Дискретная математика, пилотный поток. Решения задач экзамена 28.03.17

1. Приведите пример вероятностного пространства U и событий A и B, таких что $\Pr[A] > 0$, $\Pr[B] > 0$, $\Pr[A \mid B] = \Pr[B \mid A]$, но $\Pr[A] \neq \Pr[B]$. Все требуемые равенства и неравенства для построенного примера должны быть обоснованы.

Решение.

Пусть $U = \{0, 1, 2\}$, то есть состоит из трех исходов. Распределение равновероятное. Пусть $A = \{0\}$, $B = \{1, 2\}$. Тогда

$$\Pr[A] = \frac{|A|}{|U|} = 1/3, \quad \Pr[B] = \frac{|B|}{|U|} = 2/3, \quad \Pr[A \cap B] = \frac{|A \cap B|}{|U|} = 0.$$

Тогда

$$\Pr[A \mid B] = \frac{\Pr[A \cap B]}{\Pr[B]} = 0, \quad \Pr[B \mid A] = \frac{\Pr[A \cap B]}{\Pr[A]} = 0,$$

и все требуемые условия выполнены.

2. Существуют ли невычислимые всюду определенные функции $f, g\colon \mathbb{N} \to \mathbb{N}$, такие что функция $h(x) = f(x) \cdot g(x)$ для всех $x \in \mathbb{N}$ вычислима? В этой задаче вычислимость и невычислимость можно обосновывать неформально, не обязательно проводить рассуждения с машинами Тьюринга.

Решение. *Ответ*: да, существует.

Приведем пример такой пары функций.

Пусть $K \subseteq \mathbb{N}$ — неразрешимое множество. В курсе было доказано, что такое множество существует. Также было доказано, что если K неразрешимо, то и его дополнение $\mathbb{N} \setminus K$ неразрешимо.

Поскольку K неразрешимо, то его характеристическая функций

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

невычислима (также доказывалось в лекциях). Аналогично невычислима характеристическая функция $\chi_{\mathbb{N}\setminus K}$.

Положим $f(x) = \chi_K(x)$ и $g(x) = \chi_{\mathbb{N}\setminus K}(x)$. Тогда функции f и g невычислимы, а функция $h(x) = f(x) \cdot g(x) = 0$ вычислима, поскольку тождественно равна 0 (для всякого $x \in \mathbb{N}$ ровно одна из функций χ_K и $\chi_{\mathbb{N}\setminus K}$ равна нулю на x).

3. Есть полоска бумаги из 2017 клеток. Два игрока по очереди закрашивают часть клеток: на каждом ходу игрок должен закрасить три подряд стоящие клетки (уже закрашенные клетки повторно закрашивать нельзя). Кто не может сделать ход - проиграл. У кого из игроков есть выигрышная стратегия?

Решение. *Ответ*: выигрышная стратегия есть у первого игрока.

Предъявим выигрышную стратегию первого игрока.

Перенумеруем клетки полоски слева направо числами $-1008, -1007, \ldots, -1, 0, 1, \ldots, 1007, 1008$. Первым ходом первый игрок закрасит клетки с номерами $-1, 0, 1$. Каждый следующий ход первый игрок будет делать симметрично предыдущему ходу второго игрока. То есть, если на очередном ходу второй игрок закрашивает клетки $i, i+1, i+2$ для некоторого i, то на следующем ходу первый игрок закрасит клетки с номерами $-i-2, -i-1, -i$. Таким образом, первый игрок поддерживает такое свойство раскраски: после

каждого хода первого игрока множество закрашенных клеток симметрично относительно клетки с номером 0, то есть клетка i закрашена тогда и только тогда, когда закрашена клетка $-i$. Следовательно, у первого игрока после каждого хода второго есть возможность сделать свой симметричный ход, и первый игрок не проиграет.

4. Рассмотрим булевы схемы от переменных $x_1, \ldots, x_{10}$ с одним выходом, использующие одну операцию конъюнкции (от двух переменных) и произвольное количество операций взятия отрицания. Сколько различных функций от переменных $x_1, \ldots, x_{10}$ можно вычислить такими схемами? Функции, которые можно получить друг из друга переименованием переменных считаются разными. Например, $x_1 \wedge x_2$ и $x_3 \wedge x_4$ – разные функции от переменных $x_1, \ldots, x_{10}$. Ответом в задаче должно быть число в десятичной записи.

Решение. *Ответ*: 382.

Введем обозначения $x^1 = x$ и $x^0 = \neg x$.

Если в схеме используется только операция отрицания, то всякий элемент схемы есть либо переменная, либо отрицание предыдущего элемента. Поскольку $\neg\neg x = x$, то все элементы такой схемы есть либо переменные, либо их отрицания, то есть всякий элемент схемы является литералом.

Если в схеме используется одна операция взятия конъюнкции, то все элементы до нее получаются лишь с помощью применения отрицания. Так что единственная операция конъюнкции может применяться только к переменным или их отрицаниям. Результатом применения такой конъюнкции может быть функция $(x_i^a \wedge x_j^b)$, где $a, b \in \{0, 1\}$. После операции конъюнкции в схеме вновь могут использоваться только отрицания, так что все последующие элементы схемы есть либо переменные, либо их отрицания, либо вычисленная конъюнкция, либо ее отрицание. В частности, выход схемы также имеет один из перечисленных видов.

Переберем все эти случаи и посчитаем, сколько различных функций вычисляется в каждом из них. Различных переменных и их отрицаний всего 20 штук.

Вычисленная конъюнкция или ее отрицание в общем виде имеют вид $(x_i^a \wedge x_j^b)^c$. Если $i = j$ то полученная функция есть либо переменная, либо ее отрицание, либо константа 0 или 1 (в случае, если $a \neq b$). Переменные и их отрицания мы уже посчитали, так что в этом случае добавляется еще 2 функции: константы 0 и 1.

Если $i \neq j$, то полученные функции существенно зависят от двух переменных и отличаются от переменных, их отрицаний и констант. Для каждой пары $\{i, j\}$ при различных значениях $a, b, c \in \{0, 1\}$ получается 8 различных функций $(x_i^a \wedge x_j^b)^c$. Действительно, если $c = 1$, то указанная функция равна единице только при $x_i = a, x_j = b$. Аналогично, если $c = 0$, то указанная функция равна нулю только при $x_i = a, x_j = b$. Любые две такие функции различаются. Количество способов выбрать пару $\{i, j\}$ равно $\binom{10}{2} = 45$, для каждой пары получается 8 различных функций. Всего в этом случае получается $8 \cdot 45 = 360$ функций.

Суммарно во всех случаях получается $20 + 2 + 360 = 382$ функции.

5. Обозначим через $\mathbb{R}_+$ множество положительных действительных чисел, а через $\mathbb{R}_-$ – множество отрицательных действительных чисел. Изоморфны ли следующие порядки: $\mathbb{R} \times \mathbb{R}_+$ с покоординатным порядком и $\mathbb{R}_- \times \mathbb{R}$ с покоординатным порядком?

Решение. *Ответ*: изоморфны.

Заметим сначала, что упорядоченное множество $\mathbb{R}$ с обычным отношением порядка изоморфно множеству $\mathbb{R}_+$ с обычным отношением порядка. Действительно, функция $f(x) = e^x$ задает такой изоморфизм

из множества $\mathbb{R}$ в множество $\mathbb{R}_+$. Аналогично, функция $g(x) = -e^{-x}$ задает изоморфизм упорядоченных множеств $\mathbb{R}$ и $\mathbb{R}_-$.

Теперь нетрудно построить изоморфизм из множества $\mathbb{R} \times \mathbb{R}_+$ в множество $\mathbb{R}_- \times \mathbb{R}$. Такой изоморфизм задается функцией $h(x, y) = (g(x), f^{-1}(y))$, где f^{-1} есть функция, обратная к f. Действительно, биективность функции h следует из биективности функций f^{-1} и g.

Проверим, что h сохраняет порядок. Пусть $(x_1, y_1), (x_2, y_2) \in \mathbb{R} \times \mathbb{R}_+$. Тогда

$$(x_1, y_1) \le (x_2, y_2) \Leftrightarrow \begin{cases} x_1 \le x_2, \\ y_1 \le y_2, \end{cases} \Leftrightarrow \begin{cases} g(x_1) \le g(x_2), \\ f^{-1}(y_1) \le f^{-1}(y_2), \end{cases} \Leftrightarrow h(x_1, y_1) \le h(x_2, y_2).$$

6. Докажите, что в полном графе на $2n$ вершинах существует n остовных деревьев, таких, что каждое ребро графа входит только в одно дерево.

Решение.

Проведем доказательство индукцией по n.

Для $n = 1$ граф состоит из двух вершин и сам является своим остовным деревом.

Пусть утверждение доказано для полного графа на $2n$ вершинах. Рассмотрим полный граф на $2n + 2$ вершинах. Разобьем его вершины на два равных множества и обозначим их $v_0, v_1, \ldots, v_n$ и $u_0, u_1, \ldots, u_n$. Рассмотрим полный подграф на вершинах $v_1, \ldots, v_n, u_1, \ldots, u_n$. По предположению индукции в нем есть n остовных деревьев, никакие два из которых не имеют общих ребер. Обозначим эти деревья через $T_1, \ldots, T_n$. Для каждого i добавим к дереву T_i ребра $\{u_0, v_i\}$ и $\{v_0, u_i\}$. В результате получим n остовных деревьев в изначальном графе на $2n + 2$ вершинах. Легко видеть, что никакие два из этих деревьев не имеют общих ребер.

Построим еще одно остовное дерево T_0. Для этого соединим вершины u_0 и v_0, вершину u_0 соединим со всеми вершинами $u_1, \ldots, u_n$, а вершину v_0 — со всеми вершинами $v_1, \ldots, v_n$. Нетрудно видеть, что T_0 является остовным деревом и не имеет общих ребер с деревьями $T_1, \ldots, T_n$.

7. В системе односторонних правил подстановки в алфавите $\{a, b\}$ всякое правило имеет вид $a^k b \to b a^l$, где k и l положительны, а a^k обозначает последовательность из букв a длины k. При этом числа k и l для разных правил могут быть разными. Разрешима ли задача проверки достижимости для графа, заданного конечным множеством таких правил подстановки? В этой задаче разрешимость и неразрешимость можно обосновывать неформально, не обязательно проводить рассуждения с машинами Тьюринга.

Решение. *Ответ*: да, разрешима.

Пусть задана односторонняя система подстановок I с конечным множеством правил описанного вида. Опишем алгоритм проверки достижимости в графе, заданном этой системой. На вход такой алгоритм получает два слова X и Y, и требуется проверить, достижимо ли Y из X.

Заметим, что применение описанных правил не меняет число букв b в слове. Таким образом, из слова X достижимы только слова с тем же числом букв b. Если в Y другое число букв b, то мы сразу можем сказать, что оно недостижимо.

Обозначим число букв b в слове X через m. Всякое слово Z, содержащее ровно m букв b имеет вид

$$Z = a^{p_m} b a^{p_{m-1}} b \ldots b a^{p_0},$$

где $p_m, p_{m-1}, \ldots, p_0 \ge 0$. Обозначим через L максимальное число букв a в правых частях правил из I,

и сопоставим каждому описанному слову Z число

$$N(Z) = p_m(L+1)^m + p_{m-1}(L+1)^{m-1} + \ldots + p_1(L+1)^1 + p_0.$$

Мы утверждаем, что если Z' получается из Z применением одного из правил I, то $N(Z') < N(Z)$. Действительно, в результате применения правила $a^k b \to ba^l$ одно из чисел p_i уменьшается на $k \geq 1$, а число p_{i-1} увеличивается на $l \leq L$. В результате число $N(Z)$ с одной стороны уменьшается на $k \cdot (L+1)^i \geq (L+1)^i$, а с другой стороны увеличивается на $l \cdot (L+1)^{i-1} \leq L(L+1)^{i-1}$. Поскольку $L(L+1)^{i-1} < (L+1)^i$, то число в целом уменьшается.

Таким образом, из X можно получить только те слова Z, в которых m букв b и у которых $N(Z) \leq N(X)$. Таких слов конечно. Если Y не является таким словом, то он не достижим из X. Если Y является одним из таких слов, то можно построить конечный граф достижимости на таких словах и проверить, достижим ли Y из X в этом конечном графе (алгоритм проверки достижимости в конечном графе разбирался на лекциях).

8. Пусть $p > 2$ — простое. Докажите, что для любого простого делителя q числа $2^p - 1$ выполняется $q \equiv 1 \pmod{p}$.

Решение.

Поскольку q простое, то по малой теореме Ферма $2^{q-1} - 1$ делится на q. С другой стороны, по условию $2^p - 1$ делится на q. Тогда q входит в разложение чисел $2^{q-1} - 1$ и $2^p - 1$ на простые множители, а значит НОД$(2^{q-1} - 1, 2^p - 1)$ также делится на q.

Заметим, что для всяких k, n верно НОД$(2^k - 1, 2^n - 1) = 2^{\text{НОД}(k,n)} - 1$ (похожая задача была в одном из домашних заданий). Действительно, пусть $k \leq n$ и пусть $n = qk + r$, где $0 \leq r < k$. Тогда $2^n - 1 = 2^{n-k}(2^k - 1) + (2^{n-k} - 1)$. Из этого равенства видно, что всякий общий делитель пары чисел $(2^n - 1, 2^k - 1)$ является общим делителем пары чисел $(2^{n-k} - 1, 2^k - 1)$ и наоборот. В частности, НОД$(2^n - 1, 2^k - 1) =$ НОД$(2^{n-k} - 1, 2^k - 1)$ (этот шаг аналогичен рассуждению из обоснования корректности алгоритма Евклида). Повторяя этот шаг q раз получим

$$\text{НОД}(2^n - 1, 2^k - 1) = \text{НОД}(2^{n-k} - 1, 2^k - 1) = \ldots = \text{НОД}(2^{n-qk} - 1, 2^k - 1) = \text{НОД}(2^r - 1, 2^k - 1). \quad (1)$$

Проведем вычисления по алгоритму Евклида для чисел n и k, и пусть $r_1, \ldots, r_l = \text{НОД}(n, k)$ – остатки, получаемые на шагах алгоритма. Запишем равенство, аналогичное (1), для экспонент для каждой строки в алгоритме Евклида. Образуется цепочка равенств

$$\text{НОД}(2^n - 1, 2^k - 1) = \text{НОД}(2^k - 1, 2^{r_1} - 1) = \text{НОД}(2^{r_1} - 1, 2^{r_2} - 1) = \ldots = \text{НОД}(2^{r_l} - 1, 2^0 - 1) = 2^{r_l} - 1.$$

В частном случае условия нашей задачи мы получаем, что НОД$(2^{q-1} - 1, 2^p - 1) = 2^{\text{НОД}(q-1,p)} - 1$ и нам известно, что это число делится на q. Если НОД$(q - 1, p) = 1$, то $2^{\text{НОД}(q-1,p)} - 1 = 2^1 - 1 = 1$, что не делится на q. Следовательно, НОД$(q - 1, p) > 1$. Поскольку у простого числа p всего два делителя, то НОД$(q - 1, p) = p$. В частности, $q - 1$ делится на p, что и требовалось доказать.