Содержание

1 Определения и формулировки

1.1 Дерево. Мост. Лес

Дерево — такой связный граф, что выбрасывание любого его ребра даёт несвязный граф

Мост — это такое ребро в графе, что его удаление увеличивает количество компонент связности

Лес — произвольные графы, у которых каждое ребро является мостом

1.2 Цикл. Простой цикл. Простой путь

Цикл — путь, у которого начало совпадает с концом (замкнутый путь)

Простой цикл — цикл, в котором все вершины различны, кроме начала и конца

Простой путь — путь, в котором все вершины различны

1.3 Критерий того, что граф является лесом, в терминах простых путей и простых циклов. Аналогичный критерий для дерева

Равносильные свойства **простых** неориентированных графов:

(1) каждое ребро — мост

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

(3) нет простых циклов длины больше 2

Равносильные свойства **связных простых** неориентированных графов:

(1) граф — дерево

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

(3) нет простых циклов длины больше 2

1.4 Цикломатическое число графа. Критерий того, что граф является лесом, в терминах цикломатического числа. Критерий того, что граф является деревом, в терминах рёбер и вершин

Цикломатическое число графа — величина $r(G) = m - n + c$, где m - количество рёбер, n - количество вершин графа, c - количество компонент связности

Критерий—1. Графы, у которых $r(G) = 0$, — это в точности леса, то есть графы, у которых каждое ребро — мост

Критерий—2. Связный граф является деревом тогда и только тогда, когда число рёбер в нём на единицу меньше числа вершин

1.5 Свойства цикломатического числа графа

Свойства:

1. Граф $G' = G + e$ получается добавлением к графу G ребра $e = \{x, y\}$ к множеству рёбер, а вершины у него те же

Тогда $r(G') = r(G)$, если концы ребра x, y лежат в разных компонентах связности графа G, и $r(G') = r(G) + 1$, если x, y лежат в одной компоненте связности графа G

2. Цикломатическое число графа неотрицательное

1.6 Изолированные вершины, висячие вершины. Теорема про висячие вершины в дереве

Вершины степени 0 называются **изолированными**, а вершины степени 1 — **висячими**

Теорема. В дереве с хотя бы двумя вершинами найдутся по крайней мере две висячие вершины

1.7 Подграф. Индуцированный подграф. Остовный подграф. Теорема об остовном дереве

Подграф — некоторое подмножество вершин и некоторое подмножество рёбер с концами в выбранных вершинах

Индуцированный подграф — подграф, в котором выбраны все рёбра с концами в выбранных вершинах

Остовный подграф — подграф, в котором множество вершин совпадает с множеством вершин самого графа

Теорема. В любом связном графе есть остовное дерево

1.8 Теорема Кэли

Количество остовных деревьев в полном графе на n занумерованных вершинах равно n^{n-2} при $n \geqslant 2$

1.9 Корневые деревья. Слои. Листья. Монотонные деревья. Теорема о существовании монотонного остовного дерева

Корневое дерево — дерево, в котором выбрана вершина — корень

Вершины располагаются по слоям. Слой 0 — корень. Вершины слоя $i+1$ — вершины, не лежащие в слоях $0, 1, \ldots, i$ и имеющие соседа в слое i

Листья — висячие вершины корневого дерева, отличные от корня

Монотонное дерево — корневое остовное дерево в графе G, т.ч. для любого ребра $\{u, v\} \in G$ одна вершина лежит выше другой

Теорема. В каждом связном графе существует монотонное остовное дерево

1.10 Клика. Независимое множество. Кликовое число. Число независимости

Клика — множество вершин графа, каждая пара которых соединена ребром

Независимое множество — подмножество множества вершин графа, т.ч. ни одна пара вершин не связана ребром

Кликовое число — наибольший размер клики в графе G, обозначение — $\omega(G)$

Число независимости — наибольший размер независимого множества, обозначение — $\alpha(G)$

1.11 Теорема Рамсея. Числа Рамсея

Теорема. Для любых k, n найдется такое число N_0, что в любом графе на $N \geqslant N_0$ вершинах есть клика размера k или независимое множество размера n

Числа Рамсея — минимальное N_0, для которого справедлива теорема при заданных k, n, обозначение — $R(k, n)$

1.12 Верхняя оценка на числа Рамсея. Явные выражения для $R(2, n)$ и $R(3, 3)$

Верхняя оценка — $R(k, n) \leqslant \binom{k+n-2}{k-1}$

$R(2, n) = \binom{n}{1} = n$

$R(3, 3) = \binom{4}{2} = 6$

1.13 Уточнение верхней оценки на числа Рамсея

Если оба числа $R(k-1,n), R(k,n-1)$ четные, то $R(k,n) \leqslant R(k-1,n) + R(k,n-1) - 1$

1.14 Нижняя оценка на числа Рамсея

$R(k,k) > \lfloor 2^{(k-1)/2} \rfloor \ \forall k \geqslant 3$

Другими словами, $\forall k \geqslant 3$ существует граф $G = (V,E)$ на $n = \lfloor 2^{(k-1)/2} \rfloor$ вершинах, в котором нет ни клики размера k, ни независимого множества размера k

1.15 Правильная раскраска вершин графа. k-раскрашиваемый граф. Хроматическое число графа

Правильная раскраска графа $G(V,E)$ в k цветов — тотальная функция $c : V \to \{1,2,\ldots,k\}$, если $\{x,y\} \in E$, то $c(x) \neq c(y)$, т.е. присвоенные смежным вершинам числа различны

k-раскрашиваемый граф — граф, для которого существует хотя бы одна раскраска в k цветов

Хроматическое число графа — минимальное количество цветов, в которые можно правильно раскрасить граф, обозначение — $\chi(G)$

1.16 Критерий 1-раскрашиваемости графа. Критерий 2-раскрашиваемости графа

Критерий—1. Все **графы без ребер** 1-раскрашиваемые, т.к. если вершинам графа без рёбер присвоить число 1, то условие правильной раскраски выполняется. И наоборот: если в графе есть ребро $\{u,v\}$, то в правильной раскраске вершинам u, v присвоены разные цвета, поэтому количество цветов хотя бы 2

Критерий—2. 2-раскрашиваемые графы это в точности графы, в которых **длины всех циклов чётные**

1.17 Двудольный граф. Двудольный граф как бинарное отношение

Двудольный граф — неориентированный граф, в котором вершины заранее разделены на две доли — левую и правую, и все рёбра соединяют вершины из разных долей (нет рёбер, соединяющих вершины одной доли)

Двудольные графы с долями L, R по сути то же самое, что бинарные отношения на множествах L, R (то есть то же самое, что подмножества декартова произведения $L \times R$)

1.18 Паросочетание. Паросочетание в графе. Размер паросочетания. Совершенное паросочетание

Паросочетание — граф, у которого степени всех вершин равны 1

Паросочетние в графе — рёберный подграф этого графа: множество вершин и часть рёбер между ними, которые образуют паросочетание

Размер паросочетния — количество ребер в подграфе

Совершенное паросочетание — это паросочетание в таком графе, в котором каждая вершина графа является концом одного из рёбер паросочетания

1.19 Теорема Холла

Теорема Холла. $G = (L,R,E)$ — двудольный граф. Тогда в графе G есть паросочетаание размера $|L|$ тогда и только тогда, когда для каждого множества $S \subseteq L$ множество соседей $G(S) \subseteq R$ содержит не меньше вершин, чем S

1.20 Регулярный граф. Следствия из теоремы Холла для регулярных двудольных графов

Регулярный граф — граф, в котором степени всех вершин одинаковы

Следствие—1. В регулярном двудольном графе, степени вершин которого ненулевые, существует совершенное паросочетание

Следствие—2. Если степень каждой вершины в двудольном графе равна $d > 0$, то его рёбра можно разбить на d непересекающихся совершенных паросочетаний

1.21 Вершинное покрытие. Связь минимального размера вершинного покрытия с числом независимости

Вершинное покрытие — множество вершин S, т.ч. для любого ребра графа хотя бы один из концов лежит в S

Минимальный размер вершинного покрытия в графе G обозначается через $\tau(G)$

$\tau(G) = n - \alpha(G)$, где n — количество вершин в графе, $\alpha(G)$ — число независимости

1.22 Связь минимального размера вершинного покрытия с максимальным размером паросочетания. Теорема Кёнига

Максимальный размер паросочетания в графе G обозначается как $\mu(G)$

Верно следующее: $\tau(G) \geqslant \mu(G)$

Теорема. В любом двудольном графе G выполняется равенство $\tau(G) = \mu(G)$

1.23 Ориентированный граф. Петли. Матрица смежности. Связь с бинарными отношениями

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

Петля — упорядоченная пара (w, w). У петли начало и конец совпадают

Матрица смежности орграфа — квадратная матрица порядка n, где n — количество вершин графа. На пересечении i-й строки и j-го столбца стоит 1, если в орграфе есть ребро (i, j), иначе — стоит 0

Связь с бинарными отношениями. Возьмем множество V и бинарное отношение на этом множестве. Это подмножество декартова произведения $E \subseteq V \times V$. Это то же самое, что орграф с множеством вершин V и множеством ребер E

1.24 Исходящая и входящая степени вершин. Лемма про сумму исходящих и входящих степеней вершин

Исходящая степень — число ребер, выходящих из вершины

Входящая степень — число ребер, входящих в вершину

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

1.25 Путь по орграфу. Цикл, простой путь, простой цикл. Простой в рёбрах путь

Путь по орграфу — это последовательность вершин $v_1, v_2, v_3, \ldots, v_k$, в которой стоящие рядом члены (вершины v_i и v_{i+1} при всех допустимых i) соединены ребром, причём v_i — начало ребра, а v_{i+1} — его конец

Цикл — это путь, у которого первая и последняя вершины совпадают

Простой путь — путь, в котором все вершины различны

Простой цикл — цикл, в котором различны все вершины, кроме первой и последней вершин

Простой в ребрах путь — путь, в последовательности ребер которого все ребра различны

1.26 Отношение достижимости в орграфе, его свойства. Отношение сильной связанности в орграфе, его свойства. Компоненты сильной связности, сильно связный орграф

R — отношение достижимости в орграфе, тогда $(u, v) \in R$, если существует путь с началом в u и концом в v

Свойства любого простого ориентированного графа и любых его вершин v_1, v_2, v_3:

1. *рефлексивность:* $(v, v) \in R$ - вершина достижима из самой себя

2. *транзитивность:* если $(v_1, v_2) \in R$ и $(v_2, v_3) \in R$, то $(v_1, v_3) \in R$

Вершина u **сильно связана** с вершиной v, если v достижима из u и наоборот, т.е. если есть путь из u в v, а также путь из v в u

Формально: $(u, v) \in C$, если $(u, v) \in R$ и $(v, u) \in R$

Для любого ориентированного графа отношение сильной связанности *рефлексивно*, *симметрично* и *транзитивно*, то есть является отношением эквивалентности

Компоненты сильной связности — классы эквивалентности отношения сильной связанности

Сильно связный орграф — орграф, в котором всё множество вершин образует компоненту сильной связности

1.27 Эйлеров цикл. Эйлеров граф. Критерий эйлеровости ориентированного и неориентированного графа

Эйлеров цикл — цикл, который проходит по всем рёбрам графа ровно по одному разу (любое ребро соединяет соседние вершины в цикле, и никакое ребро не встречается в цикле дважды)

Эйлеров граф — граф, в котором есть эйлеров цикл

Критерий для орграфа. Орграф без изолированных вершин содержит эйлеров цикл тогда и только тогда, когда граф сильно связен и у любой вершины входящая степень равна исходящей

Критерий для неориентированного графа. Неориентированный граф без вершин нулевой степени содержит эйлеров цикл тогда и только тогда, когда он связен и степени всех вершин чётны

1.28 Ациклический граф. Равносильные определения ациклического графа

Ациклический граф — граф, в котором нет циклов длины больше 0 (в том числе, нет петель)

Равносильные свойства ориентированного графа без петель:

1. Каждая компонента сильной связности состоит из одной вершины

2. Орграф ациклический

3. Вершины орграфа можно пронумеровать натуральными числами таким образом, чтобы все рёбра вели из вершины с меньшим номером в вершину с бóльшим

1.29 Турнир. Степенная последовательность. Транзитивный турнир. Степенная последовательность транзитивного турнира

Турнир — ориентированный граф, в котором нет петель (u, u) и для любой пары различных вершин либо (u, v) — ребро, либо (v, u) — ребро

Степенная последовательность — последовательность результатов, $\boldsymbol{d} = (d_1, d_2, \ldots, d_n)$, где

d_i не убывают и содержат исходящие степени всех вершин турнира

Транзитивный турнир — турнир на множестве $[n]$: рёбра имеют вид (i, j), где $i < j$, соответствующее этому турниру бинарное отношение транзитивно

Пример степенной последовательности транзитивного турнира — $(0, 1, \ldots, n-1)$

1.30 Теорема Ландау о турнирах

Неубывающая последовательность $\boldsymbol{d} = (d_1, d_2, \ldots, d_n)$ натуральных чисел является степенной последовательностью какого-то турнира, тогда и только тогда, когда

$$\boxed{D_k(\boldsymbol{d}) = \sum_{i=1}^{k} d_i \geqslant \binom{k}{2} \ \forall 1 \leqslant k \leqslant n, \quad D_n(\boldsymbol{d}) = \binom{n}{2}}$$

1.31 Строгий частичный порядок. Строгий линейный порядок

Строгий частичный порядок — бинарное отношение R на множестве X, для которого выполнены свойства:

- $\forall a, b, c \in X$: если aRb и bRc, то aRc (транзитивность)
- $\forall a \in X: \ aRa$ всегда ложно (антирефлексивность)

Строгий линейный порядок — бинарное отношение R на множестве X, где R — строгий частичный порядок и для любых $a \neq b$ истинно одно из двух: aRb или bRa

1.32 Асимметричное отношение. Нестрогий частичный порядок: определение через строгий частичный порядок и через аксиомы

Асимметричное отношение — отношение R на множестве X, т.ч. $(x, y) \in R$ влечет $(y, x) \notin R$

Определение нестрого частичного порядка ***через строгий частичный порядок***

По порядку $<$ на множестве X определим отношение $x \leqslant y$ так: $x \leqslant y \iff x < y$ или $x = y$. Т.е. к упорядоченным парам $x < y$ добавляем диагональные пары (x, x)

Определение нестрого частичного порядка ***через аксиомы***

- aRa (рефлексивность)
- aRb и bRa влечет $a = b$ (антисимметричность)
- aRb и bRc влечет aRc (транзитивность)

1.33 Отношение достижимости в ациклическом графе. Соседние элементы в порядке. Наличие рёбер между соседними элементами в ациклическом графе, задающем порядок

Отношение достижимости в ациклическом графе. Для любого ациклического графа $G = (V, E)$ отношение $\leqslant_G$ является отношением *нестрогого частичного порядка*

Соседние элементы в порядке — такие элементы x, y частично упорядоченного множества $(X, <)$, что $x < y, \ \nexists z : x < z < y$

Наличие рёбер. Пусть $\leqslant$ — частичный порядок на множестве P, G — ацкилический граф со множеством вершин P, также $\leqslant = \leqslant_G$ и x, y — соседние элементы в порядке $\leqslant$. Тогда (x, y) — ребро графа G

1.34 Диаграмма Хассе. Задание конечного порядка диаграммой Хассе

Диаграмма Хассе — ориентированный граф $H_< = (P, E)$, построенный по частичному порядку $<$ на множестве P с множеством ребер

$$E = \{(u, v) : u \text{ непосредственно предшествует } v\}$$

Задание конечного порядка диаграммой. Если $<$ — частичный порядок на конечном множестве, то отношение $<$ совпадает с отношением $<_{H_<}$

1.35 Покоординатное произведение порядков. Лексикографическое произведение порядков. Лексикографический порядок на словах

Покоординатное произведение порядков. Пусть P, Q — два частичных порядка. Тогда покоординатный порядок на декартовом произведении $P \times Q$ задаётся правилом:

$$(p_1, q_1) \leqslant (p_2, q_2) \text{ по определению означает } p_1 \leqslant_P p_2 \text{ и } q_1 \leqslant_Q q_2$$

Лексикографическое произведение порядков. Пусть P, Q — два частичных порядка. Лексикографический порядок $P \times_{\text{lex}} Q$ задается правилом:

$$(p_1, q_1) \prec (p_2, q_2) \text{ по опрделению означает, что } (p_1 <_P p_2) \text{ или } (p_1 = p_2) \text{ и } (q_1 <_Q q_2)$$

Лексикографический порядок является отношением частичного порядка. Если P и Q — линейные порядки, то $P \times_{\text{lex}} Q$ также линейный

Лексикографический порядок на словах. A — линейно упорядоченное множество, например двоичные цифры с порядком $0 < 1$. На множестве слов в алфавите A определим порядок так: если слово x является началом слова y, тогда $x \leqslant y$. Если ни одно из слов x, y не является началом другого, тогда находим самую левую позицию, в которой эти слова различаются. Тогда меньше то слово, в котором на этой позиции меньший символ алфавита

1.36 Изоморфизм порядков. Сумма порядков

Изоморфизм порядков. Порядки P, Q называются *изоморфными* (обозначение $P \cong Q$), если существует такая биекция $\varphi : P \to Q$, что $x < y \iff \varphi(x) < \varphi(y)$ для всех пар x, y. Такая биекция сохраняет порядок

Сумма порядков. Пусть P, Q — два частичных порядка, $P' \cong P,\ Q' \cong Q,\ P' \cap Q' = \varnothing$

Сумма $P + Q$ — это порядок на $P' \cup Q'$, в котором все элементы из P' меньше всех элементов из Q', а пары элементов из P' или Q' сравниваются в порядках P' и Q' соответственно

1.37 Наименьший, наибольший, минимальный, максимальный элемент. Отрезок. Предельный элемент

Элемент a порядка P называется

- *наименьшим*, если $a \leqslant x\ \forall x \in P$
- *наибольшим*, если $a \geqslant x\ \forall x \in P$
- *минимальным*, если $\nexists x \in P$, т.ч. $x < a$
- *максимальным*, если $\nexists x \in P$, т.ч. $x > a$

Отрезок $[x, y]$ — множество вида $\{z : x \leqslant z \leqslant y\}$, $[x, y] \neq \varnothing$ только если $x \leqslant y$

Предельный элемент — элемент $a \in P$ порядка P, у которого нет непосредственного предшественника

1.38 Сохранение свойств порядка при изоморфизме. Изоморфность линейных порядков на конечных множествах одинакового размера

Сохранение свойств порядка при изоморфизме

Если $\varphi : P \to Q$ — изоморфизм порядков, то

а) наименьший (наибольший) переходит в наименьший (наибольший)

б) минимальный (максимальный) переходит в минимальный (максимальный)

в) каждый отрезок $[x, y] = \{z : x \leqslant z \leqslant y\}$ переходит в отрезок $[\varphi(x), \varphi(y)]$ той же мощности

г) предельный (непредельный) элемент переходит в предельный (непредельный)

Изоморфность линейных порядков на конечных множествах одинакового размера

Пусть $(X, \leqslant)$ и $(Y, \leqslant)$ — два линейных порядка на конечных множествах и $|X| = |Y|$, тогда *эти порядки изоморфны*

1.39 Цепь. Антицепь. Теорема про цепи/антицепи в бесконечном порядке

Цепь — это такое подмножество частично упорядоченного множества, которое образует линейный порядок

Антицепь — это такое подмножество, в котором элементы попарно несравнимы

Теорема. В каждом бесконечном порядке есть бесконечная цепь или бесконечная антицепь

1.40 Теорема Дилуорса

Формулировка. Наибольший размер антицепи в конечном порядке равен наименьшему количеству цепей в разбиениях порядка на непересекающиеся цепи

1.41 Вероятностное пространство. Возможные исходы. Вероятностное распределение. Вероятность исхода. Событие. Вероятность события

Вероятностное пространство — конечное множество U

Возможные исходы — элементы вероятностсного пространства

Вероятностное распределние — это такая функция $\mathbf{Pr}$: $U \to [0, 1]$, которая удовлетворяет соотношению $\sum\limits_{x \in U} \mathbf{Pr}[x] = 1$

Вероятность исхода $x \in U$ — это число $\mathbf{Pr}[x]$

Событие — произвольное подмножество $A \subseteq U$

Вероятность события A — это число $\mathbf{Pr}[A] = \sum\limits_{x \in A} \mathbf{Pr}[x]$

1.42 Вероятность события в модели с равновозможными исходами. Примеры

Вероятность события A в модели с равновозможными исходами равна $\mathbf{Pr}[A] = \dfrac{|A|}{|U|}$

Пример—1. «Подбрасывание монеты». Вероятностное пространство: числа 0 и 1. Все исходы равновозможны, вероятность каждого из них равна $\dfrac{1}{2}$

Пример—2. «Подбрасывание 6 монет». Вероятностное пространство: двоичные последовательности длины 6. Все исходы равновозможны, вероятность каждого из них равна $\dfrac{1}{2^6}$

Пример *события*, то есть множества в этом пространстве: ровно три элемента последовательности равны 1. Общее количество двоичных последовательностей длины 6 равно 2^6. Количество последовательностей, в которых ровно три единицы равно $\binom{6}{3}$

Поэтому вероятность события равна

$$\frac{\binom{6}{3}}{2^6} = \frac{5}{16}$$

Пример—3. «Подбрасывание n монет». Вероятностное пространство: двоичные слова длины n. Все слова равновозможны. Найдем вероятность события «на i-й позиции в слове стоит 1»

Всего исходов 2^n. Интересующее нас событие содержит 2^{n-1} исходов: каждый такой исход задаётся выбором 0 или 1 для всех позиций, кроме i-й. Вероятность события равна $\frac{2^{n-1}}{2^n} = \frac{1}{2}$, как и вероятность события «на i-й позиции в слове стоит 0»

1.43 Дополнительные события. Несовместные события. Лемма про попарно несовместные события. Оценка объединения

Дополнительное событие $\bar{A}$ — это разность $U \setminus A$. Из определения распределения вероятностей — $\mathbf{Pr}[A]+\mathbf{Pr}[\bar{A}] = 1$, т.к.

$$1 = \sum_{x \in U} \mathbf{Pr}[x] = \sum_{x \in A} \mathbf{Pr}[x] + \sum_{x \notin A} \mathbf{Pr}[x] = \mathbf{Pr}[A] + \mathbf{Pr}[\bar{A}]$$

Несовместные события — события A и B, которые не могут произойти одновременно, т.е. $\mathbf{Pr}[A \cap B] = 0$

Лемма. Если события A_i попарно несовемстны, то

$$\mathbf{Pr}\left[\bigcup_{i=1}^{n} A_i\right] = \sum_{i=1}^{n} \mathbf{Pr}[A_i]$$

Оценка объединения. Для любых событий $A_1, \ldots, A_n \subseteq U$ выполняется

$$\mathbf{Pr}\left[\bigcup_{i=1}^{n} A_i\right] \leqslant \sum_{i=1}^{n} \mathbf{Pr}[A_i]$$

1.44 Формула включений и исключений для вероятностей

Для всякой вероятностной модели и для произвольных множеств $A_1, \ldots, A_n \subseteq U$ верно

$$\mathbf{Pr}\left[A_1 \cup A_2 \cup \cdots \cup A_n\right] = \sum_i \mathbf{Pr}\left[A_i\right] - \sum_{i<j} \mathbf{Pr}\left[A_i \cap A_j\right] + \cdots =$$

$$= \sum_{\varnothing \neq S \subset \{1,2,\ldots,n\}} (-1)^{|S|+1} \mathbf{Pr}\left[\bigcap_{i \in S} A_i\right]$$

1.45 Условная вероятность события A при условии B. Независимые события

Условная вероятность события A при условии B — число $\boxed{\mathbf{Pr}[A|B] = \dfrac{\mathbf{Pr}[A \cap B]}{\mathbf{Pr}[B]}}$

Независимые события A и B, если $\boxed{\mathbf{Pr}[A] = \mathbf{Pr}[A|B]}$

Эквивалентное определение независимости событий: $\boxed{\mathbf{Pr}[A \cap B] = \mathbf{Pr}[B] \cdot \mathbf{Pr}[A|B] = \mathbf{Pr}[B] \cdot \mathbf{Pr}[A]}$

1.46 Формула полной вероятности. Формула Байеса

Формула полной вероятности. Пусть $B_1, \ldots, B_n$ - разбиение вероятностного пространства U, то есть $U = B_1 \cup \ldots \cup B_n$, где $B_i \cap B_j = \varnothing$ при $i \neq j$. Пусть также $\mathbf{Pr}\left[B_i\right] > 0$ для всякого i. Тогда для всякого события A

$$\boxed{\mathbf{Pr}[A] = \sum_{i=1}^{n} \mathbf{Pr}\left[A|B_i\right] \cdot \mathbf{Pr}\left[B_i\right]}$$

Формула Байеса. Если вероятности событий A и B положительны, то

$$\boxed{\mathbf{Pr}[A|B] = \mathbf{Pr}[A] \cdot \frac{\mathbf{Pr}[B|A]}{\mathbf{Pr}[B]}}$$

1.47 Парадокс Симпсона

Существует такое вероятностное пространство и события A, B, C, D, E, что $\mathbf{Pr}[A|B] < \mathbf{Pr}[A|D]$; $\mathbf{Pr}[A|C] < \mathbf{Pr}[A|E]$; $\mathbf{Pr}[A|B \cup C] > \mathbf{Pr}[A|D \cup E]$

1.48 Случайная величина. Математическое ожидание. Линейность математического ожидания

Случайная величина — это всюду определнная числовая функция на вероятностном пространстве, т.е. функция $f : U \to \mathbb{R}$

Математическое ожидание случайной величины — число $\boxed{\mathbf{E}[f] = \sum_{x \in U} f(x)\mathbf{Pr}[x]}$

Линейность математического ожидания. Пусть $f : U \to \mathbb{R}$ и $g : U \to \mathbb{R}$ — две случайные величины на одном и том же вероятностном пространстве с одним и тем же вероятностным распредеелнием, тогда

$$\mathbf{E}[f + g] = \mathbf{E}[f] + \mathbf{E}[g]$$

1.49 Оценка среднего. Разрез графа, размер разреза. Теорема о существовании в графе большого разреза

Оценка среднего. Пусть $\mathbf{E}[f] = C$ для какой-то случайной величины $f : U \to \mathbb{R}$. Тогда существует такой исход $u \in U$, что $f(u) \geqslant C$. Аналогично, существует и такой исход $u \in U$, что $f(u) \leqslant C$

Разрез графа — разбиение множества его вершин на два неперсекающихся подмножества: $V = V_1 \cup V_2,\ V_1 \cap V_2 = \varnothing$

Размер разреза графа — число ребер, попадающих в разрез

Теорема. Всякий граф $G = (V, E)$ имеет разрез размера не меньше $|E|/2$

1.50 Неравенство Маркова

Пусть f — случайная величина, принимающая только неотрицательные значения, тогда $\forall \alpha > 0$ верно

$$\boxed{\mathbf{Pr}[f \geqslant \alpha] \leqslant \frac{\mathbf{E}[f]}{\alpha}}$$

1.51 Дисперсия. Лемма о выражении дисперсии. Неравенство Чебышёва

Дисперсия — мера разброса значений случайной величины относительно её математического ожидания. Проще говоря, насколько сильно отличается случайная величина от ее мат. ожидания. Обозначение — $\mathbf{D}[f]$

$$\boxed{\mathbf{D}\left[f\right] = \mathbf{E}\left[(f - \mathbf{E}[f])^2\right]}$$

Лемма о выражении дисперсии. $\mathbf{D}\left[f\right] = \mathbf{E}\left[f^2\right] - \mathbf{E}\left[f\right]^2$

Неравенство Чебышёва. $\mathbf{Pr}\left[|f - \mathbf{E}[f]| \geqslant \alpha\right] \leqslant \dfrac{\mathbf{D}[f]}{\alpha^2}$

1.52 Независимые случайные величины. Лемма о математическом ожидании произведения независимых случайных величин

Величины f, g **независимы**, если для любых x, y события $f = x$ и $g = y$ независимы

Лемма. Если f, g независимы, то $\mathbf{E}[f \cdot g] = \mathbf{E}[f] \cdot \mathbf{E}[g]$

1.53 Неравенство Хёфдинга–Чернова

X_n — случайная величина, равная количеству выпавших орлов после n подбрасываний «честной» монеты, а $\xi_n = X_n/n$ — частота выпавших орлов

Пусть $\varepsilon > 0$, тогда

$$\mathbf{Pr}\left[\left|X_n - \frac{n}{2}\right| > \varepsilon n\right] = \mathbf{Pr}\left[\left|\xi_n - \frac{1}{2} > \varepsilon\right|\right] < 2e^{-2\varepsilon^2 n}$$

1.54 Определение того, что одно целое число делится на другое. Деление с остатком, его существование и единственность

Целое число a **делится на целое** число b, если $a = bk$ для некоторого целого числа k

Деление с остатком всегда возможно, притом единственным образом. Доказательство — 2.45

1.55 Сравнимость по модулю. Вычеты. Утверждение о корректности суммы, разности и произведения вычетов

Если два числа a и b дают одинаковые остатки при делении на положительное число N, то говорят, что они **сравнимы по модулю** N, и пишут $a \equiv b \pmod N$

Для любого N отношение сравнимости по модулю N является отношением эквивалентности. Классы эквивалентности — множества чисел, имеющих одинаковый остаток от деления на N, — называются **вычетами** по модулю N

Утверждение. Класс суммы, разности или произведения чисел зависит только от классов операндов

1.56 Признаки делимости на 2, 3, 5, 9, 11

Делимость на 2. Число $a = \overline{a_k a_{k-1} \dots a_0}$ делится на 2, если и только если последняя цифра а a_0 чётна

Делимость на 3. Число $a = \overline{a_k a_{k-1} \dots a_0}$ делится на 3, если и только если сумма его иифр делится на 3. Более того: число даёт тот же остаток при делении на 3, что и его сумма цифр

Делимость на 5. Последняя цифра числа a должна делится на 5, так как $5 \mid 10$

Делимость на 9. Число делится на 9 , если и только если сумма его цифр делится на 9; число даёт тот же остаток при делении на 9, что и его сумма цифр

Делимость на 11. Число $a = \overline{a_k a_{k-1} \dots a_0}$ делится на 11, если и только если знакопеременная сумма его цифр делится на 11. Более того: число $a = \overline{a_k a_{k-1} \dots a_0}$ даёт тот же остаток при делении на 11, что и число $a_0 - a_1 + a_2 - \ldots + (-1)^k a_k$

1.57 Обратимый вычет. Возможность деления на обратимый вычет

Вычет по модулю N называется **обратимым**, если в произведении с каким-то другим вычетом он даёт 1. Другими словами, a обратим, если уравнение $ax \equiv 1 (\mathrm{mod}\ N)$ имеет решение в арифметике вычетов

Если вычет a обратим по модулю N, то уравнение $ax \equiv b \pmod N$ имеет в вычетах единственное решение при любом b

1.58 Взаимно простые числа. Критерий обратимости вычета

Взаимно простые числа — числа, которые не имеют общего положительного делителя, не считая 1

Критерий обратимости вычета. Обратимыми по модулю N являются те и только те вычеты, которые взаимно просты с N

1.59 Наибольший общий делитель, его свойства

Наибольший общий делитель — это наименьшее положительное число в множестве $S_a = \{x : x \equiv ka \pmod N, k \in \mathbb{Z}\}$ — множестве кратных вычета a

Свойство—1. Любой общий делитель d' чисел a, N является делителем числа d=НОД(a, N)

Свойство—2. НОД(a, b) = НОД$(a - qb, b)$ для любого целого q

1.60 Линейное диофантово уравнение. Общая формула для его решений

Линейное диофантово уравнение — $ax + by = c$, где a, b, c — целые числа

Общая формула для его решений. Пусть НОД$(a, b) \mid c$, $a\tilde{x}_0 + b\tilde{y}_0 = c$. Тогда множество решений линейного диофантового уравнения — это множество пар

$$(\tilde{x}_0 + tb/\text{НОД}(a, b), \tilde{y}_0 - ta/\text{НОД}(a, b)), \quad t \in \mathbb{Z}$$

1.61 Утверждение о структуре решений линейного диофантова уравнения. Лемма о решениях однородного линейного диофантова уравнения

Утверждение. Пусть $(\tilde{x}_0, \tilde{y}_0)$ — решение линейного диофантового уравнения. Тогда все решения этого уравнения имеют вид $(\tilde{x}_0 + x, \tilde{y}_0 + y)$, где пара (x, y) является решением однородного линейного уравнения

$$ax + by = 0 \tag{1.61.1}$$

Лемма. Решениями однородного линейного уравнения (1.61.1) являются в точности такие пары (x, y), что

$$x = t \cdot \frac{b}{d},\ y = -t \cdot \frac{a}{d}, \quad d = \text{НОД}(a, b),\ t \in \mathbb{Z}$$

1.62 Свойства отношения делимости. Простые числа. Составные числа

Свойства отношения делимости

Антисимметричность: если $a \mid b$ и $b \mid a$, то $a = kb = k\ell a$, откуда получаем $k\ell = 1$, то есть $k = \ell = 1$

Транзитивность: если $c = kb$ и $b = \ell a$, то $c = k\ell a$

Простые числа — целое положительное число, которое больше 1 и делится только на 1 и на само себя

Составные числа — числа, которые не являются простыми и не равны 1

1.63 Свойства простых чисел

Свойство—1. Для любого n найдётся такое k, что все числа $k, k + 1, \ldots, k + n$ составные

Свойство—2. Простых чисел бесконечно много

1.64 Лемма о простом числе, делящем произведение двух чисел. Основная теорема арифметики

Лемма. Если p — простое число, то из $p \mid xy$ следует, что $p \mid x$ или $p \mid y$

Основная теорема арифметики. Всякое целое положительное число, большее 1, разлагается на простые множители единственным образом: любые два разложения отличаются только перестановкой сомножителей

1.65 Каноническое разложение числа на простые множители. Финитные последовательности натуральных чисел. Отношение делимости в терминах канонического разложения

Берем любое целое положительное число n и разложим на множители. Простое число p_i встречается в этом разложении $a_i \geqslant 0$ раз. Если $a_i = 0$, то p_i не делит n, такое будет выполняться для всех i, начиная с некоторого

Получаем **каноническое разложение** — формально бесконечное произведение

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_k^{a_k} \cdot \ldots, \tag{1.65.1}$$

Показатели a_i, за исключением конечного числа, равны 0. Последовательности (a_i) с таким свойством называются **финитными**

Отношение делимости в терминах канонического разложения. Пусть числу n соответствует последовательность показателей (a_i), а числу k — (b_i). Тогда $k \mid n$ равносильно $b_i \leqslant a_i$ для всех i

1.66 Изоморфизм порядка делимости и покоординатного порядка на финитных последовательностях. Выражение НОД и НОК в терминах канонического разложения. Свойство НОД и НОК

Теорема. Порядок делимости на целых положительных числах изоморфен покоординатному порядку на финитных последовательностях целых неотрицательных чисел

Выражение НОД и НОК в терминах канонического разложения. Пусть числу n соответствует последовательность показателей (a_i), а числу k — последовательность (b_i)

Тогда НОД (n, k) соответствует последовательность $(\min(a_i, b_i))$, а НОК(n, k) — последовательность $(\max(a_i, b_i))$

Свойство. НОД$(n, k) \cdot$ НОК$(n, k) = kn$

1.67 Малая теорема Ферма. Функция Эйлера. Теорема Эйлера

Малая теорема Ферма. Если p — простое число, то

$$a^{p-1} \equiv 1 \pmod{p}$$

при любом a, не делящемся на p

Функция Эйлера. Функция Эйлера $\varphi(n)$ равна количеству остатков по модулю n, взаимно простых с n

Теорема Эйлера. Пусть $n > 1$ — произвольное целое положительное число, a взаимно просто с n. Тогда

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

1.68 Китайская теорема об остатках для двух и для любого числа сравнений

Для двух сравнений. Пусть числа u и v взаимно просты, и пусть a и b — любые целые числа. Тогда можно найти число x, для которого $x \equiv a \pmod{u}$ и одновременно $x \equiv b \pmod{v}$. В промежутке от 0 до $uv - 1$ такое число единственное

Для любого числа сравнений. Пусть даны целые числа $u_1, \ldots, u_n$, любая пара которых взаимно проста. Пусть $a_1, \ldots, a_n$ — любые целые числа. Тогда можно найти число x, для которого $x \equiv a_i \pmod{u_i}$ для всех $i = 1, \ldots, n$. *В* промежутке от 0 до $u_1 \ldots u_n - 1$ такое число единственное

1.69 Мультипликативность функции Эйлера. Формула для функции Эйлера

Мультипликативность функции Эйлера. $\varphi(uv) = \varphi(u)\varphi(v)$, если u и v взаимно просты

Формула для функции Эйлера. Пусть $n = p_1^{a_1} p_2^{a_2} \cdot \ldots \cdot p_s^{a_s}, a_i > 0$, p_i — различные простые. Тогда

$$\varphi(n) = \prod_{i=1}^{s} \left(p_i^{a_i} - p_i^{a_i - 1}\right) = n \prod_{i=1}^{s} \left(1 - \frac{1}{p_i}\right)$$

2 Вопросы на доказательство

2.1 Принцип наименьшего числа. Теорема о том, что между любыми двумя связанными вершинами существует простой путь

Принцип наименьшего числа

Формулировка. Любое непустое подмножество натуральных чисел содержит наименьший элемент

Доказательство. Пусть X — подмножество натуральных чисел, в котором нет наименьшего элемента, т.е. $\forall a \in X\ \exists b \in X : b < a$

Докажем, что $n \notin X\ \forall n \iff X = \varnothing$ по полной индукции. $0 \notin X$, т.к. 0 — наименьшее натуральное число. Предположим, что $\forall k < n$ известно, что $k \notin X$. Тогда $n \notin X$, т.к. в противном случае n было бы наименьшим натуральным числом в X. Отсюда, $n \notin X\ \forall n$, т.е. X пустое

Мы доказали, что если множество натуральных чисел X не имеет наименьшего натурального элемента, то оно пусто. Контрапозиция к этому утверждению и есть принцип наименьшего числа

Теорема

Формулировка. Если две вершины x, y связанные в графе G, то в этом графе существует простой путь с началом x и концом y

Доказательство из конспекта. Используем принцип наименьшего числа. Если существует хотя бы один путь из x в y, то существует и путь наименьшей длины (нет пути короче)

Рассмотрим кратчайший путь $x = u_1, \ldots, u_k = y$ и докажем, что он простой с помощью контрапозиции. Тогда нужно доказать, что если путь $x = u_1, \ldots, u_k = y$ не простой, то он не кратчайший. Пусть $u_i = u_j,\ i < j$. Тогда последовательность $x = u_1, \ldots, u_i, u_{j+1}, u_k = y$ также является путем из x в y, а длина этого пути меньше. (Если $j = k$, то есть вершина u_{j+1} не существует, то тогда более короткий путь имеет вид $x = u_1, \ldots, u_i = u_k = y$) □

Доказательство из учебника Вялого. Рассмотрим кратчайший путь из x в y. Предположим, что в него дважды входит некоторая вершина w, тогда участок между этими вхождениями можно было бы выбросить, и получился бы более короткий (простой) путь из x в y, вопреки предположению □

2.2 Критерий того, что граф является лесом, в терминах простых путей и простых циклов

Формулировка. Равносильные свойства **простых** неориентированных графов:

(1) каждое ребро — мост

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

(3) нет простых циклов длины больше 2

Доказательство. Доказываем утверждения теоремы по очереди

Доказательство (2) $\implies$ (3). Равносильно контрапозиции $\neg(3) \implies \neg(2)$. Пусть в графе G есть простой цикл $u_0, u_1, \ldots, u_t = u_0, t > 2$

Вершины u_0, u_1 соседние, а значит связанные в этом графе, причем есть как минимум два разных простых пути с концами в этих вершинах: (u_0, u_1), т.е. путь из одного ребра, и путь по остальным ребрам цикла $(u_0 = u_t, u_{t-1}, \ldots, u_2, u_1)$, важно, что длина цикла больше 2 □

Доказательство (3) $\implies$ (1). Равносильно контрапозиции $\neg(1) \implies \neg(3)$. Пусть ребро $e = \{x, y\}$ можно удалить из графа G, и в полученном графе $G' = G - e$ количество компонент связности не увеличится. Значит, вершины x, y связанные в графе G'. По теореме из 2.1 в графе G' есть простой путь $x, u_1, u_2, \ldots, u_t, y$, все вершины которого различны

Тогда в графе G есть простой цикл $x, u_1, u_2, u_3, \ldots, u_t, y, x$ и, т.к. x, y, u_1 — три различные вершины, длина этого цикла больше 2 □

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

$$(x_0, x_1, \ldots, x_r) \text{ и } (y_0, y_1, \ldots, y_s)$$

здесь $x_0 = y_0 = u, x_r = y_s = v$. Начинаются эти пути в одной вершине, но полностью совпадать не могут. Возьмём наибольшее общее начало этих путей, то есть максимально возможное i, для которого $x_j = y_j \ \forall 0 \leqslant j \leqslant i$. Тогда $x_{i+1} \neq y_{i+1}$ и потому ребро $\{x_i, x_{i+1}\}$ не входит во второй путь, но входит в первый по определению. Если $\{x_i, x_{i+1}\}$ входит во второй путь, то этот путь не простой: вершина $y_i = x_i$ встретится в нём по крайней мере дважды: второй раз случится, когда $\{y_t, y_{t+1}\} = \{x_i, x_{i+1}\}$, по построению $t > i$

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

$$x_i, x_{i-1}, \ldots, x_1, u, y_1, \ldots, y_{s-1}, v, x_{r-1}, \ldots, x_{i+1}$$

Остальные области достижимости (отличные от $C(x_i)$) не изменяются: пути из таких вершин не проходят через ребро $\{x_i, x_{i+1}\}$ □

Поскольку мы доказали циклическую цепочку импликаций (2) $\implies$ (3) $\implies$ (1) $\implies$ (2), все эти утверждения равносильны □

2.3 Свойства цикломатического числа графа

Свойство—1. Граф $G' = G + e$ получается добавлением к графу G ребра $e = \{x, y\}$ к множеству рёбер, а вершины у него те же

Тогда $r(G') = r(G)$, если концы ребра x, y лежат в разных компонентах связности графа G, и $r(G') = r(G) + 1$, если x, y лежат в одной компоненте связности графа G

Доказательство. Рассмотри 2 случая из формулировки

(1) *Вершины x, y лежат в одной компоненте связности C графа G.* Тогда количество компонент связности не изменилось: для любого пути в G', проходящего через ребро e, существует путь в G с теми же концами. Количество ребер увеличилось на 1, количество вершин не изменилось. Значит, цикломатическое число увеличилось на 1 □

(2) *Вершины x, y лежат в разных компонентах связности графа G.* Тогда в графе G' в область достижимости вершины x добавляется $C(y)$, поскольку в G' вершина y достижима из x. Проводя аналогичные рассуждения про y, получим

$$C'(x) = C'(y) = C(x) \cup C(y).$$

Значит, области достижимости x, y в G' равны объединению областей достижимости этих вершини в графе G. Остальные области достижимости не меняются. Значит, количество компонент связности уменьшилось на 1. Количество рёбер увеличилось на 1, количество вершин не изменилось, цикломатическое число не изменилось □

Свойство—2. Цикломатическое число графа неотрицательное

Доказательство. Используем индукцию по количеству ребер графа. База индукции — графы без рёбер с произвольным количеством вершин. В таких графах цикломатическое число равно нулю, т.к. рёбер нет, каждая вершина является компонентой связности. И такой граф является лесом, т.к. каждое его ребро — мост (рёбер вообще нет, так что это утверждение верно)

Пусть цикломатическое число неотрицательное для всех графов с меньше чем k рёбрами, $k > 0$. Рассмотрим граф G' с k рёбрами и выделим в нём ребро $e = \{x, y\}$. Тогда $r(G') \geqslant r(G' - e) \geqslant 0$: первое неравенство — это предыдущее свойство, а второе — индуктивное предположение. Шаг индукции доказан, свойство выполняется в силу принципа математической индукции □

Альтернативное доказательство. Тык и в видео - тык 2.0

2.4 Критерий того, что граф является лесом, в терминах цикломатического числа

Формулировка. Графы, у которых цикломатическое число равно 0, — это в точности леса, то есть графы, у которых каждое ребро — мост

Доказательство. Используем индукцию по количеству ребер. База проверена в доказательстве свойства—2 в 2.3

Шаг индукции. Пусть теорема выполняется для графов с меньше чем k рёбрами, $k > 0$. Рассмотрим граф G с k рёбрами

Пусть $r(G) = 0$. Так как цикломатическое число любого графа неотрицательное, каждое ребро G — мост, т.к. удаление не моста уменьшает цикломатическое число. Значит, G — лес

Тогда для любого ребра e в графе $(G - e)$ нет простых циклов длины больше 2, т.к. любой такой цикл был бы и простым циклом в лесу G. По критерию 2.2 граф $(G - e)$ также лес. Согласно индуктивному предположению $r(G - e) = 0$. Однако, e — мост в G, поэтому из свойства—1 в 2.3 получаем $r(G) = r(G - e) = 0$

Шаг индукции доказан. По принципу полной математической индукции, цикломатическое число любого леса равно 0 и все графы с цикломатическим числом 0 — леса □

2.5 Теорема про висячие вершины в дереве: два доказательства. Теорема об остовном дереве

Теорема про висячие вершины в дереве

Формулировка. В дереве с хотя бы двумя вершинами найдутся по крайней мере две висячие вершины

Доказательство—1. Выберем вершину, пусть она не изолированная. Куда-нибудь пойдём, чтобы рёбра не повторялись. Вернуться в вершину, в которой мы уже были, невозможно — иначе нашёлся бы цикл. Поэтому ходить по графу бесконечно тоже невозможно, так что мы упрёмся в тупик — это и будет висячая вершина. Чтобы найти вторую висячую вершину, нужно проделать тот же алгоритм, начав с уже найденной висячей вершины □

Доказательство—2. Воспользуемся критерием—2 из 1.4. Пусть в дереве $n \geqslant 2$ вершин. Тогда количество ребер равно $n - 1$

Обозначим степени вершин $d_1, \ldots, d_n$. Так как $n \geqslant 2$, то изолированных вершин нет (каждая изолированная вершина является компонентой связности). Из теоремы о том, что сумма степеней всех вершин графа равна удвоенному числу его рёбер получим

$$d_1 + \ldots + d_n = 2(n-1) \iff (d_1 - 2) + (d_2 - 2) + \ldots + (d_n - 2) = -2$$

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

Теорема об остовном дереве

Формулировка. В любом связном графе есть остовное дерево

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

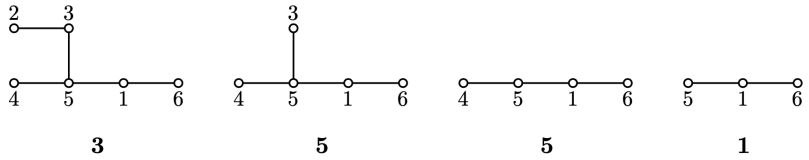
2.6 Теорема Кэли

Формулировка. Количество остовных деревьев в полном графе на n занумерованных вершинах равно n^{n-2} при $n \geqslant 2$

Доказательство. Пусть вершины полного графа занумерованы числами от 1 до n. Количество остовных деревьев в полном графе равно количеству деревьев на множестве вершин $\{1, \ldots, n\}$. Требуется доказать, что это количество равно n^{n-2}. Самый простой пример: количество последовательностей длины $n - 2$, члены которых — целые числа от 1 до n. Доказательство состоит в построении биекции между деревьями и такими последовательностями

Пусть T — дерево с множеством вершин $\{1, \ldots, n\}$. Построим по нему последовательность Прюфера $x_1, \ldots, x_{n-2}$ и соответствующую ей последовательность деревьев $T_1, \ldots, T_{n-1}$ по такому правилу. Полагаем $T_1 = T$. Если уже построено дерево T_i, находим в нём висячую вершину m с наименьшим номером. В качестве x_i берём соседа вершины m в дереве T_i. Поскольку вершина висячая,

сосед определён однозначно. Дерево T_{i+1} получается из T_i удалением вершины m. Заметим, что удаление из дерева висячей вершины даёт дерево, так как связность сохраняется, как и разность числа вершин и числа рёбер. Поскольку всякий раз удаляется ровно одна вершина, количество вершин в дереве T_i равно $n - i + 1$. То есть в последнем дереве T_{n-1} ровно 2 вершины, соединённые ребром (а последовательность Прюфера заканчивается на предыдущем шаге). Пример такого построения показан на рисунке ниже (последнее дерево пропущено, ему не отвечает никакого элемента последовательности Прюфера)



Это правило определяет тотальную функцию из множества деревьев на множестве вершин $\{1, \ldots, n\}$ в последовательности длины $n-2$ из чисел, принадлежащих множеству $\{1, \ldots, n\}$. Докажем индукцией по числу вершин, что это биекция. Возникает проблема: после удаления вершины m получается дерево, в котором вершины занумерованы не подряд

Чтобы избавиться от проблемы, усилим утверждение, которое будем доказывать. Будем доказывать существование биекции между деревьями, вершины которых принадлежат конечному множеству $V \subset \mathbb{N}$ и последовательностями длины $n - 2$, элементы которых принадлежат V. Здесь $n = |V|$

База индукции: $n = 2$. В этом случае последовательность пустая, её длина равна 0, а дерево единственное. Биекция между двумя 1-элементными множествами также единственная

Шаг индукции. Пусть уже доказано существование биекций указанного вида для любого V с $|V| = n, n \geqslant 2$. Рассмотрим множество $V' \subset \mathbb{N}$, в котором $n + 1$ число. Выполним один шаг построения последовательности Прюфера. То есть, найдём в дереве T' с множеством вершин V' висячую вершину m с наименьшим номером

Соседа этой вершины обозначим a. Удалим m из дерева. Получаем дерево на множестве вершин $V = V' \backslash \{m\}$. По предположению индукции есть биекция между деревьями на таком множестве вершин и V^{n-2}. Обозначим $\boldsymbol{x}_T$ последовательность, которая соответствует T. Тогда T' сопоставляется последовательность $(a, \boldsymbol{x})$

Докажем, что получена биекция между деревьями с множеством вершин V' и множеством последовательностей $(V')^{n-1}$. Для этого построим обратную функцию. Пусть дана последовательность $(a, x_1, \ldots, x_{n-2})$. Обозначим m наименьшее число в множестве $V' \backslash \{a, x_1, \ldots, x_{n-2}\}$. Найдём дерево T на множестве вершин $V = V' \backslash \{m\}$, соответствующее последовательности $(x_1, \ldots, x_{n-2})$ (по предположению индукции существует требуемая биекция, так как m не входит в $\{x_1, \ldots, x_{n-2}\}$). Сопоставим последовательности $(a, x_1, \ldots, x_{n-2})$ дерево T', которое получается из T добавлением висячей вершины m, соседней с a. Этому дереву мы и сопоставляем последовательность $(a, x_1, \ldots, x_{n-2})$, значит построена обратная функция □

2.7 Теорема о существовании монотонного остовного дерева

Формулировка. В каждом связном графе существует монотонное остовное дерево

Доказательство. Выберем произвольную вершину r связного графа G в качестве корня. Построим нумерацию вершин графа, т.е. биекцию $\{1, 2, \ldots, n\} \to V(G), n = |V(G)|$, и корневой подграф T с корнем r следующим индуктивным процессом

Сопоставим корню число 1, $v_1 = r$. После i шагов получаем последовательность $v_1, \ldots, v_i$. Так как граф G связный, то какие-то вершины из полученной последовательности смежны с вершинами из множетсва $V_i = V(G) \setminus \{v_1, \ldots, v_i\}$. На $(i + 1)$-м шаге выберем среди всех ребер вида $\{v_j, u\}$, $1 \leqslant j \leqslant i$, $u \in V_i$ то, для которого номер j принимает наибольшее значение. Обозначим этот номер k. Если $j > k$, то v_j смежна только с вершинами из уже построенной последовательности, а v_k смежна с какими-то вершинами из V_i. Добавим в последовательность какого-нибудь непронумерованного соседа вершины v_k и обозначим его v_{i+1}. Теперь добавляем ребро $\{v_k, v_{i+1}\}$ к ребрам T. Повторяем, пока $V_i \neq \varnothing$

Построенный граф T связный: проверяем индукцией по номерам, что каждая вершина достижима из корня. В графе T $(n-1)$ ребро, т.к. ровно одно ребро добавляется на каждом шаге, кроме

первого. Значит, это дерево (согласно критерию—2 из 1.4). Теперь проверяем индукцией по номерам, что на каждом пути из корня в любую вершину номера строго возрастают

Докажем монотонность построенного остовного дерева от противного. Пусть $\{v_i, v_j\}$ — ребро графа $G, i < j$, и v_i не лежит на пути из v_j в $r = v_1$. Обозначим как v_k вершину с максимальным номером, которая лежит выше и v_i, и v_j. Тогда из монотонности нумерации следует, что $k < i$. Рассмотрим первую вершину на пути из v_k в v_j, номер которой больше i (такая вершина существует, т.к. $j > i$). Пусть ее номер равен s. На $(s-1)$-м шаге процесса выбрано ребро $\{v_t, v_s\}$ (причем $t < i$, т.к. s — первая вершина на пути из v_k в v_j с номером, большим i), а не $\{v_i, v_j\}$, хотя $i > t,\ v_j \in V_{s-1}$, и вершина v_i уже есть в построенной последовательности, т.к. $i < s$. Получаем противоречие с правилом построения последовательности $(v_1, \ldots, v_n)$ □

2.8 Связь кликового числа и числа независимости для графа и его дополнения. Кликовое число и число независимости для полного графа. Кликовое число и число независимости для булева куба. Верхняя оценка на сумму кликового числа и числа независимости

Связь кликового числа и числа независимости для графа и его дополнения

Из определения понятно, что кликовое число графа G равно числу независимости его дополнения, $\omega(G) = \alpha(\bar{G})$, потому что рёбра и нерёбра меняются местами при переходе к дополнению

Кликовое число и число независимости для полного графа

Для полного графа из определений получаем $\omega(K_n) = n$, а $\alpha(K_n) = 1$

Кликовое число и число независимости для булева куба

Обозначим через I_0 множество вершин булева куба Q_n (двоичных слов длины n), в которых чётное количество единиц, а через I_1 — множество вершин булева куба Q_n, в которых нечётное количество единиц

При инвертировании одной позиции количество единиц в слове изменяется ровно на 1. Поэтому концами каждого ребра являются слова, у которых чётность количества единиц разная — в одном количество единиц чётно, в другом — нечётно. Значит, между вершинами из I_0 рёбер нет (как и между вершинами из I_1). Из свойств биномиальных коэффициентов мы знаем, что $|I_0| = |I_1|$. Таким образом $\alpha(Q_n) \geqslant 2^{n-1}$ (половина всех вершин)

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

Пусть I — независимое множество. Степень любой вершины в булевом кубе Q_n равна n. Поэтому количество рёбер, инцидентных I, равно $n|I|$. Это число не больше общего количества рёбер $n2^{n-1}$. Отсюда получаем неравенство $|I| \leqslant 2^{n-1}$. Итак, $\alpha(Q_n) = 2^{n-1}$

Клика размера 2 — это ребро и такие клики есть в Q_n при $n > 0$. Клика размера 3 — треугольник — в Q_n невозможна. Из любых трёх вершин две лежат в одном из множеств I_0, I_1 (имеют одинаковую чётность количества единиц) и потому не связаны ребром. Поэтому $\omega(Q_n) = 2$

Верхняя оценка на сумму кликового числа и числа независимости

Любая клика пересекает любое независимое множество разве что по одной вершине, поэтому $\alpha(G) + \omega(G) \leqslant n + 1$ для любого графа G. Оценка достигается, например, на полном графе

2.9 Теорема Рамсея

Формулировка. Для любых k, n найдется такое число N_0, что в любом графе на $N \geqslant N_0$ вершинах есть клика размера k или независимое множество размера n

Disclaimer. Теорема Рамсея говорит лишь о существовагнии чисел Рамсея, а мы докажем верхнюю оценку на них:

$$R(k, n) \leqslant R(k-1, n) + R(k, n-1),\ k > 1, n > 1$$

и сам факт существования чисел Рамсея

Доказательство. Пусть $k+n=s$. Докажем индукцией по s

База $s=2$ очевидна: $2=1+1$[1]

Шаг индукции. Предположим, что неравенство (верхняя оценка) выполняется для всех пар (k,n) таких, что $k+n=s$

Докажем неравенство для такой пары (k,n), что $k+n=s+1,\ k>1, n>1$. Согласно индуктивному предположению существуют числа Рамсея $R(k-1,n)$ и $R(k,n-1)$

Рассмотрим граф на $N_0=R(k-1,n)+R(k,n-1)$ вершинах и выберем произвольную вершину v этого графа. Вершин в графе за исключением вершины v ровно N_0-1 штук. Среди них N_1 соседей и N_2 несоседей вершины v

Докажем, что выполняется хотя бы одно из неравенств от противного

$$N_1 \geqslant R(k-1,n),$$
$$N_2 \geqslant R(k,n-1).$$

Действительно, в противном случае выполняются два неравенства

$$N_1 < R(k-1,n),$$
$$N_2 < R(k,n-1),$$

из которых следует противоречие

$$N_0-1=N_1+N_2 \leqslant R(k-1,n)-1+R(k,n-1)-1=N_0-2$$

Поэтому у вершины v есть хотя бы $R(k-1,n)$ соседей или есть хотя бы $R(k,n-1)$ несоседей. Рассмотрим случаи

Первый случай. В индуцированном соседями вершины v подграфе по предположению индукции найдётся клика размера $k-1$ или независимое множество размера n. В первом варианте добавление вершины v даёт клику в исходном графе размера k, во втором варианте в исходном графе есть независимое множество размера n

Второй случай. В индуцированном несоседями вершины v подграфе по предположению индукции найдётся клика размера k или независимое множество размера $n-1$. В первом варианте в исходном графе есть клика размера k, а во втором добавление вершины v даёт независимое множество размера n в исходном графе

Мы доказали, что для $k+n=s+1$ теорема Рамсея выполняется, как и неравенство верхней оценки. Значит, для всех k,n теорема Рамсея верна и при $k>1, n>1$ выполняется неравенство верхней оценки по принципу математической индукции □

2.10 Верхняя оценка на числа Рамсея. Явные выражения для $R(2,n)$ и $R(3,3)$

Верхняя оценка на числа Рамсея. $R(k,n) \leqslant \binom{k+n-2}{k-1}$

Доказательство. Для биномиальных коэффициентов выполняется

$$\binom{k+n}{k}=\binom{k+n-1}{k-1}+\binom{k+n-1}{k}$$

Заметим, что $R(k,1)=R(1,n)$, т.к. одна вершина является и кликой, и незаивсимым множеством. Искомое неравенство справедливо при $k=1$ или $n=1$, т.к. $R(k,1)=R(1,n)=\binom{n-1}{0}$

Для остальных случаев докажем индукцией по $k+n=s$. База доказана ранее. Проверим шаг индукции при $k>1, n>1$ с помощью неравенства из 2.9:

$$R(k,n) \leqslant R(k-1,n)+R(k,n-1) \leqslant \binom{k+n-3}{k-2}+\binom{k+n-3}{k-1}=\binom{k+n-2}{k-1}$$

[1] Так как это единственный способ разложить число 2 на сумму двух положительных чисел

Во втором неравенстве использовалось индуктивное предположение □

Явное выражение—1. $R(2,n) = \binom{n}{1} = n$

Доказательство. Если в графе G есть хотя бы одно ребро, то $\omega(G) \geqslant 2$. Если ребер нет, тогда $\alpha(G) = |V(G)|$. Значит, если в графе есть хотя бы n вершин, то в нём есть либо ребро и, тем самым, клика размера 2, либо в нём нет рёбер и есть независимое множество размера n. Если в графе нет рёбер и вершин меньше n, в нём нет ни клики размера 2, ни независимого множества размера n □

Явное выражение—2. $R(3,3) = \binom{4}{2} = 6$

Доказательство. Докажем, что $R(3,3) \leqslant 6$. Это частный случай верхней оценки числа Рамсея: $R(3,3) \leqslant \binom{3+3-2}{3-1} = 6$

Чтобы доказать $R(3,3) > 5$, приведем пример графа на 5 вершинах, в котором нет треугольника (клики размера 3) и в дополнении к которому нет треугольника. Таким графом является цикл C_5. Что в нём нет клики размера 3, очевидно из построения. А дополнение к C_5 также является циклом на 5 вершинах. Так что независимого множество размера 3 в нём также нет □

2.11 Уточнение верхней оценки на числа Рамсея

Формулировка. Если оба числа $R(k-1,n), R(k,n-1)$ четные, то

$$R(k,n) \leqslant R(k-1,n) + R(k,n-1) - 1$$

Доказательство. Пусть $R(k-1,n),\ R(k,n-1)$ четные. Рассмотрим граф на $N_0 = R(k-1,n) + R(k,n-1) - 1$ вершинах. Это число нечетное, поэтому в графе есть вершина v четной степени, т.к. сумма степеней вершин четная

Вершин в графе за исключением v ровно $N_0 - 1$ штук. Среди них N_1 соседей и N_2 несоседей вершины v и оба числа чётные, так как N_1 чётное по выбору вершины v и $N_1 + N_2 = N_0 - 1$ чётное

Докажем, что выполняется хотя бы одно из неравенств

$$N_1 \geqslant R(k-1,n),$$
$$N_2 \geqslant R(k,n-1).$$

В противном случае выполняются два неравенства

$$N_1 < R(k-1,n), \quad \text{что равносильно } N_1 \leqslant R(k-1,n) - 2,$$
$$N_2 < R(k,n-1), \quad \text{что равносильно } N_2 \leqslant R(k,n-1) - 2.$$

Получаем противоречие

$$N_0 - 1 = N_1 + N_2 \leqslant R(k-1,n) - 2 + R(k,n-1) - 2 = N_0 - 3$$

Поэтому у вершины v есть хотя бы $R(k-1,n)$ соседей или есть хотя бы $R(k,n-1)$ несоседей. Рассмотрим случаи

Далее также рассматриваем случаи, как в 2.9 □

2.12 Нижняя оценка на числа Рамсея

Формулировка. $R(k,k) > \lfloor 2^{(k-1)/2} \rfloor\ \forall k \geqslant 3$

Другими словами, $\forall k \geqslant 3$ существует граф $G = (V,E)$ на $n = \lfloor 2^{(k-1)/2} \rfloor$ вершинах, в котором нет ни клики размера k, ни независимого множества размера k

Доказательство. Оценим количество графов на n вершинах, содержащих либо клику размера k, либо независимое множество такого размера, и сравним это число с общим количеством графов. При больших n первое число намного меньше второго. Это и означает, что существуют графы на n вершинах без клик и без независимых множеств размера k

Множество графов на n вершинах находится во взаимно однозначном соответствии с подмножествами множества пар вершин (каждое ребро или проведено, или нет). Всего пар вершин (=рёбер) $\binom{n}{2}$, поэтому графов $2^{\binom{n}{2}}$

Обозначим через A множество графов, содержащих клику или независимое множество размера k. Это множество является объединением множеств A_W, где $W \subseteq V$, $|W| = k$, которые состоят из тех графов, в которых множество W образует клику или независимое множество. Запишем это формально

$$A = \bigcup_{\substack{W \subseteq V, \\ |W|=k}} A_W$$

Воспользуемся оценкой объединения: для любого семейства конечных подмножеств $X_1, \ldots, X_t$ выполняется

$$\left| \bigcup_i X_i \right| \leqslant \sum_i |X_i|$$

Оценка объединения — упрощённый вариант формулы включений и исключений. Пересчитывая все элементы во всех множествах, получаем правую часть, при этом все элементы будут пересчитаны и, возможно, даже не по одному разу

Итак,

$$|A| \leqslant \sum_{\substack{W \subseteq V \\ |W|=k}} |A_W|$$

Посчитать количество графов в A_W легко. Ребра между вершинами в W в таком графе должны либо все присутствовать, либо все отсутствовать. Ребра, хотя бы один конец которых лежит вне W, могут быть произвольными. Количество рёбер, у которых хотя бы один конец лежит вне W, есть $\binom{n}{2} - \binom{k}{2}$ (все ребра минус ребра в W). Таким образом, количество таких графов есть $2 \cdot 2^{\binom{n}{2}-\binom{k}{2}}$, где первая двойка отвечает за выбор рёбер внутри W, а второй множитель — за выбор остальных рёбер. То есть

$$|A_W| = 2^{\binom{n}{2}-\binom{k}{2}+1}$$

Таким образом, при $k \geqslant 3, n = \left\lfloor 2^{(k-1)/2} \right\rfloor$ получаем неравенство

$$\frac{|A|}{2^{\binom{n}{2}}} \leqslant \sum_{\substack{W \subseteq V, \\ |W|=k}} 2^{-\binom{k}{2}+1} = \binom{n}{k} \cdot 2^{-\binom{k}{2}+1} = \frac{n(n-1)\cdots(n-k+1)}{k!} \cdot 2^{-\binom{k}{2}+1} \leqslant$$

$$\leqslant \frac{n^k}{2 \times 3} \cdot 2^{-\binom{k}{2}+1} \leqslant \frac{2^{k(k-1)/2-\binom{k}{2}+1}}{6} = \frac{1}{3}$$

Поэтому количество графов с кликой или независимым множеством размера k не более трети от общего числа графов. Значит, не менее двух третей графов с таким количеством вершин удовлетворяют условию теоремы □

2.13 Критерий 1-раскрашиваемости графа. Критерий 2-раскрашиваемости графа. 2 - раскрашиваемость булева куба

Критерий 1-раскрашиваемости графа

Формулировка. Все **графы без ребер** 1-раскрашиваемые

Доказательство. Если вершинам графа без рёбер присвоить число 1, то условие правильной раскраски выполняется. И наоборот: если в графе есть ребро $\{u, v\}$, то в правильной раскраске вершинам u, v присвоены разные цвета, поэтому количество цветов хотя бы 2 □

Критерий 2-раскрашиваемости графа

Формулировка. 2-раскрашиваемые графы это в точности графы, в которых длины всех циклов чётные

Доказательство. Если вершины графа правильно раскрашены в 2 цвета, то цвета вершин вдоль любого пути чередуются, т.к. соседние вершины покрашены в разные цвета. Поэтому длина любого цикла в таком графе чётная (концы пути нечётной длины покрашены в разные цвета)

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

Пусть в связном графе длины всех циклов чётные. Докажем, что для любых двух вершин u, v в этом графе длины путей из u в v имеют одинаковую чётность

Если в графе есть путь $\alpha = (u, \dots, v)$ с четным числом вершин (нечетной длины), а также другой путь $\beta = (u, \dots, v)$ с нечетным числом вершин (четной длины), то соединение пути α и обратного к β пути, т.е. пути $(v, \dots, u)$, даёт цикл с нечётным числом вершин (нечётной длины). Это противоречит сделанному предположению, что все циклы в графе имеют чётную длину

Теперь укажем искомую правильную раскраску в 2 цвета. Выберем вершину v_0 и раскрасим вершину x графа в цвет 0, если длины путей из v_0 в x чётные, и в цвет 1 — если иначе. Это правило корректно по доказанному выше утверждению про одинаковую чётность длин путей с общими концами в связном графе, все циклы которого чётные

При такой раскраске смежные в графе вершины не могут быть покрашены в один цвет: если $\{x, y\}$ — ребро графа, то для пути $(v_0, \dots, x)$ существует путь в y, длина которого имеет противоположную четность: $(v_0, \dots, x, y)$ □

2-раскрашиваемость булева куба

Формулировка. Булев куб Q_n 2-раскрашиваемый

Доказательство. Вершинами булева куба Q_n являются двоичные слова длины n. Покрасим вершины с чётным количеством единиц в цвет 0; с нечётным количеством единиц — 1

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

2.14 Количество совершенных паросочетаний в полном графе на $2n$ вершинах

Формулировка. Количество совершенных паросочетаний в полном графе на $2n$ вершинах равно $(2n-1)!!$[2]

Доказательство. Определим функцию $f : S_{2n} \to \Pi_{2n}$, где S_{2n} — перестановки чисел от 1 до $2n$, а Π_{2n} — совершенные паросочетания в полном графе на множетсве вершин $\{1, 2, \dots, 2n\}$. Перестановку $x_1 x_2 \dots x_{2n}$ функция отправляет в паросочетание

$$\{\{x_1, x_2\}, \{x_3, x_4\}, \dots, \{x_{2n-1}, x_{2n}\}\}$$

Из определения понятно, что функция тотальная. Определим размер прообраза одного паросочетания. Паросочетание не изменится, если поменять местами x_{2i+1} и x_{2i} для любого $0 \leqslant i \leqslant n-1$, а также если переставить все такие n пар произвольным образом. В любом другом случае паросочетание изменяется. По правилу произведения размер прообраза любого паросочетания равен $(2!)^n n!$. Получаем равенство

$$(2n)! = (2!)^n n! P_{2n},$$

из которого выводим искомую формулу для количества совершенных паросочетаний:

$$P_{2n} = \frac{(2n)!}{(2!)^n n!} = \frac{2n \cdot (2n-1) \cdot \ldots \cdot 2 \cdot 1}{2n \cdot (2n-2) \cdot \ldots \cdot 2} = (2n-1) \cdot (2n-3) \cdot \ldots \cdot 1 = (2n-1)!!$$

[2] Двойной факториал $n!!$ означает произведение членов в арифметической прогрессии с началом n и разностью равной -2

□

2.15 Теорема Холла

Формулировка. $G = (L, R, E)$ — двудольный граф. Тогда в графе G есть паросочетаание размера $|L|$ тогда и только тогда, когда для каждого множества $S \subseteq L$ множество соседей $G(S) \subseteq R$ содержит не меньше вершин, чем S

Доказательство. Если есть паросочетание размера $|L|$, то условие Холла выполняется: у каждого $S \subseteq L$ соседей не меньше, чем $|S|$ (в эти соседи входят концы в правой доле каждого ребра паросочетания, инцидентного вершине из S)

В другую сторону докажем с помощью полной индукции по количеству элементов в L

База индукции. Если в L всего одна вершина x, тогда у нее есть хотя бы один сосед y в правой доле R (по условию теоремы). Получаем паросочетание с ребром $\{x, y\}$

Шаг индукции. Предположим, что утверждение теоремы выполняется для всех двудольных графов, в которых левая доля содержит меньше n вершин. Рассмотрим граф $G = (L, R, E)$, для которого выполняются условия теоремы и в L ровно n вершин. Разберём два случая:

Первый случай: в левой доле есть такое множество $\varnothing \neq S \subset L$, для которого $|S| = |G(S)|$

Выделим из графа два подграфа. Первый, G', имеет доли S, $G(S)$ и все рёбра графа G между этими вершинами. Второй, G'', имеет доли $T = L \setminus S$, $Q = R \setminus G(S)$ и все рёбра графа G между этими вершинами. Для обоих графов выполняются условия теоремы Холла. Для G' это выполняется, так как множество соседей подмножества $X \subseteq S$ лежит в $G(S)$

Теперь проверим условие Холла для графа G'', то есть $|G''(X)| \geqslant |X|$ для любого подмножества $X \subseteq T$. Заметим, что $G(S \cup X) = G(S) \cup G''(X)$, $S \cap X = \varnothing$, $G(S) \cap G''(X) = \varnothing$ по построению графа G''. Из условия Холла для графа G и выбора множества S получаем

$$|G(S \cup X)| = |G(S)| + |G''(X)| = |S| + |G''(X)| \geqslant |S \cup X| = |S| + |X|$$

Отсюда следует искомое неравенство $|G''(X)| \geqslant |X|$

Поскольку для G', G'' выполняются условия Холла, а количество вершин в этих графах меньше n, то по предположению индукции в каждом из этих графов есть паросочетание размера левой доли. Объединяя эти два паросочетания, получаем искомое паросочетание в G размера $|L|$

Второй случай: для каждого $\varnothing \neq S \subset L$ выполняется неравенство $|S| < |G(S)|$

Выберем вершину $a \in L$ и её соседа $b \in R$ (в этом случае соседей у каждой вершины больше одного)

Проверим, что для графа $G' = ((L \setminus \{a\}), (R \setminus \{b\}), E')$, полученного из G выбрасыванием вершин a, b и инцидентных им рёбер, выполняются условия Холла. Количество соседей множества $X \subseteq L \setminus \{a\}$ в графе G' разве что на 1 меньше, чем в графе G (различие только в вершине b). Так как $|X| < |G(X)|$, то $|X| \leqslant |G'(X)|$

Значит, по индуктивному предположению, в графе G' существует паросочетание размера $n - 1$. Добавим к рёбрам этого паросочетания ребро $\{a, b\}$. Тогда получим паросочетание размера n в графе G □

2.16 Следствия из теоремы Холла для регулярных двудольных графов

Следствие—1. В регулярном двудольном графе, степени вершин которого ненулевые, существует совершенное паросочетание

Доказательство. Пусть степень каждой вершины в регулярном двудольном графе $G = (L, R, E)$ равна d, по условию $d \neq 0$. Заметим, что тогда $|E| = d|L| = d|R|$, то есть $|L| = |R|$. Докажем, что условие теоремы Холла выполняется (и потому существует паросочетание размера L, которое является совершенным)

Рассмотрим множество $S \subseteq L$ вершин левой доли. Эти вершины являются концами $d|S|$ рёбер. По определнию $G(S)$ — концы этих ребер в правой доле. Подсчитывая рёбра между S и $G(S)$ двумя способами, получаем $d|S| \leqslant d|G(S)|$. Первое число — подсчёт рёбер по левым концам. Второе — по

правым (каждая из этих вершин является концом не более, чем d рёбер, ведущих в S, поскольку степень вершины равна d). Значит, теорема Холла выполняется □

Следствие—2. Если степень каждой вершины в двудольном графе равна $d > 0$, то его рёбра можно разбить на d непересекающихся совершенных паросочетаний

Доказательство. Индукция по степени вершин в графе d

База очевидна: $d = 1$, такой граф и есть совершенное паросочетание

Шаг индукции: применим следствие—1 и выделим рёбра полученного совершенного паросочетания. Остальные рёбра образуют регулярный граф степени $d - 1$, который разбивается на $d - 1$ совершенное паросочетание по индуктивному предположению □

2.17 Связь между вершинными покрытиями и независимыми множествами. Связь минимального размера вершинного покрытия с числом независимости. Связь минимального размера вершинного покрытия с максимальным размером паросочетания. Пример, показывающий возможность строгого неравенства из последнего утверждения

Связь между вершинными покрытиями и независимыми множествами

Формулировка. Множество S вершин графа $G = (V, E)$ является вершинным покрытием тогда и только тогда, когда $V \setminus S$ — независимое множество

Доказательство. Пусть S — вершинное покрытие. Тогда у каждого ребра хотя бы один из концов лежит в S. Поэтому рёбер между вершинами из $V \setminus S$ нет. Пусть $V \setminus S$ — независимое множество. Тогда у каждого ребра хотя бы один из концов лежит вне этого множества
Значит, S — вершинное покрытие □

Связь минимального размера вершинного покрытия с числом независимости

Формулировка. Минимальный размер вершинного покрытия в графе G: $\tau(G) = n - \alpha(G)$, где n — количество вершин в графе, $\alpha(G)$ — число независимости

Доказательство. тут ачев, следует из связи между вершинными покрытиями и независимыми множествами □

Связь минимального размера вершинного покрытия с максимальным размером паросочетания

Максимальный размер паросочетания — $\mu(G)$

Формулировка. $\tau(G) \geqslant \mu(G)$ для любого графа G

Доказательство. Если P — паросочетание, то любое вершинное покрытие содержит хотя бы по одному концу каждого ребра паросочетания, а следовательно его размер не меньше размера паросочетания □

Пример

В графе-цикле C_5 никакие две вершины не покрывают все рёбра цикла C_5, но, тремя вершинами рёбра покрываются, значит $\tau(C_5) = 3$. Так как в паросочетании из трёх рёбер должно быть 6 вершин, то $\mu(C_5) = 2$, при этом паросочетание размера 2 легко находится □

2.18 Теорема Кёнига

Формулировка. В любом двудольном графе G выполняется равенство $\tau(G) = \mu(G)$

Доказательство. Неравенство $\tau(G) \geqslant \mu(G)$ доказано в 2.17. Докажем $\tau(G) \leqslant \mu(G)$ для двудольных графов с помощью теоремы Холла

В двудольном графе $G = (L, R, E)$ рассмотрим минимальное по размеру вершинное покрытие $X \cup Y, X \subseteq L, Y \subseteq R$. Определим два подграфа: $G' = (X, G(X) \setminus Y; E'), G'' = (Y, G(Y) \setminus X; E'')$

Проверим, что для этих графов выполняется условие Холла. Рассуждения для обоих графов аналогичны, приведём их для G'. Пусть $S \subseteq X$. Множество $(X \setminus S) \cup Y \cup G'(S)$ является вершинным покрытием в G : все рёбра, покрытые вершинами из S, покрыты также либо вершинами из Y, либо соседями вершин S в правой доле. Поскольку мы выбрали минимальное по размеру вершинное покрытие, $|G'(S)| \geqslant |S|$, что и означает выполнение условия Холла

По теореме Холла в G' есть паросочетание размера $|X|$, а в G'' есть паросочетание размера $|Y|$. Рёбра этих паросочетаний не совпадают по построению. Значит, объединение этих паросочетаний даёт паросочетание размера $|X| + |Y|$ в графе G. Таким образом, размер максимального паросочетания в G не меньше размера минимального вершинного покрытия □

2.19 Лемма про сумму исходящих и входящих степеней вершин. Свойства отношения достижимости в орграфе. Свойства отношения сильной связанности в орграфе

Лемма

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

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

Свойства отношения достижимости в орграфе

Формулировка. Свойства любого простого ориентированного графа и любых его вершин v_1, v_2, v_3:

1. *рефлексивность:* $(v, v) \in R$ — вершина достижима из самой себя

2. *транзитивность:* если $(v_1, v_2) \in R$ и $(v_2, v_3) \in R$, то $(v_1, v_3) \in R$

Доказательство. Так как v — путь (длины 0), вершина v связанная с самой собой

Если в графе есть пути $v_1u_1 \dots u_sv_2$ и $v_2w_1 \dots w_tv_3$ (то есть $(v_1, v_2) \in R$ и $(v_2, v_3) \in R$), то в этом графе есть также и путь $v_1u_1 \dots u_sv_2w_1 \dots w_tv_3$, то есть $(v_1, v_3) \in R$. Значит, вершина v_3 достижима из v_1 □

Свойства отношения сильной связанности в орграфе

Форулировка. Для любого ориентированного графа отношение сильной связанности *рефлексивно, симметрично и транзитивно*, то есть является отношением эквивалентности

Доказательство.

Рефлексивность: v_1 — путь в любом графе, поэтому v_1 сильно связана сама с собой

Транзитивность: если в графе есть пути из v_1 в v_2, из v_2 в v_1, из v_2 в v_3, из v_3 в v_2, то обязательно есть и пути из v_1 в v_3 (соединяем путь из v_1 в v_2 с путём из v_2 в v_3), а также из v_3 в v_1 (соединяем путь из v_3 в v_2 с путём из v_2 в v_1)

Симметричность: если $(u, v) \in C$, то по определению $(u, v) \in R$ и $(v, u) \in R$. Отсюда следует, что и $(v, u) \in C$ □

2.20 Критерий эйлеровости ориентированного и неоринтированного графа

Критерий—1

Формулировка. В ориентированном графе без изолированных вершин существует эйлеров цикл тогда и только тогда, когда граф сильно связен и у любой вершины входящая степень равна исходящей

Доказательство. Пусть эйлеров цикл в орграфе есть. Тогда он проходит через все вершины

(поскольку они имеют ненулевую степень), и по нему можно дойти от любой вершины до любой. Значит, орграф сильно связен

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

В обратную сторону. Пусть орграф сильно связен и в каждой вершине исходящая степень равна входящей. Выберем самый длинный простой в рёбрах путь, т.е. его длина не больше общего количества рёбер

$$\tau = (v_0, v_1, v_2, \ldots, v_{t-1}, v_t)$$

и докажем, что этот путь и является искомым циклом, то есть что $v_0 = v_t$ и этот путь содержит все рёбра орграфа

Если τ самый длинный, то добавить к нему ребро (v_t, v_{t+1}) невозможно. Значит, что все выходящие из v_t рёбра уже входят в τ. Это возможно, лишь если $v_0 = v_t$: если вершина v_t встречалась только внутри пути (пусть она входит k раз внутри пути и ещё раз в конце пути), то мы использовали $k+1$ входящих рёбер и k выходящих, и больше выходящих нет. Это противоречит равенству входящей и исходящей степени

Итак, мы имеем цикл, и осталось доказать, что в него входят все рёбра. Пусть из какой-то вершины v_i выходит ребро (v_i, v), не входящее в выбранный путь (цикл на самом деле). Тогда этот путь можно удлинить до простого в рёбрах пути

$$(v_{i+1}, \ldots, v_t = v_0, \ldots, v_i, v)$$

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

Значит, во всех вершинах цикла использованы все инцидентные им рёбра. Но орграф сильно связен, поэтому выбранный цикл содержит все рёбра этого графа и проходит через все вершины□

Критерий—2

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

Доказательство аналогично критерию—1. Пусть эйлеров цикл в графе есть. Он проходит по всем вершинам, значит граф связен. В каждую вершину эйлеров цикл k раз заходит и k раз выходит. Значит, степень вершины $k + k = 2\text{k}$ чётна

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

Этот цикл обязан содержать все рёбра графа, т.к. в противном случае его можно удлинить □

2.21 Лемма о существовании в ациклическом графе вершины с исходящей степенью 0 и вершины с входящей степенью 0. Равносильные определения ациклического графа

Лемма

Формулировка. В ациклическом орграфе есть вершина, из которой не выходит ни одного ребра, а также есть вершина, в которую не входит ни одно ребро

Доказательство. Выберем в этом орграфе простой путь максимальной длины, обозначим его вершины $v_0, v_1, \ldots, v_t$. Тогда исходящая степень вершины v_t равна 0: если в орграфе есть ребро $(v_t, x), x \notin \{v_0, \ldots, v_{t-1}\}$, то длина выбранного пути не максимальна: его можно продолжить до пути $v_0, \ldots, v_t, x$. Если же в орграфе есть ребро (v_t, v_i), то в этом орграфе есть цикл $v_i, \ldots, v_t, v_i$

Аналогично доказывается, что входящая степень вершины v_0 равна 0 □

Равносильные определения ациклического графа

Формулировка. Следующие свойства орграфа без петель равносильны:

1. Каждая компонента сильной связности состоит из одной вершины

2. Орграф ациклический

3. Вершины орграфа можно пронумеровать натуральными числами таким образом, чтобы все рёбра вели из вершины с меньшим номером в вершину с бóльшим

Доказательство. Доказываем утверждения теоремы по очереди

Доказательство (1) $\implies$ (2). Равносильно контрапозиции $\neg(2) \implies \neg(1)$. Раз в орграфе нет петель, в нём нет циклов длины 1. Если в орграфе есть цикл с $n > 1$ вершинами, то вершины этого цикла сильно связаны (из любой можно попасть в любую по циклу) — и тогда они попадут в одну компоненту связности

Доказательство (2) $\implies$ (1). Равносильно контрапозиции $\neg(1) \implies \neg(2)$. Если вершины $a \neq b$ сильно связаны, то существуют пути из a в b и из b в a. Соединением этих путей получается цикл длины > 0

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

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

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

Шаг индукции. Пусть (2) $\implies$ (3) выполняется для графов с $\leqslant n$ вершинами. Рассмотрим граф без циклов на $n+1$ вершине. Выберем вершину v_{n+1} исходящей степени 0, которая существует в таком орграфе по лемме из 2.21. Ей присвоим номер $n+1$. Удалив v_{n+1} и все входящие в неё рёбра, получим ациклический граф. (Циклы в нём были бы циклами и в исходном графе.) По предположению индукции его вершины можно пронумеровать числами от 1 до n с соблюдением условия. Объединяя эту нумерацию с номером $n+1$ вершины v_{n+1}, получаем искомую нумерацию. Шаг индукции доказан □

2.22 Теорема Ландау о турнирах

Формулировка. Неубывающая последовательность $\boldsymbol{d} = (d_1, d_2, \ldots, d_n)$ натуральных чисел является степенной последовательностью какого-то турнира, тогда и только тогда, когда

$$\boxed{D_k(\boldsymbol{d}) = \sum_{i=1}^{k} d_i \geqslant \binom{k}{2} \ \forall 1 \leqslant k \leqslant n, \quad D_n(\boldsymbol{d}) = \binom{n}{2}}$$

Доказательство. Пусть последовательность $s = (s_1, \ldots, s_n)$ удовлетворяет условиям баланса[1] Будем строить турнир, вершины которого числа от 1 до n. Каждой команде i выдадим s_i жетонов победителя, обозначим множество этих жетонов X_i. Все жетоны разные, так что $X_i \cap X_j = \varnothing$ при $i \neq j$. Из условия баланса следует, что жетонов столько же, сколько матчей, $\binom{n}{2}$

Предположим, что есть такая биекция $\{i, j\} \mapsto a_{ij}$ между матчами и жетонами, что $a_{ij} \in X_i \cup X_j$. Тогда объявим, что i выиграл у j, если выбран её жетон, то есть $a_{ij} \in X_i$. Получаем турнир, поскольку жетон для матча принадлежит одной из двух команд. И в этом трунире исходящая степень i равна $|X_i| = s_i$, так как каждый жетон использован ровно один раз

Докажем существование биекции между матчами и жетонами со свойством $a_{ij} \in X_i \cup X_j$. Используем теорема Холла. Построим двудольный граф $G = (L, R; E)$, в котором

[1] Поскольку среди любых k команд в турнире каждая пара играет между собой, то сумма исходящих степеней для этого множества команд не меньше $\binom{k}{2}$. Если $k = n$, то сумма исходящих степеней равна $\binom{n}{2}$

$$L = \{\{i,j\} : i \neq j, 1 \leqslant i,j \leqslant n\}, \quad \text{(множество матчей)},$$
$$R = \bigcup_{i=1}^{n} X_i, \quad \text{(множество жетонов)},$$
$$E = \{\{\{i,j\},a\} : a \in X_i \cup X_j\}, \quad \text{(выбираются только жетоны участниц)}.$$

Проверим для этого графа выполнение условия Холла. Пусть $S \subseteq L$ — некоторое множество пар чисел от 1 до n. Обозначим через V_S те числа, которые входят хотя бы в одну из этих пар, а через r — количество таких чисел. Тогда $|S|$ не превосходит максимального количества пар из r чисел, то есть $\binom{r}{2}$. С другой стороны, $G(S)$ — это объединение X_i по $i \in V_S$. Множества X_i не пересекаются, значит, мощность этого объединения равна сумме s_i по $i \in V_S$. Из условий баланса получаем

$$|S| \leqslant \binom{r}{2} \leqslant \sum_{i \in V_S} s_i = \sum_{i \in V_S} |X_i| = |G(S)|,$$

то есть условие Холла выполняется

Выберем совершенное паросочетание размера $\binom{n}{2}$ в двудольном графе G, которое существует по теореме Холла. Оно задаёт искомую биекцию: каждому матчу $\{i,j\}, i \neq j$, сопоставлен жетон $a_{ij} \in X_i \cup X_j$ □

2.23 Асимметричность строгого частичного порядка. Задание нестрогого частичного порядка через аксиомы

Асимметричность строгого частичного порядка

Формулировка. Если R — строгий частичный порядок, то aRb влечёт ложность bRa

Доказательство. Пусть одновременно истинны aRb и bRa. Тогда по транзитивности истинно aRa, противоречие □

Задание нестрогого частичного порядка через аксиомы

Формулировка. Бинарное отношение R на множетсве X является нестрогим частичным порядком, если и только если выполнены такие свойства:

- aRa (рефлексивность)
- aRb и bRa влечет $a = b$ (антисимметричность)
- aRb и bRc влечет aRc (транзитивность)

Доказательство. Пусть для отношения R выполнены необходимые свойства. Определим отношение $<$ по правилу

$$a < b \text{ равносильно } (aRb) \wedge (a \neq b)$$

и докажем, что это строгий частичный порядок. Из определения ясно, что тогда R — нестрогий частичный порядок, отвечающий порядку $<$

Антирефлексивность $<$ ясна из определения

Транзитивность: пусть $a < b$ и $b < c$, то есть (согласно определению порядка $<$) $aRb,\ a \neq b,\ bRc,\ b \neq c$. Из транзитивности R получаем aRc

Докажем $a \neq c$ от противного. Если $a = c$, то получаем aRb и bRa. Из антисимметричности отношения R следует $a = b$ в противоречии с предположением

В другую сторону. Пусть $<$ − отношение строгого частичного порядка. Проверим для $\leqslant$ указанные в формулировке утверждения свойства. Рефлексивность записана в определении $\leqslant$

Антисимметричность: предположим, что $a \leqslant b,\ b \leqslant a$, но $a \neq b$. Тогда по определению $\leqslant$ должно выполняться $a < b$ и $b < a$, что невозможно из асиметричности $<$ □

2.24 Отношение достижимости в ациклическом графе. Наличие рёбер между соседними элементами в ациклическом графе, задающем порядок

Отношение достижимости в ациклическом графе

Формулировка. Для любого ациклического графа $G = (V, E)$ отношение $\leqslant_G$ является отношением нестрогого частичного порядка

Доказательство. Проверим свойства частичного порядка для отношения $\leqslant_G$. Рефлексивность и транзитивность были доказаны в 2.19

Если $u \leqslant_G v$ и $v \leqslant_G u$, то по определению каждая из этих вершин достижима из другой, то есть вершины u, v сильно связаны. Но в ациклическом графе каждая компонента сильной связности состоит из одной вершины согласно равносильным определниям ациклическкого графа из 2.21. Поэтому $u = v$ □

Наличие рёбер между соседними элементами в ациклическом графе, задающем порядок

Формулировка. Пусть $\leqslant$ — частичный порядок на множестве P, G — ацкилический граф со множеством вершин P, также $\leqslant = \leqslant_G$ и x, y — соседние элементы в порядке $\leqslant$. Тогда (x, y) — ребро графа G

Доказательство. Из условия следует, что в G есть ориентированный путь с началом x и концом y. Для промежуточной вершины v этого пути (отличной от x, y) выполняется $x < v < y$. Так как x, y — соседние вершины, то промежуточных вершин нет и путь имеет длину 1, то есть (x, y) — ребро в графе G □

2.25 Ацикличность диаграммы Хассе. Задание конечного порядка диаграммой Хассе

Ацикличность диаграммы Хассе

Формулировка. Для всякого частичного порядка $<$ граф $H_<$ (=диаграмма Хассе) ациклический

Доказательство. В $H_<$ нет циклов длины 1 в силу антирефлексивности $<$. Если в $H_<$ есть цикл $(a_1 a_2 \dots a_n a_1)$ длины больше 1 , то по определению графа $H_<$ выполняются сравнения:

$$a_1 < a_2 < \dots < a_n < a_1$$

(соседние в цикле непосредственно предшествуют в порядке). По транзитивности получаем $a_1 < a_1$ и приходим к противоречию с антирефлексивностью □

Задание конечного порядка диаграммой Хассе

Формулировка. Если $<$ — частичный порядок на конечном множестве, то отношение $<$ совпадает с отношением $<_{H_<}$

Доказательство. Пусть $x < y$ в порядке P. Выберем цепь

$$x = v_0 < v_1 < \dots < v_{t-1} < v_t = y$$

максимально возможной длины (она существует, так как порядок конечный, а длина цепи не больше $|P|$). Тогда v_i и v_{i+1} соседние для любого $0 \leqslant i < t$: иначе можно было бы удлинить цепь. Поэтому y достижима из x в графе $H_<$ и потому $x <_{H_<} y$

В обратную сторону: если y достижима из x в графе $H_<$, то по транзитивности $x < y$ в порядке P □

2.26 Покоординатное произведение порядков является порядком, но свойство линейности может не сохраняться. Лексикографическое произведение порядков является порядком, свойство линейности сохраняется. Сумма порядков является порядком, свойство линейности сохраняется

Покоординатное произведение порядков является порядком, но свойство линейности может не сохраняться

Формулировка. Пусть P, Q — два частичных порядка. Тогда покоординатный порядок на декартовом произведении $P \times Q$ задаётся правилом:

$$(p_1, q_1) \leqslant (p_2, q_2) \text{ по определению означает } p_1 \leqslant_P p_2 \text{ и } q_1 \leqslant_Q q_2$$

Пример, что линейность не сохраняется. Порядок не линейный, т.к. например, векторы $(0, 2)$ и $(1, 1)$ несравнимы, а в линейном порядке любая пара элементов сравнима

Лексикографическое произведение порядков является порядком, свойство линейности сохраняется

Формулировка. Лексикографический порядок является отношением частичного порядка. Если P и Q — линейные порядки, тогда $P \times_{\text{lex}} Q$ также линейный

Доказательство. Используем строгий порядок. Антирефлексивность следует из антирефлексивности порядков P и Q

Транзитивность. Пусть $(p_1, q_1) \prec (p_2, q_2)$ и $(p_2, q_2) \prec (p_3, q_3)$. Из определения лексикографического порядка видим, что $p_1 \leqslant p_2 \leqslant p_3$

Если $p_1 < p_2 < p_3$, то $p_1 < p_3$ по транзитивности порядка P и потому $(p_1, q_1) \prec (p_3, q_3)$. Если $p_1 = p_2 < p_3$ или $p_1 < p_2 = p_3$, то также $p_1 < p_3$ и $(p_1, q_1) < (p_3, q_3)$. Если же $p_1 = p_2 = p_3$, то из определения лексикографического порядка получаем $q_1 < q_2 < q_3$, в силу транзитивности порядка Q и определения лексикографического порядка получаем $(p_1, q_1) \prec (p_3, q_3)$ □

2.27 Лексикографическое произведение и сумма порядков некоммутативны

Доказательство некоммутативности суммы порядков

Формулировка. $\mathbb{N} + \mathbb{Z}$ и $\mathbb{Z} + \mathbb{N}$ неизоморфны

Доказательство. Чтобы перейти к непересекающимся множествам, рассмотрим обычные целые числа и «штрихованные натуральные»: числа вида $0', 1', \ldots$ Сравниваются эти числа так же, как нештрихованные. Но теперь множества не пересекаются (штрих либо есть, либо его нет)

В $\mathbb{N} + \mathbb{Z}$ есть наименьший элемент — $0'$ меньше всех остальных элементов суммы порядков. А в $\mathbb{Z} + \mathbb{N}$ такого элемента нет (для каждого целого числа есть меньшее его). Но при изоморфизме наименьший элемент обязан переходить в наименьший □

Доказательство некоммутативности лексикографического произведения

Формулировка. $P = \mathbb{N} \times_{\text{lex}} \mathbb{Z}$ и $Q = \mathbb{Z} \times_{\text{lex}} \mathbb{N}$ неизоморфны

Доказательство. В порядке P предельных элементов[3] нет: предшественником (x, y) является $(x, y - 1)$. А в порядке Q предельные элементы есть, их бесконечно много. Любой элемент $(x, 0)$ является предельным. Если $(x', y') \prec (x, 0)$, то обязательно $x' < x$, т.к. при $x' = x$ должно выполняться $y' < 0$, а таких чисел среди натуральных нет. Но тогда

$$(x', y') \prec (x', y' + 1) \prec (x, 0),$$

то есть (x', y') не является непосредственным предшественником □

[3] Элемент x частичного порядка называется предельным, если у него нет непосредственного предшественника

2.28 Сохранение свойств порядка при изоморфизме. Изоморфность линейных порядков на конечных множествах одинакового размера

Сохранение свойств порядка при изоморфизме

Формулировка. Если $\varphi : P \to Q$ — изоморфизм порядков, то

а) наименьший (наибольший) переходит в наименьший (наибольший)

б) минимальный (максимальный) переходит в минимальный (максимальный)

в) каждый отрезок $[x, y] = \{z : x \leqslant z \leqslant y\}$ переходит в отрезок $[\varphi(x), \varphi(y)]$ той же мощности

г) предельный (непредельный) элемент переходит в предельный (непредельный)

Доказательство. Доказывать будем каждый пункт отдельно

Доказательство (а). Если a — наименьший в порядке P, то по определению $a \leqslant x$ для всех $x \in P$. Значит, $\varphi(a) \leqslant \varphi(x)$ для всех $x \in P$. Но φ—биекция, значит, $\varphi[P] = Q$. Поэтому $\varphi(a)$ - наименьший в порядке Q

Доказательство (б). Если a — минимальный в порядке P, то по определению $x < a$ ложно для всех $x \in P$. Значит, $\varphi(x) < \varphi(a)$ ложно для всех $x \in P$. Так как $\varphi[P] = Q$, то $\varphi(a)$ — минимальный в порядке Q

Сохранение наибольшего элемента и максимального элемента доказываются аналогично

Доказательство (в). Условие $x \leqslant z \leqslant y$ равносильно $\varphi(x) \leqslant \varphi(z) \leqslant \varphi(y)$

Значит, $\varphi([x, y]) \subseteq [\varphi(x), \varphi(y)]$. Докажем обратное включение. Пусть $\varphi(x) \leqslant q \leqslant \varphi(y)$. Тогда $x \leqslant \varphi^{-1}(q) \leqslant y$, то есть $q \in \varphi([x, y])$. Отсюда следует, что ограничение φ на $[x, y]$ является биекцией $\varphi([x, y]) \to [\varphi(x), \varphi(y)]$. Поэтому мощности обоих отрезков совпадают

Доказательство (г). От противного. Пусть $a \in P$ — предельный, а $\varphi(a) \in Q$ — нет. Обозначим через q непосредственного предшественника элемента $\varphi(a)$. Тогда $\varphi^{-1}(q) < a$. По определению предельного элемента найдётся такой b, что $\varphi^{-1}(q) < b < a$ и потому $q < \varphi(b) < \varphi(a)$. Это противоречит сделанному предположению, что $\varphi(a)$ предельный. Сохранение непредельных элементов доказывается аналогично □

Изоморфность линейных порядков на конечных множествах одинакового размера

Формулировка. Пусть $(X, \leqslant)$ и $(Y, \leqslant)$ — два линейных порядка на конечных множествах и $|X| = |Y|$, тогда *эти порядки изоморфны*

Доказательство. Индукция по числу элементов. База — один элемент в порядке — очевидна

Индуктивный переход. Предположим, что все линейные порядки с n элементами изоморфны. Рассмотрим два линейных порядка P и Q с $n + 1$ элементом. В них есть наименьшие элементы p_0, q_0. Действительно, строгий порядок на конечном множестве является ациклическим графом, в котором существуют вершина нулевой исходящей степени и вершина нулевой входящей степени (по лемме 2.21). Если порядок линейный, первая из этих вершин является наибольшим элементом, а вторая — наименьшим. Порядки на оставшихся элементах изоморфны по предположению индукции. Продолжая этот изоморфизм соответствием $p_0 \mapsto q_0$, получаем искомый изоморфизм порядков P и Q □

2.29 Теорема Дилуорса

Формулировка. Наибольший размер антицепи в конечном порядке равен наименьшему количеству цепей в разбиениях порядка на непересекающиеся цепи

Доказательство. Если порядок разбит на k непересекающихся цепей, то любая антицепь пересекается с каждой из цепей не более чем по одному элементу и в антицепи не больше k элементов. Значит, наибольший размер антицепи не превосходит наименьшего количества цепей в разбиениях порядка на непересекающиеся цепи. Осталось доказать, что равенство достигается. Надо указать такую антицепь размера N, что порядок разбивается на N непересекающихся цепей

Напомним, что размер любого вершинного покрытия не меньше размера любого паросочетания. Для двудольных графов теорема Кёнига утверждает, что равенство достигается

Применим теорему Кёнига

По строгому частичному порядку $(P, <)$ с n элементами построим двудольный граф G с долями P' и P'', в каждой из которых столько же вершин, сколько элементов в P. Зафиксируем биекции между P и P' и между P и P''. Элементу $x \in P$ соответствуют вершины x' в доле P' и x'' в доле P''. Рёбрами графа G являются пары $\{a', b''\}$, для которых $a < b$ в порядке $(P, <)$

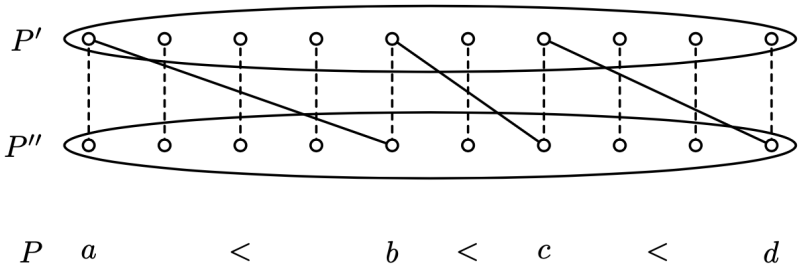
По теореме Кёнига в графе G есть паросочетание M и вершинное покрытие C одинакового размера, обозначим этот размер m. Обозначим через A те элементы порядка P, для которых соответствующие вершины не входят в C:

$$A = \{x \in P : (x' \notin C) \wedge (x'' \notin C)\}$$

В A не меньше $n - m$ элементов (возможно и больше, если $y' \in C$ и $y'' \in C$ для какого-то $y \in P$) и это антицепь в P: если $x, y \in A$ и $x < y$, то ребро $\{x', y''\}$ не покрыто вершинами из C

По паросочетанию M построим разбиение порядка на цепи. Для этого добавим к графу G диагональные рёбра вида $\{x', x''\}, x \in P$ (таких рёбер точно нет в $E(G)$, так как порядок строгий). Множество этих диагональных рёбер обозначим D. Получается граф $\widetilde{G}$. Рассмотрим подграф T графа $\widetilde{G}$, образованный всеми вершинами $(P' \cup P'')$ и рёбрами из $M \cup D$. Степени вершин в T равны 1 или 2, причём простых циклов длины больше 2 в нём нет: такой цикл давал бы множество элементов порядка, для которого $a_1 > a_2 > \cdots > a_s > a_1$, что невозможно из-за антирефлексивности. Значит, это лес. Каждой компоненте связности этого леса соответствует цепь в P (возможно, 1-элементная), см. рисунок ниже. Количество рёбер в лесу T равно $m + n$, а количество вершин равно $2n$. По критерию 2.4 цикломатическое число леса равно 0 (цикломатическое число — это сумма количества рёбер и компонент связности за вычетом числа вершин). Отсюда получаем, что количество компонент связности леса T равно $n - m$. Столько же цепей в разбиении на цепи, соответствующем паросочетанию M

Значит, что в A ровно $n - m$ элементов (их не больше, чем цепей в разбиении на цепи) □



2.30 Теорема про цепи/антицепи в бесконечном порядке

Формулировка. В каждом бесконечном порядке есть бесконечная цепь или бесконечная антицепь

Доказательство. Построим два бесконечных множества P и A следующим образом. На первом шаге выберем произвольный элемент порядка x_1. Если он сравним с бесконечным множеством W_1 элементов порядка, то полагаем $x_1 \in P$. В противном случае x_1 несравним с бесконечным множеством W_1 элементов порядка, полагаем $x_1 \in A$

На $(k+1)$-м шаге имеем множество $\{x_1, \ldots, x_k\}$, разбитое на множества P и A, и бесконечное множество W_k. При этом выполняются следующие свойства:
(1) каждый элемент $x_i \in P$ сравним со всеми элементами в W_k,
(2) каждый элемент $x_j \in A$ несравним со всеми элементами из W_k,
(3) P — цепь,
(4) A антицепь
Выберем произвольно элемент $x_{k+1} \in W_k$. Множество $W_{k+1} \subseteq W_k$ состоит либо из тех элементов, которые сравнимы с x_{k+1}, если таких элементов бесконечно много; либо, в противном случае, оно состоит из тех элементов, которые несравнимы с x_{k+1}. В первом случае помещаем x_{k+1} в P, во втором — в A

Инвариант цикла сохраняется. Множество W_{k+1} бесконечно по построению, как и свойства (1), (2). Поскольку $x_{k+1} \in W_k$, то если $x_{k+1} \in P$, то x_{k+1} сравнимо со всеми $x_i \in P$; а если $x_{k+1} \in A$,

то x_{k+1} несравнимо со всеми $x_i \in A$

Поскольку на каждом шаге множество W_{k+1} бесконечно, описанный процесс продолжается бесконечно долго. Получаем в итоге бесконечную последовательность $(x_1, \ldots, x_n, \ldots)$, элементы которой разбиты на два множества P и A. Правило построения гарантирует, что P—линейный порядок (все пары сравнимы), а A-антицепь (все пары несравнимы). Хотя бы одно из этих множеств бесконечно, откуда следует теорема □

2.31 Контрпример к "теореме Дилуорса с мощностями": пример бесконечного порядка, не разбивающегося на конечное число цепей и не имеющего бесконечной антицепи

Рассмотрим $\mathbb{N}^d$ с покоординатым сравнением:

$$x = (x_1, \ldots, x_d) \leqslant (y_1, \ldots, y_d) = y \quad \Leftrightarrow \quad x_i \leqslant y_i \text{ для всех } i$$

В этом порядке есть сколь угодно большие антицепи

Пример. Для любого $a \in \mathbb{N}$ множество

$$H_a = \left\{ x \in \mathbb{N}^d : \sum_{i=1}^{d} x_i = a \right\}$$

является антицепью. Действительно, если суммы координат двух различных векторов x, y равны, то одна из координат больше в векторе x, а какая-то другая больше в векторе y. При $d \geqslant 2$ и больших значениях a множество H_a велико: оно содержит $\binom{a+d-1}{d-1}$ векторов, что стремится к бесконечности при $a \to \infty$

Каждая цепь содержит не более одного элемента любой антицепи, поэтому порядок $(\mathbb{N}^d, \leqslant)$ невозможно разбить на конечное количество цепей. Разбиение на счётное количество цепей тривиально, поскольку $\mathbb{N}^d$ счётно

Однако бесконечных антицепей в этом порядке нет □

2.32 Соображения о симметрии в задачах на вероятность: примеры задач

Возьмем в качестве вероятностного пространства множество всех слов длины n в алфавите размера k

Задача про монотонный результат

Пусть $k = 3,\ n = 10$. Алфавит — множество $\{1, 2, \ldots, 10\}$. Исходы — последовательности длины 3 из различных букв алфавита

Определим вероятность наступления события «последовательность монотонно убывающая». Всего исходов $A_{10}^3 = 10 \cdot 9 \cdot 8 = 720$. Монотонно убывающие последовательности находятся во взаимно однозначном соответствии с 3-элементными подмножествами множества [10], поэтому их $\binom{10}{3} = \frac{720}{6} = 120$. Тогда вероятность равна $\frac{120}{720} = \frac{1}{6}$ □

Можно рассуждать и со стороны симметрии вероятностей. Любому благоприятному исходу abc соответствует 5 неблагоприятных исходов, получающихся перестановками букв a, b и c: acb, bac, bca, cab, cba. Таким образом, благоприятных исходов в 5 раз меньше, чем неблагоприятных, а, значит, вероятность интересующего нас события равна $\frac{1}{6}$ (и опять же, неважно, сколько исходов это событие содержит) □

Задача про сумму очков при подбрасывании нескольких игральных костей, которая делится на 3

Вероятностное пространство: последовательности (x_1, x_2, x_3) длины 3, состоящие из целых чисел в диапазоне от 1 до 6. Все исходы равновозможны

Найдём вероятность события «сумма чисел в последовательности делится на 3 ». Посчитать

число всех исходов нетрудно: их $6^3 = 216$. Воспользуемся методом разбиения на кусочки для определния числа благоприятных исходов

Среди 6 исходов $(x_1, x_2, 1), (x_1, x_2, 2), (x_1, x_2, 3), (x_1, x_2, 4), (x_1, x_2, 5), (x_1, x_2, 6)$ ровно 2 благоприятных

Поэтому доля благоприятных исходов будет равна $\frac{1}{3}$, это и составляет искомую вероятность □

Пример про вероятность вытянуть билет, который выучил, если идёшь первым или последним

Десять учеников сдают экзамен по десяти билетам. Ученики по очереди заходят в кабинет и вытягивают случайный билет из оставшихся (в частности, последний берет единственный оставшийся билет). Вася выучил только один билет. Какова вероятность, что Васе достанется билет, который он знает, если **a)** Вася тянет билет первым? **b)** Вася тянет билет последним?

В пункте (a) ясно, что Вася вытягивает случайно и равновозможно один из 10 билетов. Поэтому вероятность вытянуть благоприятный билет $\frac{1}{10}$

Чтобы ввести вероятностное пространство в пункте **(b)**, занумеруем студентов числами от 1 до 10 в порядке очереди. Билеты также занумеруем числами от 1 до 10, номер 10 присвоим тому билету, который Вася выучил. Тогда исходами будут перестановки чисел от 1 до 10. Все исходы равновозможны. Процесс последовательного выбора билетов как раз и представляется в виде дерева последовательного случайного выбора: сначала случайно и равновозможно выбирается билет, который берёт первый студент, затем случайно и равновозможно выбирается билет, который берёт второй студент и т.д.

Событие, вероятность которого нас интересует, — на 10-м месте стоит билет номер 10 (Вася идёт последним и знает только билет №10). Всего исходов 10!, а благоприятных — 9!. Искомая вероятность равна $\frac{9!}{10!} = \frac{1}{10}$ □

Не обязательно, но тоже на симметрию
Примером задачи на симметрию является п.2.37

Задача про лототрон
В лототроне 36 шаров, пронумерованных числами от 1 до 36 . Вытаскиваем два шара без возвращения. То есть вероятностное пространство - размещения из 36 по 2. Событие $A =$ «первый шар чётный», событие $B =$ «второй шар чётный». Независимы ли они?

Вместо размещений в качестве вероятностного пространства можно рассматривать любые упорядоченные пары чисел от 1 до 36 , но при этом нужно считать, что вероятности пар (a, a) равны 0 , а вероятности всех остальных пар одинаковы, то есть распределение неравномерное. При таком выборе вероятностного пространства мы опять получаем события $A = A' \times V, B = U \times B'$. Но теперь эти события не являются независимыми

Вероятности событий A и B равны, что ясно из симметрии. Значение этих вероятностей $-1/2$ (на нужное место выбираем один из 18 чётных шаров, на второе место ставим какой угодно из оставшихся)

Равенство

$$\mathbf{Pr}[A \cap B] = \mathbf{Pr}[B] \cdot \mathbf{Pr}[A \mid B] = \mathbf{Pr}[B] \cdot \mathbf{Pr}[A]$$

не выполняется:

$$\mathbf{Pr}[A \cap B] = \frac{18 \cdot 17}{36 \cdot 35} \neq \frac{18}{36} \cdot \frac{18}{36} = \mathbf{Pr}[A] \cdot \mathbf{Pr}[B],$$

поэтому события не являются независимыми. Вероятность того, что второй шар чётный при условии, что первый шар чётный, меньше вероятности, что второй шар чётный □

2.33 Задача про сумасшедшую бабку

Формулировка. В самолёт по очереди заходят 100 пассажиров. Первый садится на случайное место. Каждый следующий садится на своё место, если оно свободно, и на случайное свободное место, если его место занято. Какова вероятность того, что последний пассажир сядет на своё место?

Неформальное решение

Перед посадкой последнего пассажира может быть свободно либо его место, либо место первого пассажира. Если кто-то уже занял место первого пассажира раньше, то оставшиеся после этого пассажиры смогут сесть согласно купленным билетам, свободными останутся ровно их места. А значит, если место первого пассажира перед заходом последнего уже занято, то место последнего свободно и он на него и сядет

Получается, что все исходы принадлежат ровно одному из двух событий: «последний пассажир сел на своё место» и «последний пассажир сел на место первого пассажира». Значит, в сумме вероятности этих событий дают 1

Кроме того, вероятности этих событий одинаковы: если первый и последний пассажиры обменяются билетами, это не изменит рассадку, т.к. действия первого и последнего пассажиров не зависят от номера билета. Но события при этом переставляются: исходы, которые были в первом событии, попадают теперь во второе, и наоборот

Итак, вероятности двух указанных событий равны и в сумме дают 1. Поэтому каждая из них равна $1/2$ □

Формальное решение

Определим возможные исходы. Занумеруем пассажиров в порядке очереди числами от 1 до 100. Исходом будет рассадка пассажиров по местам, т.е. некоторая перестановка чисел от 1 до 100. Вероятности исходов неодинаковы. Их можно определить процессом последовательного случайного выбора: первый пассажир выбирает позицию в перестановке согласно равномерному распределению; i-й по очереди пассажир выбирает либо своё место, если оно свободно, с вероятностью 1 (вероятности остальных вариантов при этом равны 0), в противном случае он выбирает одно из свободных мест согласно равномерному распределению на них

Таким образом, мы получаем представление нашего вероятностного пространства в виде дерева. Чтобы определить вероятность исхода, нужно перемножить вероятности для всех выборов на пути из корня в соответствующий лист. Полученное распределение не равномерное. Например, любая перестановка, в которой первый пассажир сидит на своём месте, а какой-то пассажир — не на своём, имеет вероятность 0

Заметим, что вероятности перестановок-исходов зависят от раздачи билетов, т.е. соответствия между пассажирами и местами. Обозначим через π это соответствие: у первого пассажира билет на место $\pi(1)$, у второго — на место $\pi(2)$ и т.д. Мы фактически определили не одно распределение, а 100! распределений на одном и том же вероятностном пространстве. Одно такое распределение получается из другого перенумерацией мест, т.е. перестановкой исходов

Обозначим через G_π событие «последний пассажир сел на своё место», а через B_π — его дополнение, т.е. «последний пассажир сел на место первого». Каждый исход попадает в одно из этих событий, поэтому

$$\mathbf{Pr}_\pi[G_\pi] + \mathbf{Pr}_\pi[B_\pi] = 1$$

Индекс π указывает на распределение, задаваемое раздачей билетов π

Вероятности интересующих нас событий не зависят от раздачи билетов, то есть $\mathbf{Pr}_\pi[G_\pi] = \mathbf{Pr}_\sigma[G_\sigma]$ для любых π, σ: при перенумерации мест перестановки, в которых последний сидит на своём месте, переходят в точности в перестановки, в которых последний сидит на своём месте

Рассмотрим две раздачи билетов

$$\pi = (1, 2, \ldots, 99, 100), \sigma = (100, 2, \ldots, 99, 1)$$

(первый и последний обменялись билетами)

Для любой рассадки α выполняется равенство

$$\mathbf{Pr}_\pi[\alpha] = \mathbf{Pr}_\sigma[\alpha].$$

Действительно, при вычислении вероятности исхода α все числа на пути из корня дерева случайного выбора в лист α одинаковы в обоих случаях. Первое равно $1/100$ (т.к. первый пассажир

выбирает одно из 100 мест согласно равномерному распределению). Последнее равно 1 (т.к. у последнего нет выбора). Все промежуточные вероятности выборов равны, так как π и σ различаются только местами первого и последнего и это различие не меняет количества возможных выборов для i-го пассажира

Однако интересующие нас события переставляются: $\alpha \in G_\pi$ (то есть $a_{100} = 100$) тогда и только тогда, когда $\alpha \in B_\sigma$ (последний пассажир садится либо на своё место, либо на место первого). Поэтому

$$\mathbf{Pr}_\pi [G_\pi] = \mathbf{Pr}_\sigma [B_\sigma]$$

Поскольку $\mathbf{Pr}_\sigma [G_\sigma] = \mathbf{Pr}_\pi [G_\pi]$, то получаем $\mathbf{Pr}_\sigma [G_\sigma] = \mathbf{Pr}_\sigma [B_\sigma]$, то есть $\mathbf{Pr}_\sigma [G_\sigma] = 1/2$ □

2.34 Лемма про попарно несовместные события. Оценка объединения. Формула включений и исключений для вероятностей

Лемма

Формулировка. Если события A_i попарно несовемстны, то

$$\mathbf{Pr}\left[\bigcup_{i=1}^{n} A_i\right] = \sum_{i=1}^{n} \mathbf{Pr}[A_i]$$

Доказательство. Сумма вероятностей по объединению семейства попарно несовместных событий после перегруппировки слагаемых превращается в сумму по событиям вероятностей события:

$$\mathbf{Pr}\left[\bigcup_{i=1}^{n} A_i\right] = \sum_{x \in \bigcup_{i=1}^{n} A_i} \mathbf{Pr}[x] = \sum_{i=1}^{n} \sum_{x \in A_i} \mathbf{Pr}[x] = \sum_{i=1}^{n} \mathbf{Pr}\left[A_i\right]$$

При переходе от второй суммы к третьей возможно, что некоторые исходы попадут в несколько слагаемых с разными значениями i. Однако события несовместны, поэтому вероятности таких исходов равны 0, так что равенство выполняется □

Оценка объединения

Формулировка. Для любых событий $A_1, \ldots, A_n \subseteq U$ выполняется

$$\mathbf{Pr}\left[\bigcup_{i=1}^{n} A_i\right] \leqslant \sum_{i=1}^{n} \mathbf{Pr}[A_i]$$

Доказательство. И в левой, и в правой части стоит сумма вероятностей исходов

Каждый исход в левой сумме встречается и в правой (возможно, не один раз). Неравенство выполняется, так как вероятности неотрицательные □

Формула включений и исключений для вероятностей

Формулировка. Для всякой вероятностной модели и для произвольных множеств $A_1, \ldots, A_n \subseteq U$ верно

$$\mathbf{Pr}\left[A_1 \cup A_2 \cup \cdots \cup A_n\right] = \sum_i \mathbf{Pr}\left[A_i\right] - \sum_{i<j} \mathbf{Pr}\left[A_i \cap A_j\right] + \cdots =$$

$$= \sum_{\varnothing \neq S \subset \{1,2,\ldots,n\}} (-1)^{|S|+1} \mathbf{Pr}\left[\bigcap_{i \in S} A_i\right]$$

Доказательство. Снова используем индикаторные функции. Мы использовали такое равенство

$$\chi_A(x) = 1 - (1 - \chi_{A_1}(x))\,(1 - \chi_{A_2}(x)) \ldots (1 - \chi_{A_n}(x))\,,$$

которое переписывается как

$$\chi_A(x) = \sum_{S \neq \varnothing} (-1)^{|S|+1} \chi_{A_S}(x), \quad \text{где } A_S = \bigcap_{i \in S} A_i.$$

Вероятность A выражается как сумма по всему вероятностному пространству

$$\mathbf{Pr}[A] = \sum_{u \in U} \mathbf{Pr}[u]\chi_A(u)$$

(каждый благоприятный исход даёт вклад 1 в сумму, неблагоприятные исходы дают вклад 0). Для $A = A_1 \cup A_2 \cup \cdots \cup A_n$ подставим в эту сумму наше равенство и получим

$$\begin{aligned}\mathbf{Pr}[A] &= \sum_{x \in U} \mathbf{Pr}[x]\chi_A(x) = \sum_{x \in U} \mathbf{Pr}[x] \sum_{S \neq \varnothing} (-1)^{|S|+1}\chi_{A_S}(x) = \\ &= \sum_{S \neq \varnothing} (-1)^{|S|+1} \sum_{x \in U} \mathbf{Pr}[x]\chi_{A_S}(x) = \sum_{S \neq \varnothing} (-1)^{|S|+1}\mathbf{Pr}\left[A_S\right]\end{aligned}$$

это и есть формула включений и исключений □

2.35 Симметричность определения независимости событий. Формула полной вероятности. Формула Байеса

Симметричность определения независимости событий

Формулировка. Независимые события A и B, если $\boxed{\mathbf{Pr}[A] = \mathbf{Pr}[A|B]}$

Эквивалентное определение независимости событий: $\boxed{\mathbf{Pr}[A \cap B] = \mathbf{Pr}[B] \cdot \mathbf{Pr}[A|B] = \mathbf{Pr}[B] \cdot \mathbf{Pr}[A]}$

Остюда ясно, что отношение независимости событий *симметрично*, если вероятности событий положительные. Это определение применимо и к событиям нулевой вероятности

Формула полной вероятности

Формулировка. Пусть $B_1, \ldots, B_n$ - разбиение вероятностного пространства U, то есть $U = B_1 \cup \ldots \cup B_n$, где $B_i \cap B_j = \varnothing$ при $i \neq j$. Пусть также $\mathbf{Pr}\left[B_i\right] > 0$ для всякого i. Тогда для всякого события A

$$\boxed{\mathbf{Pr}[A] = \sum_{i=1}^{n} \mathbf{Pr}\left[A|B_i\right] \cdot \mathbf{Pr}\left[B_i\right]}$$

Доказательство. Прямое вычисление:

$$\mathbf{Pr}[A] = \sum_{i=1}^{n} \mathbf{Pr}\left[A \cap B_i\right] = \sum_{i=1}^{n} \mathbf{Pr}\left[A|B_i\right] \cdot \mathbf{Pr}\left[B_i\right]$$

где первое равенство получается по формуле сложения вероятностей несовместных событий (лемма из 2.34), а второе равенство — по определению условной вероятности □

Формула Байеса

Формулировка. Если вероятности событий A и B положительны, то

$$\boxed{\mathbf{Pr}[A|B] = \mathbf{Pr}[A] \cdot \frac{\mathbf{Pr}[B|A]}{\mathbf{Pr}[B]}}$$

Доказательство. Выразим вероятность события $A \cap B$ через условные вероятности двумя способами:

$$\mathbf{Pr}[A \cap B] = \mathbf{Pr}[B] \cdot \mathbf{Pr}[A|B] = \mathbf{Pr}[A] \cdot \mathbf{Pr}[B|A].$$

Формула Байеса получается из второго равенства делением обеих его частей на $\mathbf{Pr}[B]$ □

2.36 Парадокс Симпсона

Формулировка. Существует такое вероятностное пространство и события A, B, C, D, E, что $\mathbf{Pr}[A|B] < \mathbf{Pr}[A|D];\ \mathbf{Pr}[A|C] < \mathbf{Pr}[A|E];\ \mathbf{Pr}[A|B \cup C] > \mathbf{Pr}[A|D \cup E]$

Доказательство. Будем искать пример в предположении, что события B, C, D, E не пересекаются. Формула полной вероятности справедлива и для условных вероятностей: ограничим вероятностное распределение на событие-условие. Поэтому

$$\mathbf{Pr}[A|B \cup C] = \mathbf{Pr}[B|B \cup C] \cdot \mathbf{Pr}[A|B] + \mathbf{Pr}[C|B \cup C] \cdot \mathbf{Pr}[A|C],$$
$$\mathbf{Pr}[A|D \cup E] = \mathbf{Pr}[D|D \cup E] \cdot \mathbf{Pr}[A|D] + \mathbf{Pr}[E|D \cup E] \cdot \mathbf{Pr}[A|E].$$

Мы воспользовались такими равенствами

$$\mathbf{Pr}[A|B] = \mathbf{Pr}[A|B \cap (B \cup C)], \quad \mathbf{Pr}[A|C] = \mathbf{Pr}[A|C \cap (B \cup C)],$$
$$\mathbf{Pr}[A|D] = \mathbf{Pr}[A|D \cap (D \cup E)], \quad \mathbf{Pr}[A|E] = \mathbf{Pr}[A|E \cap (D \cup E)].$$

(события-условия в левых и правых частях этих равенств одинаковы)

Обозначим для краткости

$$p_1 = \mathbf{Pr}[A|B],\ p_2 = \mathbf{Pr}[A|D],\ p_3 = \mathbf{Pr}[A|C],\ p_4 = \mathbf{Pr}[A|E]; \alpha = \mathbf{Pr}[B|B \cup C],\ \beta = \mathbf{Pr}[D|D \cup E]$$

В таких обозначениях нужно удовлетворить неравенствам

$$p_1 < p_2, \quad p_3 < p_4, \quad \alpha p_1 + (1-\alpha)p_3 > \beta p_2 + (1-\beta)p_4$$

(заметим, что $\mathbf{Pr}[B|B \cup C] + \mathbf{Pr}[C|B \cup C] = 1$ и $\mathbf{Pr}[D|D \cup E] + \mathbf{Pr}[E|D \cup E] = 1$)

Множество

$$\{x : x = \lambda p + (1-\lambda)q, 0 \leqslant \lambda \leqslant 1\}$$

является отрезком $[p; q]$. Поэтому неравенства выполняются при подходящих α, β, если

$$p_3 < p_4 < p_1 < p_2$$

(отрезки $[p_3; p_1]$ и $[p_4; p_2]$ в таком случае пересекаются по внутренней точке) □

2.37 Вычисление вероятности события "два случайных k-элементных подмножества n-элементного множества не пересекаются". Асимптотика при $k \approx \sqrt{n}$

Из n-элементного множества выбираются случайно, равновозможно и независимо два k-элементных множества X и Y. Какова вероятность события «$X \cap Y = \varnothing$»?

Условие означает, что вероятностное пространство — пары (X, Y) k-элементных подмножеств n-элементного множества, вероятности всех исходов одинаковы

Для любых подмножеств A и B данного n-элементного множества количество исходов в событиях «$Y = A$» и «$Y = B$» одинаково, как и количество тех X, которые не пересекаются с Y. Поэтому вероятности условных событий «$X \cap Y = \varnothing | Y = A$» и «$X \cap Y = \varnothing | Y = B$» одинаковы

Из формулы полной вероятности получаем для любого множества $A, |A| = k$:

$$\mathbf{Pr}[X \cap Y = \varnothing] = \sum_{|S|=k} \mathbf{Pr}[X \cap Y = \varnothing \mid Y = S]\mathbf{Pr}[Y = S] =$$
$$= \mathbf{Pr}[X \cap Y = \varnothing \mid Y = A] \cdot \sum_{|S|=k} \mathbf{Pr}[Y = S] = \mathbf{Pr}[X \cap Y = \varnothing \mid Y = A]$$

Пусть $A = \{1, \ldots, k\}$. Вероятность выбрать k-элементное множество X, которое не содержит ни одного элемента из A, равна

$$\frac{\binom{n-k}{k}}{\binom{n}{k}}$$

(в числителе стоит количество k-элементных подмножеств в дополнении к A, а в знаменателе — количество k-элементных подмножеств в n-элементном множестве)

Преобразуем это выражение:

$$\frac{\binom{n-k}{k}}{\binom{n}{k}} = \left(1 - \frac{k}{n}\right) \cdot \left(1 - \frac{k}{n-1}\right) \cdot \ldots \cdot \left(1 - \frac{k}{n-k+1}\right) \leqslant \left(1 - \frac{k}{n}\right)^k$$

При больших n и $k \approx c\sqrt{n}$ последнее выражение оценивается как e^{-c^2}. Получаем, что весьма малые случайные подмножества большого конечного множества почти заведомо пересекаются □

2.38 Линейность математического ожидания. Вычисление математического ожидания случайной величины "размер пересечения двух случайных k-элементных подмножеств n-элементного множества"

Линейность математического ожидания

Формулировка. Пусть $f : U \to \mathbb{R}$ и $g : U \to \mathbb{R}$ — две случайные величины на одном и том же вероятностном пространстве с одним и тем же вероятностным распределением. Тогда

$$\mathbf{E}[f + g] = \mathbf{E}[f] + \mathbf{E}[g]$$

Доказательство. Запишем определение и перегруппируем слагаемые:

$$\mathbf{E}[f + g] = \sum_{x \in U} (f + g)(x)\mathbf{Pr}[x] = \sum_{x \in U} f(x)\mathbf{Pr}[x] + \sum_{x \in U} g(x)\mathbf{Pr}[x] = \mathbf{E}[f] + \mathbf{E}[g]$$

□

Пример вычисления мат.ожидания случайной величины

Пусть вероятностное пространство — пары k-элементных подмножеств n-элементного множества, распределение равномерное. Случайная величина $S = |X \cap Y|$ равна размеру пересечения этих подмножеств. Определим чему равно математическое ожидание S

Количество элементов в подмножестве равно сумме значений индикаторной функции этого множества по всем элементам множества. Поэтому случайная величина S разлагается в сумму случайных величин

$$s_1 + s_2 + \ldots + s_n, \quad \text{где } s_j(X, Y) = \begin{cases} 1, & \text{если } j \in X \cap Y \\ 0, & \text{иначе.} \end{cases}$$

Математическое ожидание случайной величины s_j выражается как

$$\mathbf{E}\left[s_j\right] = 1 \times \mathbf{Pr}\left[A_j\right] + 0 \times \mathbf{Pr}\left[\bar{A}_j\right] = \mathbf{Pr}\left[A_j\right]$$

где A_j — событие «$j \in X \cap Y$»

События «$j \in X$» и «$j \in Y$» независимы. Поэтому

$$\mathbf{Pr}\left[A_j\right] = \mathbf{Pr}[j \in X] \cdot \mathbf{Pr}[j \in Y] = \frac{\binom{n-1}{k-1}}{\binom{n}{k}} \cdot \frac{\binom{n-1}{k-1}}{\binom{n}{k}} = \frac{k^2}{n^2}$$

Окончательно получаем

$$\mathbf{E}[S] = \mathbf{E}\left[s_1 + s_2 + \ldots + s_n\right] = \sum_{j=1}^{n} \mathbf{E}\left[s_j\right] = n \cdot \frac{k^2}{n^2} = \frac{k^2}{n}$$

Таким образом, при $k \approx c\sqrt{n}$ имеем $\mathbf{E}[S] \approx c^2$ □

2.39 Линейность математического ожидания. Парадокс дней рождения

Линейность математического ожидания доказана в 2.38

Парадокс дней рождения

Рассмотрим n случайных людей и посмотрим на количество совпадений дней рождения у них, то есть на количество пар людей, имеющих день рождения в один день. Определим среднее значение этого числа

Уточним вопрос и упростим его. Предполагаем, что дни рождения у разных людей независимы, а в году 365 дней. То есть, вероятностное пространство: всюду определённые функции из n-элементного множества людей $\{x_1, \ldots, x_n\}$ в 365 элементное множество дней в году. Все исходы

равновозможные

Обозначим случайную величину, равную количеству пар людей с совпадающими днями рождения, через F. Нам требуется посчитать математическое ожидание случайной величины F

Обозначим через g_{ij} случайную величину, равную 1, если у людей x_i и x_j дни рождения совпадают, и равную 0 в противном случае. Тогда

$$F = \sum_{i<j} g_{ij}$$

Подсчитаем математическое ожидание случайной величины g_{ij}. Вероятность того, что у двух случайных людей дни рождения совпадают, равна $1/365$, так что с вероятностью $1/365$ случайная величина равна 1, и с вероятностью $(1 - 1/365)$ равна 0. Поэтому $\mathbf{E}[g_{ij}] = 1/365$ (для всякой пары i, j). Для математического ожидания F из линейности получаем

$$\mathbf{E}[F] = \mathbf{E}\left[\sum_{i<j} g_{ij}\right] = \sum_{i<j} \mathbf{E}[g_{ij}] = \sum_{i<j} \frac{1}{365} = \frac{n(n-1)}{2 \cdot 365}$$

Если число людей n больше 27, то $\mathbf{E}[F] > 1$, то есть стоит ожидать[4], что будет не меньше одного совпадения дней рождений □

2.40 Оценка среднего. Теорема о существовании в графе большого разреза

Оценка среднего

Формулировка. Пусть $\mathbf{E}[f] = C$ для какой-то случайной величины $f : U \to \mathbb{R}$. Тогда существует такой исход $u \in U$, что $f(u) \geqslant C$. Аналогично, существует и такой исход $u \in U$, что $f(u) \leqslant C$

Доказательство. Докажем от противного первое утверждение леммы, второе доказывается аналогично. Предположим, что утверждение неверно, а значит для всякого $u \in U$ верно $f(u) < C$

Тогда

$$\mathbf{E}[f] = \sum_{u \in U} \mathbf{Pr}[u] f(u) < \sum_{u \in U} \mathbf{Pr}[u] C = C,$$

противоречие □

Теорема о существовании в графе большого разреза

Формулировка. Всякий граф $G = (V, E)$ имеет разрез размера не меньше $|E|/2$

Доказательство. Рассмотрим случайный разрез графа G. Мы берём равномерное распределение на множестве всех разрезов. Разрез задаётся подмножеством $S \subseteq V$: такому подмножеству ставится в соответствие разрез $(S, V \setminus S)$. Всего подмножеств (=разрезов) 2^n, так что вероятность каждого разреза есть $1/2^n$. Для каждой пары вершин $x \neq y$ все четыре события «$x \in S, y \in S$», «$x \notin S, y \in S$, «$x \in S, y \notin S$», «$x \notin S, y \notin S$» имеют вероятность $1/4$[5]

Рассмотрим случайный разрез и случайную величину f, равную размеру разреза и посчитаем её математическое ожидание. Для этого разобьем случайную величину в сумму более простых случайных величин. Для всякого $e \in E$ рассмотрим случайную величину f_e, равную 1, если ребро e входит в разрез, и равную 0 в противном случае. Тогда $f = \sum_{e \in E} f_e$, а значит

$$\mathbf{E}[f] = \sum_{e \in E} \mathbf{E}[f_e]$$

Теперь найдем для случайной величины f_e математическое ожидание. Для всякого фиксированного ребра e вероятность, что оно попадёт в разрез равна $1/2$. А значит, $\mathbf{E}[f_e] = 1/2$ для всякого

[4] Если посчитать точно, то при $n = 28$ вероятность того, что будет не меньше одного совпадения дней рождения, равна ≈ 0.65; математическое ожидание числа совпадений ≈ 1.03

[5] Сопоставьте случайным множествам двоичные строки длины $|V|$, тогда интересующие нас события состоят в том, что на позициях x, y записаны конкретные значения

$e \in E$, откуда

$$\mathbf{E}[f] = \sum_{e \in E} 1/2 = |E|/2$$

Из этого следует, что есть конкретный разрез, содержащий не меньше $|E|/2$ рёбер □

2.41 Неравенство Маркова. Примеры применения

Формулировка. $\mathbf{Pr}[f \geqslant \alpha] \leqslant \dfrac{\mathbf{E}[f]}{\alpha}$

Доказательство. Докажем равносильное

$$\mathbf{E}[f] \geqslant \alpha \cdot \mathbf{Pr}[f \geqslant \alpha]$$

$$\mathbf{E}[f] = \sum_{x \in U} f(x)\mathbf{Pr}[x] = \sum_{x : f(x) \geqslant \alpha} f(x)\mathbf{Pr}[x] + \sum_{x : f(x) < \alpha} f(x)\mathbf{Pr}[x]$$

Заменим в первом слагаемом $f(x)$ на α, от этого сумма может лишь уменьшится. Во втором слагаемом заменим $f(x)$ на 0, от этого сумма также может лишь уменьшится. Получаем

$$\mathbf{E}[f] \geqslant \alpha \cdot \sum_{x : f(x) \geqslant \alpha} \mathbf{Pr}[x] + 0 \cdot \sum_{x : f(x) < \alpha} \mathbf{Pr}[x] = \alpha \cdot \mathbf{Pr}[f(x) \geqslant \alpha]$$

□

Пример—1

В лотерее на выигрыши уходит 40% от стоимости проданных билетов. Каждый билет стоит 100 рублей. Докажите, что вероятность выиграть хотя бы 5000 рублей меньше 1%
Обозначим через X случайную величину, равную выигранной сумме. Тогда из условий задачи получаем, что $\mathbf{E}[X] = 0,4 \cdot 100 = 40$. Из неравенства Маркова имеем

$$\mathbf{Pr}[X \geqslant 5000] \leqslant \frac{\mathbf{E}[X]}{5000} = \frac{40}{5000} = 0,008 < 0,01$$

□

Пример—2

Пусть есть такой алгоритм A, работающий за среднее время $O\left(n^2\right)$, где n — размер входных данных. Для наших практических целей хотелось бы, чтобы алгоритм всегда заканчивал свою работу за время $O\left(n^2\right)$. И пусть в $0,01\%$ случаев алгоритм будет выдавать неправильный ответ

Обозначим среднее время работы алгоритма A через T, и рассмотрим такой алгоритм: запускаем алгоритм A и ждём пока он сделает $10000 \cdot T$ шагов. Если алгоритм успел выдать ответ, прекрасно. Если нет, выдаём произвольный ответ. Идея в том, что алгоритм A с очень большой вероятностью закончит свою работу за $10000 \cdot T$ шагов. Действительно, обозначим через f (неотрицательную) случайную величину, равную времени работы алгоритма A. Тогда $\mathbf{E}[f] = T$. По неравенству Маркова получаем

$$\mathbf{Pr}[f > 10000 \cdot T] \leqslant \frac{T}{10000 \cdot T} = 1/10000$$

□

Время работы нового алгоритма — $O(n^2)$, а ошибка может произойти только если старый алгоритм работал дольше $10000 \cdot T$ шагов. По нашей оценке это происходит с вероятностью не больше 0.01%

2.42 Лемма о выражении дисперсии. Неравенство Чебышёва

Лемма

Формулировка. $\mathbf{D}[f] = \mathbf{E}[f^2] - \mathbf{E}[f]^2$

Доказательство. Пусть $C \in \mathbb{R}$, тогда $\mathbf{E}[C \cdot f] = C \cdot \mathbf{E}[f]$. По определению математического ожидания получаем:

$$\mathbf{E}[C \cdot f] = \sum_{x \in U} C \cdot f(x) = C \cdot \sum_{x \in U} f(x) = C \cdot \mathbf{E}[f].$$

Теперь распишем по определению $\mathbf{D}[f]$, воспользовавшись при этом линейностью математического ожидания (п. 2.38):

$$\mathbf{D}[f] = \mathbf{E}\left[(f - \mathbf{E}[f])^2\right] = \mathbf{E}\left[f^2 - 2\mathbf{E}[f] \cdot f + \mathbf{E}[f]^2\right] = \mathbf{E}\left[f^2\right] - \mathbf{E}[2\mathbf{E}[f] \cdot f] + \mathbf{E}\left[\mathbf{E}[f]^2\right] =$$
$$= \mathbf{E}\left[f^2\right] - 2\mathbf{E}[f] \cdot \mathbf{E}[f] + \mathbf{E}[f]^2 = \mathbf{E}\left[f^2\right] - \mathbf{E}[f]^2$$

□

Неравенство Чебышёва

Формулировка. $\mathbf{Pr}\left[|f - \mathbf{E}[f]| \geqslant \alpha\right] \leqslant \dfrac{\mathbf{D}[f]}{\alpha^2}$

Доказательство. Событие $|f - \mathbf{E}[f]| \geqslant \alpha$ совпадает с событием $|f - \mathbf{E}[f]|^2 \geqslant \alpha$. Применение неравенства Маркова к этому второму событию и даёт неравенство Чебышёва □

2.43 Типичный пример независимых случайных величин. Лемма о математическом ожидании произведения независимых случайных величин

Пример

Пусть множество исходов $U = A \times B$. Представим исходы как матричные элементы матрицы, строки которой индексированы множеством A, а столбцы-множеством B

Вероятность исхода (a, b) равна $p_a q_b$, где p — вероятностное распределение на A, а q — вероятностное распределение на B. Пусть величина $f(a, b)$ зависит только от строки a, а величина $g(a, b)$ — только от столбца b. Тогда эти величины независимы

Действительно, пусть $f^{-1}(x) = A_1 \times B, g^{-1}(y) = A \times B_1$. Тогда

$$\mathbf{Pr}[f = x] = \mathbf{Pr}\left[A_1\right], \quad \mathbf{Pr}[g = y] = \mathbf{Pr}\left[B_1\right]$$
$$\mathbf{Pr}[f = x \wedge g = y] = \sum_{a \in A_1} \sum_{b \in B_1} p_a q_b = \mathbf{Pr}\left[A_1\right] \cdot \mathbf{Pr}\left[B_1\right]$$

Лемма

Формулировка. Если f, g независимы, то $\mathbf{E}[f \cdot g] = \mathbf{E}[f] \cdot \mathbf{E}[g]$

Доказательство. Математическое ожидание случайной величины $f : U \to \mathbb{R}$ записывается в виде

$$\mathbf{E}[f] = \sum_{x \in f(U)} x \cdot \mathbf{Pr}[f = x]$$

(сгруппируем слагаемые с одинаковым значением f в определении математического ожидания). Поэтому

$$\mathbf{E}[f] \cdot \mathbf{E}[g] = \left(\sum_{x \in f[U]} x \cdot \mathbf{Pr}[f = x]\right) \cdot \left(\sum_{y \in g[U]} y \cdot \mathbf{Pr}[g = y]\right) =$$
$$= \sum_{x \in f[U]} \sum_{y \in g[U]} xy \cdot \mathbf{Pr}[f = x]\mathbf{Pr}[g = y] = \sum_{x \in f[U]} \sum_{y \in g[U]} xy \cdot \mathbf{Pr}[f = x \wedge g = y] =$$
$$= \sum_{z \in fg[U]} z\mathbf{Pr}[fg = z] = \mathbf{E}[fg]$$

Второе равенство — это раскрытие скобок, третье — применение определения независимых случайных величин, последнее получается группировкой одинаковых слагаемых □

2.44 Неравенство Хёфдинга–Чернова

Формулировка. Пусть $\varepsilon > 0$, тогда

$$\mathbf{Pr}\left[\left|X_n - \frac{n}{2}\right| > \varepsilon n\right] = \mathbf{Pr}\left[\left|\xi_n - \frac{1}{2} > \varepsilon\right|\right] < 2e^{-2\varepsilon^2 n}$$

Доказательство. Это неравенство получается как частный случай неравенства Маркова для подходящим образом подобранной функции от величины X_n.

Введём случайные величины $Y_n = 2X_n - n$. Если X_n равна сумме n случайных величин, принимающих независимо и равновероятно значения 0 и 1, то Y_n равна сумме n величин y_i, каждая из которых независимо принимает случайно и равновероятно значения -1 и $+1$

Теперь возьмём экспоненту от Y_n с удачным основанием (которое выберем позже). Определим случайную величину

$$Z_n = e^{\lambda Y_n} = \prod_i e^{\lambda y_i} = \prod_i z_i$$

Величины z_i независимы (это частный случай примера из 2.43). Поэтому мат. ожидание произведения равно произведению мат. ожиданий сомножителей:

$$\mathbf{E}\left[Z_n\right] = \prod_i \mathbf{E}\left[e^{\lambda y_i}\right] = \left(\frac{e^\lambda + e^{-\lambda}}{2}\right)^n = (\operatorname{ch}\lambda)^n$$

Интересующее нас событие $X_n - n/2 > \varepsilon n$ записывается через случайную величину Y_n как $Y_n > 2\varepsilon n$, а через величину Z_n как $Z_n > e^{2\lambda\varepsilon n}$

Применим неравенство Маркова к случайной величине Z_n:

$$\mathbf{Pr}\left[Z_n > e^{2\lambda\varepsilon n}\right] \leqslant \frac{\mathbf{E}\left[Z_n\right]}{e^{2\lambda\varepsilon n}} = \left(\frac{\operatorname{ch}\lambda}{e^{2\lambda\varepsilon}}\right)^n$$

Осталось выбрать λ, чтобы сделать дробь в основании степени поменьше. Для этого нужно неравенство

$$\operatorname{ch} x \leqslant e^{x^2/2}$$

Подставляя это неравенство, получаем при $\lambda = 2\varepsilon$

$$\mathbf{Pr}\left[Z_n > e^{2\lambda\varepsilon n}\right] \leqslant e^{\left(2\varepsilon^2 - 4\varepsilon^2\right)n}$$

□

Доказательство $\operatorname{ch} x \leqslant e^{x^2/2}$**.** Разложим экспоненту в ряд Тейлора:

$$e^x = \sum_{k=0}^{\infty} \frac{x^k}{k!}$$

Ряд для гиперболического косинуса получается отсюда почленным сложением рядов. Остаются только слагаемые в чётных степенях:

$$\operatorname{ch} x = \sum_{k=0}^{\infty} \frac{x^{2k}}{(2k)!}$$

Второй ряд получается подстановкой $x^2/2$ в ряд для экспоненты. Опять есть только слагаемые для чётных степеней:

$$e^{x^2/2} = \sum_{k=0}^{\infty} \frac{x^{2k}}{2^k k!}$$

Осталось заметить, что при каждом k выполняется

$$\frac{1}{(2k)!} \leqslant \frac{1}{2^k k!}$$

нужная формула получается почленным сравнением рядов □

2.45 Существование и единственность деления с остатком. Утверждение о корректности суммы, разности и произведения вычетов

Существование и единственность деления с остатком

Формулировка. Деление с остатком всегда возможно, причем единственным образом

Доказательство. *Единственность.* Если $a = bq + r = bq' + r'$, то $r - r' = b\,(q' - q)$ и потому $r - r'$ делится на b. Но оба числа r, r' находятся в интервале $0, 1, \ldots, b-1$, так что их разность (если из большего вычесть меньшее) не больше $b - 1$ и делится на b. Поэтому $r = r'$, откуда и $q = q'$

Существование для неотрицательных чисел докажем индукцией по a. Для $a = 0$ частное и остаток равны нулю: $0 = 0 \cdot b + 0$. Если $a = bq + r$, то $a + 1 = bq + (r + 1)$. При этом $r + 1 \leqslant b$, так как $r < b$. Если $r + 1 < b$, то для $a + 1$ получаем частное q и остаток $r + 1$. Если же $r + 1 = b$, то $a + 1 = bq + b = b(q + 1) + 0$, получаем частное $q + 1$ и остаток 0

Для отрицательных чисел: разделим $-a$ на b с остатком, получим $-a = bq + r$, $0 \leqslant r < b$. Тогда в случае $r = 0$ получаем $a = -bq$, а в случае $r > 0$ получаем

$$a = -bq - r = b(-q - 1) + (b - r)$$

в этом случае $0 < b - r < b$ □

Утверждение о корректности суммы, разности и произведения вычетов

Формулировка. Класс суммы, разности или произведения чисел зависит только от классов операндов

Доказательство. Если к одному из слагаемых прибавить kN, то к сумме тоже прибавится kN, аналогично для разности. С произведением: $(a + kN)b = ab + kbN \equiv ab \pmod N$

Поэтому для любых чисел, лежащих в одном классе вычетов, класс вычетов суммы, разности или произведения один и тот же □

2.46 Признаки делимости на 2, 3, 5, 9, 11

Делимость на 2. Число $a = \overline{a_k a_{k-1} \ldots a_0}$ делится на 2, если и только если последняя цифра а a_0 чётна

Доказательство. $a = a' \cdot 10 + a_0 = a' \cdot 5 \cdot 2 + a_0 \equiv a_0 \pmod 2$ □

Делимость на 3. Число $a = \overline{a_k a_{k-1} \ldots a_0}$ делится на 3, если и только если сумма его иифр делится на 3. Более того: число даёт тот же остаток при делении на 3, что и его сумма цифр

Доказательство. Так как $10 \equiv 1 \pmod 3$, то

$$a = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \cdots + a_1 \cdot 10 + a_0 \equiv a_k + a_{k-1} + \cdots + a_0 \pmod 3$$

□

Делимость на 5. Последняя цифра числа a должна делится на 5, так как $5 \mid 10$

Делимость на 9. Число делится на 9, если и только если сумма его цифр делится на 9 ; число даёт тот же остаток при делении на 9, что и его сумма цифр, поскольку $10 \equiv 1 \pmod 9$

Делимость на 11. Число $a = \overline{a_k a_{k-1} \dots a_0}$ делится на 11, если и только если знакопеременная сумма его иифр делится на 11. Более того: число $a = \overline{a_k a_{k-1} \dots a_0}$ даёт тот же остаток при делении на 11, что и число $a_0 - a_1 + a_2 - \dots + (-1)^k a_k$

2.47 Возможность деления на обратимый вычет. Критерий обратимости вычета

Возможность деления на обратимый вычет

Формулировка. Если вычет a обратим по модулю N, то уравнение $ax \equiv b \pmod N$ имеет в вычетах единственное решение при любом b

Доказательство. *Существование:* если вычет a обратим, то уравнение $ay \equiv 1 \pmod N$ имеет решение. Умножим обе части на b : $ayb \equiv b \pmod N$. Получаем, что yb — решение уравнения $ax \equiv b \pmod N$

Единственность: докажем, что сравнение $ax \equiv 1 \pmod N$ имеет единственное решение. Пусть $ax \equiv 1 \pmod N$ и $ay \equiv 1 \pmod N$. Тогда получаем $x \equiv (ya)x \equiv y(ax) \equiv y \pmod N$, то есть $x \equiv y \pmod N$

Таким образом, раз уравнение $ax \equiv 1 \pmod N$ имеет в вычетах единственное решение, можно обозначить это решение через a^{-1}. Докажем, что решение сравнения $ax \equiv b \pmod N$ также единственно. Умножим это сравнение на a^{-1} и получим, что $x \equiv ba^{-1} \pmod N$ □

Критерий обратимости вычета

Формулировка. Обратимыми по модулю N являются те и только те вычеты, которые взаимно просты с N

Доказательство. Пусть N и a не взаимно просты, то есть имеют общий положительный делитель $k > 1 : a = a'k, N = N'k$. Тогда из $ax \equiv 1 \pmod N$ получаем в обычных целых числах $ax = qN + 1$, откуда $(a'x - qN')\,k = 1$, что невозможно при $k > 1$

Теперь предположим, что N и a взаимно просты

Рассмотрим *множество кратных вычета* a, то есть множество $S_a = \{x : x \equiv ka \pmod N, k \in \mathbb{Z}\}$. По другому это множество можно определить как

$$S_a = \{x : x = ka + \ell N, k, \ell \in \mathbb{Z}\},$$

то есть как значения всевозможных целочисленных линейных комбинаций a и N. Легко понять, что множество S_a замкнуто относительно сложения, вычитания и умножения на целое число

Обозначим через d наименьшее положительное число в множестве S_a. Обратимость вычета в точности означает, что $d = 1$ (то есть, что найдётся кратное a, которое даёт остаток 1 по модулю N). Все кратные d входят в множество кратных a, так как из $d = ja + \ell N$ следует $kd = kja + k\ell N$ для любого целого k

Никаких других чисел в S_a нет. Предположим, что $x \in S_a,\ dy < x < d(y+1)$. Тогда в множество S_a входит также $r = x - dy$, который меньше d

В частности, так как N, a входят в S_a, то d делит N и d делит a. Поскольку a и N взаимно просты, $d = 1$ □

2.48 Свойства наибольшего общего делителя. Расширенный алгоритм Евклида. Последнее число в алгоритме Евклида является НОД изначальных чисел

Свойство—1

Формулировка. Любой общий делитель d' чисел a, N является делителем числа d

Доказательство. Пусть $N = N'd', a = a'd'$. Поскольку $d = xa + yN$, получаем в целых числах равенство $d = xa'd' + yN'd' = (xa' + yN')\,d'$ □

Свойство—2

Формулировка. НОД $(a, b) =$ НОД $(a - qb, b)$ для любого целого q

Доказательство. Если $d \mid a$ и $d \mid b$, то по свойствам делимости $d \mid (a - qb)$
И в обратную сторону: если $d \mid (a - qb)$ и $d \mid b$, то по свойствам делимости $d \mid ((a - qb) + qb)) = a$
Значит, множества общих делителей у этих пар чисел совпадают □

Расширенный алгоритм Евклида

Расширенный алгоритм Евклида рекуррентно вычисляет три такие последовательности чисел a_i, x_i, y_i, что для каждого i выполняется соотношение (инвариант цикла)

$$a_i = x_i a + y_i b \tag{2.48.1}$$

Начальные члены этих последовательностей:

$$\begin{aligned} a_0 = a, \quad x_0 = 1, \quad y_0 = 0 \\ a_1 = b, \quad x_1 = 0, \quad y_1 = 1, \end{aligned}$$

для них инвариант цикла (2.48.1) выполняется очевидным образом

Чтобы найти a_i, x_i, y_i при $i \geqslant 2$, делим a_{i-2} на a_{i-1} с остатком, это и есть a_i. Если $a_{i-1} = 0$, то алгоритм останавливается. В противном случае получаем $a_i = a_{i-2} - q_{i-1}a_{i-1}$. Остальные числа вычисляем по аналогичной формуле, используя найденное неполное частное q_{i-1}:

$$\begin{aligned} x_i = x_{i-2} - q_{i-1}x_{i-1}, \\ y_i = y_{i-2} - q_{i-1}y_{i-1} \end{aligned}$$

По индукции докажем, что инвариант цикла (2.48.1) выполняется на всех шагах алгоритма. База индукции проверена выше

Шаг индукции. Пусть (2.48.1) выполняется для $i - 2$ и $i - 1$. Тогда подставим эти равенства в выражение для a_i и перегруппируем слагаемые:

$$\begin{aligned} a_i = a_{i-2} - q_{i-1}a_{i-1} = x_{i-2}a + y_{i-2}b - q_{i-1}\left(x_{i-1}a + y_{i-1}b\right) = \\ = \left(x_{i-2} - q_{i-1}x_{i-1}\right)a + \left(y_{i-2} - q_{i-1}y_{i-1}\right)b = x_i a + y_i b \end{aligned}$$

Значит, (2.48.1) выполняется и для i

Последовательность a_i уменьшается, начиная со второго шага. Поэтому алгоритм рано или поздно остановится: в некоторый момент a_{k-1} будет делится на a_k, поэтому $a_{k+1} = 0$ и алгоритм остановится при попытке разделить с остатком на a_{k+1} □

Последнее число в алгоритме Евклида является НОД изначальных чисел

Формулировка. Последнее число a_k в алгоритме Евклида является НОД чисел a, b

доказательство. По индукции с помощью свойства—2 НОД проверяется, что

$$\text{НОД } (a_i, a_{i+1}) = \text{ НОД } (a, b), \quad i + 1 \leqslant k$$

База $i = 0$ следует из построения. Шаг индукции: так как $a_{i+1} = a_{i-1} - q_{i-1}a_i$, то по свойству—2 НОД $(a_i, a_{i+1}) =$ НОД (a_{i-1}, a_i). По предположению индукции второе число равно НОД (a, b)
Поскольку $a_k \mid a_{k-1}$, то $a_k =$ НОД $(a_k, a_{k-1}) =$ НОД (a, b) □

2.49 Утверждение о структуре решений линейного диофантова уравнения. Лемма о решениях однородного линейного диофантова уравнения. Общая формула

Увержение

Формулировка. Пусть $(\tilde{x}_0, \tilde{y}_0)$ — решение линейного диофантового уравнения. Тогда все решения этого уравнения имеют вид $(\tilde{x}_0 + x, \tilde{y}_0 + y)$, где пара (x, y) является решением однородного линейного уравнения

$$ax + by = 0 \tag{2.49.1}$$

Доказательство. По сути утверждается, что условия

$$ax + by = 0 \quad \text{и} \quad a\,(x_0 + x) + b\,(y_0 + y) = c$$

равносильны, если $ax_0 + by_0 = c$. Проверка равносильности состоит в применении равносильных преобразований к равенствам □

Лемма

Формулировка. Решениями однородного линейного уравнения (2.49.1) являются в точности такие пары (x, y), что

$$x = t \cdot \frac{b}{d}, y = -t \cdot \frac{a}{d}, \quad d = (a, b), t \in \mathbb{Z}$$

Доказательство. Разделив обе части уравнения на наибольший общий делитель (a, b), получим равносильное уравнение, коэффициенты которого взаимно просты. Поэтому достаточно решить уравнение $ax + by = 0$ со взаимно простыми коэффициентами

Если $(a, b) = 1$, то $au + bv = 1$ для некоторых $u, v \in \mathbb{Z}$. Умножим равенство $ax + by = 0$ на u :

$$u(ax + by) = uax + uby = (1 - bv)x + uby = x + b(uy - vx) = 0.$$

Поэтому $x = tb$ при некотором $t \in \mathbb{Z}$. Но тогда $by = -ax = -tab$ и $y = -ta$. С другой стороны, любая пара $(tb, -ta)$ является решением уравнения $ax + by = 0$ □

Общая формула

Формулировка. Пусть НОД $(a, b) \mid c$, $a\tilde{x}_0 + b\tilde{y}_0 = c$. Тогда множество решений линейного диофантового уравнения — это множество пар

$$(\tilde{x}_0 + tb/ \text{ НОД } (a, b), \tilde{y}_0 - ta/ \text{ НОД } (a, b)), \quad t \in \mathbb{Z}$$

2.50 Свойства простых чисел

Свойство—1

Формулировка. Для любого n найдётся такое k, что все числа $k, k + 1, \ldots, k + n$ составные

Доказательство. Возьмём $k = 2 + (n + 2)! = 2 + 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (n + 2)$. Тогда $k + i$ делится на $2 + i$ для любого i от 0 до n □

Свойство—2

Формулировка. Простых чисел бесконечно много

Доказательство. Любое целое число > 1 делится на простое

Доказательство полной индукцией (по всем меньшим числам) по величине числа. База $n = 2$ очевидна, а шаг индукции состоит в том, что либо число n простое, либо делится на какое-то меньшее число k. Применяя индуктивное предположение к числу k, получаем простой делитель для n

Теперь рассмотрим любое конечное множество простых чисел $p_1, p_2, \ldots, p_s$. Число $p_1 \cdot p_2 \cdot \ldots \cdot p_s + 1$ даёт остаток 1 от деления на $p_1, p_2, \ldots, p_s$. Значит, его простые делители (а они существуют, как мы показали выше) не принадлежат этому множеству □

2.51 Лемма о простом числе, делящем произведение двух чисел. Основная теорема арифметики

Лемма о простом числе, делящем произведение двух чисел

Формулировка. Если p — простое число, то из $p \mid xy$ следует, что $p \mid x$ или $p \mid y$

Доказательство. Заметим, что из простоты p следует, что либо $p \mid x$, либо НОД $(x, p) = 1$. Действительно, НОД (x, p) является делителем p, а значит, он равен либо p, либо 1

Если $p \mid x$, то всё доказано. Допустим, что НОД $(x, p) = 1$. Тогда из критерия обратимости вычета (2.47) следует, что x обратим. Пусть $xz \equiv 1 (\mathrm{mod}\ p)$. Тогда из $xy \equiv 0 (\mathrm{mod}\ p)$ следует $0 \equiv xyz \equiv 1 \cdot y = y (\mathrm{mod}\ p)$. Значит, $p \mid y$ □

Основная теорема арифметики

Формулировка. Всякое целое положительное число, большее 1, разлагается на простые множители единственным образом: любые два разложения отличаются только перестановкой сомножителей

Доказательство. *Существование разложения.* (Полная) индукция по величине числа. База $n = 2$ очевидна. Шаг индукции. Как мы уже проверяли в доказательстве бесконечности простых чисел, каждое число > 1 делится на простое. Если число n простое, то получилось разложение (из одного сомножителя). Иначе $n = k\ell, 1 < k, \ell < n$. Индуктивное предположение говорит, что у k и ℓ есть разложения на простые множители. Соединяя их, получим разложение n на простые

Единственность разложения. Пусть некоторое число имеет два различных разложения на простые множители (то есть, разложения отличаются не только порядком множителей). Приравняем эти разложения и сократим общие множители. По предположению сократится не всё и получаем равенство

$$p_1 \cdot p_2 \cdot \ldots \cdot p_r = q_1 \cdot q_2 \cdot \ldots \cdot q_s$$

здесь числа p_i отличаются от q_j (иначе возможно сокращение на общий множитель)

Левая часть делится на p_1. А правая часть равна произведению чисел, ни одно из которых не делится на p_1 : они ведь простые и p_1 среди них по предположению нет. Теперь применим лемму о простом числе, делящем произведение двух чисел и придём к противоречию □

2.52 Отношение делимости в терминах канонического разложения. Изоморфизм порядка делимости и покоординатного порядка на финитных последовательностях. Выражение НОД и НОК в терминах канонического разложения. Свойство НОД и НОК

Отношение делимости в терминах канонического разложения

Формулировка. Пусть числу n соответствует последовательность показателей (a_i), а числу k — (b_i). Тогда $k \mid n$ равносильно $b_i \leqslant a_i$ для всех i

Доказательство. В одну сторону: если $b_i \leqslant a_i$ для всех i, то

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_k^{a_k} \cdot \ldots = \left(p_1^{b_1} \cdot p_2^{b_2} \cdot \ldots \cdot p_k^{b_k} \cdot \ldots\right) \cdot \left(p_1^{a_1 - b_1} \cdot p_2^{a_2 - b_2} \cdot \ldots \cdot p_k^{a_k - b_k} \cdot \ldots\right)$$

и $k \mid n$

В другую сторону: если $k \mid n$, то из разложения n на простые возможно выделить разложение k на простые (перегруппируем множители). Поэтому $b_i \leqslant a_i$ для всех i □

Изоморфизм порядка делимости и покоординатного порядка на финитных последовательностях

Формулировка. Порядок делимости на целых положительных числах изоморфен покоординатному порядку на финитных последовательностях целых неотрицательных чисел

Выражение НОД и НИК в терминах канонического разложения

Формулировка. Пусть числу n соответствует последовательность показателей (a_i), а числу k — последовательность (b_i)

Тогда НОД (n,k) соответствует последовательность $(\min(a_i,b_i))$, а НОК(n,k) — последовательность $(\max(a_i,b_i))$

Доказательство. Пользуемся изоморфизмом порядков.

Если $x_i \leqslant a_i$ и $x_i \leqslant b_i$ для всех i, то $x_i \leqslant \min(a_i,b_i)$ для всех i. Поскольку $\min(a_i,b_i) \leqslant a_i$ и $\min(a_i,b_i) \leqslant b_i$ для всех i, эта последовательность и будет последовательностью показателей для НОД (n,k)

Точно так же рассуждаем про кратные, знак $\leqslant$ нужно всюду заменить на $\geqslant$, а min - на max $\square$

Свойство НОД и НОК

Формулировка. НОД $(n,k) \cdot$ НОК$(n,k) = kn$

Доказательство. Достаточно проверить, что $\max(a,b) + \min(a,b) = a + b$. Поскольку a, b входят в равенство симметрично, считаем без ограничения общности, что $a \leqslant b$. Тогда $\min(a,b) = a, \max(a,b) = b$ $\square$

2.53 Малая теорема Ферма. Функция Эйлера. Теорема Эйлера

Малая теорема Ферма

Формулировка. Если p — простое число, то

$$a^{p-1} \equiv 1 \pmod{p}$$

при любом a, не делящемся на p

Доказательство. На ненулевых вычетах по модулю p (это в точности вычеты $1, 2, \ldots, p-1$) рассмотрим функцию $f : x \mapsto ax$. Так как a не делится на p, вычет a обратим, и поэтому функция f — биекция (на обратимые вычеты можно делить). Значит, множество вычетов $a, 2a, \ldots, (p-1)a$ совпадает с множеством вычетов $1, 2, \ldots, p-1$ (но, возможно, теперь эти вычеты записаны в каком-то другом порядке). Перемножим и получим: $a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$. На множитель $(p-1)!$ можно сократить, так как он взаимно прост с p. Получаем, что $a^{p-1} \equiv 1 \pmod{p}$ $\square$

Функция Эйлера

Формулировка. Функция Эйлера $\varphi(n)$ равна количеству остатков по модулю n, взаимно простых с n

Пример. $\varphi(2) = 1, \varphi(3) = 2, \varphi(4) = 2$. Проверим последнее равенство. Остатки 0, 2 не взаимно просты с 4, а остатки 1, 3 — взаимно просты

Теорема Эйлера

Формулировка. Пусть $n > 1$ — произвольное целое положительное число, a взаимно просто с n. Тогда

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

Доказательство. Функция $x \mapsto ax$ является биекцией на множестве вычетов, взаимно простых с n. Если x и a взаимно просты с n, то и ax взаимно просто с n (это следует, например, из основной теоремы арифметики). Далее, если $ax \equiv ay \pmod{n}$, то, поделив на обратимый вычет a, получим $x \equiv y \pmod{n}$

Пусть $b_1, b_2, \ldots, b_{\varphi(n)}$ - все вычеты, взаимно простые с n, тогда $ab_1, ab_2, \ldots, ab_{\varphi(n)}$ - также все вычеты, взаимно простые с n (возможно, записанные в другом порядке). Перемножим и получим $a^{\varphi(n)} b_1 b_2 \ldots b_{\varphi(n)} \equiv b_1 b_2 \ldots b_{\varphi(n)} \pmod{n}$. Так как все $b_1, b_2, \ldots, b_{\varphi(n)}$, на них можно поделить (это обратимые вычеты). Получаем, что $a^{\varphi(n)} \equiv 1 \pmod{n}$ $\square$

2.54 Китайская теорема об остатках для двух и для любого числа сравнений

Для двух сравнений

Формулировка. Пусть числа и и v взаимно просты, и пусть а и b-любые целые числа. Тогда можно найти число x, для которого $x \equiv a (\mathrm{mod}\ u)$ и одновременно $x \equiv b (\mathrm{mod}\ v)$. В промежутке от 0 до $uv - 1$ такое число единственное

Доказательство. *Существование.* Поскольку НОД $(u, v) = 1$, существует такое $\widetilde{u}$, что $u \cdot \widetilde{u} \equiv 1 \pmod{v}$. Поэтому числа вида

$$x = a + u\tilde{u}(b - a) + kuv, \quad k \in \mathbb{Z},$$

удовлетворяют обоим сравнениям: $x \equiv a \pmod{u}$ и $x \equiv a + 1 \cdot (b - a) = b \pmod{v}$. Кроме того, можно так подобрать целое число k, чтобы x попало в промежуток от 0 до $uv - 1$

Единственность. Пусть $x \equiv a \pmod{u}, x \equiv b \pmod{v}$ и $y \equiv a \pmod{u}, y \equiv b \pmod{v}$, а также $0 \leqslant x, y < uv$. Тогда $(x - y) \equiv 0 \pmod{u}$ и $(x - y) \equiv 0 \pmod{v}$. То есть $x - y = ku = tv$. Но НОД $(u, v) = 1$, поэтому k кратно v, а t кратно u. Таким образом, $x - y$ делится на uv. В промежутке от 0 до $uv - 1$ такое число единственное — это 0. Поэтому $x = y$ □

Для любого числа сравнений

Формулировка. Пусть даны целые числа $u_1, \ldots, u_n$, любая пара которых взаимно проста. Пусть $a_1, \ldots, a_n$ — любые целые числа. Тогда можно найти число x, для которого $x \equiv a_i \pmod{u_i}$ для всех $i = 1, \ldots, n$. *В* промежутке от 0 до $u_1 \ldots u_n - 1$ такое число единственное

Доказательство. Доказывается индукцией по числу сравнений. Допустим, что теорема верна для n сравнений: существует и единственно число x в промежутке от 0 до $u_1 \ldots u_n - 1$, для которого $x \equiv a_i \pmod{u_i}$ (для всех $i = 1, \ldots, n$). Обозначим это число через b. Тогда $x \equiv b \pmod{u_1 \ldots u_n}$ равносильно $x \equiv a_i \pmod{u_i}$ (для всех $i = 1, \ldots, n$). Таким образом, система из $n+1$ сравнения вида $x \equiv a_i \pmod{u_i}$ (для всех $i = 1, \ldots, n+1$) свелась к системе из двух сравнений: $x \equiv b \pmod{u_1 \ldots u_n}$ и $x \equiv a_{n+1} \pmod{u_{n+1}}$. Для такой системы по китайской теореме для двух сравнений существует и единственно число в промежутке от 0 до $u_1 \ldots u_{n+1} - 1$, удовлетворяющее обоим сравнениям. Значит, это же число (и только оно из указанного промежутка) удовлетворяет системе из $n + 1$ сравнения $x \equiv a_i \pmod{u_i}$ (для всех $i = 1, \ldots, n + 1$) □

2.55 Мультипликативность функции Эйлера. Формула для функции Эйлера

Мультипликативность функции Эйлера

Формулировка. $\varphi(uv) = \varphi(u)\varphi(v)$, если u u v взаимно просты

Доказательство. Китайская теорема гарантирует, что для любой пары остатков a (по модулю u) и b (по модулю v) существует ровно один такой остаток c по модулю uv, что $c \equiv a (\mathrm{mod}\ u)$ и $c \equiv b (\mathrm{mod}\ v)$. То есть имеется биекция между парами остатков по модулям u, v и остатками по модулю их произведения

Докажем, что та же биекция устанавливает взаимно однозначное соответствие между вычетами по модулю uv, взаимно простыми с uv, и парами вычетов (a, b) по модулям u, v соответственно, которые взаимно просты с u, v соответственно

Если a взаимно просто с u, то и c взаимно просто с u (они лежат в одном классе вычетов по модулю u); аналогично, если b взаимно просто с v, то и c взаимно просто с v. Но тогда c взаимно просто просто с uv: все простые делители uv являются делителями либо u, либо v и потому не делят c; поэтому НОД$(c, uv) = 1$

Верно и обратное: если НОД$(c, uv) = 1$, то НОД$(a, u) = 1$ и НОД$(b, v) = 1$. Действительно, c и a лежат в одном классе вычетов по модулю u, а c и b лежат в одном классе вычетов по модулю v. Но все числа в одном классе вычетов либо взаимно просты с модулем, либо нет

Чтобы закончить доказательство, осталось заметить, что пар остатков, взаимно простых с модулями u, v, ровно $\varphi(u)\varphi(v)$ штук; остатков, взаимно простых с uv, ровно $\varphi(uv)$ штук. Построенная биекция доказывает, что эти числа равны □

Формула для функции Эйлера

Формулировка. Пусть $n = p_1^{a_1} p_2^{a_2} \cdot \ldots \cdot p_s^{a_s}, a_i > 0$, p_i — различные простые. Тогда

$$\varphi(n) = \prod_{i=1}^{s} \left(p_i^{a_i} - p_i^{a_i - 1}\right) = n \prod_{i=1}^{s} \left(1 - \frac{1}{p_i}\right)$$

Доказательство. Применяя мультипликативность функции Эйлера и формулу для функции Эйлера от степени простого, получаем:

$$\varphi(n) = \prod_{i=1}^{s} \varphi\left(p_i^{a_i}\right) = \prod_{i=1}^{s} \left(p_i^{a_i} - p_i^{a_i - 1}\right) = n \prod_{i=1}^{s} \left(1 - \frac{1}{p_i}\right)$$

□