}^2$, где вместо $(*)$ можно подставить $<, \leqslant, =, \neq, \geqslant, >$. Когда рассматривают операции сравнения в терминах бинарных отношений, их обычно заключают в круглые скобки. Например, $(<) = \{(a,b) \mid a < b\} \subseteq \mathbb{R}^2$.

Задача 1

Какие из указанных в 8.3 и 8.4 свойств выполнены для следующих бинарных отношений: $(<), (\leqslant), (=), (\neq), (\geqslant), (>)$? Считайте, что $\mathbb{R}$ — множество, на котором заданы отношения.

Решение задачи 1

Нетрудно заметить, что все отношения тотальные и сюръективные. Также все отношения, кроме $(\neq)$, транзитивные. Отношение $(=)$ при этом также функциональное, инъективное, рефлексивное и симметричное. Отношение $(\neq)$ антирефлексивное и симметричное. Отношения $(\leqslant)$ и $(\geqslant)$ рефлексивные и антисимметричные. Наконец, отношения $(<)$ и $(>)$ антирефлексивные и асимметричные.

Так как бинарные отношения являются множествами, к ним применимы теоретико-множественные операции: отношения можно объединять, пересекать, вычитать, брать дополнение к ним и так далее. Однако этим операции над бинарными отношениями не ограничиваются.

Определение 8.6. ***Обратным отношением*** к бинарному отношению $R \subseteq A \times B$ называется отношение $R^{-1} = \{(b,a) \mid aRb\} \subseteq B \times A$.

Определение 8.7. ***Композицией*** двух бинарных отношений $R \subseteq A \times B$ и $Q \subseteq B \times C$ называется бинарное отношение $(Q \circ P) = \{(a,c) \mid \exists b \in B :\ aRb \wedge bRc\}$.
Акцентируем особое внимание на порядок записи отношений в композиции. Он повторяет порядок записи функций в композиции.

Задача 2

Найдите результат операций над отношениями, определенными на множестве действительных чисел.

а) $(>)^c$; **б)** $(>)^{-1}$; **в)** $(\geqslant) \triangle (\leqslant)$; **г)** $(>) \cap (<)$; **д)** $(=) \circ (>)$; **е)** $(<) \circ (<)$; **ж)** $(<) \circ (>)$.

Решение задачи 2

а) $(\leqslant)$; **б)** $(<)$; **в)** $(\neq)$; **г)** $\varnothing$; **д)** $(>)$; **е)** $(<)$; **ж)** $\mathbb{R}^2$;

8.1 Отношения эквивалентности

Отношения подобия треугольников или параллельности прямых также являются бинарными отношениями. Можно заметить, что оба этих отношения (если считать прямую параллельной самой себе) вместе с отношением $(=)$ и многими другими являются рефлексивными, симметричными и транзитивными. Такие отношения выделяют в отдельную группу.

Определение 8.8. Рефлексивное, симметричное и транзитивное бинарное отношение называют ***отношением эквивалентности***.

Теорема 8.9. Пусть на конечном множестве A задано отношение эквивалентности R. Тогда $A = B_1 \sqcup B_2 \sqcup \ldots \sqcup B_k$, причём $\forall i\ B_i \neq \varnothing$ и $\forall a \in B_i\ \forall b \in B_j\ [aRb \leftrightarrow (i = j)]$. То есть, два элемента образуют пару, лежащую в отношении, тогда и только тогда, когда они взяты из одного блока разбиения.

Замечание 8.10. Теорема 8.9 справедлива и для бесконечных A. Тогда число блоков не обязательно конечно или даже счётно.

Определение 8.11. Блоки B_i из 8.9 называются ***классами эквивалентности***, а про A говорят, что оно разбито на классы эквивалентности.

Из теоремы 8.9 следует, что для любого элемента A однозначно определён класс эквивалентности, в котором данный элемент лежит. В связи с этим получаем эквивалентное определение класса эквивалентности:

Определение 8.12. Пусть $R \subseteq A^2$ — отношение эквивалентности, $a \in A$. Тогда ***классом эквивалентности*** отношения R, построенным по представителю a называется множество $[a]_R = \{b \in A \mid aRb\}$.

Следствие 8.13. Любые два класса эквивалентности либо совпадают, либо не пересекаются: $\forall a, b \in A\ \ ([a]_R = [b]_R) \oplus ([a]_R \cap [b]_R = \varnothing)$.

Задача 3

Рассмотрим множество S фундаментальных последовательностей, состоящих из рациональных чисел. Введём следующее бинарное отношение $(\sim) \subseteq S^2$:

$$\{x_i\}_{i=1}^{\infty} \sim \{y_j\}_{j=1}^{\infty} \quad \Longleftrightarrow \quad \forall \varepsilon > 0\ \ \exists N \in \mathbb{N} : \forall n, m > N\ \ |x_n - y_m| < \varepsilon$$

Является ли $(\sim)$ отношением эквивалентности?

Решение задачи 3

Симметричность очевидным образом следует из симметричности формулы в условии. Рефлексивность эквивалентна фундаментальности любой последовательности из S (совпадение с определением буквальное), что дано по условию. Осталось проверить транзитивность. Для этого достаточно взять $\varepsilon' = \varepsilon/2$ и воспользоваться неравенством треугольника:

$$\left.\begin{array}{l} \forall n, k > N_1(\varepsilon')\ \ |x_n - y_k| < \varepsilon' \\ \forall k, m > N_2(\varepsilon')\ \ |y_k - z_m| < \varepsilon' \end{array}\right\} \quad \Longrightarrow \quad \forall n, m, k > \max\{N_1, N_2\}\ \ |x_n - z_m| =$$

$$= |x_n - y_k + y_k - z_m| < |x_n - y_k| + |y_k - z_m| < 2\varepsilon' = \varepsilon$$

Отсюда имеем транзитивность.

Интересно, что для классов эквивалентности рассматриваемого отношения можно ввести стандартные математические операции (например, $[\{x_i\}_{i=1}^{\infty}]_{(\sim)} + [\{y_i\}_{i=1}^{\infty}]_{(\sim)} = [\{x_i + y_i\}_{i=1}^{\infty}]_{(\sim)}$; проверьте непротиворечивость такого определения). Более того, после этого классы приобретают свойства *действительных чисел*. Можно в некотором смысле сказать, что это и есть все действительные числа (см. *изоморфизм*).

8.2 Отношения частичного порядка

В прошлом разделе мы упомянули один из важнейших классов бинарных отношений, представители которого по свойствам близки к отношению равенства. Логично предположить, что и у других изученных бинарных отношениях на числах есть аналогичные «братья». Действительно, можно, например, заметить, что у отношений $(\leqslant)$ и $(\subseteq)$[4] много общих свойств: оба отношения *рефлексивные*, *антисимметричные* и *транзитивные*. Также, например, $(<)$ и $(\subsetneq)$ *антирефлексивные*, *антисимметричные* и *транзитивные*. Такие отношения также выделяют в отдельную группу.

Определение 8.14. Транзитивное, антисимметричное и либо рефлексивное, либо антирефлексивное бинарное отношение называют ***отношением (частичного) порядка***. В случае рефлексивности говорят, что отношение порядка ***нестрогое***, иначе — ***строгое***.

Замечание 8.15. Из любого отношения нестрогого порядка можно получить строгое, вычтя из него отношение $(=)$ как множество. Аналогично можно совершить и обратное преобразование. Таким образом, между множеством строгих и нестрогих порядков определена биекция.

Определение 8.16. Пусть R — отношение частичного порядка. Будем обозначать $(<_R)$ и $(\leqslant_R)$ строгую и нестрогую версию R соответственно, полученные согласно биекции из 8.15. *Во избежание путанницы заметим, что хотя бы с одной из этих версий R совпадает по определению.*

Определение 8.17. Отношения порядка, в которых любые два элемента сравнимы (то есть $\forall a \forall b \in A\ [aRb \vee bRa]$), называются ***линейными***.
Заметим, что линейными могут быть только отношения нестрогого порядка.

В некоторых задачах исследование отношения порядка может быть неудобным из-за большого числа, в некотором смысле, неинфоматичных пар. Например, отношение $(<)$ на $\mathbb{Z}$ однозначно задаётся парами вида $(n, n+1)$ и знанием о его транзитивности и линейности; необязательно рассматривать все пары, для того чтобы полностью восстановить всё отношение. В связи с этим вводится следующее понятие:

Определение 8.18. Пусть $R \subseteq A^2$ — отношение частичного порядка. Отношением ***непосредственного следования***, построенным по R, является бинарное отношение

$$(\prec_R) = \{(x, y) \mid (x <_R y) \wedge \neg\,(\exists z \in A : (x <_R z) \wedge (z <_R y))\}$$

Название отношения полностью соответствует его определению. Рассмотрим несколько примеров:

Пример 8.19.

1. Рассмотрим $(<) \subseteq \mathbb{Z}^2$. Тогда $\prec_{(<)} = \{(n, n+1) \mid n \in \mathbb{Z}\}$.
2. Рассмотрим $(<) \subseteq \mathbb{R}^2$. Из плотности действительных чисел самих в себе следует, что $\prec_{(<)} = \varnothing$. Это действительно согласуется с интуицией: ни для какого действительного числа нельзя назвать другое, следующее непосредственно за ним.
3. Рассмотрим $(\subsetneq) \in \mathcal{S}^2$, где $\mathcal{S}$ — некоторое семейство множеств. Тогда

$$\prec_{(\subsetneq)} = \{(x, y) \mid (x \subseteq y) \wedge (|y \setminus x| = 1)\}$$

[4] не будем пока формально определять, на чём они заданы

Видно, что полученное отношение не обязательно инъективно: у множества может быть несколько непосредственно следующих после него множеств.

Определение 8.20. Пусть $R \subseteq A^2$ — отношение частичного порядка. Ориентированный граф $G(A, \prec_R)$ называется ***диаграммой Хассе***.

Определение 8.21. Диаграмма Хассе, построенная для частичного порядка $(\subseteq) \subseteq 2^A \times 2^A$, где $|A| = n < \infty$, называется ***ориентированным булевым кубом***. Его неориентированная версия называется просто ***булевым кубом*** и обозначается B_n.

Замечание 8.22. Вершины булева куба обычно обозначают двоичными словами длины n, являющимися векторами значений индикаторных функций соответствующих подмножеств (i-ый бит отвечает за наличие i-ого элемента A в соответствующем подмножестве).

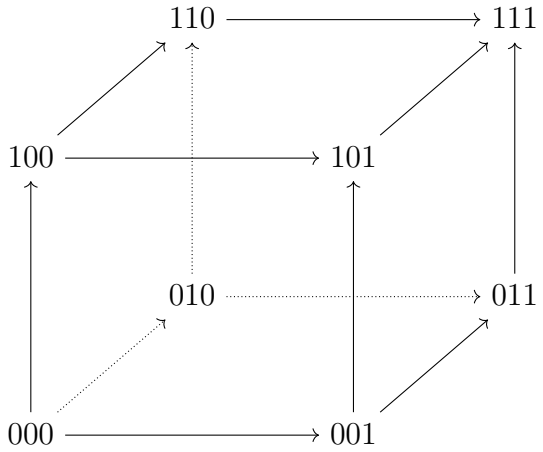


Рис. 8.1: пример ориентированного булева куба для $n = 3$.

На практике часто встречаются задачи, в которых надо ввести частичный порядок на некотором декартовом произведении. При этом на множителях обычно некоторый порядок уже введён. В этих случаях удобна следующая конструкция:

Определение 8.23. Пусть $P \subseteq A^2$, $Q \subseteq B^2$ — отношения порядка. Их ***произведением*** называется бинарное отношение $P \subseteq (A \times B)^2$:

$$(x, y)\, P\, (x', y') \iff \begin{cases} xRx' \\ yQy' \end{cases}$$

Вводится следующее обозначение: $P = A \times B$, хотя формально с точки зрения множеств оно означает другое.

Заметим, что произведение отношения порядков не всегда является отношеним порядка. Для этого требуется, чтобы множители были либо одновременно нестрогими порядками, либо строгими.

Замечание 8.24. Ориентированный булев куб также является диаграммой Хассе для отношения порядка $(\leqslant \times \leqslant \times \ldots \times \leqslant) \subseteq \{0,1\}^n \times \{0,1\}^n$ — ***отношения покоординатного порядка***, введённого на двоичных словах длины n. Обратим внимание, что **это каноническое определение булева куба в нашем курсе**.

Данное замечание хорошо иллюстрируется следующей задачей:

Задача 4

Граф $G_n = (V, E)$ имеет множество вершин $V = 2^{\{1,2,\ldots,n\}}$ (вершина $v \in V$ — подмножество множества $\{1, 2, 3, \ldots, n\}$); вершины v и u соединены ребром тогда и только тогда, когда $|u \triangle v| = 1$.

а) Докажите, что граф G_n изоморфен булеву кубу B_n.

б) Сколько существует различных наборов (попарно различных) подмножеств $A_1, A_2, A_3 \subseteq \{1, 2, \ldots, n\}$, для которых выполняется условие $|A_1 \triangle A_2| = |A_2 \triangle A_3| = 1$?

Решение задачи 4

а) Изоморфизм, по сути, уже построен в замечании 8.24: действиетльно, любому подмножеству $A \subseteq V$ взаимнооднозначно сопоставляется двоичное слово длины $|V|$ (вектор значений индикаторной функции), причём $A_1 \subseteq A_2$ тогда и только тогда, когда вектор, соответствующий A_1, сравним по отношению покоординатного порядка с вектором, соответвтующим A_2, и покоординатно не больше его. Убирая ориентацию рёбер, мы не нарушаем изоморфизм. Что и требовалось доказать.

б) В силу предыдущего пункта задача эквивалентна поиску путей длины два в булевом кубе. Так как всего вершин 2^n, а степень каждой вершины в B_n равна n, таких путей — $\frac{1}{2} \cdot 2^n \cdot A_n^2$ (делим на два так как посчитали каждый путь дважды). То есть, ответ — $N = n(n-1)2^{n-1}$.

Введём, наконец, некоторый дополнительный глоссарий, связанный с отношениями порядка.

Определение 8.25. Рассмотрим отношение частичного порядка $R \subseteq A^2$. Элемент $x \in A$ является

1. ***максимальным*** в случае $\neg\,[\exists a \in A : (x <_R a)]$.
2. ***наибольшим*** в случае $\forall a \in A\ (a \leqslant_R x)$.

Аналогично определяются ***минимальный*** и ***наименьший*** элементы.

Замечание 8.26. Наибольший/наименьший элемент обязательно является максимальным/минимальным.

Доказательство. Действительно, предположим противное: есть наибольший, но не максимальный по отношению порядка $R \subseteq A^2$ элемент x. Тогда, отрицая максимальность, имеем $\exists a \in A : (x <_R a)$. Но в силу антисимметричности R тогда не может быть, чтобы $a \leqslant_R x$. Противоречие с максимальностью. Аналогично для наименьшего элемента. □

Задача 5

Постройте отношение частичного порядка, в ктором деревья (и только они) на некотором наборе вершин V будут минимальными элементами. Существуют ли для этого отношения наименьшие элементы?

Решение задачи 5

Рассмотрим $A = \left\{G(V,E) \mid \left(E \subseteq \binom{V}{2}\right) \wedge (G \text{ связный})\right\}$. Отношение введём следующим образом: $R = \{(G, G') \mid E(G) \subseteq E(G')\}$. Нетрудно заметить, что это отношение нестрогого частичного порядка, так как таковым является $(\subseteq)$.

В терминах введённого отношения определение минимального элемента эквивалентно определению дерева: связный граф, удаление любого ребра из которого нарушает связность, что эквивалентно связному графу, для которого не существует связного подграфа на тех же вершинах.

Наименьшего элемента в общем случае нет: если $|V| > 2$, то может быть построено несколько деревьев. Так как это все минимальные элементы, среди них согласно 8.26 и надо искать наименьший элемент. Но понятно, что любые два разных дерева не сравнимы. Значит, наименьшего элемента нет.

В предыдущей задаче мы ввели отношение порядка, которое, вообще говоря, может быть задано на всех графах с вершинами V, а не только на связных. Здесь логично ввести следующее определение:

Определение 8.27. Пусть бинарное отношение R задано на множестве A. Пусть $B \subseteq A$. Тогда $R \cap B^2$ является бинарным отношением, заданным на множестве B, и называется ***сужением*** R на B.

В связи с этим определением аналогично 8.25 вводятся понятия максимального, минимального, наибольшего и наименьшего элемента в подмножестве.