Домашнее задание 1

Задача 1

$$1 \cdot (n-1) + 2 \cdot (n-2) + \ldots + (n-1) \cdot 1 = \frac{(n-1) \cdot n \cdot (n+1)}{6}.$$

Решение.

База.

$n = 1$.

$1 \cdot 0 = \frac{(1-1) \cdot 1 \cdot (1+1)}{6}$.

$0 = 0$

Шаг.

Мы можем представить левую часть уравнения как

$$\sum_{i=1}^{n-1} i \cdot (n-i) = \sum_{i=1}^{n-1} (i \cdot n - i^2) = \sum_{i=1}^{n-1} (i \cdot n) - \sum_{i=1}^{n-1} i^2.$$

Также заметим, используя формулу суммы арифмитической прогрессии, что

$$\sum_{i=1}^{n-1} (i \cdot n) = \left(\frac{1 + (n-1)}{2} \cdot (n-1) \right) \cdot n = \frac{n^3 - n^2}{2}.$$

и

$$\sum_{i=1}^{n} (i \cdot (n+1)) = \sum_{i=1}^{n} (i \cdot n) + \sum_{i=1}^{n} (i) = \frac{n^3 + n^2}{2} + \frac{n^2 + n}{2} = \frac{n^3 + 2n^2 + n}{2}.$$

Тогда докажем, что

$$\left(\sum_{i=1}^{n} (i \cdot n) - \sum_{i=1}^{n} i^2 \right) - \left(\sum_{i=1}^{n-1} (i \cdot n) - \sum_{i=1}^{n-1} i^2 \right) = \frac{n \cdot (n+1) \cdot (n+2)}{6} - \frac{(n-1) \cdot n \cdot (n+1)}{6}.$$

$$\frac{n^3 + 2n^2 + n}{2} - \frac{n^3 - n^2}{2} - n^2 = \frac{(n^3 + 2n^2 + n^2 + 2n) - (n^3 + n^2 - n^2 - n)}{6}.$$

$$\frac{3n^2 + n}{2} - n^2 = \frac{3n^2 + 3n}{6}.$$

$$\frac{n^2 + n}{2} = \frac{n^2 + n}{2}.$$

Задача 2

$$\cos(x) + \cos(2x) + \ldots + \cos(nx) = \frac{\sin(n+\frac{1}{2})x}{2sin\frac{x}{2}} - \frac{1}{2}.$$

База.

$n = 1$

$$\cos(x) = \frac{\sin\frac{3}{2}x}{2sin\frac{x}{2}} - \frac{1}{2}.$$

$$\cos(x) = \frac{\sin\frac{3}{2}x}{2sin\frac{x}{2}} - \frac{\sin\frac{1}{2}x}{2sin\frac{x}{2}}.$$

$$\cos(x) = \frac{2\sin\frac{x}{2}\cdot\cos(x)}{2\sin\frac{x}{2}}.$$

$$\cos(x) = \cos(x).$$

Шаг. Докажем, что

$$\cos(x) + \cos(2x) + \ldots + \cos(nx) + \cos x(n+1) = \frac{\sin(n+1+\frac{1}{2})x}{2sin\frac{x}{2}} - \frac{1}{2}.$$

$$\frac{\sin(n+1+\frac{1}{2})x}{2sin\frac{x}{2}} - \frac{1}{2} = \frac{\sin(n+\frac{1}{2})x}{2sin\frac{x}{2}} - \frac{1}{2} + cosx(n+1).$$

$$\frac{\sin(n+1+\frac{1}{2})x}{2sin\frac{x}{2}} - \frac{1}{2} = \frac{\sin(n+\frac{1}{2})x - \sin\frac{x}{2} + 2\sin\frac{x}{2}\cos x(n+1)}{2\sin\frac{x}{2}}.$$

$$\frac{\sin(n+1+\frac{1}{2})x}{2sin\frac{x}{2}} - \frac{1}{2} = \frac{\sin(n+\frac{1}{2})x - \sin\frac{x}{2} + \sin(\frac{x}{2}+nx+x) + \sin(\frac{x}{2}-nx-x)}{2\sin\frac{x}{2}}.$$

$$\frac{\sin(\frac{x}{2}+nx+x) - \sin\frac{x}{2}}{2sin\frac{x}{2}} = \frac{\sin(n+\frac{1}{2})x - \sin\frac{x}{2} + \sin(\frac{x}{2}+nx+x) + \sin(\frac{x}{2}-nx-x)}{2\sin\frac{x}{2}}.$$

$$\frac{\sin(n+\frac{1}{2})x + \sin(\frac{x}{2}-nx-x)}{2\sin\frac{x}{2}} = 0.$$

$$\frac{\sin(n+\frac{1}{2})x - \sin(n+\frac{1}{2})x}{2\sin\frac{x}{2}} = 0.$$

$$\frac{0}{2\sin\frac{x}{2}} = 0.$$

$$0 = 0.$$

Задача 4

$$\frac{1}{n+1} + \frac{1}{n+2} + \ldots + \frac{1}{2n} > 13/24, \text{ для всех } n > 1.$$

База.

$n = 2$

$$\frac{1}{3} + \frac{1}{4} = 14/24 > 13/24.$$

Шаг.

Докажем, что послдеовательность будет возрастающей, а значит, что $f(n+1) > f(n)$ и тогда из базы $=>$ $f(n) \geq 14/24$ при $n \geq 2$ и значит $f(n) > 13/24$ при $n > 1$.

$\left(\frac{1}{n+2} + \frac{1}{n+3} + \ldots + \frac{1}{2(n+1)}\right) - \left(\frac{1}{n+1} + \frac{1}{n+2} + \ldots + \frac{1}{2n}\right) = \frac{1}{2n+1} + \frac{1}{2(n+1)} - \frac{1}{n+1} = \frac{2(n+1)+2n+1-2(2n+1)}{2(n+1)(2n+1)} = \frac{1}{2(n+1)(2n+1)} > 0.$

Последовательность возрастающая, так как разность между ее текущим и предыдущим членом положительна.

Задача 7

$$\frac{1}{n+1} + \frac{1}{n+2} + \ldots + \frac{1}{2n} > 13/24, \text{ для всех } n > 1.$$

База.

$n = 1$.

$4/2^1 = 2$.

Шаг.

Заметим, что текущее число на шаге n будет делиться на 2^{n+1} либо нацело, либо с остатком равным единице.

Обозначим число на шаге n за t. Будем просто приписывать слева 3 или 4. Тогда мы можем представить следующее число как $3 * 10^n + t = 3*(2^n*5^n)+t$ в случае, если мы приписали тройку и $4*10^n+t = 2^{n+2}*5^n+t$. Легко заметить, что $2^{n+2} * 5^n$ делится на 2^{n+1} нацело, а $3 * (2^n * 5^n)$ с остатком один. Тогда мы можем в случае, если t делится на 2^{n+1} нацело добавлять в начало числа четверку, а если же с остатком 1 – тройку.

Домашнее задание 2

Во всей работе $\binom{n}{k}$ – это количество сочетаний по k из n элементов.

Задача 1

Найти сумму всех пятизначных чисел, составленных из нечетных цифр.

Решение.

Заметим, что всего у нас пять нечетных цифр: $1, 3, 5, 7, 9$. Их сумма равна 25. Будем рассматривать поразрядно пятизначные числа. Каждое число в каждом разряде может войти $5 * 5 * 5 * 5$ раз, потому что у когда мы "установили"одно число у нас остается четыре разряда в которх может быть любое другое нечетное число. Отсюда мы можем заметить, что и сумма в одном разряде может войти 5^4 раз. Также заметим, что сумма в первом разряде будет $25 * 10^1$, $25 * 10^2$ во втором ... и $25 * 10^5$ в пятом.

Тогда, если нумеровать разряды справа налево и обозначить текущий номер разряда за i для каждого разряда формула будет: $25 * 10^i * 5^4$. То есть итоговая формула:

$$\sum_{i=1}^{5} 25 * 5^4 * 10^i = 173609375.$$

Задача 2

Для определенности будем говорить о *натуральных* числах.

Пункт а)

Посчитаем все числа до миллиона в которых нет единицы. Мы можем сделать это так: Будем считать, что у нас есть шесть позиций на которых могут стоять числа от нуля до девяти, исключая единицу, то есть их девять штук. Тогда, к примеру, когда на первых пяти позициях будут стоять нули мы учтем все однозначные числа, потом когда на первых четырех позициях будут стоять нули мы учтем двухзначные и так далее до того, когда нулей не будет и мы учтем все шестизначные числа без единиц. $9^6 = 531441$. Теперь отнимем от 10^6 вычисленное кол-во чисел без единиц, очевидно, получим кол-во чисел с единицами. $10^6 - 9^6 = 468559$. Надо отметить, что здесь учтен ноль, но не учтено 10^6. То есть итоговые

значения будут: 531440 чисел без единиц и 468560 чисел с единицами. Но на общий ответ пункта а это, как видим, не влияет. Ответ: в первом миллионе больше чисел без единиц.

Пункт б)

Аналогично. Чисел без единиц $9^7 - 1$(не учитываем ноль). $= 4782968$. С единицами $10^7 - 9^7 + 1$(учитываем 10^7) $= 5217032$. Ответ: в певых десяти миллионах больше чисел с единицами.

Задача 3

Найдем количество десятизначных чисел в которых все цифры различны. Будем рассматривать число с левого края. На первое место мы можем поставить любую из 10 цифр, кроме нуля(так как число не может начинаться с нуля), то есть 9. На второе место, чтобы сохранялось свойство различности всех цифр, мы можем поставить любую цифру, включая теперь уже ноль, но исключая то, которое было на первом месте $=$ 9. На третье место мы можем поставить любую цифру за исключением двух, что стояли на предыдущих местах $= 8$. И так же рассуждаем далее, до 10-го места, на которое мы можем поставить уже лишь одну цифру. В итоге имееи $9 * 9 * 8 * 7 * 6 * 5 * 4 * 3 * 2 * 1 = 3265920 = 9 * 9!$ десятизначных чисел в которых все цифры различны. Тогда мы можем получить кол-во десятизначных чисел у которых хотя бы две цифры совпадают просто отняв полученное значение от общего кол-ва десятизначных цифр. $(10^10 - 10^9) - 3265920 = 8996734080 = (9 * 10^9) - 9 * 9!$. А теперь просто посчитаем вероятность по известной формуле (кол-во благоприятных исходов)/(кол-во всех исходов). $8996734080/(10^10 - 10^9) = \frac{9*(10^9-9!)}{9*10^9} = \frac{10^9-9!}{10^9}$.

Ответ: $\frac{10^9-9!}{10^9}$.

Задача 4

а)Возьмем некого человека. Способов выбрать ему пару у нас будет $2n - 1$. Первая пара готова. После чего возьмем другого человека. Способов выбрать ему пару уже будет $2n - 3$. И т.д. вплоть до предпоследнего человека, способов выбрать которому пару будет один, так как останется лишь один человек. Можем записать это как $\prod_{i=0}^{n-1}(2n - 2 * i + 1)$. б) Из предыдущего пункта: 2n и $2*i$ очевидно четные и четное-четное=четное.

Тогда как четное+1 = нечетное. И нечетное*нечетное = нечетное, а у нас произведения ряда нечетных чисел – значит и все произведение будет нечетное.

Задача 5

Пусть первая масть у нас уже стоит в порядке возрастания. Теперь нам нужно вставить в колоду вторую масть в порядке возрастания. Вставлять каждую карту новой масти мы можем как до всех карт первой масти, так и между ними, так и после них, а значит мы точно можем воспользоваться методом перегородок, разбивая их на 14 групп: $\binom{13+14-1}{13}$. У нас станет уже 26 карт в колоде. Будем втсавлять карты третьей масти аналогично. Получим 39 карт и вставим точно таким же способом карты четвертой масти. Тогда итоговая формула будет: $\binom{26}{13} * \binom{39}{13} * \binom{52}{13}$.

Количество всех способов расположений карт – 52!. Тогда итоговая вероятность $\frac{52!}{\binom{26}{13}*\binom{39}{13}*\binom{52}{13}!} = \frac{1}{3*13!}$.

Задача 6

Всего способов выбрать шесть карт из колоды в 36 существует $\binom{36}{6} = \frac{31*32*33*34*35*36}{6!} = 1947792$.

а) Туза всего четыре, тогда в колоде без них 32 карты, а значит выбрать шесть карт без тузов совсем будет $\binom{32}{6} = \frac{27*28*29*30*31*32}{6!}$ способа. Значит количество способов выбрать шесть карт с хотя бы одним тузом будет равняться разности количества всех способов выбрать шесть карт и количества способов выбрать шесть карт без тузов.

Тогда вероятность будет равна: $\frac{\frac{31*32*33*34*35*36}{6!} - \frac{27*28*29*30*31*32}{6!}}{\frac{31*32*33*34*35*36}{6!}} \approx 0,534$.

б) Рассмотрим как вообще мы можем соотнести четыре масти к шести картам. У нас будет всего два способа такого разбиения: $2+2+1+1$ и 3+1+1+1. Теперь посчитаем кол-во способов подобрать такие разбиения. Для $2+2+1+1$: Выбрать две карты из одной масти у нас $\binom{9}{2}$ и это войдет в квадрате, так как мы выбираем две карты два раза для двух разных мастей. Еще, так как масти четыре, а нам нужно выбрать две из которых мы и будем брать по две карты, то это еще домножим на $\binom{4}{2}$ – кол-во способов выбрать две масти из четырех. И еще нам остается выбрать две любых карты из двух оставшихся мастей – это 9^2. В общем

получаем $\binom{4}{2} * (\binom{9}{2})^2 * 9^2$. Для $3+1+1+1$: Выбрать три карты из одной масти у нас $\binom{9}{3}$ и, так как масти четыре нам еще нужно домножить это на 4 – кол-во способов выбрать одну масть из четырех. Теперь нам нужно выбратть три оставшихся карты других мастей. В других мастях так же по 9 карт, а значит способов сделать это 9^3. В общем получаем $4 * \binom{9}{3} * 9^3$.

Раз у нас два способа различных разбиений на масти, то ответом будет сумма вариантов каждого из способов. Конечная формула: $\binom{4}{2} * (\binom{9}{2})^2 * 9^2 + 4 * \binom{9}{3} * 9^3$.

А вероятность равна: $\frac{\binom{4}{2}*(\binom{9}{2})^2*9^2+4*\binom{9}{3}*9^3}{1947792} \approx 0,45$.

Задача 7

Начнем рассматривать комнаты по пордяку. Логично, что так как студентов 7, то у нас существует 7 способов поселить их в одноместную комнату. Далее будем заселять двухместную комнату, но так как мы перед этим уже заселили одноместную, то расчет будем делать уже из шести студентов. Тогда кол-во таких способов: $\binom{6}{2} = /frac6!2! * 4! = 15$. В конце будем заселять четырехместную комнату, но, так как у нас к этому моменту осталось всего четыре студента, то и способ будет один. Итоговая формула примет вид $7 * 15 * 1 = 105$.

Задача 8

Будем выбирать команды, которые играют на домашнем поле. Из 16 нам нужно выбрать 8 команд. Это $\binom{16}{8}$. Мы выбрали некую последовательность команд, играющих на домашнем поле, теперь нужно сопоставить каждому члену этой последовательности противника из оставшихся команд, которых восемь, а значит кол-во способов сопоставить противников 8!. Итоговая формула $\binom{16}{8} * 8!$.

Задача 9

Представим книги числами от одного до 20. После заметим, что нам нужно разделить их четырьмя перегородками, т.е. до первой перегородки – на первую полку, между первой и второй – на вторую, ... после четвертой – на пятую. Тогда добавим эти перегородки в наш ряд книг(к

примеру представим их цифрой "0") и всего цифр получится 24. Тогда чтобы каждая книга побывала на всех возможных местах нам нужно рассмотреть все перестановки получившегося "ряда"чисел, а их будет 24!. Но так как мы считали перегородки тоже за книги у нас появились лишние перестановки. Так как перегородок было 4, то итоговая формула примет вид $24!/4! = 10626$.

Домашнее задание 2

Примечание: я запутался с обозначением C_n^k и $\binom{n}{k}$, подумав, что в формуле с буквой С большее число так же пишется сверху. Это оказалось не так, но, к сожалению, я узнал об этом слишком поздно, а этой формулы в работе достаточно и я просто не успел ее поправить во всех местах, поэтому, во избежание путаницы, везде оставил ее в виде C_k^n, т.е. с написанием большего числа сверху.

Задача 2

Начнем рассматривать комнаты по пордяку. Способов поселить в первую двухместную комнату у нас C_2^{18}. Далее способов поселить во вторую уже C_2^{16}. Человек осталось 16, так как двоих мы уже "поселили". Далее так же продолжим рассуждать для трехместных и четырехместных комнат. Тогда итоговая формула примет вид: $C_2^{18} \cdot C_2^{16} \cdot C_3^{14} \cdot C_3^{11} \cdot C_4^8 \cdot C_4^4 = 77189112000$.

Задача 3

а)

$$\binom{n}{m} \cdot \binom{m}{k} = \binom{n}{k} \cdot \binom{n-k}{m-k}.$$

$$\frac{n!}{m! * (n-m)!} \cdot \frac{m!}{k! * (m-k)!} = \frac{n!}{k! * (n-k)!} \cdot \frac{(n-k)!}{(m-k)! * (n-k-(m-k))!}$$

$$\frac{n!}{(n-m)!} \cdot \frac{1}{k! * (m-k)!} = \frac{n!}{k!} \cdot \frac{1}{(m-k)! * (n-k-(m-k))!}$$

Разделим обе части уравнения на $n!$ и домножим на $(m-k)!$.

$$\frac{1}{(n-m)!} \cdot \frac{1}{k!} = \frac{1}{k!} \cdot \frac{1}{(n-k-(m-k))!}$$

Домножим обе части уравнения на $k! * (n-m)!$.

$$1 = 1$$

Задача 4

Отнимем от общего числа акций пять, так как людей пять и каждому должно достаться хотя бы по одной акции, эти мы как бы изначально "раздадим" им по одной. Теперь мы можем просто воспользоваться методом перегородок, при котором кому-то может и не достаться акций вообще, но ответ будет верный, так как мы уже раздали по одной акции. У нас будет 95 акций и четыре перегородки: $C_{95}^{99} = \frac{99!}{95!*4!} = \frac{96*97*98*99}{24} = 3764376$.

Задача 5

Воспользуемся методом перегородок, при этом будем помнить, что в пределах дня порядок пациентов важен. Перегородки будет четыре. Тогда количество всех перестановок элементов и перегородок равно 10!. Но нас не интересуют перестановки самих перегородок, нас интересуют только перестановки пациентов. Тогда, чтобы не учитывать перестановки четырех перегородок, нам нужно количество перестановок всех разделить на количество перестановок, которое равно 4!. Итоговая формула примет вид 10!/4!.

Задача 6

а) Будем рассматривать количество способов проголосовать для одного человека. Так как он может голосовать за любого, в том числе и за себя, способов n. У следующего так же n. Тогда выходит, что есть n ччеловек, каждый из которых может проголосовать n способами, тогда итоговая формула будет n^n.

б) Слегка преформулируем задачу. У нас есть n голосов, которые нужно распреедлить между n кандидатами. Видно, что можем воспользоваться методом перегородок, при этом перегородок $n - 1$. Тогда итоговая формула C_{n-1}^{2n-1}.

Задача 7

Рассмотрим сначала пересечение двух событий: играющей музыки и идущего дождя, которые продолжались, соответственно, 90% и 50%. Очевидно, что только 10% не заполнено первым событием, а значит их пе-

ресечение не может быть меньше 40%. Теперь будем рассматривать пересечение объединения первых двух событий с третьим событием, которое продолжалось 80% времени – выключенным светом. Очевидно, что только пересечение третьего события с подсчитанным уже пересечением первых двух и будет составлять ответ. Опять же видно, что третее событие не заполняет лишь 20%, а значит его пересечение с пересечением первых двух, составляющим 40%, будет никак не меньше 20%, что и будет ответом.

Ответ: 20%.

Задача 9

Из материала учебника мы знаем, что найти кол-во решений уравнения в целых неотрицательных числах $x_1+x_2+\cdots+x_k = n$ мы можем методом перегородок, формулой C_{k-1}^{n+k-1}. В задаче везде под "количество решений уравнения" подразумевается кол-во решений в целых неотрицательных числах.

а) Посчитаем количество решений данного уравнения, когда $x_1 > 3$. Воспользуемся методом преегородок, перегородок три, так как переменных 4. При этом сначала отнимем от десяти четыре для того, чтобы изначально сделать x1 = 4, чтобы когда мы будем считать перегородками и в x1 не "уйдет"ничего, все равно выполнялось условие. Тогда количество решений при $x_1 > 3$ равно $C_3^9 = 84$.

Теперь мы можем просто посчитать вышеописанным способом общее количество решений данного уравнения, отнять от него кол-во неподходящих решений и получить ответ. Общее кол-во решений равно $C_3^{13} = 286$.

А ответ будет $286 - 84 = 202$.

б) Теперь будем рассматривать четыре случай, когда $x_1 = 0, x_1 = 1, x_1 = 2, x_1 = 3$. Для каждого случая мы можем посчитать количество решений уравнения еще с условием $x_2 \leq 3$ аналогично тому, как мы делали в предыдущем пункте. К примеру, рассмотрим первый вариант, когда $x_1 = 0$.

Тогда общее кол-во решений уравнения можно посчитать, только теперь переменных уже осталось три, так как одну мы определили, а значит перегородок будет две. Общее кол-во решений равно C_2^{12}. Теперь нам остается только посчитать кол-во "лишних" решений, т.е. когда $x_2 > 3$. Это мы можем сделать аналогично прошлому пункту, то есть отняв от

десяти четыре, как бы изначально приравняв x_2 к четырем и посчитав кол-во решений для уравнения. Таких решений будет C_2^8. А подходящих нам решений будет $C_2^{12} - C_2^8 = 38$.

Аналогично мы можем посчитать для $x_1 = 1, x_1 = 2, x_1 = 3$, только сначала нужно не забыть отнять текущее значение x_1 от десяти. Ответы для этих случаев будут соответсвенно 34, 30 и 26. Тогда общее кол-во решений это кол-во решений уравнения по всем случаям и оно равно 128.

Домашнее задание 4

Задача 1

Представим задачу в виде графа. Тогда вершины это люди, а ребра – их знакомство. Тогда количество пар знакомых людей – это количество ребер в графе. И из того, что у каждых двух человек ровно пять общих знакомых мы можем заключить, что каждое ребро входит в ровно пять циклов длины три(цикл: ребро между двумя рассматриваемыми людьми – ребро от первого человека до общего знакомого – ребро от второго человека до общго знаокомого). Тогда 5 * (кол-во ребер) = 3 * (кол-во циклов длины 3). А так как 5 не делится на три, то кол-во ребер(кол-во пар знакомых) должно делиться на 3.

Задача 2

Обозначим кол-во ребер за $num(E)$.

а) Чтобы граф из n вершин был связным нужно как минимум n-1 ребро (это будет дерево). А полносвязный граф имеет $\frac{n(n-1)}{2}$ ребер. Тогда $n-1 \leq num(E) \leq \frac{n(n-1)}{2}$.

б) Граф с минимальным кол-вом ребер, а значит с максимальным кол-вом вершин при каком-то кол-ве ребер – дерево и в нем $(num(E)) + 1$ вершина. А наименьшее кол-во вершин при наибольшем количестве ребер достигается в полносвязном графе. Значит минимальное кол-во вершин в графе с $num(E)$ ребер будет равно количеству вершин $n_{num(E)}$ в полносвязном графе, для которого $num(E) \leq \frac{n_{num(E)}(n_{num(E)}-1)}{2}$, потому что мы рассматриваем только простые графы, а значит в них не может быть кратных ребер и петель. Значит $n_{num(E)} \leq num(E) \leq (num(E))+1$.

Задача 4

Количество ребер в графе равно половине суммы степеней его вершин. Количество вершин у нас n и степень каждой вершины равна k по определению регулярного графа. Тогда nk должно быть четным, иначе при делении его на два получится нецелое число, а кол-во ребер не может быть нецелым.

Степень вершины в графе из n вершин без кратных ребер и петель(а мы такие и рассматриваем) не может быть по определению больше, чем $n - 1$.

Задача 5

Мы можем взять подграф нашего графа, который будет являться связным и ацикличным. Такой подграф можно найти с помощью алгоритма: начнем с любой вершины. Отметим ее как посещенную. После перейдем во все вершины, доступные из нее и также пометим их как посещенные, а ребра по которым перешли добавим в подграф. Далее перейдем во все вершины, которые доступны из этих вершин и опять добавим ребра по которым преешли в подграф. И так до тех пор, пока останутся непосещенные вершины. Так как граф неориентированный и связный мы точно посетим все вершины. После мы можем просто удалить любой лист этого подграфа и удалить в наешм основном графе вершину ему соответсвующую и основной граф все равно останется связен, поскольку наша вершина – лист, она имеет только одно ребро в подграфе, притом с вершиной до которой мы смогли дойти из предыдущих вершин. А с другими вершинами она не имеет ребер ,что означает, что мы смогли добраться до тех вершин каким-то другим путем и удаление этой вершины никак не повлияет на его существование.

Задача 6

а) Пример прикрепил во вложении к письму.

.

Домашнее задание 5

Задача 1

% – деление с остатком. а) Рассмотрим сначала исходный граф-цикл на 2n вершинах.Пронумеруем его вершины. Единтственная его возможная раскраска в два цвета – это когда вершины с четными номерами покрашены в один цвет, а с нечетными – в другой. Заметим, что противоположная вершина к текущей(t) будет $(t+2n/2)\%2n$. Осюда если n четное, то и номер противолежащей вершины к текущей вершине будет давать тоот же остаток при делении на 2, что и номер текущей вершины, т.к. (четное + четное) = четное и (нечетное + четное) = нечетное и деление с остатком так же оставляет ту же четность.

А вот если n – нечетное, то номер противолежащаей вершины будет четным, если номер текущей вершины нечетен и нечетным иначе.

Значит при нечетных n граф можно расскрасить в два цвета, а при нечетных – нет.

б) Если граф можно раскрасить в два цвета, то его, очевидно, можно раскрасить и в три цвета. То есть при нечетных n граф можно раскрасить в три цвета. Теперь рассмотрим случай четных n.

Сразу отметим, что при n = 2, если провести все ребра соединяющие противоположные вершины, то получим полносвязный граф на четырех вершинах, который нельзя раскрасить в три цвета.

Рассмотрим остальные графы при нечетных n. Пусть у нас будут 3 цвета: I, II, III. Покрасим первые n вершин чередуя цвета I и II. n + 1 и 2n покрасим в цвет III. А все, между n + 1 и 2n покрасим, опять же, чередуя I и II. Тогда исходный граф-цикл и вершины n + 1 и 2n и им противолежащие правильно раскрашены по построению. А также остальные тоже, потому что первая половина графа покрашена в чередующиеся I и II и вторая так же, но со "сдвигом"на одну вершину, то есть вершина, противолежащая к вершине из первой половины графа, будет как раз иметь другой цвет.

Задача 2

а) Простой путь мы моежм строить только переходя из вершин одной доли в вершины другой доли и его длина будет не больше, чем количе-

ство вершин в наименьшей доли +1 (так как мы можем вернуться еще в первую долю). Значит k <= 2 * min(n, m) + 1.

б) Из рассуждений к задаче 5 видно, что при m=n в таком графе будет гамильтонов цикл длиной 2*n. Также мы заметили, что если вершин в одной из долей меньше, то нам потом будет "не хватать"вершин для завершения цикла. Отметим, что при построении простого цикла, также как и при построении Гимильтонова мы можем переходить из вершины одной доли только к вершинам другой доли, а так же нам в конце нужно вернуться в исходную долю. Из этого всего следует, что для цикла k <= 2 * min(m, n).

Задача 3

Это граф, состоящий из двух компонент связности из 4 и 5 вершин, каждая из которых полносвязна. Тогда в первой будет четыре вершины со степенью 3, а во второй пять вершин со степенью 4, что и требуется по условию задачи. А так как наш граф несвязный, то он не содержит гамильтонов цикл по определению, то есть не является гамильтоновым графом.

Задача 5

а) Эйлеров цикл существует тогда и только тогда, когда граф связный и в нем отсутсвуют вершины нечетной степени. Так как в полном двудольном графе степень каждой вершины по определению равна количеству вершин в доле, в которой ее нет, то он Эйлеров цикл будет существовать в графе $K_{m,n}$ только при четных m и n.

б) Так как граф двудольный, то при построении гамильтонова цикла мы можем переходить из вершины одной доли только в вершины другой доли и при этом не можем посещать одну вершину более чем один раз. Отсюда следует, что m должно быть равно n, так как иначе в какой-то момент при построении нам просто не "хватит"вершин в одной доле, чтобы обойти оставшиеся в другой. И при этом оба числа должны быть больше одного, так как в графе из двух вершин, по одной в каждой доле, не будет гамильтонова цикла.

в) Обозначим вершины первой доли как $1, 2, \ldots 6$, а второй как $1i, 2i, \ldots 6i$.

Тогда Гамильтонов цикл: $1 - 1i - 2 - 2i - 3 - 3i - 4 - 4i - 5 - 5i - 6 - 6i - 1$.

Задача 5

Добавим кратные ребра между теми вершинами, между которыми в исходном графе есть ребро. Тогда кол-во ребер инцендентных каждой вершине удвоится, а значит четные степени вершин останутся четными, а нечетные станут четными. А по теореме, доказанной Эйлером, Эйлеров цикл существует тогда и только тогда, когда граф связный и в нем отсутствуют вершины нечетной степени.

Полученный граф связен, потому что исходный граф был связен, а мы не удаляли ребра, а только добавляли их. То есть в полученном графе с кратными ребрами существует эйлеров цикл, то есть такой обход, в процессе которого мы пройдемся по каждому его ребру единожды. Теперь, если в порядке этого обхода прохождение по добавленным нами кратным ребрам рассматривать как прохождение по соответствующим ребрам исходного графа, мы как раз и получим такой обход в исходном графе, при котором мы пройдемся по каждому его ребру дважды.

Домашнее задание 6

Задача 1

Как известно, в дереве есть 2-раскраска. Так как в дереве 2n вершин, то кол-во вершин одного из цветов точно больше или равно n. Тогда мы можем просто выбрать n вершин этого цвета, а они по определению раскраски графа не будут соединены ребрами.

Задача 2

Предположим, что число листьев меньше или равно половине вершин. Для определенности предположим, что равно. В нашем дереве n-1 ребро. Тогда по лемме о рукопожатиях сумма степеней всех вершин должна быть равна 2n - 2.

Посчитаем теперь сумму степеней, получающуюся у нас. Для определенности будем считать, что, раз у не листовых вершин степень не равна 0(так как дерево связно), 1(так как листья мы уже отобрали) и 2(по условию задачи) оно равно трем. $n/2(\text{суммастепенейлистьев}) + n/2 * 3 = 2n$, что больше оценки, полученной с помощью леммы у рукопожатиях. Получили противоречие. При этом, если мы решим сделать все-таки кол-во листьев меньше, чем n/2, то сумма степеней вершин будет увеличиваться, потому что "переделывая"лист во внутреннюю вершину мы увеличиваем его степень как минимум на два(потому что миимальная степень три, как было показано выше).

Значит в дереве обязательно должно быть больше половины листьев.

Задача 4

Сразу заметим, что кубики, которые находятся на границе, можно "отбросить только учтя, что нам необходимо сделать к ним "выход" из внутренних кубиков.

Тогда внутренних кубиков останется $(n-2)^3$. Значит всего компонент связности графа $(n-2)^3+1$, учитывая необходимость связать все внутренние кубики хотя бы с одним внешним.

Значит, чтобы сделать одну компоненту связности, нам нужно добавить как минимум $(n-2)^3$ ребер, то есть, говоря в терминах задачи, удалить $(n-2)^3$ перегородок.

Задача 5

Сделаем ориентированный граф из всех цифр и соединим ребрами те, которые образуют двузначное число, делящееся на 7. Направлено ребро из той вершины, которое обозначает десятки в числе в ту, которая обозначает единицы.

Тогда для поиска необходимого числа мы можем просто начать с как можно большего числа и переходить в максимально возможное, при этом помня, что можно заходить в каждую вершину только один раз.

На построенном графе(рисунок прикрепил к письму) такой обход будет таким: начнем с 9, как с самого большого, перейдем в 8, оттуда в 4 из 4 в 2 и оттуда в 1. Получится 98421.

Это число удовлетворяет условию о том, что соседние числа должны образовывать двузначное, делящееся на семь и оно наибольшее, так как в графе мы начали в максимально возможной цифре и переходили в максимально возможную.

Задача 6

Начнем обход в ширину из той вершины, которую мы желаем сделать достижимой из всех остальных. То есть сначала перейдем во все доступные из нее вершины, потом из этих вершин во все доступные и них. При этом каждый раз переходя от одной вершины к другой, будем добавлять ребро, направление которого противоположно направлению нашего перемещения между этими двумя вершинами. Тогда в итоге мы получим граф из каждой вершины которого мы можем попасть в нашу начальную вершину, поскольку в исходном неориентированном графе существовал путь от нашей начальной вершины до некоторой другой и мы, проходя по этому пути добавляли ребра, ведущие по направлению к нашей начальной вершине.

Задача 7

Докажем по индукции.

База.
n=3. Как бы не направили ребра в таком графе"треугольнике" мы можем просто начать с той вершины из которой будет путь длиной два, а такой точно будет и который и будет являться ггамильтоновым.
Шаг.
Пусть существует гамильтонов обход в любом турнире на n вершинах. Докажем, что он существует так же и в графе на n+1 вершине.

Рассмотрим граф на n+1 вершине. Выберем в нем любую вершину v. Тогда в графе с удаленной вершиной v и всеми инцидентными ей ребрами, существует гамильтонов путь по предположению индукции. Обозначим данный путь как $g_1 \to g_2 \to \cdots \to g_n$.

В нашем графе на n+1 вершине по определению должно быть либо ребро $v \to g_1$, либо ребро $g_1 \to v$. Если у нас есть ребро $v \to g_1$, то все – мы нашли гамильтонов путь в данном графе, то есть мы преходим из нашей вершины по ребру в гамильтонов путь на графе из n вершин и получаем как раз гамильтонов путь на нашем графе.

Если же у нас ребро $g_1 \to v$, то посмотрим есть ли такое ребро, которое ведет из нашей вершины в гамильтонов путь на графе из n вершин, т.е. $v \to g_t$. Если есть, то возьмем вершину с минимальным t, а значит все ребра до этого будут вести в нашу вершину v и тогда мы можем просто перейти из предыдущей вершины в гамильтоновом пути – g_{t-1} – в нашу вершину v и это и получится гамильтонов путь в графе на n+1 вершине.

Если же у нас нет такой вершины, в которую ведет ребро из нашей вершины, то тогда обязательно есть ребро $g_n \to v$, то есть пройдя по гамильтонову пути для графа на n вершинах мы перейдем в нашу вершину v по данному ребру, а это и есть гамильтонов путь для графа на n+1 вершине.

Получается, что в любом турнире мы можем построить гамильтонов путь.

Домашнее задание 7

Задача 1

a) Верно. $a = k \cdot c, b = l \cdot c + r$. Тогда $a + b = (k + l) \cdot c + r.$, а значит $a + b$ не делится на c.
b) Неверно. Контрпример: $a = 1, b = 5, c = 3$.
1 не делится на 3 и 5 не делится на 3, но $1 + 5 = 6$ делится на 3.
c) Неверно. $a = k \cdot c + r, b = l \cdot c + t$. Тогда $a \cdot b = c \cdot (klc + kt + lr) + rt$. Значит если произведение остатков будет делиться на c, то и ab будет делиться на c. Как контрпример можно привести: $a = 12, b = 15, c = 10$. 180 делится на 10.
d) Верно. $a = b \cdot l, b = c \cdot k$, тогда $a = c \cdot k \cdot l$ и $a \cdot b = c^2 \cdot k^2 \cdot l$, что, очевидно, делится на c^2.

Задача 2

*a)*При разложении каждого множителя факториала на простые двойка присутствует в 2(1), 4(2), 6(1), 8(3), 10(1), 12(2), 14(1), 16(4), 18(1), 20(2). В скобках указано в какой степени она в него входит. Всего получается 2^{18}. Значи 20! при делении на 2^{15} даст остаток 0.
b) Остаток будет равен 2^{18}.
Как видно из предыдущего пункта 20! можно представить в виде $2^{18} \cdot (2k + 1) = 2^{19} \cdot k + 2^{18}$. Видно, что $2^{19} \cdot k + 2^{18} \equiv 2^{18} (mod\ 2^{19})$.

Задача 4

Воспользуемся алгоритмом Евклида.
$(2^{2016} - 1, 2^{450} - 1)$.
$(2^{2016} - 1 - (2^{450} - 1), 2^{450} - 1)$.
$(2^{2016} - 2^{450}, 2^{450} - 1)$.
$(2^{2016} - 2 \cdot 2^{450} + 1, 2^{450} - 1)$.
$(2^{2016} - 2^{1566} \cdot 2^{450} + 2^{1566} - 1, 2^{450} - 1)$.
$(2^{1566} - 1, 2^{450} - 1)$.
Тогда далее:
$(2^{1566} - 1, 2^{450} - 1)$.
$(2^{216} - 1, 2^{450} - 1)$.

$(2^{216} - 1, 2^{18} - 1)$.
$(2^{18} - 1, 2^{18} - 1)$.
$gcd(2^{2016} - 1, 2^{450} - 1) = 2^{18} - 1$.

Задача 5

$74 \cdot t \equiv 1 \ (mod\ 47)$. Решим диофантово уравнение вида $74x + 47y = 1$
$47x + 27y = 1$
$27x + 20y = 1$
$20x + 7y = 1$
$7x + 6y = 1$
$6x + y = 1$
$x = 1$
$y = -7$
Значит искомый обратный элемент равен семи.

Задача 6

Решим диофантово уравнение вида $39x + 221y = 104$
$221x + 39y = 104$
$39x + 26y = 104$
$26x + 13y = 104$
$13x = 104$
$x = 8$
$gcd(221, 39) = 13$.

Задача 7

Чтобы данное число делилось на 22 оно должно делиться на 2 и 11. Очевидно, что для делимости $n^{10} - 1$ на 2 n должно быть нечетным. По малой теореме Ферма для любого n, не делящегося на 11, n^{10} при делении на 11 даст остаток 1. Тогда $n^{10} - 1$ кратно 11.
Значит $n^{10} - 1$ кратно 22 для всех нечетных n, не кратных 11.

Домашнее задание 8
Шумилкин Андрей, группа 163

Задача 1

Переформулируя задачу, нам нужно получить такую строчку, состоящую только из чисел 2, 3, 4 и 5, чтобы можно было между некоторыми из них поставить знаки умножения и полученное выражение равнялось 2007.
По ОТА мы можем разложить 2007 на простые множители, притом единственным образом. Это разложение будет иметь вид $3^2 \cdot 223$.
Тогда искомая строчка будет иметь вид 33223 и Вовочка расставил знаки следующим образом: $3 \cdot 3 \cdot 223 = 2007$. Значит у него две двойки и три тройки, то есть итоговая в четверти у него выйдет "3".
Можно задуматься, а не существует ли другой подходящей строки. Нет, поскольку по-другому представить число 2007 множителями(не только простыми), состоящими только из 2, 3, 4 и 5 нельзя, так как вообще единственное другое разложение(не считая самого 2007) имеет вид $669 \cdot 3$.

Задача 2

Нужно доказать, что произведение $(m+1) \cdot (m+2) \cdot \ldots \cdot (m+n)$ делится на:
а) n.
Пусть $(m+1) \equiv t \ (mod\ n)$. Тогда $(m+2) \equiv t+1 \ (mod\ n)$. И в какой-то момент мы найдем такое $(m+k)$, когда $(t+k-1)$ будет равно n(поскольку k принимает значения от 1 до n и значит t в нашем сравнении принимает значения от 0 до n-1 по определению сравнений), а значит $(m+k) \equiv 0 \ (mod\ n)$, т.е. $(m+k)$ делящееся на n, а значит и произведение в которое оно входит в качестве множителя тоже будет делиться на n.
б) n!.
Надо доказать, что $\frac{(m+1)\cdot(m+2)\cdot\ldots\cdot(m+n)}{n!}$. Можно заметить, что это равно C^n_{m+n}., потому что $C^n_{m+n} = \frac{(m+n)!}{n!*(m+n-n)!} = \frac{(m+1)\cdot(m+2)\cdot\ldots\cdot(m+n)!}{n!}$, а, как известно, биноминальные коэффициенты – это целые числа(можно заметить с помощью треугольника Паскаля, т.е. определения в виде $C^k_n = C^k_{n-1} + C^{k-1}_n$ и того, что в первых двух строках треугольника все числа – это единицы, т.е. они целочисленны), т.е. n подряд идущих чисел делятся на $n!$.

Задача 4

а)
Пусть число из 69 единиц будет x. Тогда заметим, что $9x + 1 = 10^{69}$.
71 – простое число, тогда по малой теореме Ферма $10^{70} \equiv 1 \ (mod\ 71)$.
Значит пусть $t = 10^{69}$. Тогда $10t \equiv 1 \ (mod\ 71)$. Легко заметить, что решением сравнения будет $t_0 = 64$ и тогда $10^{69} \equiv 64 \ (mod\ 71)$.
Из представления x получаем: $9x \equiv 63 \ (mod\ 71)$. $(9, 71) = 1 = 9 \cdot (8) - 71$. $8 \cdot 63 \equiv$

$4 \cdot 126 \equiv 4 \cdot 55 \equiv 2 \cdot 110 \equiv 220 \equiv 7 \ (mod\ 71)$.
Ответ: 7.
б)

Задача 5

Переформулируя: $4^{n!} \equiv 1 \ (mod\ n)$.
Любое нечетное положительное n будет взаимно просто с 4. Тогда по теореме Эйлера $4^{\varphi(n)} \equiv 1 \ (mod\ N)$. И тогда $4^{n!} \equiv 1 \ (mod\ N)$, поскольку n! делится на $\phi(n)$(т.к. $phi(n) < n$),то есть $4^{n!} - 1$ делится на n.

Задача 6

Если число делится на 4 и 5, то оно делится на 20. И если число делится на 20 и 6, то оно делится на 60.
Значит нам нужно найти минимальное число, которое на 60 делится с остатком 1, а на 7 с остатком ноль. Мы можем сделать это просто подбором(61, 121, 181, ...) и таким числом будет 301.

Задача 9

Переформулируя задачу, нужно найти подходящий x, при том, что $7^x \equiv 1 \ (mod\ 10000)$.Заметим, что 7 взаимно просто с N.
По теореме Эйлера $7^{\varphi(10000)} \equiv 1 \ (mod\ 10000)$ и значит такая тепень существует.
Теперь осталось вычислить функцию Эйлера от 10000. Разложим 10000 - 1 = 9999 на протые множители. $9999 = 3^2 \cdot 11 \cdot 101$. Тогда функция Эйлера от 10000 равна: $(3^2 \cdot \frac{2}{3}) \cdot (11 \cdot \frac{10}{11}) \cdot (101 \cdot \frac{100}{101}) = 6000$. Имеем $7^{6000} \equiv 1 \ (mod\ 10000)$.

Домашнее задание 9
Шумилкин Андрей, группа 163

Задача 1

Только для бинарных отношений над пустыми множествами.
Поскольку над любым непустым множством A отношение вида $P(x, x), x \in A$ будет принадлежать либо $\bar{P}$, либо P^{-1}, поскольку:
Пусть изначальное отношение P включает в себя пары (x, x), тогда его дополнение не будет их включать, а вот обратное отношение будет.
Если же изначальное отношение не содержит данные пары, то его дополнение будет их включать, а вот обратное отношение нет.

Задача 2

а) Нет, не будет. Контрпример:
$A = a_1, a_2, a_3$. $P_1 = (a_1, a_3)$. $\bar{P_1} = (a_1, a_1), (a_1, a_2), (a_2, a_1), (a_2, a_2), (a_2, a_3), (a_3, a_1), (a_3, a_2), (a_3, a_3)$.
Как видим, P_1 транзитивно, а вот $\bar{P_1}$ нет, поскольку $\bar{P_1}(a_1, a_2) \wedge \bar{P_1}(a_2, a_3) \not\Rightarrow \bar{P_1}(a_1, a_3)$.
б) Назовем пересечение множеств I – оно будет транзитивно, поскольку пусть $(a, b) \in I \wedge (b, c) \in I$ – из этого по определению пересечения множест следует, что $(a, b) \in P_1 \wedge (b, c) \in P_1$ и $(a, b) \in P_2 \wedge (b, c) \in P_2$, а так как и P_1 и P_2 транзитивны, то из этого следует $(a, c) \in P_1, P_2$, а так как I – пересечение множеств, то и $(a, c) \in I$.
в) Контрпример. $A = a, b, c, d, P_1 = (a, b), (b, c), (a, c), P_2 = (c, d)$. Тогда $P_1 \cup P_2 = (a, b), (b, c), (a, c), (c, d)$ и оно не транзитивно, поскольку $P_1 \cup P_2(a, c) \wedge P_1 \cup P_2(c, d) \not\Rightarrow P_1 \cup P_2(a, d)$.
г) Нет. Контрпример: $P_1 = (c, b), (x, c), (x, b), P_2 = (a, c), (b, x)$. Оба отношения транзитивны и $P_1 \circ P_2 = (a, b), (b, c), (b, b)$ и, как видно, композиция не транзитивна, так как $P_1 \circ P_2(a, b) \wedge P_1 \circ P_2(b, c) \not\Rightarrow P_1 \circ P_2(a, c)$.

Задача 3

Обозначим отношение R, карты меньшие или равные десятке соответствующей цифрой и карты больше десятки заглавной буквой, которая является первой в слове их обозначающем: Валет - В и т.д. Будем, не теряя общности, рассматривать карту произвольной масти и обозначать просто согласно выбранным обозначением без указания конкретной масти.
а) Да, будет, потому что сказано "одна из карт ... другая", а не "первая ... вторая", к примеру. То есть будет спаведливо как R(6, Валет), так и R(Валет, 6).
б) Нет, оно нерефликсивно. Потому что никакая карта не может одновременно быть как младше деятки, так и старше десятки, т.е. контрпример: R(8, 8) – ложно.
в) Нет, оно не транзитивно. Контрпример R(9, Валет) $\wedge$ R(Дама, 8) – истинно, но из R(9, Валет) $\wedge$ R(Дама, 8) $\not\Rightarrow$ R(9, 8), поскольку R(9, 8) ложно.
Посчитаем кол-во возможных пар относительно карт меньших десятки, при этом уже рассматривая карты конкретных мастей.

Карт меньших десятки у нас 4 и у каждой из них четыре масти. Ставим их на место слева в нашем отношении. Тогда справа может стоять любая карта, большая десятки, которых так же четыре и у каждой четыре масти. Также нужно не забыть домножить все это на 2, так как каждую пару мы можем "перевернуть" и она так же будет истинна.
$4 \cdot 4 \cdot 4 \cdot 4 \cdot 2 = 512$.

Задача 4

а) Да, может, если операция нерефлексивна. Тогда, к примеру, мы можем взять все возможные пары для первого элемента, притом так, чтобы он был как слева, так и справа. Всего получится 30 пар. Потом возьмем пару второго третьим, и наоборот – третьего со вторым. Выходит 32 пары. И последней парой возьмем (первый элемент, первый элемент). Выходит 33 элемента и полученное отношение симметрично.

Задача 5

а) Любоая комбинация пар элементов A(даже пустая) определяется неким отношением на множестве. Посчитаем общее количество пар возможных для составления из элементов множества A.
Мы каждый элеммент можем поставить в пару с каждым, значит это 2^n. Как известно, количество подмножест множества C равно $2^{|C|}$. Тогда количество всех возможных комбинаций пар равно 2^{n^2}.
б) Чтобы отношение было рефлексивным оно должно содержать в себе $(x, x), \forall x \in A$. Тогда, можем сказать, что нужно посчитать количество подмножеств множества, n элементов которого принадлежат любому из подмножеств и это 2^{n^2-n}.
в) Построим для каждого отношения матрицу, состоящую из единиц и нулей. Единица будет стоять в клетке с индексом (x, y) тогда, когда в отношение входит пара (x, y). Тогда заметим, что мы можем ставить единицы на главной диагонали или выше нее и, чтобы соблюдалось условие симметричности отношения, так же ставить единицу в клетке ниже главной диагонали, симметричной относительно нами выбранной относительно главной диагонали. А всего клеток выше главной диагонали(считаем идя по столбцам или строкам) $1+2+\ldots+n$ – арифметическая прогрессия, сумма которой равна $\frac{n^2+n}{2}$. И, по уже известной формуле количества подмножеств множества получаем $2^{\frac{n^2+n}{2}}$.

Задача 6

*а)*Из данных отношений мы можем посмотреть как отношение P делит множество A на классы эквивалентности. Мы можем заметить, что a, b, c лежат в одном классе, а d, e в другом.
Тогда весь вопрос к какому классу относится f, при этом f точно не принадлежит ко

второму классу, где d, e по условию. Тогда она может либо принадлежать тому же классу, что и a, b, c, либо входить в новый класс, куда будет относиться только этот элемент – f.
Выходит, что у нас будет либо два, либо три класса эквивалентности.
б) Данный элемент, так как про него ничего не известно может либо относится к одному из уже существующих классов эквивалентности, либо входить в свой собственный класс, куда относится только он. И вариантов какие классы могут получится при наличествовании такого элемента в A получится семь, поскольку:
Если f принадлежит классу эквивалентности, где лежат a, b, c, то g может либо так же принадлежать этому классу, либо принадлежать классу, где находятся d, e, либо образовывать свой собственный новый класс – всего 3 варианта.
Если же f образует свой собственный класс, то g может либо относиться к одному из трех существующих классов, либо образовывать свой собственный класс – всего 4 варианта.

Домашнее задание 9
Шумилкин Андрей, группа 163

Задача 1

a) Нарисуем ориентированный граф, согласно танным отношениям и, смотря на него, будет легко составить линейный порядок(рисунок прикрепил во вложениях к письму). Один из возможных порядков таков: Очки $<$ Носки $<$ Брюки $<$ Туфли $<$ Ремень $<$ Рубашка $<$ Галстук $<$ Пиджак $<$ Часы.

Задача 2

Из определения ацикличности видим, что отношение антирефлексивно. Достаточно взять $k = 1$ и заметим, что $\forall a \in AaPa$ не выполняется.
Также из определения ацикличности заметим, что отношение для каждой пары либо выполняется, либо нет, поскольку $\forall a, b \in AaPbPa$ не выполняется, т.е. отношение антисимметрично, а значит и транзитивно. Поскольку если aPb и bPc из-за связности отношения должно быть либо aPc, либо cPa, но если aPc, то это противоречит ацикличности.
А по условию оно так же связно. И, как известно, отношение, обладающее всеми этими свойствами как раз является строгим линейным порядком.

Задача 4

По условию отношение антирефлексивно, антисимметрично и связно. Если оно к тому же транзитивно, то это линейный порядок по определению, а если же нет, то тогда и возникают альтернативы a,b,c для которых aPb, bPc и cPa, откуда следует(если учесть и антисимметричность), что aPc – ложно , т.е. отношение нетранзитивно

Задача 7

a) $I_p = \bar{P}^{-1} \cap \bar{P}$, поскольку если ни (x, y), ни (y, x) не входят в P, то они будут входить в его дополнение, но там же будут и "лишние"пары (a, b), (b, a) которых входит в P. Но если мы построим обратное отношение к дополнению P, то (x, y) преобразуется в (y, x) и наоборот и войдут в пересечение, а вот (a, b) преобразуется в (b, a) и не войдет в пересечение, так как (b, a) не присутствует в $\bar{P}$.

Домашнее задание 11
Шумилкин Андрей, группа 163

Задача 1

Назовем функции f и g. По определению функции она сопоставляет каждому элементу из области определения ровно один элемент из области значения. Пусть A – область опередения для обеих функция, так как они обе определены всюду. F – область значений f, а G – область значений g.
а) Если объединение функций тоже функция, то она доложны всем элементам(так как обе функции всюду определены) из множества A сопоставлять только лишь один элемент из множества $(A \cup B)$. Тогда если $\forall\ x\ in\ A \Rightarrow f(x) = g(x)$, то объединение функций так же будет функцией.
б) Если пересечение функций тоже функция, то она доложны всем элементам(так как обе функции всюду определены) из множества A сопоставлять только лишь один элемент из множества $(A \cap B)$. А так как в пересечении функций и так будут только лишь те элементы, для которых $f(x) = g(x)$, то оно всегда будет функцией.

Задача 2

Сразу приведем контрпример для $=$ и $\subseteq$. Пусть $X = \{1, 2, 3, 4\}, Y = \{1, 2\}, A = \{1\}$ и $f(1) = 1, f(2) = 1, f(3) = 1, f(4) = 2$. Тогда $f^{-1}(f(A)) = \{1, 2, 3\}$ и оно явно не равно A а так же не является его подмножеством.
А вот $\supseteq$ подходит по определению, поскольку $f(A) = \{y : y = f(x), x \in A\}$ и $f^{-1}(f(A)) = \{x : f(x) \in f(A)\}$, а значит $\forall a \in A$ точно окажутся в прообразе, так как $f(a) \in f(A)$.

Задача 3

Сразу приведем контрпример для $=$ и $\subseteq$. Пусть $A = \{1, 2\}, B = \{3, 4\}$и $f(1) = 1, f(2) = 1, f(3) = 1, f(4) = 2$. Тогда $f(A \setminus B) = \{1\}$, а $f(A) \setminus f(B) = \varnothing$.
А вот $\supseteq$ подходит, поскольку в $f(A \setminus B)$ будут значения от всех элементов из A, которых нет в B. А вот в $f(A)$ могут быть значения элементов, которые есть в A и при этом есть в B, но они пропадут, когда мы применим разность множеств, поскольку их значения так же будут и в $f(B)$. С ними так же могут пропасть и некоторые значения от элементов только из A, если $f(a) = f(b)$, но точно ничего не добавиться, поэтому это множество и будет подмножеством $f(A \setminus B)$.

Задача 4

Сразу приведем контрпример для $=$ и $\subseteq$. Пусть $A = \{1\}, B = \{2\}$и $f(1) = 1, f(2) = 1, f(3) = 1, f(4) = 2$. Тогда $f^{-1}(A \setminus B) = \{1\}$, а $f^{-1}(A) \setminus f^{-1}(B) = \varnothing$.

Задача 5

а) Нам нужно каждому элементу из A поставить в соответствие некий элемент из B или не сопоставлять, считая, что для него функция не определена. Выбрать один элемент у нас $b+1$ способов(так как мы еще можем его вообще не брать) и это надо сделать a раз. Значит количество способов это сделать b^a.
б) Нам нужно элементам из A поставить в соответствие некий элемент из B, притом так как это инъекция все выбранные элементы из B должны быть различны, но так же мы можем не сопоставлять некоторым элементам из A никакие элементы из B вообще.
Будем определять для какого кол-ва элементов(обозначим n) функция опередедена. Тогда кол-во таких функций будет: $C_a^n \cdot C_b^n$ – кол-во способов выбрать сами эти элементы, умноженное на кол-во способов выбрать сопоставленные им. Кол-во элементов, для которых определена функция может быть от нуля до a и тогда итоговая формула:

$$\sum_{n=0}^{a} C_a^n \cdot C_b^n.$$

Задача 6

Домашнее задание 12
Шумилкин Андрей, группа 163

Задача 1

Любое подмножество декартова произведения данных множеств будет бинарным отношением, т.е. всего исходов $2^4 = 16$.
Теперь посчитаем кол-во неблагоприятных исходов. Обозначим элементы множества A цифрами, т.е. a_1 будет 1, a_2 – 2. Заметим, что это только три подмножества: $\{(1,1),(1,2),(2,1)\}$, $\{(2,2),(1,2),(2,1)\}$и$\{(1,2),(2,1)\}$.
Тогда благоприятных исходов будет 13 и вероятность будет равна кол-ву благоприятных исходов поделеному на кол-во всех исходов.
Ответ: $\frac{13}{16}$.

Задача 2

Если $a \neq b$, то вероятность будет равна нулю, поскольку мы не сможем построить биекцию между неравномощными множествами.
Будем рассматривать случай. когда $a = b$. Найдем количество благоприятных исходов. Будем сопоставлять множеству A какую-либо перестановку элементов множества B так, что первый элемент множества A будет отображен в первый элемент этой перестановки, второй – во второй и т.д. Тогда количество благоприятных исходов будет равно $a!$, т.к. $a = b$.
А количество всех исходов будет равно a^a, так как мы каждый элементу из A выбираем отображение в элемент из B, которых всего b и $b = a$.
Тогда вероятность благоприятного исхода будет равна кол-ву благоприятных исходов поделенному на кол-во всех исходов.
Ответ: $\frac{a!}{a^a}$.

Задача 3

19-ый элемент в перестановке может быть любым и никак не повлияет на ответ, поскольку не будет в ходить ни в первые 18, ни в последние 18.
Так как это перестановка, то наибольшее среди первых восемнадцати либо строго больше наибольшего среди последних восемнадцати, либо строго меньше него. Тогда у нас количество благоприятных исходов будет равно количеству неблагоприятных, поскольку мы можем кажой перестановке с благоприятным исходом сопоставить перестановку с неблагоприятным исходом, просто перевернув ее и при этом этом это будет биекция между множеством благоприятных исходов и множеством неблагоприятных. То есть количество благоприятных исходов будет равна кол-ву неблагоприятных и вероятность благоприятного исхода будет равна 0.5
Ответ: $\frac{1}{2}$.

Задача 4

Всего исходов будет C_{36}^5, то есть мы выбираем из 36 чисел 5 и просто располагаем их в порядке убывания.
Тогда количество благоприятных исходов будет C_{35}^4, так как единицу мы как бы выбрали заранее и она по построению последовательности будет стоять последней, так как меньше нее чисел нет.
Тогда вероятность благоприятного исхода будет равна кол-ву благоприятных исходов поделенному на кол-во всех исходов.
Ответ: $\frac{5}{36}$.

Задача 5

Всего исходов будет C_{36+5-1}^5 – кол-во сочетаний с повторениями.То есть мы просто выбираем 5 элементов(возможно с повторениями) из 36.
Тогда количество благоприятных исходов будет C_{36+4-1}^4, так как единицу мы как бы выбрали заранее и она по построению последовательности будет стоять последней(даже если мы), так как меньше нее чисел нет.
Тогда вероятность благоприятного исхода будет равна кол-ву благоприятных исходов поделенному на кол-во всех исходов.
Ответ: $\frac{39!}{36!\cdot 4!} \cdot \frac{36!\cdot 5!}{40!} = \frac{5}{40} = \frac{1}{8}$.

Задача 6

Будем рассматривать первые 10 позиций и последние 10. Обозначим их множества как A и B.
У нас может быть три случая:
1.$|A| > |B|$
2.$|A| < |B|$
3.$|A| = |B|$.

Все двоичные слова подходящие под первый случай будут неблагоприятными исходами, поскольку что бы ни стояло на 11 позиции в последних 11-ти единиц будет уже явно меньше или равно, чем в первых 10, т.е. в первых десяти никак не может быть меньше единиц, чем в последних 11-ти.
Все двоичные слова подходящие под второй случай будут благоприятными исходами, поскольку что бы ни стояло на 11 позиции в последних 11-ти единиц будет уже явно больше, чем в первых 10, потому что их и так больше, а мы либо добавляем еще единицу, либо оставляем все как есть.
Мы можем построить биекцию между множеством двоичных слов, подходящих к первому случаю и множеством двоичных слов, подходящих ко второму. Тогда после рассмотрения двух этих случаев у нас будет поровну благоприятных случаев и неблагоприятных.
В третьем же случае все будет зависить от того стоит ли на 11-ой позиции единица или ноль, а значит половина будет благоприятными исходами, а половина – нет, так

как у нас множество *всех* двоичных слов.
То есть у нас по итогу равное количество благоприятныхх и неблагоприятных исходов, а значит вероятность благоприятного исхода будет равна 0.5.
Ответ: $\frac{1}{2}$.

Задача 7

Вероятностное пространство – Посчитаем вероятность неблагоприятного исхода, тогда когда оно будет меньше или равно 0.5 и будет достигаться то, что вероятность благоприятного исхода будет больше или равно 0.5.
Обозначим кол-во карт, которые мы вытягиваем x. Тогда количество всех исходов будет равно C_{36}^x, а количество неблагоприятных C_{32}^x. Значит вероятность неблагоприятного исхода равноа $\frac{(36-x)!}{(32-x)!\cdot 33\cdot 34\cdot 35\cdot 36} = \frac{(33-x)\cdot(34-x)\cdot(35-x)\cdot(36-x)}{33\cdot 34\cdot 35\cdot 36}$.
Далее посмотрим значение этого выражения при x и когда оно достигнет 0.5 мы и найдем ответ.
При $x = 1$ оно будет равно 1256640/1413720.
При $x = 2$ оно будет равно 1113024/1413720.
При $x = 3$ оно будет равно 982080/1413720.
При $x = 4$ оно будет равно 863040/1413720.
При $x = 5$ оно будет равно 755160/1413720.
При $x = 6$ оно будет равно 657720/1413720.

Видим, что при $x = 5$ оно еще больше 0.5, а при $x = 6$ меньше. Значит достаточно вытащить шесть карт из колоды.
Ответ: достаточно вытащить 6 карт.

Задача 8

Вероятностное пространство – группы студентов по 30 человек
Посчитаем количество неблагоприятных исходов, т.е. такую ситуацию, когда ни у окого из группы не будут совпадать дни рождения(остальные будут благоприятными, поскольку если день рождения совпадают у троих человек, то они, конечно же, совпадают и у двоих).
Берем день рождения первого человека и вероятность того, что оно не совпадет с день рождением кого-то из ранее выбранных будет равна 1, так как до этого мы никого еще не выбрали. Затем будем рассматривать день рождения второго. Вероятность того, что они различны будет $\frac{364}{365}$, поскольку благоприятными исходами будут 364 дня, исключая день рождения первого человека из группы. Для третьего выбранного соответственно вероятность будет $\frac{363}{365}$. И так далее, а дял последнего $\frac{365-30}{365} = \frac{335}{365}$.
Тогда итоговая вероятность благоприятного исхода будет $\frac{365\cdot 364\cdot 363\cdot \ldots \cdot 335}{365^n}$ и она будет примерно равна 0.3.
А количество благоприятных исходов будет равно 1 - (кол-во неблагоприятных), т.е. будет больше или равно 0.6, а значит больше 0.5.

Линал

При фиксированном $m = 10$, то есть когда n заметно больше чем m эффективнее оказывается метод Гаусса.

Иначе же, если фиксированное $n = 100$, то есть m заметно больше, то эффективнее оказывается метод, использующий обратную матрицу.

Посчитаем их сложность. При этом, поскольку лабораторная по линейной алгебре, будем руководствоваться методами, которые мы изучили в курсе линейной алгебры, не беря во внимание, что во внутренних функциях python они каким-то образом могут быть реализованы несколько быстрее.

Метод обратной матрицы: 1. Мы можем найти обратную матрицу за $O(n^3)$, методом Гаусса-Жордана, к примеру. 2. Потом нам надо будет обратную матрицу умножить на матрицу B и это можно сделать за $O(n^2 \cdot m)$ операций.

Итог: $O(n^2 \cdot m + n^3)$.

Метод Гаусса: 1. Сложность самого метода Гаусса составляет $O(n^3)$, но нам нужно еще повторять каждую операцию на присоединенной нами матрице B, то есть, по сути, нам нужно n^2 раз сложить ее строки и тогда итоговая сложность будет $O(n^3 + n^2 \cdot m)$.

Домашнее задание 13
Шумилкин Андрей, группа 163

Задача 1

Пусть множество исходов – это последовательность, в которой родились дети и тогда все исходы равновероятны, так как рождение мальчика и девочки равновероятны. То, что мальчик родился в понедельник никак не влияет на вероятность, поскольку в тот же понедельник могла за ним родиться девочка или наоборот(двойняшки) и по условию рождение каждого – равновероятно. Обозначим М – мальчик, Д – девочка. Тогда множество исходов имеет вид $\{\text{ММ}, \text{МД}, \text{ДМ}, \text{ДД}\}$ и вероятность каждого исхода равна $1/4$. С учетом того, что по условию один из детей должен быть мальчиком, а другой – девочкой, нам пододят два из этих исходов – МД и ДМ, и тогда итоговая вероятность равна $1/2$.
Ответ: $\frac{1}{2}$.

Задача 3

Пусть множество исходов – это пятерки выбранных чисел и все исходы равновероятны.
Количество всех исходов равно C_{36}^5. Вероятность выбрать пятерку, среди элементов которой есть число 2 будет равна $\frac{C_{35}^4}{C_{36}^5}$, так как пятерка должна быть выбрана по условию и еще четыре элемента мы выбираем из оставшихся 35-и элементов множества. Вероятность выбрать пятерку, среди элементов которой будет число 5 так же равна $\frac{C_{35}^4}{C_{36}^5} = \frac{5}{36}$.
Теперь посчитаем вероятность выбрать элемент 5 при том, что двойка уже выбрана. Вероятность выбрать пятерку в которой есть элементы и 5, и 2 равна $\frac{C_{34}^3}{C_{36}^5}$.
Тогда вероятность выбрать элемент 5 при том, что элемент 2 уже выбран равна $\frac{C_{34}^3}{C_{36}^5} \cdot \frac{C_{36}^5}{C_{35}^4} = \frac{C_{34}^3}{C_{35}^4} = \frac{4}{35}$.
И, так как $\frac{5}{36} \neq \frac{4}{35}$, то есть вероятность события не равна вероятности его же при условии какого-то другого делаем вывод, что события зависимы.
Ответ: Данные события зависимы.

Задача 4

Пусть множество исходов – это какая-то определенная функция и все исходы равновероятны. Всего вариантов составить какую-либо функцию у нас будет n^n, поскольку она всюду определена и каждому из n элементов одного множества мы можем и должны сопоставить один из n элементов другого множества.
Составить же инъективную функцию у нас $n!$ способов, то есть мы будем элементам первого множества сопоставлять некую перестановку из элементов второго. Значит вероятность того, что функция инъективна равна $\frac{n!}{n^n}$.
Составить функцию так, чтобы $f(1) = 1$ у нас будет $(n-1)^n$ способов, то есть один

элемент мы определяем изначально, а для остальных $n-1$ выбираем один из n элементов другого множества. Тогда вероятность того, что $f(1)=1$ будет $\frac{1}{n}$
Если же хотим получить инъективную функцию у которой $f(1)=1$, то у нас будет $(n-1)!$ способов сделать это, поскольку мы определяем $f(1)=1$ и нам нужно для оставшихся $n-1$ элемента сопоставить различные элементы другого множества, в которое уже не входит 1, так как мы уже составили с ней пару.
Тогда вероятность того, что $f(1)=1$, при условии, что функция инъективна равна $\frac{(n-1)!}{n^n} \cdot \frac{n!}{n^n} = \frac{1}{n}$.
Можно заметить, что она равна вероятности того, что $f(1)=1$, а значит данные события независимы.
Ответ: Данные события независимы.

Задача 5

Пусть множество исходов –
Обозначим правильное решение как 1, а неправильное – как 0. Рассмотрим все возможные исходы выбора первыми двумя членами жюри. Это: $\{00, 01, 10, 11\}$.
Теперь посчитаем вероятность того, что третий член жюри сделает правильный выбор для каждого случая:

1. 00. Итоговая вероятность равна 0, так как правильного решения тут нет.
2. 01. Вероятность такого случая равна $(1-p)\cdot p$, тогда вероятость правильного выбора третьим членом жюри равна $\frac{p\cdot(1-p)}{2}$.
3. 10. Вероятность такого случая равна $p\cdot(1-p)$, тогда вероятость правильного выбора третьим членом жюри равна $\frac{p\cdot(1-p)}{2}$.
4. 11. Вероятность такого случая равна p^2, тогда вероятость правильного выбора третьим членом жюри равна p^2.

А общая вероятность выбора правильного решения третьим из судей будет равна сумме данных вариантов:
$p\cdot(1-p)+p^2 = p^2+p-p^2 = p$.
Видно, что эта вероятность равна p – вероятности правильного решения, принимаемого одним добросовестным членом жюри. **Ответ:** Вероятность выбора верного решения равна p и равна вероятности правильного решения, принимаемого одним добросовестным членом жюри.

Задача 7

Посчитаем вероятность как бы спускаясь вниз, при этом вероятность выигрыша при счете 10:9 возьмем, конечно же, за 1.
Тогда вероятность выигрыша при 9:9 $= 1/2$.
9:8 – это будет сумма вероятностей вариантов (выиграть сразу) и (проиграть, а потом выиграть) и она равна $1/2\cdot 1/2 + 1/2 = 3/4$.

9:7 – это будет сумма вероятностей вариантов (выиграть сразу) и (перейти в случай 9:8), для которого мы уже посчитали вероятность и тогда она будет равна $1/2 + 1/2 \cdot 3/4 = 7/8/$. 8:9 – для выигрыша можем перейти в вариант 9:9 для которго уже посчитали, тогда равна $1/2 \cdot 1/2 = 1/4$. 8:8 – перйти в вариант 9:8, либо 8:9, тогда равна $1/2 \cdot 3/4 + 1/2 \cdot 1/4 = 1/2$. 8:7 – перейти в вариант 9:7, либо в вариант 8:8. Тогда вероятность равна $1/2 \cdot 1/2 + 1/2 \cdot 7/8 = 11/16$.
Ответ: 11/16.

Вероятность A при условии B:

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

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

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 .....

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

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:

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

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

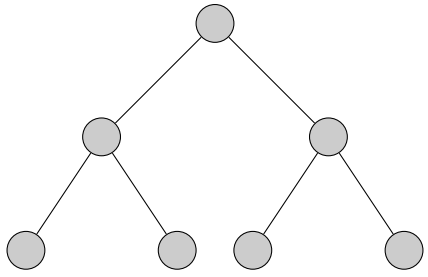
Связность - граф связен тогда и только тогда, когда две любые вершины соединены путем.
Компонента связности - максимальный по включению связный подграф графа $G - G(U)$, порожденный подмножеством вершин исходного графа, в котором для любой пары $v_1, v_2 \in U$ существует путь, а для всех других пар пути нет.

Дерево. Примеры. Полные бинарные деревья

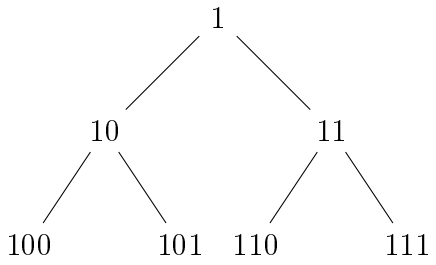
Дерево - минимальный связный ациклический граф. В нем любые две вершины соединены единственным путем.

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 *сюръективным*, 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.

Материалы для подготовки к коллоквиуму по дискретной математике
Теоремы

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

13 декабря 2016 г.

---

1. Вывод принципа полной математической индукции из принципа математической индукции

Принцип математической индукции. *Если для утверждения зависящего от положительного натурального n выполняются следущие условия:*

- *1. Утверждение истинно при $n = 1$*
- *2. Когда утверждение истинно при $n = k$, оно истинно и при $n = k + 1$*

Тогда утверждение истинно при всех положительных n.

Принцип полной математической индукции. *Если для утверждения зависящего от положительного натурального n выполняются следущие условия:*

- *1. Утверждение истинно для $n = 1$*
- *2. Если утверждение истинно для всех $n \leqslant k$, оно также истинно и для $n = k + 1$*

Тогда утверждение истинно при всех положительных n.

Утверждение. *Если уместна математическая индукция, то уместна и сильная индукция.*

Доказательство. В дальньейших рассуждениях будем считать, что n - натуральное, большее или равное 1, а также обозначим утверждение зависящее от n за $\varphi(n)$.

Предположим, что для $\varphi(n)$ выполняются условия (1) и (2) для сильной индукции.

Пусть $\psi(k) \Leftrightarrow$ «$\varphi(n)$ истинно для всех $n \leqslant k$».

Попытаемся доказать, что утверждение $\psi(n)$ истинно для всех положительных натуральных n по индукции. Как следствие, мы получим, что и $\varphi(n)$ верно для всех положительных n, т.е. тот же вывод, который должен дать принцип сильной индукции.

База. В силу нашего предположения $\varphi(1)$ истинно (гипотеза (1) сильной индукции верна), но тогда истинно и $\psi(1)$, по опеределению $\psi(n)$.

Предположение. Пусть верно $\psi(k)$.

Шаг. Мы предположили, что для $\varphi(n)$ выполняются гипотезы сильной индукции, а значит, если «$\varphi(n)$ верно для всех $n \leqslant k$», то и $\varphi(k + 1)$ - верно. По предположению индукции - $\psi(k) \Rightarrow \varphi(k + 1)$ (см. определение $\psi(n)$ и гипотезу (2) сильной индукции). Получаем, что $\psi(k + 1)$ - истинно, т.к. $\varphi(n)$ истинно для всех $n \leqslant k + 1 \Rightarrow \psi(k + 1)$.

Согласно принципу мат. индукции $\psi(k)$ - верно для всех положительных k, занчит утверждение «$\varphi(n)$ истинно для всех $n \leqslant k$» верно при всех k, а значит $\varphi(n)$ - верно для всех n.

Таким образом, из принципа мат. индукции следует принцип полной мат. индукциию. □

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 сгруппировать. 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:

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

□

3. Основные свойства треугольника Паскаля

Скоро на экранах.

4. Задача Муавра (решение уравнения $x_1 + \ldots + x_m = k$)

Утверждение. *Число решений уравнения $x_1 + x_2 + \ldots + x_k = n$ в неотрицательных целых числах равно $\binom{n+k-1}{k-1}$*

Доказательство. Воспользуемся методом «шаров и перегородок». Пусть есть n шаров и $k-1$ перегородок, тогда какая-то их расстановка однозначно задаёт решение уравнения: x_1 – количество шаров перед первой перегородкой, x_2 – между 1 и 2, и так далее, количество шаров после последней перегородки - x_k. Тогда число решений равно $\binom{n+k-1}{k-1}$.

Докажем справедливость данной формулы. Рассмотрим n одинаковых объектов, добавим к ним ещё $k-1$ таких же объектов. Тогда, заменив какие-то $k-1$ объектов на перегородки, мы получим разбиение множества из n элементов на k непересекающихся подмножеств. □

5. Доказательство формулы включений и исключений

Определение (Формула включений и исключений.)**.** *Формула включений-исключений — комбинаторная формула, позволяющая определить мощность объединения конечного числа конечных множеств, которые в общем случае могут пересекаться друг с другом.*

Утверждение. *Пусть $A_1, A_2, \ldots, A_n$ — конечные множества. Формула включений-исключений утверждает:*

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_i |A_i| - \sum_{i<j} |A_i \cap A_j| + \sum_{i<j<k} |A_i \cap A_j \cap A_k| - \ldots + (-1)^{n-1}|A_1 \cap A_2 \cap \ldots \cap A_n|.$$

Доказательство. Рассмотрим произвольный элемент $x \in \left|\bigcup_{i=1}^{n} A_i\right|$, входящий в ровно S множеств $A_{q_1}, \ldots A_{q_S}$ и подсчитаем, сколько раз он учитывается в правой части формулы включений-исключений (вернее покажем, что учитывается ровно 1 раз):

- В первой сумме $\sum_i |A_i|$ элемент x посчитан ровно $\binom{S}{1} = S$ раз (В слагаемых $A_{q_1}, \ldots A_{q_S}$).

- Во второй сумме $\sum_{i<j} |A_i \cap A_j|$ элемент x посчитан ровно $\binom{S}{2}$ раз (количесво попарных пересечений $A_i \cap A_j$, таких, что $A_i, A_j \in A_{q_1}, ...A_{q_S}$).
- В третьей сумме $\sum_{i<j<k} |A_i \cap A_j \cap A_k|$ x будет посчитан $\binom{S}{3}$ раза (количество пересечений $A_i \cap A_j \cap A_k$ для которых $i, j \in q_1, \dots q_S$).

  ...
- В S-ой сумме $\sum_{i_1<i_2<\ldots<i_S} |A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_S}|$ x будет посчитан $\binom{S}{S} = 1$ раз (x войдет только в слагаемое $|A_1 \cap A_2 \cap \ldots \cap A_n|$).
- суммы, содержащие $S+1$ и более пересечений, не учитывают элемент x, поскольку x не входит в пересечение более чем S множеств.

Таким образом x оказывается посчитанным ровно $S - \binom{S}{2} + \binom{S}{3} - \ldots + (-1)^{S+1}\binom{S}{S}$ раз. Покажем, что эта сумма в точности равна 1. Воспользуемся биномом Ньютона:

$$0 = (1-1)^S = \sum_{k=0}^{S} \binom{S}{k} \cdot 1^{S-k} \cdot (-1)^k = 1 - \sum_{k=1}^{S} \binom{S}{k} \cdot 1^{S-k} \cdot (-1)^{k+1}$$

$$\Updownarrow$$

$$1 = \sum_{k=1}^{S} \binom{S}{k} \cdot (-1)^{k+1} = S - \binom{S}{2} + \binom{S}{3} - \ldots + (-1)^{S+1}\binom{S}{S}$$

Таким образом, каждый $x \in \left|\bigcup_{i=1}^{n} A_i\right|$ учитывается и левой и правой частью формулы ровно 1 раз, и очевидно, что все прочие $y \notin \left|\bigcup_{i=1}^{n} A_i\right|$ не учитываются ни правой, ни левой частями. □

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

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

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.*

8. Критерий двураскрашиваемости графа.

Утверждение. *Неориентированный граф является 2-раскрашиваемым тогда и только тогда, когда в нём нет циклов нечётной длины.*

Доказательство. $\Rightarrow$ Пусть в графе есть цикл нечётной длины. Покрасим какую-то вершину цикла в первый цвет и будем двигаться по нему в одном направлении, крася каждую следующую вершину в противоположный цвет. Тогда, вернувшись в исходную вершину, получим противоречие.

$\Leftarrow$ Пусть циклов нечётной длины нет. Выберем произвольную вершину A и покрасим её в первый цвет. Для любой другой вершины B рассмотрим количество рёбер в пути $A \to B$.

Если есть два пути $A \to B$ таких, что в одном чётное число рёбер, а в другом – нечётное, то есть цикл с нечётным числом рёбер, который получается, если пройти $A \to B$ по первому пути и вернуться $B \to A$ по второму.

Следовательно, между любыми двумя вершинами все пути либо чётной, либо нечётной длины. Раскрасить граф можно следующим образом:

- выделим остовное дерево, раскрасим корень в первый цвет
- раскрасим его потомков во второй цвет
- для каждого из потомков раскрасим всех его потомков опять в первый цвет, и.т.д

Полученная раскраска будет корректной, так как в остовном дереве любой путь между вершинами одного цвета имеет чётную длину (по построению), а по доказанному выше путей нечётной длины между такими вершинами нет. □

7. Нижняя оценка числа связных компонент в неориентированном графе

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

Доказательство. Докажем по индукции по вершинам.

База индукции. При $n = 1$ граф состоит из одной вершины, которая является единственной компонентой связности в графе. Разность количества вершин и ребер равно 1, база доказана.

Шаг индукции. 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 наn 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 компонентов 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: $(C + 1 - k) + (E + k) = C + E + 1$. Но $C + E + 1 \geq V + 1$ из $C + E \geq V$. Значит для $n + 1$ оценка верна. □

10. Деревья – это в точности минимально связные графы

Доказательство.
[$\Rightarrow$] 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.
[$\Leftarrow$] 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. □

11. Деревья - это в точности связные графы с $n-1$ ребром

Доказательство. Докажем в обе стороны.

$\Rightarrow$. Докажем по индукции по вершинам.

База индукции. Для $n = 2$ существует в точности одно дерево, для которого утверждение очевидно.

Шаг индукции. Пусть есть дерево на n вершинах, в котором в точности $n-1$ ребро. Если мы добавим в него вершину, нам необходимо будет ее связать с графом. Если мы проведем из нее больше одного ребра мы получим цикл, так как между проведенными вершинами существовал единственный путь. Добавлением двух ребер мы замкнули цикл, а значит мы не можем добавить больше одного ребра. Тогда получается, мы можем добавить в точности одно ребро, а значит и число ребер увеличилось на один, а значит и утверждение доказано.

$\Leftarrow$. См. пункт 10.

□

12. Эквивалентность определений дерева и графа с простым путём между любыми двумя вершинами.

Утверждение. *Деревья это в точности графы, в которых для любых двух вершин есть ровно один простой путь с концами в этих вершинах.*

Доказательство. $\Rightarrow$

По определению дерева оно является связным графом без циклов. Рассмотрим какие-то две вершины a и b. Докажем, что существует ровно один простой путь между ними.

Поскольку дерево по определению связно, путь есть. Докажем его единственность.

Если есть несколько путей, то маршрут из a в b по первому пути и обратно по другому пути будет являться циклом – значит, путь только один.

$\Leftarrow$

Рассмотрим две вершины a и b данного графа, по условию между ними существует простой путь. Если таких путей несколько, то маршрут из a в b по первому пути и обратно по другому пути будет являться циклом. Следовательно, путей не более одного. Если же такого пути нет, то вершина b не достижима из a, то есть граф не связен. Следовательно, такой граф является деревом. □

13. Существование остовного дерева

Определение. ***Частичный граф*** *исходного графа $G = (V, E)$ — граф $G' = (V, E')$, $E' \subseteq E$.*

Определение. ***Остовное дерево*** *связного графа $G = (V, E)$ — всякий его частичный граф, являющийся деревом.*

Лемма. *Если граф связен, то у него есть остовное дерево.*

Доказательство. Для начала докажем вспомогательную лемму:

Лемма. *Если граф связен и содержит хотябы один цикл, то из него можно удалить ребро не нарушая связности.*

Доказательство леммы. Пусть $G = (V, E)$ и цикл в нем: $u_0 \to u_1 \to ...u_n \to u_0$, $u_i \in V$. Поймем, что если удалить любое ребро принадлежащее цикул, связность не нарушится. Покажем в частности, что можно удалит ребро (u_0, u_1). Действительно, если есть какой-нибудь путь из $v \in V$ в $w \in V$, проходящий через ребро (u_0, u_1), то существует путь проходящий через прочие ребра цикла, ведь в цикле до каждой вершины можно дойти хотя бы двумя разными путями, значит удаление ребра не изменит того факта, что v соединено путем с w. Если пути из v к w не содержат ребра (u_0, u_1), то очевидно, что его удаление на их связи не отразится $\Rightarrow$ граф без этого ребра останется связанным. Тогда удалим его и получим связный граф. □

Пусть теперь $G = (V, E)$ - связный граф, для которого нужно доказать существование остовног дерева. Возможны два сценария:

1. Граф G - связный граф без циклов.
2. В графе G есть хотя бы один цикл.

В первом случае G - дерево по определению, а значит сам является своим остовным деревом.

Во втором случае, по доказанной лемме, мы можем удалить из G ребро не нарушая связности. Так сделаем же это. Если полученный граф - цикличен, то снова удалим ребро не нарушая связности, иначе остановимся и порадуемся; индуктивно будем повторять описанные операции, на каждой иттерации имея связный граф; число ребер в графе - конечно, значит процесс не может продолжаться вечно $\Rightarrow$ в какой-то момент мы не сможем удалить ребро не нарушая связности, что было бы не возможно, если бы в графе остался цикл. В ходе описанных операций мы не добавляли новых ребер и не удаляли вершин $\Rightarrow$ если $G' = (V', E')$ - итоговый граф, то $V' = V$, $E' \subseteq E \Rightarrow G'$ - частичный граф графа G, связный и без цилов, т.е. дерево $\Rightarrow G'$ по определению - остовное дерево графа G. □

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 сиьной 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) $\square$

15. Критерий существования эйлерова цикла в орграфе

Теорема. *Орграф содержит эйлеров цикл тогда и только тогда, когда он сильно связен и у любой вершины входящая степень равна степени исходящей.*

Доказателъство. $\Rightarrow$. Пусть эйлеров цикл есть. Тогда он проходит через все вершины и по нему можно пройти от любой вершины до любой другой, а значит, он сильно связен.

Возьмем произвольную вершину v в графе и пусть она встречается в цикле k раз. Тогда, идя по циклу, мы придем в нее k раз и уйдем из нее k раз. При этом, так как цикл эйлеров, мы должны пройти все ребра, а значит мы должны выйти и войти в вершину одинаковое количество раз. Значит, входящая и исходящая степени равны.

$\Leftarrow$. Будем рассматривать пути, которые не проходят дважды по одному ребру. (Таков, например, путь, состоящий из одного ребра) Выберем среди них самый длинный путь $a_1 \to a_2 \ldots a_n$ и покажем, что он является искомым циклом, то есть что $a_1 = a_n$ и что он содержит все рёбра. Если он самый длинный, то добавить к нему ребро $an \to a_{n+1}$ уже нельзя, то есть все выходящие из an рёбра уже использованы (иначе мы нашли бы длиннее). Это возможно, лишь если $a_1 = a_n$. Почему? В самом деле, если вершина a_n встречалась только внутри пути(то есть не являлась началом 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(путь самый длинный). Это противоречит равенству входящей и исходящей степени. Если во всех вершинах цикла использованы все рёбра, то из вершин этого цикла нельзя попасть вне цикла, то есть использованы все вершины (мы предполагаем, что граф связен или сильно связен) и, следовательно, все рёбра. Если из какой-то вершины a_i выходит ребро $a_i \to v$, то путь можно удлинить до $a_i \to a_{i+1} \to \ldots \to a_n = a_1 \to a_2 \to \ldots \to a_i \to v$, вопреки нашему выбору (самого длинного пути). Если в какую-то вершину a_i входит ребро $v \to a_i$, добавим v в начало, тем самым удлинив путь, что опять же противоречит нашему выбору самого длинного пути. $\square$

17. Сравнение $ax \equiv 1\ (mod\ N)$ имеет решение тогда и только тогда, когда $(a, N) = 1$

Замечание. *Здесь и далее условимся обозначать НОД(a, N), как $(a,\ N)$.*

Утверждение. *Сравнение* $ax \equiv 1\ (modN)$ *имеет решение* (1) $\Leftrightarrow (a, N) = 1$ (2).

Доказательство. Докажем следствие (1) $\Rightarrow$ (2)

$$ax - 1 \equiv 0\ (mod\ N)$$

$$\Downarrow$$

$$N|(ax - 1)$$

$$\Downarrow$$

$$(ax - 1) = Nk,\ k \in Z.$$

Пусть $(a,\ N) = b$ ($1 \leqslant b$, т.к. 1 - всегда делитель). Тогда $a = a' \cdot b$, $N = N' \cdot b \Rightarrow$

$$a'bx - 1 = N'bk$$

$$\Downarrow$$

$$1 = b(a'x - N'k)$$

По определению $b|1$, но тогда $|b| \leqslant 1$, но тогда $b = 1 \Rightarrow (a,\ N) = 1$.

Докажем следствие (2) $\Rightarrow$ (1): (2) $\Rightarrow$ $(a,\ N) = 1$, тогда по соотношению Безу $\exists m,\ k$: $am+Nk = 1 \Rightarrow am = 1-Nk \Rightarrow am \equiv 1\ (mod\ N)$, и $x = m$ - решение сравния $ax \equiv 1\ (mod\ N)$. □

18. Признаки делимости на 3, 9 и 11

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

Доказательство. Пусть $x = \overline{a_n a_{n-1} \dots a_1 a_0} = 10^n a_n + 10^{n-1} a_{n-1} + \dots + 10a_1 + a_0$. 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:

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

□

19. Малая теорема Ферма и лемма Вильсона

Теорема. *Пусть p - простое и a, такое, что оно не делится на p. Тогда утверждается, что*

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

Доказательство. Сперва докажем следующую лемму: Умножение остатков $1, 2, 3, \ldots, p-1$ на a даст те же остатки, но в другом порядке. *Доказательство от противного.* Пусть нашлись каких-то два числа ax и ay, дающих одинаковый остаток при делении на p (x и y — остатки). Тогда $a(x-y)$ делится на p, что невозможно. Тогда нет совпадающих остатков. Так как произведений, как и остатков, $p-1$, то лемма верна.

Рассмотрим произведения $a, 2a, 3a, \ldots, (p-1)a$. Тогда

$$a \cdot 2a \cdot \ldots \cdot (p-1)a \equiv a^{p-1}(p-1)! \ (mod \ p)$$

С другой стороны, по лемме это эквивалентно $(p-1)!$ по модулю p. Тогда $a^{p-1} \equiv 1 \ (mod \ p)$, что и требовалось доказать. □

20. Теорема Эйлера

Теорема. *Пусть N – произвольное простое число, $\varphi(N)$ – функция Эйлера (то есть число остатков от 0 до $N-1$), а число a – один из этих остатков, взаимно простой с N. Тогда:*

$$a^{\varphi(N)} \equiv 1 \bmod N$$

Доказательство. Поскольку a взаимно просто с N и x_i взаимно просто с N, то и $x_i \cdot a$ также взаимно просто с N, то есть существует x_j такой, что $x_i a \equiv x_j \bmod N$.

Отметим, что все остатки $x_i \cdot a$ различны по модулю N. Пусть это не так, тогда $x_{i_1} a \equiv x_{i_2} a \bmod N \Rightarrow a(x_{i_1} - x_{i_2}) = 0$, то есть $x_{i_1} \equiv x_{i_2} \bmod N$ – это противоречит тому, что все остатки $x_1 \ldots x_{\varphi(N)}$ различны.

Перемножим все сравнения $x_i \cdot a \equiv x_j \bmod N$, получим

$$x_1 \cdots x_{\varphi(N)} a^{\varphi(N)} \equiv x_1 \cdots x_{\varphi(N)} \bmod N x_1 \cdots x_{\varphi(N)}(a^{\varphi(N)} - 1) \equiv 0 \bmod N$$

Поскольку каждый из остатков $x_1 \ldots x_{\varphi(N)}$ взаимно прост с N, можно записать:

$$a^{\varphi(N)} - 1 \equiv 0 \bmod N$$

□

21. Корректность алгоритма Евклида и расширенного алгоритма Евклида.

Алгорим Евклида. *Пусть a и b - целые числа одновеременно не равные нулю, и последовательность чисел $x_0 > x_1 > x_2 > x_3 \cdots > x_n > 0$ определена тем, что $x_0 = a$, $x_1 = b$, каждое x_k, $k > 1$ — это остаток от деления предпредыдущего числа на предыдущее, а предпоследнее делится на последнее нацело, то есть:*

$$a = x_0 q_1 + x_1,$$

$$b = x_1 q_2 + x_2,$$

$$x_2 = x_3 q_3 + x_4,$$

$$\dots$$

$$x_{k-2} = x_{k-1} q_{k-1} + x_k,$$

$$\dots$$

$$x_{n-2} = x_{n-1} q_{n-1} + x_n,$$

$$x_{n-1} = x_n q_n.$$

Тогда (a, b) равен x_n, последнему ненулевому члену этой последовательности.

Доказательство. Поймем, что такие $x_1, x_2, x_3, x_4, \cdots x_n$ - существуют, причем единственно: всегда можно найти остаток m (причем единственным образом) при делении x_k на x_{k+1}, если $x_{k+1} \neq 0$, причем $a > b > r_k > x_{k+1} > m$, т.е. каждый следующий член последовательности строго меньше предыдущего, но т.к. числа ее составляющие - целые, то убывать бесконечно она не может, а значит $\exists x_{n+1} = 0$ - последний член последовательности.

Докажем тогда, что если x_n - последний не нулевой член последовательности, то $(a, b) = (x_n, 0) = x_n \neq 0$. Для этого заметим две вещи:

1. $r \neq 0 \Rightarrow (r, 0) = |r|$ так как 0 делится на любое целое число, кроме нуля.

2. Пусть $a = bq + r$, тогда $(a,\ b) = (b,\ r)$. Пусть k — любой общий делитель чисел a и b, не обязательно наибольший, тогда $a = t_1 k$ и $b = t_2 k$, где t_1 и t_2 — целые числа из определения.

   Тогда k является также общим делителем чисел b и r, так как b делится на k по определению, а $r = a - b \cdot q = (t_1 - t_2 \cdot q) \cdot k$ (выражение в скобках есть целое число, следовательно, k делит r без остатка).

   Обратное также верно. Любой делитель k чисел b и r так же является делителем a и b: $a = b \cdot q + r = k \cdot (b'q + r') \Rightarrow k|a$.

   Следовательно, все общие делители пар чисел a, b и b, rсовпадают. Другими словами, нет общего делителя у чисел a, b, который не был бы также делителем b, r, и наоборот.

   В частности, наибольший общий делитель остается тем же самым. Что и требовалось доказать.

Тогда по построению последовательности $\{x_i\}$: $(x_0,\ x_1) = (x_1,\ x_2) = (x_2,\ x_3) = \dots = (x_n,\ 0) = x_n$. □

Алгорим Евклида (Расширенный алгоритм Евклида)**.** *Формулы для x_i могут быть переписаны следующим образом:*

$$x_0 = aq_0 + bp_0,$$

$$x_1 = aq_1 + bp_1,$$

$$x_2 = aq_2 + bp_2,$$

$$x_3 = aq_3 + bp_3,$$

$$\vdots$$

$$(a,\ b) = x_n = as + bt$$

Т.е. НОД$(a,\ b)$ можно представить в виде $ax + by$, где x, y - какие-то целые числа.

Доказательство. Докажем по индукции по n.

База. $x_0 = a + b \cdot 0$, $x_1 = a \cdot 0 + b$. Т.е. $q_0 = P_1 = 1$, $p_0 = q_1 = 0$

Предположение. Пусть $x_{k-2} = aq_{k-2} + bp_{k-2}$ и $x_{k-1} = aq_{k-1} + bp_{k-1}$.

Шаг. Докажем, что $x_k = aq_k + bp_k$, где q_k, p_k - целые. Мы помним, что x_k - остаток от деления x_{k-2} на x_{k-1}, значит по определнию: $m \cdot x_{k-1} + x_k = x_{k-2}$, где m - какое-то целое число. Тогда $x_k = x_{k-2} - m \cdot x_{k-1}$, по п.и., $x_k = aq_{k-2} + bp_{k-2} - m(aq_{k-1} + bp_{k-1}) = a(q_{k-2} - mq_{k-1}) + b(p_{k-2} - mp_{k-1}) = aq_k + bp_k$.

Таким образом каждое из чисел x_i представимо в виде линейной комбинации a и b (В частности, если $(a, b) = 1$, то $\exists x, y : ax + by = 1$). □

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. Пусть n – наименьшее целое число не разложимое в произведение простых чисел. Оно не может быть единицей по формулировке теоремы. Оно не может быть и простым, потому что любое простое число является произведением одного простого числа – себя. Если n составное, то оно – произведение двух меньших натуральных чисел. Каждое из них можно разложить в произведение простых чисел, значит n тоже является произведением простых чисел. Противоречие.
Единственность. Пусть n – наименьше натуральное число, разложимое в произведение простых чисел двумя разными способами. Если оба разложения пустые — они одинаковы. В противном случае, пусть p – любой из сомножителей в любом из двух разложений. Если p входит и в другое разложение, мы можем сократить оба разложения на p и получить два разных разложения числа $\frac{n}{p}$, что невозможно. А если p не входит в другое разложение, то одно из произведений делится на p, а другое – не делится (как следствие из леммы), что противоречит условию. □

23. Китайская теорема об остатках

Теорема. *Для любых попарно взаимно-простых $a_1, a_2, ..., a_n$ и для любых $r_1, r_2, ..., r_n$ таких, что $0 \leqslant r_i < a_i$, существует и единственен с точностью до операции взятия по модулю*

$M = \prod_1^n a_i$ *x являющийся решением системы (1):*

$$\begin{cases} x \equiv r_1 \pmod{a_1} \\ x \equiv r_2 \pmod{a_2} \\ \vdots \\ x \equiv r_n \pmod{a_n} \end{cases}$$

И любой $x' \equiv x \pmod{\prod_1^n a_i}$ *так же является решением этой системы.*

(Иная формулировка: Если натуральные числа $a_1,a_2,\ldots,a_n$ *попарно взаимно просты, то для любых целых* $r_1,r_2,\ldots,r_n$ *таких, что* $0 \leqslant r_i < a_i$ *при всех* $i \in \{1,2,\ldots,n\}$*, найдётся число* N*, которое при делении на* a_i *даёт остаток* r_i *при всех* $i \in \{1,2,\ldots,n\}$ *. Более того, если найдутся два таких числа* N_1 *и* N_2 *, то* $N_1 \equiv N_2 \pmod{a_1 \cdot a_2 \cdot \ldots \cdot a_n}$*.)*

Доказательство. Покажем, что $x = \sum_{i=1}^n r_i M_i M_i^{-1}$ (2), где $M_i = \frac{M}{a_i}$, а M_i^{-1} - обратный к M_i элемент по модулю a_i, является решением указанной выше системы.

Проверим, что для него выполняется i-е равенство в системе:

$$x \equiv \sum_{j=1}^{n} r_j M_j M_j^{-1} \equiv r_i M_i M_i^{-1} \equiv r_i \pmod{a_i}$$

Второе равенство справедливо т.к. $M_j \equiv \prod_{k \neq j}^n a_k \equiv 0 \pmod{a_i}$ при всех $i \neq j$ (т.е. все слагаемые кроме j-ого делятся на a_j), третье т.к. M_i^{-1} является обратным для M_i по модулю a_i. Повторяя рассуждения для всех i, убедимся, что x, определенный формулой (2), является решением для (1).

В силу выбранного числа M все числа $x' \equiv x \pmod{M}$ будут удовлетворять системе.

Покажем теперь, что среди чисел 0, 1, ..., $M-1$ (множество A) не найдется другого решения кроме найденного нами ранее. Проведем доказательство этого факта от противного. Предположим, что получилось найти хотя бы два решения x_1, $x_2 \in A$ для некоторого набора остатков r. Так как множество B всех допустимых наборов $(r_1, r_2, \ldots, r_n)$ является равномощным множеству A (количество наборов остатков в B: $|B| = a_1 \cdot a_2 \ldots = M = |A|$), то для $\overline{A}_x := A \setminus \{x_1,x_2\}$ и $\overline{B}_r := B \setminus \{r\}$ выполнено $|\overline{A}_x| < |\overline{B}_r|$. Однако по доказанному ранее, для любого набора из $\overline{B}_r$ существует решение из $\overline{A}_x$, следовательно по принципу Дирихле найдутся как минимум 2 набора остатков, которым соответствует одно и то же $x \in A$. Для такого x найдется a_i такое, что $x \equiv r_1$, $x \equiv r_2 \pmod{a_i}$ и $r_1 \neq r_2$. Противоречие.

□

24. Мультипликативность функции Эйлера. Формула для функции Эйлера

Утверждение. *Для взаимно простых* m *и* n *верно, что* $\varphi(mn) = \varphi(m)\varphi(n)$

Доказательство. □

25. Доказательство корректности определения классов эквивалентности

Теорема. *Для любого отношения эквивалентности на множестве A множество классов эквивалентности образует разбиение множества A. Обратно, любое разбиение множества A задает на нем отношение эквивалентности, для которого классы эквивалентности совпадают с элементами разбиения.*

Доказательство. Докажем прямое следствие.

Каждому $x \in A$ сопоставим $[x] = \{y|\ x \sim y\}$ - пожмножетсво множество всех элементов с которыми x вступает в отношение $\sim$.

Утверждается, что система подмножеств $[x]$ образует разбиение A. Действительно, во-первых, каждое подмножество $[x] \neq \emptyset$, так как в силу рефлексивности отношения $\sim$ $x \in [x]$.

Во-вторых, два различных подмножества $[x]$ и $[y]$ не имеют общих элементов. Рассуждая от противного, допустим существование элемента z такого, что $z \in [x]$ и $z \in [y]$. Тогда $z \sim x$ и $z \sim y$. Поэтому для любого элемента $t \in [x]$ из $t \sim x$, $z \sim x$ и $z \sim y$ в силу симметричности и транзитивности отношения а вытекает aPy ($t \sim x$ и $x \sim z \Rightarrow tPz$, но $z \sim y \Rightarrow t \sim y$), то есть $a \in [y]$. Следовательно, $[x] \subseteq [y]$. Аналогично получаем, что $[y] \subseteq [x]$. Полученные два включения влекут равенство $[x] = [y]$, противоречащее предположению о несовпадении подмножеств $[x]$ и $[y]$. Таким образом, $[x] \cap [y] = \emptyset$.

В-третьих, объединение всех подмножеств $[x]$ (классов эквивалентности) совпадает со множеством A, ибо для любого элемента $x \in A$ выполняется условие $x \in [x]$.

Итак, система подмножеств эквивалентности $[x]$, образует разбиение множества A.

Обратное следствие.

Пусть есть разбиение A на непересекающиеся множества $M_0, \ldots, M_1$. Тогда отношение эквивалентности на A задается так:

$$a \sim b \leftrightarrow (a \in M_i \wedge b \in M_i)$$

Свойства транзитивности, рефлексивности и симметричности очевидны (Например для транзитивности: $a \sim b$ и $b \sim c$, значит $(a \in M_i \wedge b \in M_i) \wedge (b \in M_i \wedge c \in M_i) \Leftrightarrow (a \in M_i \wedge c \in M_i) \Leftrightarrow a \sim c$). Тогда, два элемента принадлежат одному классу тогда и только тогда, когда они лежат в одном подмножестве M_i, т.е. классы задаются разбиением. □

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.

[⇒] 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.

[⇐] 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 $(x,y) \in P$. □

28. Теорема о представлении частичного порядка в виде пересечения линейных

Теорема 1. *Любой частиный порядок, определенный на множестве из n элементов, можно предстваить, как пересечение не более, чем n^2 линейных порядков.*

Доказателъство. Пусть у нас есть частичный порядок P. Рассмотрим несравнимую пару x и y. Образуем новый частичный порядок P', полученный из P добавлением сравимости xPy и некоторых других для того, чтобы транзитивность сохранилась. Образуем еще один частичный порядок P'', полученный из P добавлением сравнимости yPx и некоторых других сравнимостей для сохранения тразитивности. Тогда каждый из этих двух частичных порядков можем достроить до линейного порядка (по теореме Шпильрайна). Назовем их $Lin_{p'}$ и $Lin_{p''}$ соответсвенно.

Теперь оценим количество несравнимых пар. Всего пар в отношении может быть $n \cdot n = n^2$ штук, однако нас не интересует порядок элементов внутри пар, тогда без учета порядка их *не более* $2 \cdot \frac{n^2}{2!} = \frac{n^2}{2}$. Получаем, что несравнимых пар также не более $\frac{n^2}{2}$. Тогда рассмотрим для каждой из них $Lin_{p'}$ и $Lin_{p''}$, таких линейных порядков в сумме не более $\frac{n^2}{2} = n^2$. Теперь изучим, что будет, если их пересечь. В действительности, мы получим как раз P, так как если xPy, то она принадлежит и $Lin_{p'}$, и $Lin_{p''}$, иначе она будет принадлежать только одному из них, и тогда при пересечении её уже не будет.

P.S. Внимательный читатель скажет, что мы рассмотрели только случай, когда нам нужно получить строгий частичный порядок, однако на самом деле получение нестрогого обходится нам «дёшево» и не влияет на нашу оценку, так как её можно осуществить параллельно с другими пересечениями.

□

29. Критерий существования функции, обратной к данной. Критерий биекции в терминах обратной функции

Критерий существования функции, обратной к данной. Пусть f - функциональное соответствие $f : X \to Y$. Тогда обратное соответствие: $f^{-1} = (y,\, x) |\ (x,\, y) \in f \Leftrightarrow f(x) = y$.

Замечание. f^{-1} - *функционально* $\Leftrightarrow$ f - *инъетивно.*

Доказателъство. Докажем $\to$.

Из того, что f^{-1} - функционально $\Rightarrow \forall\ y \in Y :\ f^{-1}(y) = x$ и $f^{-1}(y) = x' \Leftrightarrow x = x' \Rightarrow$ если $f(x) = f(x') = y$, то $f^{-1}(y) = x = x'$, что и означает инъективность f.

Докажем $\leftarrow$.

Из инъективности $f \Rightarrow \forall\ y \in Y : f(x) = y$ и $f(x') = y \Leftrightarrow x = x' \Rightarrow$ если $(y,\, x) \in f^{-1}$ и $(y,\, x') \in f^{-1}$, то $x = x' \Rightarrow f^{-1}$ - функционально. □

Критерий биекции в терминах обратной функции

Теорема. *Критерией биективности:*

1. *Если f - биекция $A \leftrightarrow B$, то $f \circ f^{-1} = id_B$ и $f^{-1} \circ f = id_A$.*

2. *Если f - функция $A \to B$ и существует $g : B \to A$, такая что $f \circ g = id_B$ и $g \circ f = id_A$, то $f^{-1} = g$ и f - биекция.*

Доказательство. Утверждение 1 проверяется непосредственно, по свойствам биекции: $\forall a \in A : \ f^{-1} \circ f(a) = a$ и $\forall b \in B : \ f \circ f^{-1}(b) = b$.

Докажем 2, проверив f на свойства биекции.

Всюду определенность Если f не всюду определена, то $g \circ f(x) = g(f(x))$ - не всюду определена, а значит не тождественна, что противоречит гипотизе. Значит f - тотальна.

Инъективность. Пусть $f(x_1) = f(x_2) \Rightarrow g(f(x_1)) = g(f(x_2)) \Rightarrow x_1 = x_2$.

Сюръективность. Пусть f не принимает значение $b \in B$, тогда $f(g(\ldots))$ не принимает значение b, значит $f \circ g$ - не тождественна, что противоречит условию. Тогда $\forall b \in B : \ \exists a \in A : \ f(a) = b$.

Таким образом f - биекция. Тогда очевидно, что $g = f^{-1}$ (проверяется поэлементно из композиции $g \circ f = id_A$, $f \circ g = id_B$: $(a,\, b) \in f \Rightarrow (b,\, a) \in g$ и аналогично, если $(b,\, a) \in g$, то $(a,\, b) \in f$). □

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.