Материалы для подготовки к коллоквиуму по дискретной математике Теоремы

ПМИ 2016

Орлов Никита, Рубачев Иван, Ткачев Андрей, Евсеев Борис

13 декабря 2016 г.

2. Бином Ньютона. Формула для биномиальных коэффициентов

Число сочетаний из n по k равно:

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

Доказательство. На первое место можно поставить любой из n элементов, на второе любой из $n-1$ оставшихся, ..., на k-е любой из $n-k+1$. Тогда по правилу произведения существует $n(n-1)(n-2)\cdots(n-k+1)$ упорядоченных наборов. Но порядок нам не важен, поэтому существует $\dfrac{n(n-1)(n-2)\cdots(n-k+1)}{k!} = \dfrac{n!}{k!(n-k)!}$ неупорядоченных наборов. □

Формула бинома Ньютона имеет вид:

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

Доказательство. Раскрытие скобок даст все возможные комбинации a и b длины n. Так как умножение коммутативно, то элементы с одинаковым количеством b можно сгрупировать. Тогда перед $a^{n-k}b^k$ будет стоять коэффициент c. Количество слогаемых, в которых b встречается ровно k раз равно $\binom{n}{k}$. Тогда $c = \binom{n}{k}$, а значит:

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

□

6. Формулы для суммы степеней вершин в неориентированном и в ориентированном графе

Определение. *Сумма степеней всех вершин в неориентированном графе равна удвоенному числу ребер.* $\sum\limits_{v \in V(G)} \deg(v) = 2 \cdot |E(G)|$

Доказательство. Пусть в графе степень каждой вершины равна 0 (в графе нет ребер). При добавлении ребра, связывающего любые две вершины, сумма всех степеней увеличивается на 2 единицы. Таким образом, сумма всех степеней вершин четна и равна удвоенному числу ребер. □

Определение. *Число исходящих степеней вершин равно числу входящих, равно числу ребер.*

Доказательство. Первая часть утверждения очевидна. Каждое ребро выходит из одной вершины и входит в другую, поэтому каждое ребро дает одинаковый вклад в суммы исходящих и входящих степеней вершин. Для доказательства второй части утверждения докажем что число ребер равно числу исходящих степеней вершин. Исходящая степень вершины равна числу ребер, которые из нее выходят. Ребро не может выходить более чем из одной вершины, поэтому сумма исходящих степеней вершин равна числу ребер. По транзитивности отношения «=» число ребер равно также и сумме исходящих вершин. □

10. Деревья – это в точности минимально связные графы

Доказательство.
[⇒] Пусть есть дерево G. По определению дерева, такой граф связен. Пусть после удаления ребра (u,v) граф G' остался связен. То есть в нем есть простой путь $u, a_1, a_2, \ldots, a_k, v$, но тогда после добавления ребра uv получим цикл $u, a_1, a_2, \ldots, a_k, v, u$, но в дереве циклов не бывает по определению. Противоречие.
[⇐] Пусть граф G минимально связен и он не дерево. То есть иммется цикл $u, a_1, a_2, \ldots, a_k, v, u$. Но тогда удаляя ребро (u, v) из этого цикла, мы не нарушим связность, так как будет существовать путь $u, a_1, a_2, \ldots, a_k, v$.
Теперь покажем, что добавление ребра к дереву, сделает его не деревом. Действительно, в дереве G уже существует простой путь $u, a_1, a_2, \ldots, a_k, v$ из вершины u в вершину v, а при добавлении ребра (u, v) появится цикл $u, a_1, a_2, \ldots, a_k, v, u$, то есть по определению это уже получится не дерево. □

14. Равносильность совойств ориентированных графов...

Формулировка. *Следующие свойства ориентированных графов равносильны:*

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

Доказательство.
(2) $\Rightarrow$ (1) Рассмотрим вершины пронумерованные так. Из того, что номера все время возрастают, следует отсутствие циклов в графе, так как в вершину с меньшим номером мы попасть не можем. Раз циклов нет, то существует единственная вершина из котрой можно попасть во все остальные – вершина с наименьшим номером. Она будет связана со всеми вершинами. Однако в нее попасть не возможно (в силу того, что номера у них больше, а значит ребер от них к вершине с наименьшим номером нет), значит первая вершина не сильно связана с другими вершинами. По свойству связности орграфов: u сильно связна с u. Значит в компоненту связности $C(1)$ входит только первая вершина. Из второй можно попасть во все кроме первой, но из них в нее попасть нельзя и т.д.

(3) $\Rightarrow$ (2) Предположим противное. Пусть в графе есть циклы. Тогда правильной нумерации вершин не существует так как если $v_{i_1}, v_{i_2}, \ldots, v_{i_k}, v_{i_1}$, тогда $i_1 < i_2 < \ldots < i_k < i_1$ – противоречие. Пусть граф ациклический, существование правильной нумерации докажем индукцией по числу вершин. Если вершина одна, то правильная нумерация очевидно существует. Пусть утверждение справедливо для графа с p вершинами, рассмотрим ациклический граф с $p+1$ вершиной. Возьмем любую вершину в нем и начнем строить путь с началом в этой точке. Так как граф ациклический и конечный, то мы придём к вершине, из которой никуда нельзя попасть. Присвоим ей номер $p+1$ и уберем из графа. Получим ациклический граф на p вершинах, в котором по предположеню индукции можно сделать правильную нумерацию.

(1) $\Rightarrow$ (3) Это следствие практически очевидно. Условие о том, что каждая компонента сильной связности состоит ровно из одной вершины делает невозможным существование циклов длины больше 1.

Из доказанного выше (1) $\Rightarrow$ (3) $\Rightarrow$ (2) $\Rightarrow$ (1) следует, что (1) $\iff$ (2) $\iff$ (3) □

18. Признаки делимости на 3, 9 и 11

Число x делистся на 3 (на 9) тогда и только тогда, когда сумма его цифр делится на 3 (на 9)

Доказательство. Пусть $x = \overline{a_n a_{n-1} \ldots a_1 a_0} = 10^n a_n + 10^{n-1} a_{n-1} + \ldots + 10a_1 + a_0$. Так как $10 \equiv 1 \pmod 3$, то:

$$x \equiv \sum_{i=0}^{n} a_i \pmod 3$$

Для делимости на 9 доказательство аналогично. □

Число x делится на 11, тогда и только тогда, когда:

$$11 \Big| \left(\sum_{2|i}^{n} a_i - \sum_{2\nmid i}^{n} a_i \right)$$

Доказательство. $10 \equiv -1 \pmod{11}$, значит $10^n \equiv (-1)^n \pmod{11}$. Тогда:

$$x \equiv (-1)^n a_n + (-1)^{n-1} a_{n-1} + \ldots + (-1) a_1 + a_0 \equiv \sum_{2|i}^{n} a_i - \sum_{2\nmid i}^{n} a_i \pmod{11}$$

□

22. Основная теорема арифметики

Лемма. *Если простое число p делит без остатка произведение двух целых чисел $x \cdot y$, то p делит x или y.*

Доказательство. Пусть $x \cdot y$ делятся на p, но x не делится на p, тогда x и p – взаимнопростые, следовательно, найдутся такие целые числа u и v, что:

$$x \cdot u + p \cdot v = 1$$

Умножая обе части на y получаем:

$$(x \cdot y) \cdot u + p \cdot v \cdot y = y$$

Здесь оба слогаемых в левой части делятся на p, значит и y делится на p. □

Теорема. *Каждое натуральное число $n > 1$ представляется в виде $n = p_1 \cdot \ldots \cdot p_k$, где $p_1, \ldots, p_k$ – простые числа, причём такое представление единственно с точностью до порядка следования сомножителей.*

Доказательство.

Существование. Если n – простое, разложение очевидно: $n = n_1$. Иначе $n = x \cdot y$ для некоторых $1 < x,y < n$. Так как для x и y разложения существуют, их можно подставить в выражение $n = x \cdot y$ и получить разложение числа n.

Единственность. Если n – простое, единственность очевидна. Иначе предположим, что существуют два различных разложения:

$$n = p_1 p_2 \cdots p_i = q_1 q_2 \cdots q_j$$

Заметим, что среди p и q нет равных чисел, иначе на них можно было бы сократить и получилось бы число $n' < n$, а у него, согласно предположению индукции, разложение единственно.

Пусть $p_a q_b$ – наименьшие в своих разложениях. Так как в каждом разложении как минимум два числа, $n \geqslant p_a^2; n \geqslant q_b^2$. Так как $p_a \neq q_b$, одно из неравенств строгое. Тогда $p_a \cdot q_b < n$. Значит, $n - p_a q_b$ – натуральное и меньше n, значит, раскладывается единственным образом; при этом оно делится на p_a и на q_b, значит, они входят в его разложение.

Значит, $p_1 p_2 \cdots p_i$ делится на $p_a q_b$; значит, произведение всех p, кроме a-того, делится на q_b, что невозможно, так как они просты и среди них нет числа равного q_b. Противоречие. □

26. Критерий того, что бинарное отношение записывается с помощью функции полезности

Формулировка. *Пусть множество A конечно, тогда соотношение:*

$$xPy \iff u(x) > u(y)$$

Выполняется для некоторой функции $u(x)$ в том и только в том случае, когда P – отношение слабого порядка.

Доказательство.
[$\Rightarrow$] Докажем это утверждение в одну сторону. Пусть выполняется данное соотношение. Для того чтобы доказать, что P – отношение слабого порядка, необходимо проверить его антирефлексивность, транзитивность и транзитивность его дополнения.

Антирефлексивность. Пусть $x \in A$. Тогда $u(x)$ не больше $u(x)$, то есть $x\overline{P}x$. Значит отношение P антирефлексивно.

Транзитивность. Пусть $x,y,z \in A$, таковы, что xPy и yPz. Это значит, что $u(x) > u(y)$ и $u(y) > u(z)$. Следовательно, $u(x) > u(z)$, или xPz, значит P транзитивно.

Транзитивность дополнения. Пусть $x,y,z \in A$ таковы, что $x\overline{P}y$ и $y\overline{P}z$. В силу соотношения из формулировки $u(x) \leqslant u(y)$ и $u(y) \leqslant u(z)$, отсюда $x\overline{P}z$, то есть $\overline{P}$ транзитивно.

[$\Leftarrow$] Пусть P – слабый порядок. Определим значение $u(x)$, как число элементов во множестве $\{y|xPy\}$, то есть число альтернатив, которые менее предпочтительны, чем x. Докажем, что при этом $xPy \iff u(x) > u(y)$.

Пусть xPy. Поскольку отношение P транзитивно, то для любого z, такого, что yPz, верно и xPz. Поэтому из x выходят дуги как минимум в те же вершины, что и из y, значит $u(x) \geqslant u(y)$. Кроме того P антирефлексивно, поэтому из y не ведет дуга в y, а из x в y ведет. Значит, $u(x) > u(y)$.

Обратно, пусть $u(x) > u(y)$, т.е. из x выходит больше дуг, чем из y. Значит, существует такой элемент z, что xPz, но $y\overline{P}z$. Если $x\overline{P}y$, то отношение $\overline{P}$ не транзитивно, что противоречит условию, значит $(x,y) \in P$. $\square$

30. Биекция между двоичными словами, подмножествами конечного множества и характеристическими функциями

Определение. *Характеристической функцией множества $X \subset U$ называют функцию χ_X, которая равна 1 на элементах X и 0 на остальных элементах U.*

Составим двоичное слово следующим образом: если i элемент лежит в X, то на i-м месте ставим 1, иначе 0. Биекция между характеристической функцией и подмножеством очевидна – значения характеристической функции однозначно задают подмножество.