13. Основы дискретной математики

13.1. Графы

Графом $G(V, E)$ называется совокупность двух множеств – непустого множества V (множества вершин) и множества E неупорядоченных пар различных элементов множества V (E – множество ребер): $G(V, E) = \langle V; E\rangle$, $V \neq \varnothing$, $E \subset V \times V$, $E = E^{-1}$. Число вершин графа G обозначим p, а число ребер – q, то есть $p := p(G) := |V|$, $q := q(G) := |E|$.

Пусть v_1, v_2 – вершины, $e = (v_1, v_2)$ – соединяющее их ребро. Тогда вершина v_1 и ребро e *инцидентны*, вершина v_2 и ребро e также инцидентны. Два ребра, инцидентные одной вершине, называются *смежными*; две вершины, инцидентные одному ребру, также называются смежными. Говорят, что два графа $G_1(V_1, E_1)$ и $G_2(V_2, E_2)$ изоморфны (обозначается $G_1 \sim G_2$), если существует биекция h: $V_1 \to V_2$, сохраняющая смежность:

$$e_1=(u, v) \in E_1 \Rightarrow e_2=(h(u), h(v)) \in E_2,\ e_2=(u, v) \in E_2 \Rightarrow e_1=(h^{-1}(u), h^{-1}(u)) \in E_1$$

Отношение изоморфизма графов есть отношение эквивалентности на множестве графов. Графы, как правило, рассматриваются с точностью до изоморфизма, то есть рассматриваются классы эквивалентности по отношению изоморфизма. Задачи, использующие изоморфизм графов, используются в информационной безопасности в протоколах так называемых «доказательств с нулевым разглашением». Граф, в котором каждая пара вершин смежна, называется *полным*. Полный граф с p вершинами обозначается K_p и имеет максимально возможное число ребер $q(K_p) = \frac{p(p-1)}{2}$. Полный подграф называется *кликой*.

13.2. Комбинаторика

Комбинаторные конфигурации

В широком смысле слово «комбинаторика» можно понимать как синоним термина «дискретная математика», то есть исследование дискретных конечных математических структур. На элементарном уровне с термином «комбинаторика» связывают набор известных формул, служащих для вычисления так называемых комбинаторных чисел. Вычисления на дискретных конечных математических структурах, которые часто называют комбинаторными вычислениями, требуют комбинаторного анализа для

установления свойств и получения оценок применимости используемых алгоритмов. В английском языке используют также термины «комбинаторная теория» и «комбинаторное искусство», куда принято включать такие основные разделы, как «перечислительная комбинаторика», занимающаяся задачами построения алгоритмов конструирования комбинаторных конфигураций, и «вычислительная комбинаторика», занимающаяся задачами вычисления количества возможных вариантов комбинаторных конфигураций.

Во многих практических случаях возникает необходимость подсчитать количество возможных комбинаций объектов, удовлетворяющих определенным условиям. Такие задачи и называются комбинаторными, или задачами вычислительной комбинаторики. Разнообразие комбинаторных задач не поддается исчерпывающему описанию, но среди них есть ряд особенно часто встречающихся, для которых известны способы подсчета. Явные формулы для комбинаторных чисел обычно используются при оценке размера пространства поиска в переборных задачах программирования и информационной безопасности.

Для формулировки и решения комбинаторных задач часто используются различные модели комбинаторных конфигураций на обыденном языке. Рассмотрим следующие две наиболее важные.

1. Дано m предметов. Их размещают по n ящикам так, чтобы выполнялись заданные ограничения. Сколькими способами это можно сделать?

2. Рассмотрим множество функций $F: X \to Y$, где $|X| = m$, $|Y| = n$, $X = \{1, \dots, m\}$.

Без ограничения общности можно считать, что

$Y = \{1, \dots, n\}$, $F = \langle F(1), \dots, F(m) \rangle$, $1 \le F(i) \le n$.

Сколько существует функций F, удовлетворяющих заданным ограничениям?

Часто соответствие конфигураций, описанных на «языке ящиков» и на «языке функций», очевидно, поэтому доказательство правильности способа подсчета (вывод формулы) можно провести на любом языке. Если сведéние одной модели к другой не очевидно, то необходимо обоснование. Таким рассуждением является, например, принцип Дирихле (он же – принцип ящиков, в англоязычной версии – принцип кроличьих нор): если кроликов (или зайцев) больше, чем ящиков, и все кролики сидят в ящиках, то существует такой ящик, в котором сидит более чем один кролик.

Число всех функций (при отсутствии ограничений), или число всех

возможных способов разместить m предметов по n ящикам называется, числом размещений и обозначается $U(n, m)$. $U(n, m) = n^m$.

Число инъективных функций, или число всех возможных способов разместить m предметов по n ящикам, не более чем по одному в ящик, называется числом размещений без повторений и обозначается $A(n, m)$ или $[n]_m$, или $(n)_m$. $A(n, m) = A_n^m = \frac{n!}{(n-m)!}$.

Число взаимно-однозначных функций, или биекций, или число перестановок n предметов, обозначается $P(n)$. $P(n) = n!$

Число строго монотонных функций, или число размещений m неразличимых предметов по n ящикам, не более чем по одному в ящик, то есть число способов выбрать из n ящиков m ящиков с предметами, называется числом сочетаний и обозначается $C(n, m)$ или C_n^m. $C(n, m) = \frac{n!}{m!(n-m)!}$.

Число монотонных функций, или число размещений m неразличимых предметов по n ящикам, называется числом сочетаний с повторениями и обозначается $V(n, m)$. $V(n, m) = C(m + n - 1, m)$.

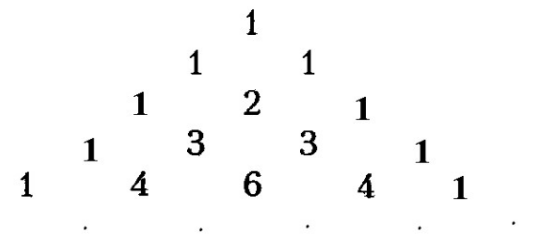
Практические комбинаторные задачи не всегда напрямую сводятся к известным комбинаторным конфигурациям. В этом случае применяют различные методы сведения одних комбинаторных конфигураций к другим. Таким, например, является принцип включения и исключения. Часто комбинаторная конфигурация является объединением других, число комбинаций в которых вычислить проще. В таком случае требуется уметь вычислять число комбинаций в объединении. В простых случаях формулы таковы: $|A \cap B| = |A| + |B| - |A \cap B|$; $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |A \cap C| + |A \cap B \cap C|$.

Следующая общая формула, известная как принцип включения и исключения, (иначе – принцип включений-исключений) позволяет вычислить мощность объединения множеств, если известны их мощности и мощности всех пересечений. $\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{i=1}^{n} |A_i| - \sum_{1 \le i < j \le n} |A_i \cap A_j| + \sum_{1 \le i < j < k \le n} |A_i \cap A_j \cap A_k| - \ldots + (-1)^{n-1} |A_1 \cap \ldots \cap A_n|$.

Основная формула для числа сочетаний позволяет получить следующие простые тождества.

1. $C(n, m) = C(n, n - m)$;
2. $C(n, m) = C(n - 1, m) + C(n - 1, m - 1)$;
3. $C(m, i)C(i, n) = C(m, n)C(m - n, i - n)$.

Из второго тождества вытекает эффективный способ рекуррентного вычисления значений биномиальных коэффициентов, который можно представить в графической форме, известной как треугольник Паскаля (на рисунке справа). В этом равнобедренном треугольнике каждое число (кроме единиц на боковых сторонах) является суммой двух чисел, стоящих над ним. Число сочетаний $C(n, m)$ находится в $(n + 1)$-м ряду на $(m + 1)$-м месте.



Число сочетаний $C(n,m)$ называются также биномиальными коэффициентами. Смысл этого названия устанавливается следующей теоремой, известной как формула бинома Ньютона: $(x + y)^m = \sum_{m=0}^{n} C(n,m)x^m y^{n-m}$.

Подстановки

Далее рассматриваются подстановки и перестановки, которые на самом деле являются равнообъемными понятиями. Применяя формулу для вычисления количества перестановок при решении практических задач, не следует забывать, что факториал – это очень быстро растущая функция, в частности, факториал растет быстрее экспоненты.

Взаимно-однозначная функция f: $X \to X$ называется подстановкой на X. Если множество X конечно ($|X| = n$), то, не ограничивая общности, можно считать, что $X = 1...n$. В этом случае подстановку f: $1..n \to 1..n$ удобно задавать таблицей из двух строк. В первой строке – значения аргументов, во второй – соответствующие значения функции.

Тождественная подстановка – это подстановка e, такая что $e(x) = x$. Обратная подстановка – это обратная функция, которая всегда существует, поскольку подстановка является биекцией. Таблицу обратной подстановки можно получить, если просто поменять местами строки таблицы исходной подстановки.

В таблице подстановки нижняя строка (значения функции) является перестановкой элементов верхней строки (значения аргумента). Если принять соглашение, что элементы верхней строки (аргументы) всегда располагаются в определенном порядке (например, по возрастанию), то верхнюю строку можно не указывать – подстановка определяется одной нижней строкой. Таким

образом, подстановки взаимно однозначно соответствуют перестановкам. Перестановку (и соответствующую ей подстановку) элементов 1, ... , n будем обозначать $\langle a_1, \dots, a_n\rangle$, где все a_i – различные числа из диапазона 1..n.

Операция суперпозиции (или композиции) преобразований $f\circ g$ (или просто fg)– это произведение преобразований f и g. Суперпозиция преобразований само является преобразованием и можно записать тождество $(f\circ g)(x)=g(f(x))$. Оно означает, что для вычисления суперпозиции преобразований, сначала находится значение функции f от аргумента x, затем находим значение функции g от $f(x)$ как от аргумента.

Пример. Пусть $f=\begin{pmatrix}1&2&3&4&5\\5&3&4&1&2\end{pmatrix}$, $g=\begin{pmatrix}1&2&3&4&5\\4&1&2&5&3\end{pmatrix}$. Тогда

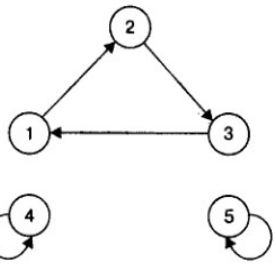
$$f\circ g=\begin{pmatrix}1&2&3&4&5\\5&3&4&1&2\end{pmatrix}\circ\begin{pmatrix}1&2&3&4&5\\4&1&2&5&3\end{pmatrix}=\begin{pmatrix}1&2&3&4&5\\3&2&5&4&1\end{pmatrix},$$ с учетом свойства транзитивности. Это проиллюстрировано на рисунке справа: стрелками показаны отображения функцией одного элемента в другой, жирными выделены первая и вторая строка итогового преобразования, являющегося суперпозицией:

$$f=\begin{pmatrix}\mathbf{1}&\mathbf{2}&\mathbf{3}&\mathbf{4}&\mathbf{5}\\\downarrow&\downarrow&\downarrow&\downarrow&\downarrow\\5&3&4&1&2\end{pmatrix}$$

$$g=\begin{pmatrix}1&2&3&4&5\\\downarrow&\downarrow&\downarrow&\downarrow&\downarrow\\\mathbf{4}&\mathbf{1}&\mathbf{2}&\mathbf{5}&\mathbf{3}\end{pmatrix}$$

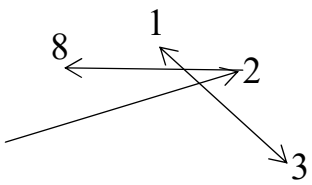
Цикл – это последовательность элементов x_0, ... , x_k, такая что $f(x_i)=\begin{cases}x_{i+1}, & 0\le i<k,\\ x_0, & i=k.\end{cases}$ Из графического представления подстановки наглядно видно происхождение термина «цикл».

Пример. Для подстановки $f=\begin{vmatrix}1&2&3&4&5\\2&3&1&4&5\end{vmatrix}$ определить цикличность.

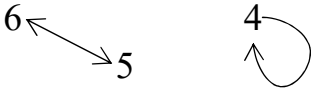


Решение. Графическое представление подстановки $f=\begin{vmatrix}1&2&3&4&5\\2&3&1&4&5\end{vmatrix}$ представлено на рисунке справа, цикличность из него очевидна.

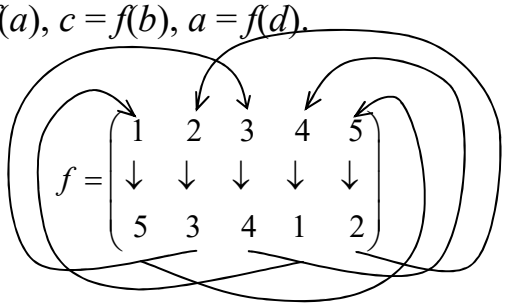
Пример. Доказать, что $u=\begin{bmatrix}1&2&3&4&5&6&7&8\\3&8&1&4&6&5&2&7\end{bmatrix}=(13)(287)(65)(4)$.



Решение. Графическое представление этой подстановки представлено на рисунке слева, цикличность из него очевидна.



Любую подстановку можно представить в виде произведения циклов. В цикле последующий элемент является функцией предыдущего элемента, а первый элемент в цикле – последнего. Показать на примере 2-3-1-4-5. $f = (a, b, c \ldots, d)\cdot\ldots\cdot(e, f, \ldots, g)$. Для первого цикла, например, справедливы соотношения $b = f(a)$, $c = f(b)$, $a = f(d)$.



$f = (1 \to 5 \to 2 \to 3 \to 4)$ или $f = (1\ 5\ 2\ 3\ 4)$

Любой циклический сдвиг влево в цикле будет правильным, поэтому $f = (1\ 5\ 2\ 3\ 4) = (2\ 3\ 4\ 1\ 5)$.

Цикл минимального периода длины 1 называется неподвижной точкой. При выписывании подстановки в виде циклов неподвижные точки можно опускать.

Пример. $f \circ g = (1\ 3\ 5)(2)(4) = (1\ 3\ 5)$.

Цикл длины 2 называется транспозицией.

Если в перестановке $f = \langle a_1, \ldots, a_n \rangle$ для элементов a_i и a_j имеет место неравенство $a_i > a_j$ при $i < j$, то пара (a_i, a_j) называется инверсией. Обозначим $I(f)$ – число инверсий в перестановке f.

Теорема. Произвольную подстановку f можно представить в виде суперпозиции $I(f)$ транспозиций соседних элементов.

Следствие. Всякая сортировка может быть выполнена перестановкой соседних элементов.

Любая транспозиция имеет вид $\tau = (j\ i)$ и оставляет на месте все символы, отличные от j, i.

Теорема. Любая перестановка $\tau \in S_n$ является произведением транспозиций. Доказательством является то, что любой цикл можно записать в виде транспозиций как $(1\ 2 \ldots\ l-1\ l) = (1\ l)(1\ l-1)\ldots(1\ 3)(1\ 2)$.

Таким образом, множество подстановок образует группу относительно операции суперпозиции. Эта группа – S_n – называется симметрической группой степени n. Порядок группы S_n равен $|S_n| = (S_n : e) = n!$

Единственности записи перестановки через транспозиции нет. Неединственность разложения видна из равенства $\sigma\tau^2 = \sigma$ для любых транспозиций σ и τ. Тем не менее, один инвариант разложения перестановки

через транспозиции все-таки существует. Пусть $\sigma \in S_n$ и $f(X_1, \ldots, X_n)$ – функция от любых n аргументов. Полагаем: $(\sigma \circ f) = (X_1, \ldots X_n) = f(X_{\sigma\text{-}1(1)}, \ldots X_{\sigma\text{-}1(n)})$.

Говорят, что функция $g = \sigma \circ f$ получается действием σ на f. Функция f называется кососимметрической, если $\sigma \circ f = -f$ для любой транспозиции $\sigma \in S_n$, то есть если α, β – любые перестановки из S_n. Тогда $(\alpha\beta) \circ f = \alpha \circ (\beta \circ f)$.

Теорема. Пусть π – перестановка из S_n, $\pi = \tau_1\tau_2\ldots\tau_k$ – какое-нибудь разложение π в произведение транспозиций. Тогда число $\varepsilon_\pi = (-1)^k$, называемое четностью π (иначе сигнатурой или знаком π) полностью определяется перестановкой π и не зависит от способа разложения, т. е. четность целого числа k для данной перестановки π всегда одна и та же. Кроме того, $\varepsilon_{\alpha\beta} = \varepsilon_\alpha\varepsilon_\beta$ для всех $\alpha, \beta \in S_n$.

Перестановка $\beta \in S_n$ называется четной, если $\varepsilon_\beta = 1$, и нечетной, если $\varepsilon_\beta = -1$. Из определения четной и нечетной перестановки следует, что все транспозиции – нечетные перестановки. В связи с этим справедливо следующее утверждение. Все четные перестановки степени n образуют подгруппу $A_n \in S_n$ порядка $n!/2$ (она называется знакопеременной группой степени n).

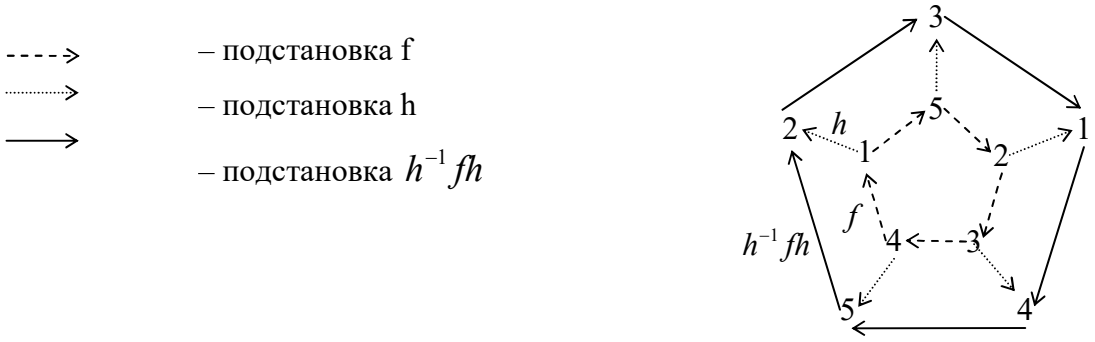
Роль изоморфизма в теории групп иллюстрирует теорема Кэли: Любая конечная группа порядка n изоморфна некоторой подгруппе симметрической группы S_n. Теорема Кэли, несмотря на свою простоту, имеет большое значение в теории групп. Она выделяет некий универсальный объект (семейство $\{S_n | n = 1, 2, \ldots\}$ симметрических групп) – вместилище всех конечных групп, рассматриваемых с точностью до изоморфизма. Фраза «с точностью до изоморфизма» отражает сущность не только теории групп, стремящейся объединить в один класс все изоморфные группы, но математики в целом, которая без таких обобщений была бы лишена смысла.

Важным понятием теории групп, имеющим применения в защите информации и современной криптографии, является понятие сопряжения.

Сопряжение элемента f элементом h – это подстановка вида $h^{-1}fh$

Пример. Если $h=\begin{pmatrix}1&2&3&4&5\\2&1&4&5&3\end{pmatrix}$, то для f=(1 5 2 3 4) имеем

$$h^{-1}fh=\begin{pmatrix}1&2&3&4&5\\2&1&5&3&4\end{pmatrix}\begin{pmatrix}1&2&3&4&5\\5&3&4&1&2\end{pmatrix}\begin{pmatrix}1&2&3&4&5\\2&1&4&5&3\end{pmatrix}=\begin{pmatrix}1&2&3&4&5\\4&3&1&5&2\end{pmatrix}=(1\quad 4\quad 5\quad 2\quad 3)$$



На рисунке сверху это наглядно показано. Возьмем для примера переход $h^{-1}fh$: 5→2 преобразованием: он получается переходом h–1: 5→4 (обратить стрелку), f: 4→1, h: 1→2.

Нормальной называется подгруппа, замкнутая относительно сопряжений. Такая подгруппа также называется нормальным делителем группы.

Неединичную группу (G, ·) не имеющую собственных нормальных делителей, называют простой.

Обратное преобразование $f^1(x)$.

Для подстановки всегда существует обратная функция в силу биективности. Таблицу обратного преобразования можно получить, если просто поменять местами строки таблицы исходного и отсортировать верхнюю строку по возрастанию (что быстро делается в Excel). Пример, на графе – стрелка в другую сторону.

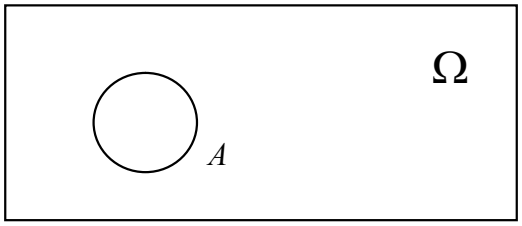
Обратная к операции суперпозиции преобразований операция называется делением правым или левым u/v или $v\backslash u$. Ее можно представить через суперпозицию с обратным элементом: $u/v = u\circ v^{-1}$; $v\backslash u = v^{-1}\circ u$. u и v называются сопряженными если $\exists\, z$: $u = z^{-1}\circ v \circ z$

13.3. Случайные события. Алгебра событий.

Под *испытанием (опытом)* будем понимать осуществление определенного комплекса условий. *Событием (явлением)* назовем любой факт, который может произойти или не произойти в результате испытания. Событие называется *случайным,* если в результате данного испытания оно может произойти, но может и не произойти. Как крайние случаи, событие называется *достоверным,* если в результате данного испытания оно обязательно произойдет и *невозможным,* если в результате данного испытания оно произойти не может. Достоверное событие иначе называются *единственно возможным.* События обозначаются заглавными буквами латинского алфавита A, B, C, … когда надо – с индексами. Достоверное событие обозначается Ω, а невозможное – знаком пустого множества $\emptyset$.

Рассмотрим в качестве примера урну (ящик) с белыми и черными шарами, из которой вынимают один шар. Это и есть испытание (опыт). В результате испытания может появиться одно из двух событий: "вынут белый шар", "вынут черный шар". Если шар вынимают наудачу, оба события ("вынут белый шар" и "вынут черный шар") являются случайными. Если в урне находятся только белые шары, то событие "вынут белый шар" является достоверным, а событие "вынут черный шар" – невозможным.

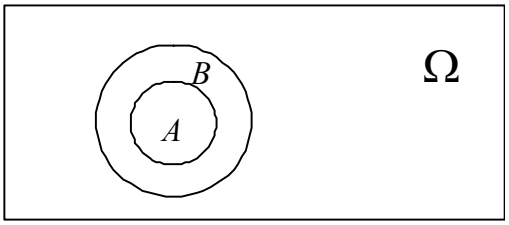
Среди случайных событий выделяются, наряду с невозможными и единственно возможными, события несовместные и равновозможные. События называются *несовместными*, если появление одного из них исключает появление других событий в одном и том же опыте. События называются *равновозможными*, если имеются основания считать, что ни одно из этих событий не является более возможным, чем другое.



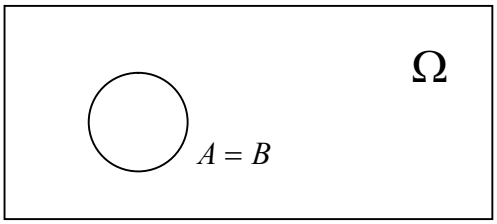
Множество, которому принадлежат все элементарные (неделимые) события, называется *универсальным множеством* и обозначается через Ω. Для геометрического изображения универсального множества будем использовать прямоугольник. Каждая точка множества Ω есть элементарное (неделимое) событие. Составное

событие A будем обозначать в виде круга, который называется *кругом Эйлера*. Изображение на плоскости множества Ω и кругов Эйлера называется *схемой Венна*.

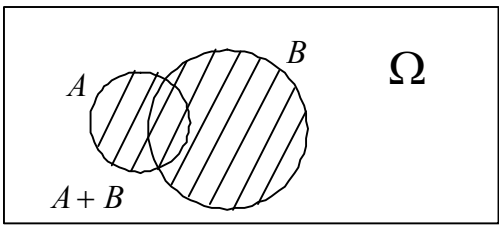
С помощью этой схемы рассмотрим операции над событиями.



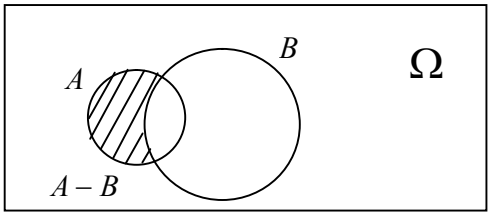
Если при каждом испытании, в результате которого происходит событие A, происходит и событие B, то событие A *влечет* за собой событие B. Символически это можно записать так: $A \subset B$ или $B \supset A$, т.е. множество A в этом случае оказывается подмножеством множества B.



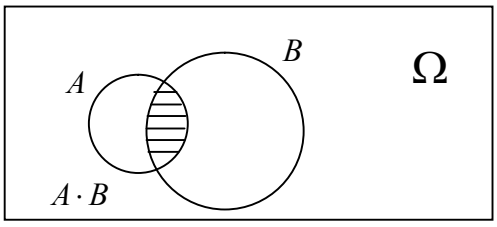
Если при каждом испытании оба события происходят или не происходят, то такие события называются *эквивалентными* или *равносильными* и могут заменять друг друга, т.е. если $A \subseteq B$ и $B \subseteq A$, то A~B или $A = B$.



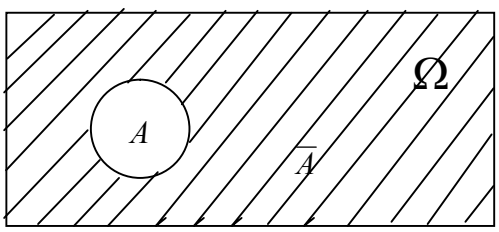
Событие, заключающееся в наступлении хотя бы одного из событий A или B, называется *суммой* или *объединением* событий и обозначается $A + B$ или $A \cup B$.



Событие, состоящее в том, что произойдет событие A, но не произойдет событие B, называется *разностью* событий A и B и обозначается $A - B$ или $A \setminus B$.



Событие, состоящее в совместном наступлении событий A и B в данном опыте, называется *произведением* или *пересечением* событий и обозначается $A \cdot B$ или $A \cap B$.



Событие, состоящее в ненаступлении события A, называется *противоположным событием* и обозначается $\overline{A}$.

Какими бы ни были события A, B, C введенные над событиями операции подчиняются следующим законам:

$\overline{\overline{A}} = A$; $A + A = A$; $A \cdot A = A$; $A + \overline{A} = \Omega$; $A \cdot \overline{A} = \varnothing$;

$A \cdot \Omega = A$; $A + \varnothing = A$; $A + \Omega = \Omega$; $A \cdot \varnothing = \varnothing$;

$A + B = B + A$, $A \cdot B = B \cdot A$ – коммутативные законы

$(A + B) + C = A + (B + C)$, $(A \cdot B) \cdot C = A \cdot (B \cdot C)$ – ассоциативныйе законы

$(A + B) \cdot C = A \cdot C + B \cdot C$, $A \cdot B + C = (A + C) \cdot (B + C)$ – дистрибутивные законы

$\overline{A + B} = \overline{A} \cdot \overline{B}$, $\overline{A \cdot B} = \overline{A} + \overline{B}$ – законы де Моргана

Пример. Шарик бросают на стол и отмечают точку его падения. Пусть A обозначает событие, заключающееся в попадании шарика внутрь круга A, а B – попадание внутрь круга B. Какой смысл имеют события: $\overline{A}$, $\overline{B}$, $A + B$, $\overline{A + B}$, $A \cdot B$, $\overline{A \cdot B}$?

Решение

Если A – попадание шарика внутрь круга A, то противоположное событие $\overline{A}$ означает, что шарик попал в область, лежащую вне круга A. Аналогично, $\overline{B}$ – попадание шарика в область, лежащую вне круга B. Событие $A + B$ означает, что шарик попал в область, в которую входят все точки кругов A и B, т.е. в их объединение. Событие $\overline{A + B}$ – противоположное к $A + B$, следовательно, шарик попал в область вне обоих кругов A и B, $A \cdot B$ – попадание шарика в общую часть кругов A и B. Соответственно, $\overline{A \cdot B}$ – шарик попал в область, лежащую вне общей части кругов A и B.

Пример. Пусть события A_1 и A_2 означают попадание в мишень соответственно при первом и втором выстрелах. Тогда события $\overline{A_1}$ и $\overline{A_2}$ – промахи при соответствующих выстрелах. Выразить через A_1, A_2, $\overline{A_1}$ и $\overline{A_2}$ следующие события:

а) B – ровно одно попадание в мишень при двух выстрелах;

б) C – два попадания в мишень при двух выстрелах;

в) D – хотя бы одно попадание в мишень при двух выстрелах;

г) E – ни одного попадания в мишень при двух выстрелах.

Решение

а) Событие B может произойти в случае попадания в мишень при первом выстреле (событие A_1) и промаха при втором выстреле (событие $\overline{A_2}$) или – промаха при первом выстреле (событие $\overline{A_1}$) и попадания при втором (событие A_2), т.е. в случае совмещения событий (A_1 и $\overline{A_2}$) или ($\overline{A_1}$ и A_2). Это означает, что $B = A_1 \cdot \overline{A_2} + \overline{A_1} \cdot A_2$.

б) Событие C имеет место в случае попадания в мишень при первом и втором выстрелах (совмещение событий A_1 и A_2), т.е. $C = A_1 \cdot A_2$.

в) Событие D означает, что имеет место либо одно попадание в мишень (событие B), либо два (событие C). Таким образом, $D = B + C = A_1 \cdot \overline{A_2} + \overline{A_1} \cdot A_2 + A_1 \cdot A_2$.

г) Событие E обозначает совмещение промахов при первом и втором выстрелах, т.е. $E = \overline{A_1} \cdot \overline{A_2}$.

Пример. Доказать, что $A + \overline{A} \cdot B + \overline{A + B} = \Omega$.

Решение

На основе одного из дистрибутивных законов $A \cdot B + C = \left(A + C\right) \cdot \left(B + C\right)$, можно утверждать, что $A + \overline{A} \cdot B = \left(A + \overline{A}\right) \cdot \left(A + B\right)$.

Учитывая равенства $A + \overline{A} = \Omega$ и $A \cdot \Omega = A$, имеем: $\left(A + \overline{A}\right) \cdot \left(A + B\right) = \Omega \cdot \left(A + B\right) = A + B$.

Используя еще раз равенство $A + \overline{A} = \Omega$, окончательно получаем:

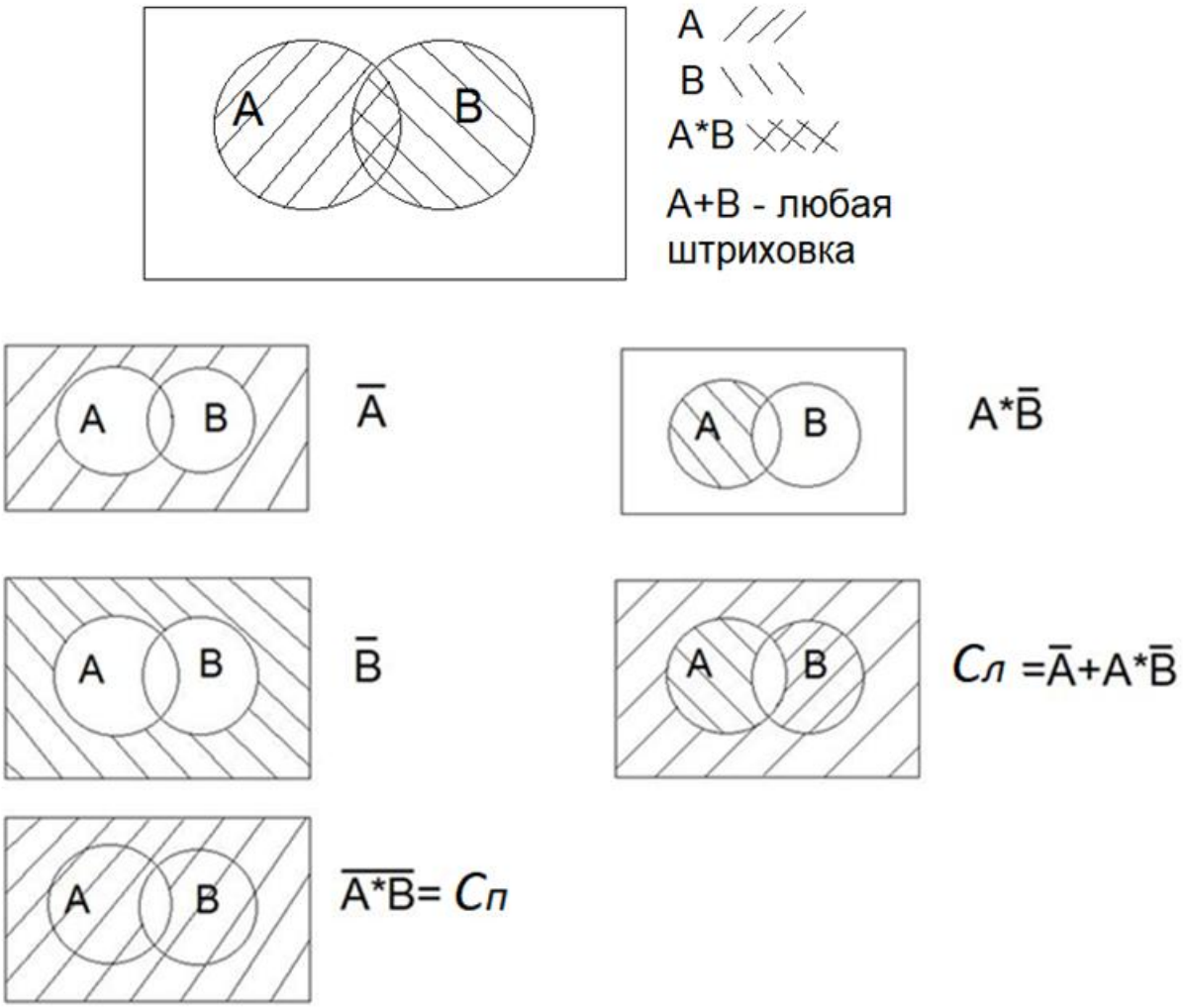
$$A + \overline{A} \cdot B + \overline{A + B} = \left(A + \overline{A}\right) \cdot \left(A + B\right) + \left(\overline{A + B}\right) =$$

$$= \left(A + B\right) + \left(\overline{A + B}\right) = \Omega .$$

Пример. С помощью диаграмм Эйлера-Венна проиллюстрировать справедливость алгебраической формулы $\bar{A} + (A * \bar{B}) = \overline{(A * B)}$.

Решение

Проиллюстрируем по отдельности левую $\left(C_{\text{л}} = \bar{A} + (A * \bar{B})\right)$ и правую $\left(C_{\text{п}} = \overline{(A * B)}\right)$ части равенства диаграммами Эйлера-Венна:



Так как иллюстрации идентичны и $C_{\text{л}} = C_{\text{п}}$, равенство доказано.

Замечание. Аналитическое доказательство для этой формулы несложно получить, используя алгебраические свойства событий:

$$\bar{A} + (A * \bar{B}) = \left[\begin{array}{c}\text{раскрыты скобки}\\ \text{относительно}\\ \text{общего слагаемого}\end{array}\right] = (\bar{A} + A) * (\bar{A} + \bar{B}) = [\bar{A} + A = \Omega] =$$

$$\Omega * (\bar{A} + \bar{B}) = \bar{A} + \bar{B} = \left[\begin{array}{c}\text{использован один из}\\ \text{законов де Моргана}\end{array}\right] = \overline{(A * B)} - \text{совпало с правой частью}$$

равенства.

Пример. Брошена игральная кость. Событие *A* – выпадение НЕ менее 3-х очков, событие *B* – выпадение четного числа очков. *C* – выпадение более четырех очков. Указать множество элементарных результатов, благоприятных к этим событиям. Выразить через *A*, *B* и *C* событие *D* – выпадение шести очков.

Решение

1. Запишем элементарные исходы, благоприятные к указанным событиям:

A = [не менее 3 очков] $= \{3; 4; 5; 6\}$

B = [четное количество очков] = $\{2; 4; 6\}$

C = [более 4 очков] = $\{5; 6\}$

$\mathrm{D} = [\text{выпадение шести очков}] = \{6\}$

2. Рассмотрим искомое. Так как событию *D* благоприятствует только один вариант, ожидаем, что ответ не будет получен сложением событий, а умножением или отрицанием после сложения.

Рассмотрим данное и попробуем выполнить элементарные действия с указанными событиями:

$\mathrm{A} + \mathrm{B} = \{2; 3; 4; 5; 6\}$

$\mathrm{A} * \mathrm{B} = \{4; 6\}$

$\bar{\mathrm{C}} = \{1; 2; 3; 4\}$

…

$$B * C = \{6\} = \begin{bmatrix} \text{видим, что получился} \\ \text{желаемый состав} \\ \text{элементарных результатов} \end{bmatrix} = D$$