Материалы для подготовки к коллоквиуму по дискретной математике Определения

ПМИ 2016
Орлов Никита, Рубачев Иван, Ткачев Андрей, Евсеев Борис

12 декабря 2016 г.

Принцип математической индукции

Принципом математической индукции называют метод доказательства бесконечной цепочки утверждений, пронумерованных натуральными числами. Тогда для их доказательства достаточно справедливости следующих фактов:

1. Верно утверждение $A(0)$, называемое *базой индукции*.

2. Для любого натурального n верно, что из $A(n)$ следует $A(n+1)$. Этот переход называется *шагом индукции*.

В качетсве примера может служить доказательство формул арифметической, геометрической прогрессий, коды Грея.

Правила суммы, произведения, дополнения

Пусть есть непересекающиеся множества A, B. Тогда

$$|A \cup B| = |A| + |B|,$$

$$|A \times B| = |A| \times |B|$$

называются правилами суммы и произведения множеств соответственно.

Дополнением $\overline{A}$ множества A называется множество, состоящее из не удовлетворяющих произвольному условию элементов. Тогда

$$|\overline{A}| = U - A,$$

где U - пространство, в котором решается задача.

Алфавит, конечные слова, формулы комбинаторики

Алфавитом называется произвольное конечное множество, элементы которого называются символами или буквами.

Словом называется произвольная упорядоченная последовательность букв.

Числом перестановок $n!$ слова называется количество слов длины n, отличающихся друг от друга порядком следования букв.

$$n! = 1 \cdot 2 \cdot \ldots \cdot (n-1) \cdot n$$

Упорядоченным выбором с возвращением из n по k называется слово длины k, состоящее из букв слова длины n, с повторяющимися буквами. Число таких слов будет равняться

$$n^k$$

Упорядоченным выбором без возвращения из n по k называется слово длины k, состоящее из букв слова длины n, без повторяющихся букв. Число таких слов будет равняться

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

Неупорядоченным выбором без возвращения из n по k называется слово длины k, состоящее из букв слова длины n, без повторяющихся букв, причем слова, отличающиеся только порядком следования букв будем считать одинаковыми. Тогда число таких слов будет равняться

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

Неупорядоченным выбором с возвращением ....

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

Двоичными словами называются слова, составленные из двух букв, называемых *нулем* и *единицей*:

$$a \in \{0; 1\}$$

Число подмножеств множества считается по формуле

$$2^{|A|},$$

где A - множество.

Формула включений-исключений

Формулой включений-исключений называется формула, по которой можно посчитать мощность объединения счетного количества множеств:

$$|A_1 \cup \ldots \cup A_n| = \sum_{k=1}^{n} -1^{(k+1)} \cdot \Big(\sum_{1 < m_1 < \ldots < m_k \leq n} |A_{m_1} \cap \ldots \cap A_{m_k}| \Big)$$

Биноминальные коэффициенты, основные свойства. Бином Ньютона

Биноминальными коэффициентами называются коэффициенты в разложении бинома Ньютона $(1+x)^n$ по степеням x. При k степени x – $\binom{n}{k}$.

Бином Ньютона - формула разложения степени двучлена в сумму:

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

Свойства биноминальных коэффициентов:

1. $\binom{n}{k} = \binom{n-k}{k}$.
2. $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$.
3. $\sum_{k=0}^{n} \binom{n}{k} = 2^n$

Треугольник Паскаля. Реккурентное соотношение

Реккурентным соотношением называется формула, где каждый следующий член определен через предыдущие числа. Пример: числа Фибонначи.

Треугольник Паскаля - треугольник биномиальных коэффициентов, где каждый следующий элемент определяется суммой двух элементов над ним:

$$\begin{array}{ccccccc} & & & 1 & & & \\ & & 1 & & 1 & & \\ & 1 & & 2 & & 1 & \\ 1 & & 3 & & 3 & & 1 \end{array}$$

Графы

Пусть у нас есть множество элементов V - множество *вершин*. *Граф* - математический объект, являющийся совокупностью *вершин* и *ребер*, то есть:

$$G := (V, E),\ E \subseteq V \times V$$

Ребром графа называется пара вершин.

Неориентированный гарф - такой граф, где ребрам не задано направление.

Ориентированный гарф - такой граф, где у каждого ребра есть направление, иными словами, у каждого ребра есть начальная и конечная вершины.

Матрица смежности - квадратная матрица размера $V \times V$, строки и столбцы одинаково пронумерованы, элемент a_{ij} показывает наличие ребра или его вес:

	1	2	3	4
1	a_{11}	a_{12}	a_{13}	a_{14}
2	a_{21}	a_{22}	a_{23}	a_{24}
3	a_{31}	a_{32}	a_{33}	a_{34}
4	a_{41}	a_{42}	a_{43}	a_{44}

Изоморфные графы - такие графы G и G', что можно построить биекцию между их вершинами и соответствующими ребрами, или их вершины можно перенумеровать так, что их матрицы смежности совпадут

Степень вершины - число ребер, исходящих из нее, причем сумма степеней вершин равна удвоенному числу ребер.

Пути и циклы в графах

Маршрут - последовательность ребер, т.ч. соседние ребра имеют общий конец.

Путь - маршрут без повторений ребер.

Простой путь - путь без повторения вершин.

Цикл - путь, в котором первая и последняя вершины совпадают

Простой цикл - цикл, в котором все вершины, кроме начальной и конечной, различны.

Длина пути/цикла - число ребер, в них входящих.

Отношение связанности и компоненты связности графа

Связность - граф связен тогда и только тогда, когда две любые вершины соединены путем.

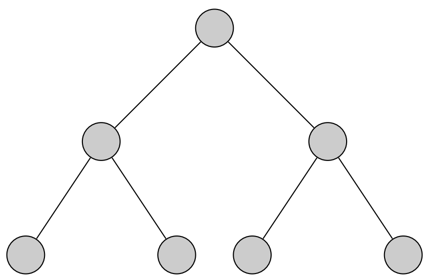
Компонента связности - максимальный по включению связный подграф графа $G - G(U)$, порожденный подмножеством вершин исходного графа, в котором для любой пары $v_1, v_2 \in U$ существует путь, а для всех других пар пути нет.

Дерево. Примеры. Полные бинарные деревья

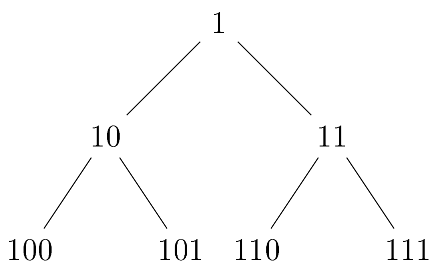
Дерево - минимальный связный ациклический граф. В нем любые две вершины соединены единственным путем.

Во всяком связном графе существует *остовное дерево* — подграф–дерево, содержащий все вершины.

Пример дерева:



Полное бинарное дерево - дерево, вершинами которого являются бинарные слова, а ребра получаются приписыванием 0 или 1 в конец предыдущего слова (слова - родителя):



Правильные раскраски графов

Правильной раскраской графа называется такой способ пронумеровать(покрасить) вершины, что никакие две вершины одинакого номера(цвета) не соединены ребром.

Двудольный, или *двураскрашиваемый* граф - граф, вершины которого можно разбить на два непересекающихся подмножества, таких что ни одно ребро не соединяет вершины, лежащие в одном подмножестве.

Граф двураскрашиваем тогда и только тогда, когда в нем нет цикла нечетной длины.

Ориентированный граф

Ориентированный граф - такой граф, на ребрах которого установлено направление обхода.

Маршрут в орграфе - чередующаяся последовательность вершин и дуг, где вершины могут повторяться. *Путь* в орграфе - маршрут без повторяющихся дуг, *простой путь* - без повторяющихся вершин. Если существует путь из одной вершины в другую, тогда говорят, что вторая достижима из первой.

Компоненты сильной связности

Компонентой сильной связности называют подграф, в котором любая вершина достижима из любой другой. *Ациклический орграф* - такой граф, в котором нет циклов, и все компоненты сильной связности состоят из одной вершины.

Эйлеровы и гамильтоновы циклы

Эйлеров цикл - цикл, проходящий через каждое ребро графа ровно по одному разу. Он существует тогда, когда степени всех вершин четны. *Гамильтонов цикл* - цикл, проходящий через каждую вершину графа по одному разу.

Делимость целых чисел

Говорят, что a делится на b, или b делит a, если существует такое k, что

$$a \vdots b = b | a \to a = kb$$

Свойства: ....

Деление целых чисел с остатком

Остатком деления числа a на b называется такое число r, что

$$a = kb + r,\ 0 \leq r < b$$

Частное и остаток определены однозначно для всех пар чисел.

Сравнения по модулю

Два числа *сравнимы по модулю*, если их остатки при делении на число, называемое *модулем* совпадают.

$$a \equiv b \ mod \ c$$

Эта запись означает, что остатки от деления a и b на c равны.

Основные свойства:

1. $a \equiv b \ mod \ c$ и $d \equiv e \ mod \ c \Rightarrow (a + d) \equiv (b + e) \ mod \ c$
2. $a \equiv b \ mod \ c$ и $d \equiv e \ mod \ c \Rightarrow (ad) \equiv (be) \ mod \ c$

---

17. Арифметика остатков

---

18. Малая теорема Ферма. Лемма Вильсона

Малая теорема Ферма гласит о том, что если $p > 2$ - простое число, a - целое число, не делящееся на p, то

$$a^{(p-1)} \equiv 1 \ mod \ p$$

Лемма Вильсона гласит о том, что число p простое тогда и только тогда, когда

$$(p - 1)! \equiv -1 \ mod \ p$$

---

19. Функция Эйлера. Теорема Эйлера

Функция Эйлера $\varphi(n)$ возвращает количество чисел, меньших n и взаимно простых с ним. *Теорема Эйлера* утверждает, что если a и m взаимно просты, то

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

---

20. Наибольший общий делитель. Алгоритм Евклида

Наибольшим общим делителем двух чисел a и b называют такое наибольшее число c, что $c|a$ и $c|b$.

Алгоритм Евклида - итеративный алгоритм, который ищет НОД двух чисел. Он состоит в следующем:

1. Вычитаем из большего числа меньшее
2. Заменяем большее на полученную разность
3. Повторяем 1 – 2 до тех пор, пока не получим равные числа. Если числа равны, то говорим, что последнее полученное таким образом число и есть наибольший общий делитель.

---

21. Расширенный алгоритм Евклида

Линейное диофантово уравнение - уравнение вида $ax + by = c$, где a, b, c - коэффициенты, x, y - неизвестные.

Расширенный алгоритм Евклида ищет решения линейного диофантова уравнения. ....

---

22. Простые числа. Формулировка основной теоремы арифметики.

Простое число - большее единицы число, такое что оно делится только на 1 и на себя.

Основная теорема арифметики гласит о том, что всякое число представимо в виде произведения простых, причем такое представление единственно с точностью до порядка следования сомножителей.

---

23. Бинарные отношения и операции над ними

Бинарным отношением над множествами A и B называется множество $P \subseteq A \times B$. Элементы этого множества суть пары, которые определяют, состоят ли два элемента *в отношении*, или нет. Тогда говорят, что пара (x, y) либо состоит в отношении, либо нет. Записать это можно как xPy.

Над бинарными отношениями определены следующие операции:

1. *Пересечение отношений* - обычное пересечение множеств.
2. *Объединение отношений* - простое объединение множеств.
3. *Включение* - обычное включение множеств.
4. *Инверсия* - операция, при которой все пары, которые не были до этого в отношении, в него становятся, и наоборот, все те, которые были в отношении - из него выходят.

5. *Композиция* - пусть есть два отношения $R \subseteq A \times B$, $S \subseteq B \times C$. Их композицией назовем отношение $R \circ S$, такое что

$$R \circ S = \{(x,y) | \forall z \in B : xRz \wedge zSy\}$$

---

24. Свойства бинарных отношений

Пусть есть множество A и $P \subseteq A \times A$. Тогда у такого отношения можно рассмотреть возможность наличия свойств:

1. *Рефлексивность*: $\forall a \in A: \ (a,a) \in P$
2. *Антирефлексивность*: $\forall a \in A: \ (a,a) \notin P$
3. *Симметричность*: $\forall a,b \in A : (a,b) \in P \Rightarrow (b,a) \in P$
4. *Антисимметричность*: $\forall a,b \in A : (a,b) \in P \wedge (b,a) \in P \Rightarrow a = b$
5. *Транзитивность*: $\forall a,b,c \in A : (a,b) \in P \wedge (b,c) \in P \Rightarrow (a,c) \in P$

---

25. Отношения эквивалентности

Бинарное отношение называется *отношением эквивалентности*, если оно рефлексивно, симметрично и транзитивно.

---

26. Отношения порядка

Бинарное отношение может называться *нестрогим частичным порядком*, если оно рефлексивное, антисимметричное и транзитивное.

Бинарное отношение может называться *строгим частичным порядком*, если оно антирефлексивно, антисимметрично и транзитивно.

Линейный порядок это частичный порядок с условием связности, то есть

$$\forall a,b \in X \Rightarrow (a,b) \in P \vee (b,a) \in P$$

27. Соответствия и функции. Образы и прообразы множеств

Соответствием или *функцией* называется такое отношение двух множеств, при котором элементам одного множества ставится в соответствие элементы другого множества.

$$f \subseteq A \times B$$

$$(x,y) \in f \Leftrightarrow f(x) = y$$

Существует операция взятия обратного соответствия:

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

Образом элемента x называется такой элемент y, что $f(x) = y$. *Образ множества* - множество всех образов элементов множества.

Прообразом элемента y называется такой элемент x, что $f(x) = y$. *Прообразом множества* называется множество всех прообразов элементов множества.

---

28. Виды функций

Соответствие называется *функциональным*, если $\forall (a = b) \Rightarrow f(a) = f(b)$.
Соответствие называется *всюду определенным*, или *тотальным*, если $\forall x\ \exists y : f(x) = y$.
Соответствие называется *сюрьективным*, если $\forall y\ \exists x : f(x) = y$.
Соответствие называется *инъективным*, если $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$
Соответствие называется *биекцией*, если оно одновременно и сюръекция, и инъекция.

---

29. Композиция функций, ее свойства

Композицией функций $f \circ g$ называется функция $f(g(x))$.

---

30. Обратная функция, ее свойства

Обратная функция $f^{-1}(x)$ - это такая функция, что $f(f^{-1}(x)) = x$.
Если f - инъективна, то f^{-1} - функциональна.
Если f - сюрьективна, то f^{-1} - тотальна.
Если f^{-1} - сюрьективна, то f - инъективна.
