

1 Определения

1. Логические операции: конъюнкция, дизъюнкция и отрицание.

1) Конъюнкция - это сложное логическое выражение, которое считается истинным в том и только том случае, когда оба простых выражения являются истинными, во всех остальных случаях данное сложное выражение ложно.

Обозначение: $F = A \wedge B$.

Таблица истинности для конъюнкции:

A	B	$A \wedge B$
0	0	0
0	1	0
1	0	0
1	1	1

2) Дизъюнкция - это сложное логическое выражение, которое истинно, если хотя бы одно из простых логических выражений истинно и ложно тогда и только тогда, когда оба простых логических выражения ложны.

Обозначение: $F = A \vee B$.

Таблица истинности для дизъюнкции:

A	B	$A \vee B$
0	0	0
0	1	1
1	0	1
1	1	1

3) Отрицание - это сложное логическое выражение, в котором если исходное логическое выражение истинно, то результат отрицания будет ложным, и наоборот, если исходное логическое выражение ложно, то результат отрицания будет истинным.

Обозначение: $F = \neg A$

Таблица истинности для отрицания:

A	$\neg A$
0	1
1	0

2. Логические операции: импликация, XOR (исключающее или) и эквивалентность.

1) Импликация - это сложное логическое выражение, которое истинно во всех случаях, кроме случая, когда из истины следует ложь. То есть данная логическая операция связывает два простых логических выражения, из которых первое является условием (A), а второе (B) является следствием.

Обозначение: $F = A \rightarrow B$

Таблица истинности для импликации:

A	B	$A \rightarrow B$
0	0	1
0	1	1
1	0	0
1	1	1

2) XOR (исключающее или) - это сложное логическое выражение, которое является истинным тогда и только тогда, когда оба простых логических выражения имеют разную истинность.

Обозначение: $F = A \oplus B$

Таблица истинности для исключающего или:

A	B	$A \oplus B$
0	0	0
0	1	1
1	0	1
1	1	0

3) Эквивалентность - это сложное логическое выражение, которое является истинным тогда и только тогда, когда оба простых логических выражения имеют одинаковую истинность.

Обозначение: $F = A \leftrightarrow B$

Таблица истинности для эквивалентности:

A	B	$A \leftrightarrow B$
0	0	1
0	1	0
1	0	0
1	1	1

3. Булевы функции. Задание таблицей истинности и вектором значений.

1) Булева функция - функция от N аргументов из N -ой степени множества $E = \{0,1\}$ в множество $E = \{0,1\}$. То есть:

$$f : E_2^n \rightarrow E_2, E_2 = \{0, 1\}$$

Булеву функцию от N переменных можно задать *таблицей истинности*:

x_1	x_2	...	x_{n-1}	x_n	$f(x_1, x_2, \dots, x_{n-1}, x_n)$
0	0	...	0	0	$f(0, 0, \dots, 0, 0)$
0	0	...	0	1	$f(0, 0, \dots, 0, 1)$
...
1	1	...	1	0	$f(1, 1, \dots, 1, 0)$
1	1	...	1	1	$f(1, 1, \dots, 1, 1)$

Значения переменных можно не хранить если принять соглашение о перечислении наборов переменных в определенном порядке. Обычно таким порядком принимается порядок возрастания целых чисел, заданных наборами переменных как двоичными числами. (Еще этот порядок называют *установленным*). Таблицу истинности можно "транспонировать", выписав последнюю строку:

$$f(0, 0, \dots, 0, 0), f(0, 0, \dots, 0, 1), \dots, f(1, 1, \dots, 1, 1)$$

Такой способ задания булевой функции называется задание вектором значений.

4. Существенные и фиктивные переменные булевой функции.

Переменная x_i называется *существенной* переменной функции булевой функции f , если существует такой набор значений $a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_n$, что:

$$f(a_1, \dots, a_{i-1}, 0, a_{i+1}, \dots, a_n) \neq f(a_1, \dots, a_{i-1}, 1, a_{i+1}, \dots, a_n)$$

В противном случае переменная x_i называется *фиктивной*.

5. Дизъюнктивная нормальная форма.

Дизъюнктивная нормальная форма (ДНФ) - это представление булевой формулы в виде дизъюнкции конъюнктов литералов. Любая булева формула может быть приведена к ДНФ. *Литерал* - это x или \bar{x} , где x - некая логическая переменная. *Конъюнкт* - это конъюнкция литералов. Например, $x_1 \wedge x_2 \wedge x_3$ - конъюнкт. k -дизъюнктивной нормальной формой называют ДНФ, в которой каждая конъюнкция содержит ровно k литералов.

6. Множество, подмножество, равенство множеств.

Множество — это совокупность каких-то элементов, полностью определяемая своими элементами. Элементами множества могут быть другие множества.

Будем говорить, что элемент x *принадлежит* множеству A , если он является его элементом. Обозначение: $x \in A$ (эта запись означает утверждение и принимает логические значения "истина" , "ложь" – входит или не входит в множество).

Если любой элемент множества A принадлежит множеству B , то множество A называется *подмножеством* множества B , обозначение $A \subseteq B$.

Равенство множеств $A = B$ — это утверждение, которое означает, что множества состоят из одних и тех же элементов. То есть: любой элемент множества A принадлежит множеству B и любой элемент множества B принадлежит множеству A .

Есть уникальное множество - *пустое*, - которое не содержит никаких элементов. Обозначение: \emptyset .

Если элементов в множестве мало, его можно задать, указав все эти элементы (в фигурные скобки). Порядок не играет роли. Поэтому $\{a, b, c, d\} = \{d, a, c, b\}$.

Количество элементов в множестве A , если оно конечно, непустое, обозначается $|A|$ и называется *мощностью множества*.

7. Операции с множествами: объединение, пересечение, разность, симметрическая разность. Диаграммы Эйлера-Венна.

1) *Объединение множеств*. Обозначение $A \cup B$. Это множество, состоящее в точности из тех элементов, которые принадлежат хотя бы одному из множеств A и B .

2) *Пересечение множеств*. Обозначение $A \cap B$. Это множество, состоящее в точности из тех элементов, которые принадлежат обоим множествам A и B .

3) *Разность множеств*. Обозначение $A \setminus B$. Это множество, состоящее в точности из тех элементов, которые принадлежат множеству A , но не принадлежат множеству B .

4) *Симметрическая разность множеств*. Обозначение $A \Delta B$. Это множество, состоящее в точности из тех элементов, которые принадлежат ровно одному из множеств: либо А, либо В.

5) *Диаграммы Эйлера-Венна* - геометрическая схема, с помощью которой можно изобразить отношения между множествами, для наглядного представления. При этом способе множество изображается условным кругом (или другой геометрической фигурой) и предполагается, что внутренность круга изображает элементы множества. (Я думаю, нарисовать сможете).

8. Законы Моргана (с обобщением на произвольное семейство множеств).

Законы де Моргана задают правило взятия отрицания от конъюнкции и дизъюнкции:

$$\neg(x \vee y) = \neg x \wedge \neg y$$

$$\neg(x \wedge y) = \neg x \vee \neg y$$

(Доказывается по таблицам истинности).

Равенства обобщаются на случай нескольких переменных:

$$\neg(x_1 \vee x_2 \vee \dots \vee x_n) = \neg x_1 \wedge \neg x_2 \wedge \dots \wedge \neg x_n$$

$$\neg(x_1 \wedge x_2 \wedge \dots \wedge x_n) = \neg x_1 \vee \neg x_2 \vee \dots \vee \neg x_n$$

Доказательство (для первой формулы, аналогично для второй):

1. База: Выражение верно для $n = 2$: $\neg(x_1 \vee x_2) = \neg x_1 \wedge \neg x_2$

2. Предположение: Пусть верно для $n = k - 1$:

$$\neg(x_1 \vee x_2 \vee \dots \vee x_{k-1}) = \neg x_1 \wedge \neg x_2 \wedge \dots \wedge \neg x_{k-1}$$

3. Шаг: проверим для $n = k$. Сделаем замену $y = x_1 \vee x_2 \vee \dots \vee x_{k-1}$

$$\begin{aligned} \neg(x_1 \vee x_2 \vee \dots \vee x_k) &= \neg(y \vee x_k) = \neg y \wedge \neg x_k = \neg(x_1 \vee x_2 \vee \dots \vee x_{k-1}) \wedge \neg x_k = \\ &= \neg x_1 \wedge \neg x_2 \wedge \dots \wedge \neg x_{k-1} \wedge \neg x_k \end{aligned}$$

(Последний переход выполнен по предположению индукции)

(*) На языке множеств законы де Моргана формулируются так: (I) элемент x не принадлежит объединению семейства множеств тогда и только тогда, когда он не принадлежит ни одному из этих множеств; (II) элемент x не принадлежит пересечению семейства множеств тогда и только тогда, когда он не принадлежит хотя бы одному из этих множеств. В таком виде законы де Моргана применимы и к бесконечным семействам множеств.

9. Закон контрапозиции.

Принцип контрапозиции - теорема равносильна обратной к противоположной. Тожество

$$x \rightarrow y = \neg y \rightarrow \neg x$$

выражает принцип контрапозиции. Этот принцип часто используется в математических доказательствах: вместо доказательства утверждения «если А, то В» зачастую удобнее изменить посылку и доказывать равносильное утверждение «если не В, то не А». Проверка тождества легко производится по таблице истинности.

10. Правило суммы.

Правило суммы для множеств. Если какое-то множество A разделено на две части B и C , не имеющие общих элементов, то $|A| = |B| + |C|$. (определение из чернивика книги. не примут - тыкните их в собственную книгу)

Комбинаторное правило суммы. Пусть объект A можно выбрать M способами, а объект B можно выбрать N способами, причём выбор одного объекта исключает одновременный выбор другого объекта. Тогда выбрать A или B можно $M + N$ способами.

11. Метод математической индукции.

Доказательства по индукции применяются, когда есть последовательность утверждений

$$A_1, A_2, A_3, \dots, A_n, \dots$$

и мы хотим доказать, что все они верны. Принцип индукции говорит, что для этого достаточно сделать две вещи:

1. Базис индукции: надо доказать, что A_1 (первое утверждение в цепочке) верно.
2. Шаг индукции: надо доказать (для произвольного n), что A_{n+1} верно, предполагая известным, что A_n верно.

Мы должны доказать, что из A_n следует A_{n+1} . Доказав следование и базу, мы можем применить шаг индукции к A_1 и получить A_2 . Постепенно применяя шаг, мы дойдем до любого A_n .

12. Формула включений и исключений.

Формула включений-исключений обобщает правило суммы и даёт выражение для объединения нескольких, возможно пересекающихся, множеств.

Пример для двух множеств:

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

Пример для трех множеств:

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

Общий вид:

$$|A_1 \cup A_2 \cup \dots \cup A_n| = |A_1| + \dots + |A_n| - |A_1 \cap A_2| - |A_1 \cap A_3| - \dots + |A_1 \cap A_2 \cap A_3| + \dots + |A_1 \cap A_2 \cap A_4| + \dots - (-1)^n |A_1 \cap A_2 \cap \dots \cap A_n|$$

Удобно представить итоговую формулу в более компактном виде. Для этого введём обозначения. Через S будем обозначать подмножество множества $\{1, \dots, n\}$, каждое такое подмножество выделяет некоторое семейство подмножеств

$$\{A_i : i \in S\}$$

Через A_S обозначим пересечение всех множеств, входящих в семейство S , т.е.

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

В таких обозначениях формула включений-исключений записывается достаточно компактно:

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

13. Правило произведения.

Из лекций: Если есть N способов выбрать 1-ый объект и после каждого выбора есть M способов выбрать 2-ой объект, то всего есть $N \times M$ способов выбрать два объекта.

Из книги: Правило произведения. Если объект интересующего нас вида строится в несколько шагов $(1, 2, \dots, k)$, и на каждом шаге есть выбор из какого-то числа вариантов (m_1, m_2, \dots, m_k) , причём количество выборов на каждом шаге не зависит от сделанных ранее выборов, то общее количество объектов N равно произведению количеств вариантов выбора для каждого из шагов: $N = m_1 \times m_2 \times \dots \times m_k$.

14. Комбинаторные числа. Число перестановок, число подмножеств размера k у n -элементного множества

Пусть $A = \{a_1, \dots, a_n\}$ - множество из n элементов.

Комбинаторный объект - это подмножество с определенными свойствами из элементов множества A .

Комбинаторное число (связанное с комбинаторным объектом) - это количество комбинаторных объектов этого вида.

Некоторые комбинаторные числа имеют собственные названия и устоявшиеся обозначения.

В комбинаторике *размещением из n по k* называется упорядоченный набор из k различных элементов из некоторого множества различных n элементов. $(1, 3, 2, 5)$ — это 4-элементное размещение из 6-элементного множества $\{1, 2, 3, 4, 5, 6\}$

$$A_n^k = n(n-1)(n-2)\dots(n-k+1) = \frac{n!}{(n-k)!}$$

Перестановка — это упорядоченный набор из чисел $1, 2, \dots, n$, в котором числу i сопоставляется i -ый элемент из набора. Другими словами, это биекция на множестве $\{1, 2, \dots, n\}$. Например, $(2, 1, 3)$ — это перестановка $(1, 2, 3)$. Число всех перестановок обозначают за P_n . Так как перестановка — это то же самое, что размещение по n элементам, то

$$P_n = A_n^n = \frac{n!}{(n-n)!} = \frac{n!}{0!} = n!$$

Сочетаниями из n по k называется набор k элементов, выбранных из данного множества, содержащего n различных элементов. Наборы, отличающиеся только порядком следования элементов (но не составом), считаются одинаковыми, этим сочетания отличаются от размещений.

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

Сочетанием с повторениями называются сочетания, в которых каждый элемент набора может встречаться несколько раз. Количество сочетаний с повторениями из n по k равно $C_{n+k-1}^k = C_{n+K-1}^{n-1}$. (можно доказать с помощью метода точек и перегородок).

15. Характеристическая функция и её использование при подсчёте числа элементов множества.

Характеристическая функция - это функция, определённая на множестве X , которая указывает на принадлежность элемента x , принадлежащего X , подмножеству A .

$$\chi_A(x) = \begin{cases} 1, & x \in A \\ 0, & x \notin A \end{cases}$$

Можно определить понятие мощности подмножества A на множестве X , используя характеристическую функцию:

$$|A| = \sum_{x \in X} \chi_A(x)$$

16. Функции. Область определения и множество значений.

Функцией из множества A в множество B мы назовём такое соответствие, которое сопоставляет некоторым элементам множества A какой-то элемент множества B . Данному $x \in A$ (его называют аргументом функции) функция f из A в B либо не сопоставляет никакого элемента в B , либо сопоставляет ровно один такой элемент y .

Область определения функции f из A в B состоит в точности из тех элементов x множества A , которым сопоставлен элемент $f(x)$ множества B .

Обозначение: $Dom(f) = \{a | a \in A; \exists b : f(a) = b\}$

Элементы $f(x)$ для всех x из области определения функции f образуют *множество значений* функции f .

Обозначение: $Range(f) = \{b | \exists a \in A : f(a) = b\}$

17. Биномиальные коэффициенты, основные свойства. Бином Ньютона.

Хорошо известны формулы раскрытия скобок (формулы сокращенного умножения). Например, $(a + b)^2 = a^2 + 2ab + b^2$. Оказывается, что есть подобная формула для любой целой неотрицательной степени — *бином Ньютона*:

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

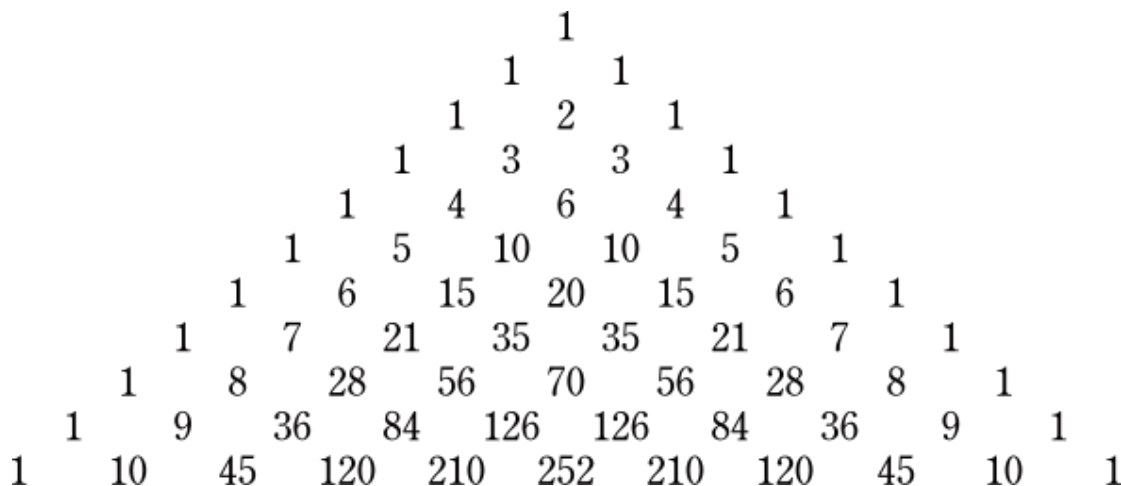
$$\binom{n}{k} - \text{биномиальный коэффициент.}$$

Свойства биномиальных коэффициентов:

- $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$
- k -й коэффициент есть количество сочетаний из n по $k - 1$.
- $\binom{n}{k} = \frac{n!}{(n-k)!k!}$

18. Треугольник Паскаля. Рекуррентное соотношение

Треугольник Паскаля - бесконечная треугольная таблица, в которой на вершине и по боковым сторонам стоят единицы, каждое из остальных чисел равно сумме двух чисел, стоящих над ним в предшествующей строке.



Пусть $T(n, k)$ - k -й в нумерации с нуля элемент n -й строки. Свойства:

- $T(n, k) = \binom{n}{k}$
- Симметричность строк: $T(n, k) = T(n, n - k)$, n - строка, k - столбец.
- Возрастание чисел в первой половине строки: $T(n, i) \leq T(n, i + 1), 0 \leq i < n/2, i \in \mathbb{Z}$
- $\sum_{k=0}^n T(n, k) = 2^n$
- $\sum_{k=0}^n (-1)^k T(n, k) = 0, n \neq 0$

Рекуррентная соотношение - последовательность, в которой каждый следующий член выражается через предыдущие элементы и, возможно, номер элемента.

Рекуррентная формула - формула вида $a_n = f(n, a_{n-1}, a_{n-2}, \dots, a_{n-p})$, выражающая каждый член последовательности a_n через p предыдущих членов и возможно номер члена последовательности n .

19. Образы и прообразы множеств. Полный прообраз.

Пусть функция f из множества A в множество B устанавливает соответствие между элементами множеств A и B . Пусть $X \subseteq A$ – подмножество множества A . Функция f сопоставляет ему *образ* $f(X) \subseteq B$ подмножества X . По определению $f(X)$ состоит в точности из тех элементов множества B , которые являются значениями элементов из X . Используя введённые нами для множеств обозначения, это можно записать как

$$f(X) = \{b | \exists x \in X : b = f(x)\}$$

Совокупность всех тех элементов $a \in A$, образом которых является данный элемент $b = f(a)$, $f(a) \in B$, называется *прообразом* элемента b и обозначается $f^{-1}(b)$

Подмножеству $Y \subseteq B$ можно сопоставить *полный прообраз* $f^{-1}(Y) \subseteq A$ подмножества Y . По определению $f^{-1}(Y)$ состоит в точности из тех элементов A , значения которых лежат в Y . Или формально:

$$f^{-1}(Y) = \{a | f(a) \in Y\}$$

20. Отображения (всюду определённые функции). Инъекции, сюръекции и биекции.

Отображение множества A в множество B - функция, которому каждому элементу $a \in A$ ставит в соответствие элемент $b \in B$.

Пусть $f : A \rightarrow B$. Тогда функция f называется:

1) *Инъективной (или инъекцией)*, если:

$$(b = f(a_1)) \ \& \ (b = f(a_2)) \Rightarrow (a_1 = a_2)$$

2) *Сюръективной (или сюръекцией)*, если:

$$\forall b \in B \ \exists a \in A : b = f(a)$$

3) *Биективной (или биекцией)*, если она сюръективна и инъективна. Биекции также называют *взаимно-однозначными функциями*.

21. Бинарные отношения. Транзитивность, симметричность, рефлексивность.

Бинарным отношением между множествами A и B называется подмножество R произведения $A \times B$. В том случае, когда $A = B$, мы говорим просто об отношении R на A .

Для бинарных отношений часто используется инфиксная форма записи:

$$aRb \stackrel{Def}{=} (a, b) \in R \subset A \times B$$

Пусть $R \subset A^2$. Тогда отношение R называется:

<i>рефлексивным,</i>	если $\forall a \in A (aRa)$
<i>антирефлексивным,</i>	если $\forall a \in A \neg(aRa)$
<i>симметричным,</i>	если $\forall a, b \in A (aRb \Rightarrow bRa)$
<i>антисимметричным,</i>	если $\forall a, b \in A (aRb \ \& \ bRa \Rightarrow a = b)$
<i>транзитивным,</i>	если $\forall a, b, c \in A (aRb \ \& \ bRc \Rightarrow aRc)$
<i>линейным,</i>	если $\forall a, b \in A (a = b \vee aRb \vee bRa)$

22. Теоретико-множественные операции с отношениями. Операция обращения.

Бинарные отношения — это множества пар элементов, связанных этими отношениями, поэтому к отношениям применимы все операции, выполняемые над множествами. Пусть $P \subseteq A \times A$ и $Q \subseteq A \times A$, тогда:

1) Пересечение отношений $P \cap Q$ - отношение, которое содержит только те упорядоченные пары, которые есть и в P и в Q :

$$P \cap Q = \{(x, y) \mid (x, y) \in P \wedge (x, y) \in Q\}$$

2) Объединение отношений $P \cup Q$ - отношение, которое содержит все упорядоченные пары отношения P и все упорядоченные пары отношения Q :

$$P \cup Q = \{(x, y) \mid (x, y) \in P \vee (x, y) \in Q\}$$

3) Разность отношений $P \setminus Q$ - отношение, которое содержит только те упорядоченные пары, которые содержатся в P , но не содержатся в Q :

$$P \setminus Q = \{(x, y) \mid (x, y) \in P \wedge (x, y) \notin Q\}$$

4) Симметрическая разность отношений $P \Delta Q$ - отношение, которое содержит только те упорядоченные пары, которые содержатся в объединении P и Q , но не содержатся в пересечении P и Q :

$$P \Delta Q = \{(x, y) \mid (x, y) \in (P \cup Q) \wedge (x, y) \notin (P \cap Q)\}$$

5) Дополнение отношения P - это отношение, состоящее из всех пар $(x, y) \in (A \times A)$, которые не входят в отношение P :

$$\bar{P} = \{(x, y) \mid (x, y) \in (A \times A) \wedge (x, y) \notin P\}$$

6) Обратным отношением P^{-1} к P называется такое отношение, которое содержит пару (x, y) тогда и только тогда, когда P содержит пару (y, x) :

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

23. Композиция бинарных отношений

Пусть $R_1 \subset A \times C$ - отношение между A и C , а $R_2 \subset C \times B$ - отношение между C и B . Композицией двух отношений R_1 и R_2 называется отношение $R \subset A \times B$ между A и B , определяемое следующим образом:

$$R \stackrel{Def}{=} R_1 \circ R_2 \stackrel{Def}{=} \{(a, b) \mid a \in A \ \& \ b \in B \ \& \ \exists c \in C \ (aR_1c \ \& \ cR_2b)\}$$

Другими словами, $aR_1 \circ R_2 b \iff \exists c \in C \ (aR_1c \ \& \ cR_2b)$.

24. Отношения эквивалентности.

Отношение на некотором множестве, которое одновременно рефлексивно, симметрично и транзитивно, называют *отношением эквивалентности*.

Классы эквивалентности - непересекающиеся подмножества множества X , при этом любые два элемента одного класса находятся в отношении R , а любые два элемента разных классов не находятся в отношении R .

25. Графы. Основные определения: ребра, вершины, степени вершин.

Граф G - совокупность двух множеств - непустого множества V (множества вершин) и множества E двухэлементных подмножеств множества V (E - множество ребер).

$$E = \{\{u, v\} \mid u, v \in V, u \neq v\}$$

Степень вершины u - количество вершин, смежных с u . Обозначение: $d(u)$.

26. Пути и циклы в графах.

Путь - последовательность вершин v_1, v_2, \dots, v_n , такая что $\forall i \in \{1, 2, \dots, n-1\}$: v_i и v_{i+1} - соединены ребром.

Простой путь - путь, такой что в нем все вершины различны.

Цикл - путь, такой что $v_1 = v_n$

Простой цикл - цикл, все вершины которого, кроме первой и последней различны.

27. Отношение достижимости (связанности) и компоненты связности графа.

Говорят, что вершина v достижима из вершины u , если существует путь v_1, v_2, \dots, v_n , где $v_1 = u$, а $v_n = v$. Связность вершины u и v означает их достижимость друг из друга.

Обозначение связности: $u \rightarrow v$

Основные свойства:

1) $u \rightarrow u \quad \forall u \in V$

2) если $u \rightarrow v$, то $v \rightarrow u$ (для неор.графов)

3) Транзитивность (для неор.графов): если $u \rightarrow v$ и $v \rightarrow w$, то $u \rightarrow w$

Компонента связности - подмножество множества вершин V графа G такое, что любая пара вершин в этом подмножестве связаны, а также любая вершина этого подмножества не связана с любой другой не из этого подмножества.

Компонента связности - класс эквивалентности по отношению достижимости (валидно, т.к. отношение достижимости является отношением эквивалентности, это следует из свойств).

28. Правильные раскраски графов. Формулировка критерия 2 - раскрашиваемости

Раскраска вершин графа называется правильной, если концы каждого ребра покрашены в разные цвета. *2-раскрашиваемые графы* - это графы, которые можно правильно раскрасить в 2 цвета. Граф 2-раскрашиваемый, когда в нем нет циклов нечетной длины.

Теорема. 2 - раскраска описанного типа возможна тогда и только тогда, когда в графе нет циклов нечётной длины.

29. Двудольные графы. Двудольные и двураскрашиваемые графы.

Граф $G(V, E)$ называется *двудольным*, если множество V может быть разбито на два непересекающихся множества V_1 и V_2 ($V_1 \cup V_2 = V, V_1 \cap V_2 = \emptyset$), причем всякое ребро из E инцидентно вершине из V_1 и вершине из V_2 (соединяет вершину из V_1 с вершиной из V_2). Множества V_1 и V_2 называются *долями* двудольного графа.

2-раскрашиваемые графы - это графы, которые можно правильно раскрасить в 2 цвета. Граф является 2-раскрашиваемым тогда и только тогда, когда является двудольным.

30. Подграфы. Изоморфизм графов. Клики и независимые множества.

Граф $G'(V', E')$ называется *подграфом* графа $G(V, E)$, если $V' \subset V$ & $E' \subset E$.

Изоморфизм графов. Говорят, что два графа, $G_1(V_1, E_1)$ и $G_2(V_2, E_2)$, *изоморфны*, если существует биекция $h : V_1 \rightarrow V_2$, такая что две вершины u и v графа G_1 смежны тогда и только тогда, когда вершины $h(u)$ и $h(v)$ смежны в графе G_2 .

Клик называется такое подмножество вершин графа, каждая пара которых связана ребром.

Независимым множеством называется такое подмножество вершин графа, никакая пара которых не связана ребром.

31. Эйлеровы циклы.

Цикл называется *эйлеровым*, если он проходит по всем рёбрам графа, причём только один раз.

Критерии существования. Эйлеров цикл существует в неориентированном графе тогда и только тогда когда выполнены условия:

- 1) Граф связен.
- 2) Все вершины имеют четную степень.
- 3) Цикл проходит через все ребра.

Эйлеров цикл существует в ориентированном графе тогда и только тогда когда выполнены условия:

- 1) Граф сильно связен.
- 2) Для любой вершины v верно $d^-(v) = d^+(v)$

32. Деревья. Полные бинарные деревья.

Дерево - связный граф без простых циклов длины ≥ 3 . Для деревьев выполняются эти свойства:

- 1) G - связный граф, где нельзя удалить ни одного ребра без нарушения связности.
 - 2) G - связный граф, где число рёбер на единицу меньше числа вершин.
 - 3) G - связный граф, где для любых двух вершин u, v существует единственный простой путь из u в v .
 - 4) G - связный граф, где нет простых циклов длины больше 2.
- (Все 4 определения эквивалентны)

Еще свойства деревьев:

- 1) Для любых трёх вершин дерева, пути между парами этих вершин имеют ровно одну общую вершину.
- 2) Из любого связного неориентированного графа можно получить дерево удалением части ребер. (Полученное дерево будет называться остовным деревом исходного графа).
- 3) В любом дереве есть висячая вершина.

Полное бинарное дерево глубины n — неориентированный граф-дерево, вершины которого — двоичные слова длины не больше n , а рёбра соединяют слова, которые можно получить друг из друга добавлением (или исключением соответственно) символа в конец слова. Корень дерева — пустое слово.

33. Ориентированные графы, основные определения.

Ориентированный граф (орграф) - такой граф, в котором направление ребра

имеет значение; ребра (v, u) и (u, v) - разные. Записать можно следующим образом: $E = \{(A, B), (C, D), \dots\}$. Часто ребра в орграфе называют *дугами*.

Для орграфов и неорграфов верно, что $u \rightarrow v, v \rightarrow w \Rightarrow u \rightarrow w$.

Для ориентированных графов отличают входящую степень $d^-(v)$ — количество входящих в вершину ребер, то есть ребер вида (u, v) , и исходящую степень $d^+(v)$ — количество исходящих ребер, то есть ребер вида (v, u) .

Путь, простой путь, цикл, простой цикл - эквивалентно определениям для неорграфа.

34. Компоненты сильной связности ориентированного графа.

Будем говорить, что вершины u и v сильно связны, когда $u \rightarrow v$ и $v \rightarrow u$. Обозначается как $u \leftrightarrow v$.

Компонента сильной связности — определено только для орграфов; аналогично обычной компоненте связности, но между любой парой вершин в компоненте должна быть сильная связность.

Теорема: Вершины ориентированного графа можно однозначно разбить на непересекающиеся группы, называемые сильно связными компонентами, при этом:

- 1) Каждая вершина графа попадает ровно в одну группу;
- 2) Любые две вершины из одной группы сильно связаны;
- 3) Любые две вершины из двух разных групп не являются сильно связанными (в одну из сторон — или даже в обе — пути нет).

35. Отношения частичного порядка (строгие и нестрогие), линейные порядки

Отношение порядка - антисимметричное транзитивное отношение.

Нестрогое отношение порядка - рефлексивное отношение порядка.

Строгое отношение порядка - антирефлексивное отношение порядка.

Линейное отношение порядка - отношение порядка, обладающее свойством линейности ($\forall a, b \in A (a = b \vee aRb \vee bRa)$).

Частичное отношение порядка - отношение порядка, не обладающее свойством линейности.

Обычно отношение строгого порядка (линейного или частичного) обозначается знаком \prec , а отношение нестрогого порядка - знаком \preceq .

36. Отношение непосредственного следования

Отношение непосредственного следования - это отношение порядка \prec , такое что если $x < y$, то $\nexists z : x < z \wedge z < y$. Кратко записывается так:

$$\prec = \{(x, y) \mid (x < y) \wedge \neg(\exists z : x < z \wedge z < y)\}$$

37. Изоморфные отношения частичного порядка

Отношения частичного порядка $R_1 \subseteq A \times A$ и $R_2 \subseteq B \times B$ называются изоморфными, если существует такая биекция $f : A \rightarrow B$, что для $\forall x, y$ $xR_1y \iff f(x)R_2f(y)$

2 Теоремы с доказательствами

1. Разложение в ДНФ булевой функции.

Теорема: Любая булева функция представима в виде дизъюнкции конъюнктов её переменных и может быть записана так:

$$f(x_1, \dots, x_n) = \bigvee_{\{(\sigma_1, \dots, \sigma_n) \mid f(\sigma_1, \dots, \sigma_n)=1\}} x_1^{\sigma_1} \wedge x_2^{\sigma_2} \wedge \dots \wedge x_n^{\sigma_n}$$

Замечание: запись x^σ означает буквально:

$$x^\sigma = \begin{cases} x, & \sigma = 1 \\ \bar{x}, & \sigma = 0 \end{cases}$$

Для того, чтобы доказать данную теорему, докажем теорему о разложении булевой функции по k переменным.

Теорема: о разложении булевой функции по переменным.

$$f(x_1, \dots, x_m, x_{m+1}, \dots, x_n) = \bigvee_{(\sigma_1, \dots, \sigma_m)} x_1^{\sigma_1} \wedge \dots \wedge x_m^{\sigma_m} \wedge f(\sigma_1, \dots, \sigma_m, x_{m+1}, \dots, x_n)$$

Причем дизъюнкция берется по всем возможным наборам $(\sigma_1, \dots, \sigma_m) \in \{0, 1\}^m$.

Доказательство: Рассмотрим значение формулы на наборе значений (a_1, \dots, a_n) .

Имеем:

$$\begin{aligned} & \left(\bigvee_{(\sigma_1, \dots, \sigma_m)} x_1^{\sigma_1} \wedge \dots \wedge x_m^{\sigma_m} \wedge f(\sigma_1, \dots, \sigma_m, x_{m+1}, \dots, x_n) \right) (a_1, \dots, a_n) = \\ & = \bigvee_{(\sigma_1, \dots, \sigma_m)} a_1^{\sigma_1} \wedge \dots \wedge a_m^{\sigma_m} \wedge f(\sigma_1, \dots, \sigma_m, a_{m+1}, \dots, a_n) \end{aligned}$$

Достаточно очевидно, что $a^\sigma = 1$, если $a = \sigma$, иначе $a^\sigma = 0$:

a	σ	a^σ
0	0	1
0	1	0
1	0	0
1	1	1

Следовательно, все конъюнкции, в которых $\exists i : a_i \neq \sigma_i$, равны 0 и их можно опустить, поэтому остается только одно слагаемое, для которого $\forall i \in \{1, \dots, n\} (a_i = \sigma_i)$. Следовательно:

$$\begin{aligned} & \bigvee_{(\sigma_1, \dots, \sigma_m)} a_1^{\sigma_1} \wedge \dots \wedge a_m^{\sigma_m} \wedge f(\sigma_1, \dots, \sigma_m, a_{m+1}, \dots, a_n) = \\ & = a_1^{a_1} \wedge \dots \wedge a_m^{a_m} \wedge f(a_1, \dots, a_m, a_{m+1}, \dots, a_n) = f(a_1, a_2, \dots, a_n) \end{aligned}$$

■

Вернемся к первоначальной задаче. Достаточно очевидно, что искомое разложение в ДНФ - это разложение функции по всем переменным, $m = n$. (При таком разложении полностью исчезает часть с $f(\dots)$).

2. Обобщенный закон Моргана.

$$\neg(x_1 \vee x_2 \vee \dots \vee x_n) = \neg x_1 \wedge \neg x_2 \wedge \dots \wedge \neg x_n$$

$$\neg(x_1 \wedge x_2 \wedge \dots \wedge x_n) = \neg x_1 \vee \neg x_2 \vee \dots \vee \neg x_n$$

Доказательство (для первой формулы, аналогично для второй):

1. База: Выражение верно для $n = 2$: $\neg(x_1 \vee x_2) = \neg x_1 \wedge \neg x_2$
2. Предположение: Пусть верно для $n = k - 1$:

$$\neg(x_1 \vee x_2 \vee \dots \vee x_{k-1}) = \neg x_1 \wedge \neg x_2 \wedge \dots \wedge \neg x_{k-1}$$

3. Шаг: проверим для $n = k$. Сделаем замену $y = x_1 \vee x_2 \vee \dots \vee x_{k-1}$

$$\begin{aligned}\neg(x_1 \vee x_2 \vee \dots \vee x_k) &= \neg(y \vee x_k) = \neg y \wedge \neg x_k = \neg(x_1 \vee x_2 \vee \dots \vee x_{k-1}) \wedge \neg x_k = \\ &= \neg x_1 \wedge \neg x_2 \wedge \dots \wedge \neg x_{k-1} \wedge \neg x_k\end{aligned}$$

(Последний переход выполнен по предположению индукции)

3. Формула включений и исключений.

Теорема:

$$\left| \bigcup_{i=1}^n A_i \right| = \sum_{i=1}^n |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| + \dots + (-1)^{n-1} |A_1 \cap \dots \cap A_n|$$

Доказательство (по индукции):

- 1) База индукции: докажите по диаграммам Эйлера-Венна для $n = 2, 3$
- 2) Предположение индукции: пусть верно для $n - 1$

$$\left| \bigcup_{i=1}^{n-1} A_i \right| = \sum_{i=1}^{n-1} |A_i| - \sum_{1 \leq i < j \leq n-1} |A_i \cap A_j| + \dots + (-1)^{n-2} |A_1 \cap \dots \cap A_{n-1}|$$

Дальше, нужно заметить, что из-за того, что операция пересечения ассоциативна по операции объединения, то верно вот что:

$$\left(\bigcup_{i=1}^{n-1} A_i \right) \cap A_n = \bigcup_{i=1}^{n-1} (A_i \cap A_n)$$

Кроме того, надо заметить, что для штуки, которую мы получили, верно предположение индукции (мы можем её разложить):

$$\left| \bigcup_{i=1}^{n-1} (A_i \cap A_n) \right| = \sum_{i=1}^{n-1} |A_i \cap A_n| - \sum_{1 \leq i < j \leq n-1} |A_i \cap A_j \cap A_n| + \dots + (-1)^{n-2} |A_1 \cap \dots \cap A_{n-1} \cap A_n|$$

- 3) А теперь, зная все формулы выше, мы делаем шаг индукции:

$$\left| \bigcup_{i=1}^n A_i \right| = \left| \left(\bigcup_{i=1}^{n-1} A_i \right) \cup A_n \right|$$

По формуле для $n = 2$ раскрываем эту скобку:

$$\begin{aligned} \left| \left(\bigcup_{i=1}^{n-1} A_i \right) \cup A_n \right| &= \left| \bigcup_{i=1}^{n-1} A_i \right| + |A_n| - \left| \left(\bigcup_{i=1}^{n-1} A_i \right) \cap A_n \right| = \\ &= \left| \bigcup_{i=1}^{n-1} A_i \right| + |A_n| - \left| \bigcup_{i=1}^{n-1} (A_i \cap A_n) \right| = \\ &= \left(\sum_{i=1}^{n-1} |A_i| - \sum_{1 \leq i < j \leq n-1} |A_i \cap A_j| + \dots + (-1)^{n-2} |A_1 \cap \dots \cap A_{n-1}| \right) + |A_n| - \\ &- \left(\sum_{i=1}^{n-1} |A_i \cap A_n| - \sum_{1 \leq i < j \leq n-1} |A_i \cap A_j| + \dots + (-1)^{n-2} |A_1 \cap \dots \cap A_{n-1} \cap A_n| \right) = \\ &= \left(\sum_{i=1}^{n-1} |A_i| + |A_n| \right) - \left(\sum_{1 \leq i < j \leq n-1} |A_i \cap A_j| + \sum_{i=1}^{n-1} |A_i \cap A_n| \right) + \dots - \\ &- (-1)^{n-2} |A_1 \cap \dots \cap A_{n-1} \cap A_n| = \sum_{i=1}^n |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| + \dots + (-1)^{n-1} |A_1 \cap \dots \cap A_n| \end{aligned}$$

■

4. Число k -элементных подмножеств n -элементного множества есть $\binom{n}{k}$

Будем выбирать элементы множества по очереди. Первый элемент можно выбрать n способами, второй $(n - 1)$ способами (годятся все, кроме первого, уже выбранного), третий $(n - 2)$ способами, и т.д. пока не выберем k элементов. По правилу произведения всего способов выбрать таким образом есть

$$n \times (n - 1) \times (n - 2) \times \dots \times (n - k + 1)$$

способ. Однако так мы посчитали не число возможных подмножеств, а число упорядоченных списков. Получается, нужно не обращать внимания на позицию элемента в списке. Всего можно составить $k!$ таких упорядоченных списков из k элементов ($k!$ - количество способов переставить элементы в списке). Значит количество способов выбрать k -элементное подмножество из n -элементного множества равно

$$\begin{aligned} \frac{n(n - 1)(n - 2) \cdot \dots \cdot (n - k + 1)}{k!} &= \frac{n(n - 1)(n - 2) \cdot \dots \cdot 2 \cdot 1}{(n - k)(n - k - 1) \cdot \dots \cdot 2 \cdot 1} \times \frac{1}{k!} = \\ &= \frac{n!}{(n - k)!} \times \frac{1}{k!} = \frac{n!}{(n - k)! \cdot k!} = \binom{n}{k} \end{aligned}$$

■

5. Бином Ньютона. Формула для биномиальных коэффициентов.

Теорема:

$$(a+b)^n = \sum_{k=0}^n \binom{n}{k} a^{n-k} b^k$$

Доказательство (по индукции):

1) База индукции: $n = 1$

$$(a+b)^1 = a+b = a^1 b^0 + a^0 b^1 = \binom{1}{0} a^1 b^0 + \binom{1}{1} a^0 b^1 = \sum_{k=0}^1 \binom{1}{k} a^{1-k} b^k$$

2) Пусть верно для n :

$$(a+b)^n = \sum_{k=0}^n \binom{n}{k} a^{n-k} b^k$$

3) Докажем для $n+1$:

$$\begin{aligned} (a+b)^{n+1} &= (a+b)(a+b)^n = (a+b) \left(\sum_{k=0}^n \binom{n}{k} a^{n-k} b^k \right) = \\ &= a \times \left(\sum_{k=0}^n \binom{n}{k} a^{n-k} b^k \right) + b \times \left(\sum_{k=0}^n \binom{n}{k} a^{n-k} b^k \right) = \\ &= \left(\sum_{k=0}^n \binom{n}{k} a^{n-k+1} b^k \right) + \left(\sum_{k=0}^n \binom{n}{k} a^{n-k} b^{k+1} \right) \end{aligned}$$

Вынесем из первой скобки одно слагаемое при $k=0$, а из второй скобки слагаемое при $k=n$:

$$\begin{aligned} &\left(\sum_{k=0}^n \binom{n}{k} a^{n-k+1} b^k \right) + \left(\sum_{k=0}^n \binom{n}{k} a^{n-k} b^{k+1} \right) = \\ &= a^{n+1} + \left(\sum_{k=1}^n \binom{n}{k} a^{n-k+1} b^k \right) + b^{n+1} + \left(\sum_{k=0}^{n-1} \binom{n}{k} a^{n-k} b^{k+1} \right) \end{aligned}$$

Сделаем сдвиг в сумме во второй скобке. Будем проходиться не от 0 до $n-1$, а от 1 до n . Тогда, чтобы сумма осталась неизменной нужно из всех k под знаком суммы отнять единичку. Получаем:

$$\begin{aligned} &a^{n+1} + \left(\sum_{k=1}^n \binom{n}{k} a^{n-k+1} b^k \right) + b^{n+1} + \left(\sum_{k=0}^{n-1} \binom{n}{k} a^{n-k} b^{k+1} \right) = \\ &= a^{n+1} + \left(\sum_{k=1}^n \binom{n}{k} a^{n-k+1} b^k \right) + b^{n+1} + \left(\sum_{k=1}^n \binom{n}{k-1} a^{n-(k-1)} b^k \right) = \\ &= a^{n+1} + b^{n+1} + \left(\sum_{k=1}^n \binom{n}{k} a^{n-k+1} b^k \right) + \left(\sum_{k=1}^n \binom{n}{k-1} a^{n-k+1} b^k \right) = \end{aligned}$$

$$\begin{aligned}
&= a^{n+1} + b^{n+1} + \sum_{k=1}^n \left(\binom{n}{k} a^{n-k+1} b^k + \binom{n}{k-1} a^{n-k+1} b^k \right) = \\
&= a^{n+1} + b^{n+1} + \sum_{k=1}^n \left(a^{n-k+1} b^k \left(\binom{n}{k-1} + \binom{n}{k} \right) \right) = \\
&= a^{n+1} + b^{n+1} + \sum_{k=1}^n \left(a^{n-k+1} b^k \times \binom{n+1}{k} \right) = \\
&= a^{n+1} + \sum_{k=1}^n \binom{n+1}{k} a^{n-k+1} b^k + b^{n+1} = \sum_{k=0}^{n+1} \binom{n+1}{k} a^{(n+1)-k} b^k
\end{aligned}$$

■

6. Основные свойства треугольника Паскаля: симметричность строк, возрастание чисел в первой половине строки.

- 1) $\binom{n}{k} = \binom{n}{n-k}$, следовательно все строки треугольника Паскаля симметричны. (доказывается раскрытием обеих частей).
- 2) Решить неравенство $\binom{n}{k} < \binom{n}{k+1}$. Получаем, что оно выполняется только при $k \leq \frac{n}{2}$. Из симметричности получаем возрастание в первой половине строки и убывание во второй половине строки.

7. Основные свойства треугольника Паскаля: формула для суммы чисел в строке, нижняя оценка на центральный коэффициент

Теорема 1: Сумма чисел в n-ой строке треугольника Паскаля = 2^n .

Доказательство: Вспомним, что в n-ой строке треугольника Паскаля лежат числа

$$\begin{aligned}
\binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{n} &= \binom{n}{0} 1^0 1^{n-0} + \binom{n}{1} 1^1 1^{n-1} + \dots + \binom{n}{n} 1^n 1^{n-n} = \\
&= \sum_{k=0}^n \binom{n}{k} 1^{n-k} 1^k = (1+1)^n = 2^n
\end{aligned}$$

Теорема 2: Нижняя оценка на центральный коэффициент.

$$\binom{2n}{n} \geq \frac{2^{2n}}{2n+1}$$

Доказательство:

- 1) Рассмотрим сумму 2n-ой строки треугольника Паскаля:

$$\binom{2n}{0} + \binom{2n}{1} + \dots + \binom{2n}{2n} = 2^{2n}$$

- 2) Из возрастания биномиальных коэффициентов следует, что:

$$\binom{2n}{n} \geq \binom{2n}{k}, \forall k \in \{1, 2, \dots, 2n\}$$

3) Следовательно:

$$\underbrace{\binom{2n}{n} + \dots + \binom{2n}{n}}_{2n+1} \geq \binom{2n}{0} + \binom{2n}{1} + \dots + \binom{2n}{2n}$$

4) Тогда:

$$(2n+1)\binom{2n}{n} \geq \binom{2n}{0} + \binom{2n}{1} + \dots + \binom{2n}{2n}$$

5) Получаем:

$$(2n+1)\binom{2n}{n} \geq 2^{2n}$$

6) И наконец:

$$\binom{2n}{n} \geq \frac{2^{2n}}{2n+1}$$

■

8. Число решений уравнения $x_1 + x_2 + \dots + x_k = n$ в неотрицательных целых числах. (Задача Муавра.)

Есть ещё одна задача, где естественным (но не вполне очевидным) образом возникают числа сочетаний. Сколько решений имеет уравнение $x_1 + x_2 + \dots + x_k = n$ в целых неотрицательных числах? Если это недостаточно наглядно, можно спросить иначе: есть k различных человек и n одинаковых монет. Сколькими способами можно раздать этим людям эти монеты? Каждый такой способ определяется тем, сколько монет получил каждый (но какие именно монеты — не учитывается, все монеты одинаковые). Это целые неотрицательные числа (допускаются варианты, где некоторые получили по нулю монет). Как найти это число? Представим себе, что наши n монет разложены в ряд. Прежде чем раздавать эти монеты, разделим их на k групп перегородками, и договоримся, кому идёт самая левая группа, кому вторая слева и т.д. Заметим, что мы допускаем случай, когда две перегородки оказываются рядом — это значит просто, что человеку, которому была назначена группа между ними, не повезло и в этом раскладе ему ни одной монеты не достанется. Каждому варианту раздачи (каждому решению уравнения в неотрицательных числах) соответствует последовательность из n монет и $k-1$ перегородок. (Число перегородок на единицу меньше числа группы: первая группа стоит слева от первой перегородки, а последняя — справа от последней.) Наоборот, каждой последовательности из n монет и $k-1$ перегородок соответствует некоторый способ раздачи монет. Поэтому надо подсчитать число способов расставить перегородки. А это совсем просто — каждый содержащее n монет и $k-1$ перегородок. Это количество, как мы знаем, равно $\binom{n+k-1}{n}$ или $\binom{n+k-1}{k-1}$.

9. Основная теорема об отношениях эквивалентности (классы эквивалентности на множестве A — в точности разбиения множества A на подмножества)

Теорема: Любое отношение R , являющееся отношением эквивалентности на

множестве A , делит A на классы эквивалентности - непересекающиеся подмножества множества X , при этом любые два элемента одного класса находятся в отношении R , а любые два элемента разных классов не находятся в отношении R .

Доказательство: Для каждого $x \in A$ рассмотрим множество тех y , для которых верно $R(x, y)$. Обозначим его через $[x]$. Его можно было бы назвать «классом эквивалентности элемента x » - собственно говоря, так его и называют, но само по себе это название не гарантирует разбиения на классы, это ещё надо доказывать. А именно, надодокazać, что

1. объединение всех множеств вида $[x]$ совпадает с множеством A ;
2. два множества $[x]$ и $[y]$ либо не пересекаются, либо совпадают;
3. наконец, надо ещё доказать, что $[x] = [y]$ в том и только том случае, когда $R(x, y)$, то есть R совпадает с отношением «принадлежать одному классу».

По порядку:

1. В силу рефлексивности множество $[x]$ содержит x в качестве своего элемента: $x \in [x]$, поскольку $R(x, x)$. Отсюда следует, что объединение всех этих множеств совпадает с A . (Выйти за пределы A они не могут, так как мы рассматриваем отношение на множестве A и элементы множества A .)
2. Пусть для двух элементов $x, y \in A$ их классы $[x]$ и $[y]$ пересеклись. Это означает, что есть такой $z \in A$, что $R(x, z)$ и $R(y, z)$. Симметричность даёт $R(z, y)$, после чего мы применяем транзитивность к $R(x, z)$ и $R(z, y)$ и заключаем, что $R(x, y)$. Выведем отсюда, что $[x] = [y]$. В самом деле, если произвольный элемент t принадлежит $[y]$, то $R(y, t)$. Вспоминая, что $R(x, y)$ и применяя транзитивность, получаем $R(x, t)$, то есть $t \in [x]$. Мы доказали, таким образом, что $[y] \subseteq [x]$. Аналогично доказывается, что $[x] \subseteq [y]$, так что $[x] = [y]$.
3. Если для каких-то x, y верно $R(x, y)$, то x и y оба лежат в одном классе, а именно, в $[x]$. Обратно, если x и y лежат в каком-то $[z]$, то по определению имеем $R(z, x)$ и $R(z, y)$, симметричность даёт $R(x, z)$ и после этого транзитивность даёт $R(x, y)$.

10. Нижняя оценка числа связных компонент в неориентированном графе.

Теорема: Число компонент связности в графе не меньше, чем разность количества вершин и ребер.

Доказательство (по индукции):

1) База индукции ($n = 1$): граф состоит из 1 вершины, которая является единственной компонентой связности в графе. Разность количества вершин(1) и ребер(0) равно 1, но компонента связности одна. База доказана.

2) Шаг индукции ($n \mapsto n + 1$): пусть для всех графов на n вершинах выполняется эта оценка, добавим еще одну вершину и рассмотрим случай связи, при котором сумма количества компонент связности и количество ребер наименьшая: выберем такой граф на n вершинах (C - количество компонент связности в этом графе, E - количество ребер в этом графе), чтобы в нем эта сумма была наименьшей и добавим к нему еще одну вершину. Заметим, что если связать новую вершину хотя бы одним ребром с k уже существовавшими компонентами связности, то количество ребер увеличится, как минимум, на k , а компонент связности станет на $k - 1$ меньше, чем в графе на n вершинах. (Если не связывать, то станет на одну больше, так как будет еще одна компонента связности, если связать компоненты связности, то они станут одной компонентой связности, то есть количество уменьшится на единицу.) Так как нужна наименьшая сумма, то нужно использовать, как можно меньше ребер: будем соединять вершину 1 ребром с каждой из k существовавших компонент связности - ребер станет на k больше, а количество компонентов связности уменьшится на $k - 1$, то есть сумма компонентов связности и ребер нового графа будет такой: $(C - (k - 1)) + (E + k) = C + E + 1$. Но $C + E + 1 > V + 1$ из $C + E > V$. Значит для $n + 1$ верна оценка.

■

11. Доказательство критерия 2-раскрашиваемости неориентированного графа.

Формулировка: Раскраска вершин графа в два цвета так, чтобы рёбра соединяли вершины разных цветов, возможна когда и только тогда, когда в графе нет циклов нечётной длины.

Доказательство: Если в графе есть цикл нечётной длины, то его нельзя раскрасить: соседние вершины должны быть противоположных цветов, и дойдя до конца, мы получим противоречие. Чтобы доказать обратное, предположим, что циклов нечётной длины нет. Выберем некоторую вершину a и не ограничивая общности окрасим её в цвет 1. Для любой другой вершины b посмотрим, сколько рёбер в пути от a к b . Заметим, что если есть путь $a \rightarrow b$ с чётным числом рёбер, а также другой путь $a \rightarrow b$ с нечётным числом рёбер, то есть цикл с нечётным числом рёбер (из a в b по одному пути и из b в a - по другому). Это противоречит предположению. Таким образом, мы поделили вершины графа на два типа: соединённые с a путями чётной длины и путями нечётной длины. Если какая-то вершина соединена с a путями чётной длины, то её соседи соединены путями нечётной длины (один такой путь - через соседа - заведомо есть, а тогда и все пути имеют нечётную длину). Раскрасим те, что на чётном расстоянии в то же цвет, что и a , а те, что на нечётном - в другой. Требуемая раскраска одной компоненты связности построена. Остальные можно раскрашивать совершенно независимо от этой, так как нет рёбер, которые могли бы помешать.

■

12. 13. 14. Я не знаю, как это доказывать по отдельности. Они еще напихали только те переходы, которых нет в книжке, это было спланировано. Поэтому буду пытаться, если что, доказывать экви-

валентность всего.

Теорема: Все четыре указанных свойства равносильны: граф, обладающий одним из них, обладает и всеми остальными

1) Связный граф, где нельзя удалить ни одного ребра без нарушения связности.

2) Связный граф, где число рёбер на единицу меньше числа вершин.

3) Связный граф, где для любых двух вершин u, v существует единственный простой путь из u в v .

4) Связный граф, где нет простых циклов длины больше 2.

Доказательство:

(2) \Rightarrow (1). Если в графе число рёбер на единицу меньше числа вершин, то после удаления ребра их будет на 2 меньше, а мы уже знаем, что в этом случае связность нарушится.

(1) \Rightarrow (2). Пусть дан связный граф с n вершинами, в котором ни одного ребра нельзя удалить без нарушения связности. Как мы доказывали, что в нём не меньше $n-1$ рёбер? Мы представляли себе, что рёбра добавляются по очереди, и смотрели, как меняется число связных компонент. Если добавленное ребро соединяло вершины, которые уже и так связаны, число компонент не менялось; в противном случае оно уменьшалось на единицу. Теперь первый случай невозможен: в нём добавленное ребро соединяет то, что соединено и так (другими рёбрами), поэтому оно лишнее и в окончательном графе (его можно удалить без нарушения связности, вопреки предположению). Поэтому к моменту, когда останется одна компонента, было добавлено как раз $V - 1$ рёбер, где V - число вершин.

Итак, (1) и (2) равносильны. Теперь докажем, что из этих свойств следует (3), то есть единственность простых путей. Здесь снова нужно будет смотреть за процессом добавления рёбер - мы знаем, что добавляемое ребро всегда соединяет две разные компоненты - и по индукции доказывать, что нет двух простых путей с одинаковыми началом и концом.

Итак, предположим, что это свойство выполнено для графа из нескольких связных компонент, и мы добавляем туда ребро $p-q$, соединяя две различные компоненты P и Q (содержащие p и q соответственно). Нам надо доказать, что и для нового графа это свойство выполнено. Пусть это не так, и есть два простых пути с одинаковым началом u и одинаковым концом v . Как минимум один из этих путей должен включать новое ребро $p-q$, поскольку до его добавления свойство единственности выполнялось (предположение индукции). Ребро это может входить только один раз, поскольку путь простой. Значит, начало пути лежит в одной из компонент P или Q , а конец в другой (остальные рёбра старые и не переводят в другую компоненту). Пусть, например, u лежит в P , а v лежит в Q . Тогда путь состоит из трёх частей: простой путь от u до p , ребро $p-q$, и простой путь от v до q . Посмотрим теперь на другой путь из u в v и убедимся, что он совпадает с первым. Он тоже должен использовать ребро $p-q$, поскольку перед добавлением этого ребра вершины u и v лежали в разных компонентах. Тогда по тем же причинам он разбивается на часть от u до p , ребро $p-q$, и часть от q до v . Остаётся воспользоваться предположением индукции (единственность пути в старом графе от u до p , и от q до v) и увидеть, что два рассматриваемых пути совпадают.

Из (3) легко следует (4). В самом деле, если есть простой цикл $a_1 \leftrightarrow a_2 \leftrightarrow$

$\dots a_n \leftrightarrow a_1$, где $n > 2$ и все a_1, \dots, a_n различны, то есть два простых пути из a_1 в a_n , а именно путь $a_1 \leftrightarrow a_2 \leftrightarrow \dots \leftrightarrow a_n$ и путь из одного ребра $a_1 \leftrightarrow a_n$.

Наконец, надо убедиться, что из (4) следует (1) и (2). Снова нужно вспомнить процесс слияния компонент при добавлении рёбер. Если (1) и (2) неверны, то в какой-то момент добавляется ребро, соединяющее уже связанные друг с другом вершины. Эти вершины связаны простым путём (как мы доказали), и вместе с добавленным ребром получится цикл. При этом длина цикла по крайней мере 3, потому что имевшийся простой путь был с пересадками (ребра-то раньше не было).

Теорема об эквивалентности четырёх свойств доказана



15. Равносильность свойств ориентированных графов: (1) каждая компонента сильной связности состоит из одной вершины; (2) вершины графа возможно занумеровать так, чтобы каждое ребро вело из вершины с меньшим номером в вершину с большим номером; (3) в графе нет циклов длины больше 1.

Теорема: Следующие свойства ориентированного графа равносильны:

1. Каждая сильно связная компонента состоит из одной вершины.
2. В графе нет циклов длины больше 1.
3. Вершины графа возможно занумеровать так, чтобы каждое ребро вело из вершины с меньшим номером в вершину с большим номером.

Доказательство: Начнём с очевидных утверждений. Если в графе есть цикл с $n > 1$ вершинами, то вершины этого цикла сильно связаны (из любой можно попасть в любую по циклу), так что из первого свойства следует второе. Наоборот, если различные вершины a, b сильно связаны, то существуют пути из a в b и из b в a , и из этих двух путей можно составить цикл. Наконец, если возможна нумерация вершин, при которой рёбра ведут от вершин с меньшим номером к вершинам с большим, то цикла нет: вдоль него номера вершин должны расти, и вернуться в начало мы не сможем. Осталось доказать единственное нетривиальное утверждение: если в ориентированном графе нет циклов, то его вершины можно пронумеровать требуемым способом.

Лемма. В ориентированном графе без циклов есть вершина, из которой не выходит ни одного ребра.

Доказательство леммы: Пусть это не так и из любой вершины выходит хоть одно ребро. Возьмём какую-то вершину a_1 , из неё идёт ребро в какую-то другую вершину a_2 , из неё идёт ребро ещё куда-то, и так далее. Поскольку граф конечен, то рано или поздно мы придём второй раз в какую-то вершину a_i , где уже были, и участок пути после a_i свернётся в цикл - вопреки предположению, что циклов нет.

Теперь можно закончить доказательство теоремы. Выберем вершину, из которой не ведёт ни одного ребра. Ей можно без опаски присвоить номер, больший всех остальных номеров. Поэтому рассуждаем по индукции: удалив эту вершину (и все входящие в неё рёбра) из графа, получим граф без циклов. (Циклы в нём были бы циклами и в исходном графе.) Пронумеруем его вершины

от 1 до какого-то числа n (число оставшихся вершин) с соблюдением условия (рёбра ведут из меньшего к большему), и после этого вернём выброшенную вершину под номером $n + 1$. (Базис индукции — граф с одной вершиной — очевиден.)

■

16. Критерий существования эйлерова цикла в неориентированном графе.

Теорема: Неориентированный граф без вершин нулевой степени содержит эйлеров цикл тогда и только тогда, когда он связан и степени всех вершин чётны.

Доказательство: Пусть в графе эйлеров цикл есть. Тогда он проходит через все вершины (поскольку они имеют ненулевую степень), и по нему можно пройти от любой вершины до любой. Значит, граф связан. Теперь про степени. Возьмём какую-то вершину v , пусть она встречается в цикле k раз. Идя 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 графе её степень равна $2k$. Таким образом, в одну сторону критерий доказан.

В обратную сторону. Будем рассматривать пути, которые не проходят дважды по одному ребру. (Таков, например, путь из одного ребра.) Выберем среди них самый длинный путь

$$a_1 \rightarrow a_2 \rightarrow a_3 \rightarrow \dots \rightarrow a_{n-1} \rightarrow a_n$$

и покажем, что он является искомым циклом, то есть что $a_1 = a_n$ и что он содержит все рёбра. В самом деле, если он самый длинный, то добавить к нему ребро $a_n \rightarrow a_{n+1}$ уже нельзя, то есть все выходящие из a_n рёбра уже использованы. Это возможно, лишь если $a_1 = a_n$. В самом деле, если вершина a_n 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 чётности степени.

Итак, мы имеем цикл, и осталось доказать, что в него входят все рёбра. В самом деле, если во всех вершинах цикла использованы все рёбра, то из вершин этого цикла нельзя попасть в вершины, не принадлежащие циклу, то есть использованы все вершины (мы предполагаем, что граф связан или сильно связан) и, следовательно, все рёбра. С другой стороны, если из какой-то вершины a_i выходит ребро $a_i \rightarrow v$, то путь можно удлинить до

$$a_i \rightarrow a_{i+1} \rightarrow \dots \rightarrow a_n = a_1 \rightarrow a_2 \rightarrow \dots \rightarrow a_i \rightarrow v$$

вопреки нашему выбору (самого длинного пути). Аналогично можно получить противоречие и для входящего ребра $v \rightarrow a_i$, добавив его в начало. (А можно заметить, что если есть неиспользованное входящее ребро, то есть и неиспользованное выходящее.) Это рассуждение было для ориентированного случая, но в неориентированном всё аналогично. Теорема доказана.

■

17. Критерий обратимости остатка (вычета) по модулю N.

Теорема: Число a обратимо по модулю p , если a и p взаимно просты, то есть их наибольший общий делитель равен единице.

Доказательство:

1) Пусть $\text{НОД}(a, p) = d$, $d > 1$. Заметим, что $1 < d < p$, так как делитель не может быть больше самого числа.

2) Раз d - наибольший общий делитель a и p , то существуют k_1, k_2 такие что:

$$a = k_1 \cdot d$$

$$p = k_2 \cdot d$$

3) Тогда $a \cdot k_2$ сравнимо с нулём по модулю p , т.к:

$$a \cdot k_2 \equiv k_1 \cdot k_2 \cdot d \equiv k_1 \cdot p \equiv 0 \pmod{p}$$

4) Обратимость числа a значит, что $\exists a^{-1}$, такое что:

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

5) Кроме того, имеем: $a \cdot k_2 \equiv 0 \pmod{p}$. Домножим обе части уравнения в пункте 4 на k_2 :

$$k_2 \cdot a \cdot a^{-1} \equiv k_2 \pmod{p}$$

6) Получаем:

$$0 \cdot a^{-1} \equiv k_2 \pmod{p}$$

$$0 \equiv k_2 \pmod{p}$$

7) Получили противоречие. Следовательно, $\nexists a^{-1}$, который удовлетворяет этим условиям, если a и p не взаимно просты. Тогда исходная теорема доказана по принципу контрапозиции.

■

18. Малая теорема Ферма.

Теорема: Если p — простое число и a — целое число, не делящееся на p , то $a^{p-1} \equiv 1 \pmod{p}$.

Доказательство:

1. Пусть $f(x) = x^p$. Докажем, что $\forall x \ f(x) = x \pmod{p}$.

2. Докажем это:

$$(a) \ f(0) \equiv 0^p \equiv 0 \pmod{p}$$

$$(b) \ f(1) \equiv 1^p \equiv 1 \pmod{p}$$

$$(c) \ \forall x, y \notin \{0, 1\} \ f(x+y) \equiv$$

$$\equiv (x+y)^p \equiv x^p + \binom{p}{1} x^{p-1} y^1 + \dots + \binom{p}{p-1} x^1 y^{p-1} + y^p \equiv$$

$$\equiv x^p + \frac{p!}{1!(p-1)!} x^{p-1} y^1 + \dots + \frac{p!}{(p-1)!1!} x^1 y^{p-1} + y^p \equiv$$

$$\equiv x^p + y^p \equiv f(x) + f(y) \pmod{p}$$

(d) Т.к $f(x + y) \equiv f(x) + f(y) \pmod{p}$, то мы можем вычислить f для всех остальных x :

- i. $f(2) \equiv f(1) + f(1) \equiv 1 + 1 \equiv 2 \pmod{p}$
- ii. $f(3) \equiv f(2 + 1) \equiv f(2) + f(1) \equiv 2 + 1 \equiv 3 \pmod{p}$
- iii. ...
- iv. $f(x) \equiv f((x - 1) + 1) \equiv x - 1 + 1 \equiv x \pmod{p}$

3. Получаем, что $f(a) \equiv a^p \equiv a \pmod{p}$

4. Число p - простое, поэтому все остатки по модулю p взаимно просты с $p \Rightarrow \forall x \exists x^{-1} : x \cdot x^{-1} \equiv 1 \pmod{p}$ (по критерию обратимости).

5. Следовательно, $\exists a^{-1} : a^{-1} \cdot a \equiv 1 \pmod{p}$

6. Тогда используя эту лемму: "Если $a \equiv b \pmod{m}$ и $c \equiv d \pmod{m}$, то $ac \equiv bd \pmod{m}$ " получаем:

$$\begin{cases} a^p \equiv a \pmod{p} \\ a^{-1} \equiv a^{-1} \pmod{p} \end{cases} \Rightarrow a^{p-1} \equiv 1 \pmod{p}$$

■