Дискретная математика. Коллоквиум весна 2017. Теоремы

Ваномас

12 марта 2017 г.

Содержание

Теорема 1 . . . . **2**

Теорема 2 . . . . **2**

Теорема 3 . . . . **3**

Теорема 4 . . . . **3**

Теорема 5 . . . . **3**

Теорема 7 . . . . **4**

Теорема 14 . . . . **5**

Теорема 18 . . . . **5**

Теорема 19 . . . . **6**

Теорема 20 . . . . **6**

Теорема 21 . . . . **7**

Теорема 22 . . . . **7**

Теорема 22 . . . . **7**

Теорема 1

Теорема. *Пусть* $(\Omega,\mathfrak{F},\mathcal{P})(\Omega,\mathfrak{F},\mathcal{P})$ *— вероятностное пространство. Тогда для произвольных событий* $A_1,A_2,\ldots,A_nA_1,A_2,\ldots,A_n$ *справедлива формула*

$$\mathcal{P}\left(\bigcup_{i=1}^{n} A_i\right) = \sum_i \mathcal{P}(A_i) - \sum_{i<j} \mathcal{P}(A_i \cap A_j) + \sum_{i<j<k} \mathcal{P}(A_i \cap A_j \cap A_k) + \ldots + (-1)^{n-1}\,\mathcal{P}\left(\bigcap_{i=1}^{n} A_i\right).\mathcal{P}\Big(\bigcup_{i=1}^{n}$$
$\sum_i \mathcal{P}(A_i) - \sum_{i<j} \mathcal{P}(A_i \cap A_j) + \sum_{i<j<k} \mathcal{P}(A_i \cap A_j \cap A_k) + \ldots + (-1)^{n-1}\,\mathcal{P}\left(\bigcap_{i=1}^{n} A_i\right)$.

Доказательство. Её можно получить из принципа включений-исключений в форме индикаторных функций:

$$\mathbf{1}_{\bigcup_i A_i} = \sum_i \mathbf{1}_{A_i} - \sum_{i<j} \mathbf{1}_{A_i \cap A_j} + \sum_{i<j<k} \mathbf{1}_{A_i \cap A_j \cap A_k} + \ldots + (-1)^{n-1}\,\mathbf{1}_{A_1 \cap \ldots \cap A_n}.\mathbf{1}_{\bigcup_i A_i} = \textstyle\sum_i \mathbf{1}_{A_i} - \sum_{i<j} \mathbf{1}_{A_i \cap A_j} +$$
$\sum_{i<j<k} \mathbf{1}_{A_i \cap A_j \cap A_k} + \ldots + (-1)^{n-1}\,\mathbf{1}_{A_1 \cap \ldots \cap A_n}$.

Пусть A_iA_i — события вероятностного пространства $(\Omega,\mathfrak{F},\mathcal{P})(\Omega,\mathfrak{F},\mathcal{P})$, то есть $A_i \in \mathfrak{F}A_i \in \mathfrak{F}$. Возьмем математическое ожидание $\mathcal{M}\mathcal{M}$ от обеих частей этого соотношения, и, воспользовавших линейностью математического ожидания и равенством $\mathcal{P}(A) = \mathcal{M}(\mathbf{1}_A)\mathcal{P}(A) = \mathcal{M}(\mathbf{1}_A)$ для произвольного события $A \in \mathfrak{F}A \in \mathfrak{F}$, получим формулу включения-исключения для вероятностей.

[:|||:]

Теорема 2

Теорема. *Условную вероятность* $Pr[A|B]$ *можно вычислить по формуле Байеса:*

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

Доказательство.

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

Т.к. $A \cap B = B \cap A$, то последнее равенство верно, а значит верна формула Байеса. **[:|||:]**

Теорема 3

Теорема. *Условной вероятностью события A при условии события B называется*

$\mathbb{P}(A \mid B) = \dfrac{\mathbb{P}(A \cap B)}{\mathbb{P}(B)} \mathbb{P}(A \mid B) = \frac{\mathbb{P}(A \cap B)}{\mathbb{P}(B)}$, *где* $\mathbb{P}(A \cap B) \mathbb{P}(A \cap B)$ *— вероятность наступления обоих событий сразу.*

Доказательство. Пусть ровно r исходов события B входят и в событие A. Исходы события B уже реализовались В данном испытании произошло одно из t событий, входящих в B. Все элементарные события равновероятны, следовательно, для данного испытания вероятность наступления произвольного элементарного события, входящего в B равна 1/t. Тогда по классическому определению вероятности, в данном испытании событие A произойдет с вероятностью r/t. $P(A|B) = \frac{\frac{r}{m}}{\frac{t}{m}} = \frac{P(AB)}{PB}$

[:|||:]

Теорема 4

Теорема. *Математическое ожидание E линейно.*

Доказательство. Пусть ξ и η — случайные величины, заданные на одном вероятностном пространстве. Тогда выполняется равенство

$$E(\xi + \eta) = \sum_w (\xi(w) + \eta(w))p(w) = \sum_w \xi(w)p(w) + \sum_w \eta(w)p(w) = E(\xi) + E(\eta)$$

То есть математическое ожидание суммы случайных величин равно сумме математического ожидания каждой из этих величин. Пусть теперь ξ — случайная величина, α — действительное число. Тогда выполняется равенство

$$E(\alpha \cdot \xi) = \sum_w (\alpha \cdot \xi(w)p(w)) = \alpha \cdot \sum_w \xi(w)p(w) = \alpha \cdot E(\xi)$$

То есть математическое ожидание произведения константы и случайной величины равно произведению этой константы и математического ожидания самой величины.
Таким образом, линейность математического ожидания доказана. **[:|||:]**

Теорема 5

Теорема. *Неравенство Маркова в теории вероятностей дает оценку вероятности, что случайная величина превзойдет по модулю фиксированную положительную константу, в терминах её математического ожидания. Получаемая оценка обычно груба, однако она позволяет получить определённое представление о распределении, когда последнее не известно явным образом.*

Пусть случайная величина $X \colon \Omega \to \mathbb{R}+$ *определена на вероятностном пространстве* $(\Omega, F, \mathbb{R})$, *и ее математическое ожидание* $\mathbb{E}|\xi| < \infty$. *Тогда* $\forall\ x > 0 \ \ \mathbb{P}(|\xi| \geq x) \leq \frac{\mathbb{E}|\xi|}{x}$

Доказательство. Возьмем для доказательства следующее понятие:

Пусть A - некоторое событие. Назовем индикатором события A случайную величину I, равную единице если событие A произошло, и нулю в противном случае. По определению величина I(A) имеет распределение Бернулли с параметром

$p = \mathbb{P}(I(A) = 1) = \mathbb{P}(A),$

и ее математическое ожидание равно вероятности успеха $p = \mathbb{P}(A)$. Индикаторы прямого и противоположного событий связаны равенством $I(A) + I(\overline{A}) = 1$. Поэтому $|\xi| = |\xi| * I(|\xi| < x) + |\xi| * I(|\xi| \geq x) \geq |\xi| * I(|\xi| \geq x) \geq x * I(|\xi| \geq x)$. Тогда $\mathbb{E}|\xi| \geq \mathbb{E}(x * I(|\xi| \geq x)) = x * \mathbb{P}(|\xi| \geq x)$.

Разделим обе части на x:

$\mathbb{P}(|\xi| \geq x) \leq \frac{\mathbb{E}|\xi|}{x}$

Пример:

Ученики в среднем опаздывают на 3 минуты. Какова вероятность того, что ученик опоздает на 15 минут и более? Дать грубую оценку сверху.

$\mathbb{P}(|\xi| \geq 15) \leq 3/15 = 0.2$

[:|||:]

Теорема 7

Теорема. *Объединение счетного числа счетных или конечных множеств счетно или конечно*

Доказательство. Пусть имеется счётное число счётных множеств A1, A2, . . .

Расположив элементы каждого из них слева направо в последовательность (Ai = ai0, ai1, . . .) и поместив эти последовательности друг под другом, получим таблицу

a00 a01 a02 a03 . . .

a10 a11 a12 a13 . . .

a20 a21 a22 a23 . . .

a30 a31 a32 a33 . . .

. . . .

Теперь эту таблицу можно развернуть в последовательность, например, проходя по очереди диагонали: a00, a01, a10, a02, a11, a20, a03, a12, a21, a30, . . . Если множества Ai не пересекались, то мы получили искомое представление для их объединения.

Если пересекались, то из построенной последовательности надо выбросить повторения. Если множеств конечное число или какие-то из множеств конечны, то в этой конструкции части членов не будет — и останется либо конечное, либо счётное множество.

[:|||:]

Теорема 14

Теорема. *Верхняя оценка $O(n2^n)$ схемной сложности булевой функции от n переменных.*

Доказательство. Для всякого $a \in 0,1^n$ рассмотрим функцию $f_a : 0,1^n \to 0,1$, такую что $f_a(x) = 1$ тогда и только тогда, когда $x = a$. Будет удобно ввести обозначение $x^1 = x$ и $x_0 = \neg x$. Тогда функцию f_a можно записать формулой

$$f_a(x) = \bigwedge_{i=1}^{n} x_i^{a_i},$$

где $x = (x_1, \ldots, x_n)$ и $a = (a_1, \ldots, a_n)$. Для произвольной функции f уже не сложно записать формулу через функции

$$f(x) = \bigvee_{a \in f^{-1}(1)} f_a(x).$$

Теперь эти формулы можно переделать в схему. Наша схема сначала будет вычислять отрицания всех переменных, на это нужно n элементов. После этого можно вычислить все функции f_a. Для вычисления каждого нужно $n-1$ раз применить конъюнкцию. Всего получается $2^n(n-1)$ элемент. Наконец, для вычисления f нужно взять дизъюнкцию нужных функций f_a, на это уйдет не более 2^n элементов (всего различных функций f_a ровно 2^n – над каждым аргументом отрицание либо есть, либо нет). Суммарно в нашей схеме получается $O(n2^n)$ элементов. **[:|||:]**

Теорема 18

Теорема. *Множество M и его дополнение $\overline{M}$ разрешимы тогда и только тогда, когда M и $\overline{M}$ перечислимы.*

Доказательство.

Необходимость:

Пусть M и $\overline{M}$ разрешимы. Случаи, когда $M = \mathbb{N}$ или $M = \varnothing$, тривиальны. Будем считать, что $M \neq \varnothing$ и M $\neq \mathbb{N}$. Тогда существуют такие a и b, что $a \in M$ и $b \in \overline{M}$. Поскольку M разрешимо, его характеристическая функция χ_M вычислима. Рассмотрим функцию

$$f(x) = \begin{cases} x \text{ при } \chi_M(x) = 1 \\ a \text{ при } \chi_M(x) = 0 \end{cases}$$

M является множеством значений f: ничего, кроме значений M, в $E(f)$, очевидно, быть не может, а для любого $m \in M$ верно, что $f(m) = m$. Аналогично, рассмотрим функцию

$$g(x) = \begin{cases} x \text{ при } \chi_M(x) = 0 \\ b \text{ при } \chi_M(x) = 1 \end{cases}$$

$\overline{M}$ является областью значений g. Таким образом, M и $\overline{M}$ перечислимы (перечисляющие алгоритмы могут быть, например, устроены так: последовательно для всех натуральных n, начиная с нуля, алгоритм выводит значение $f(n)$ или $g(n)$ соответственно).

Достаточность:

Пусть M и $\overline{M}$ перечислимы. Тогда существуют алгоритмы соответственно $\mathfrak{A}$ и $\mathfrak{B}$, с помощью которых могут быть получены все элементы этих множеств. Рассмотрим алгоритм, запускающий $\mathfrak{A}$ и $\mathfrak{B}$ паралленьно, который выводит сначала первое число, полученное $\mathfrak{A}$, затем — первое число, полученное $\mathfrak{B}$, затем — второе число, полученное $\mathfrak{A}$, и так далее. Такой алгоритм будет являться перечисляющим алгоритмом $\mathbb{N}$, который получает элементы M на нечётных выводах и элементы $\overline{M}$ — на чётных. Соответсвенно, для любого элемента x верно, что он будет выведен рассматриваемым алгоритмом за конечное число шагов. Если он был выведен как нечётный по счёту вывод, то $\chi_M(x) = 1$, если как чётный — $\chi_M(x) = 0$. Таким образом, χ_M вычислима, а значит, M и $\overline{M}$ разрешимы. **[:|||:]**

Теорема 19

Теорема. *Перечислимые множества являются множествами значений вычислимых функций.*

Доказательство. Пусть M — перечислимое множество. Тогда существует алгоритм $\mathfrak{A}$, выводящий все его элементы. Рассмотрим алгоритм, который принимает на вход натуральное число n, после чего запускает $\mathfrak{A}$ и считает его выводы. Дойдя до n-го по счёту (начиная с 0) вывода, алгоритм останавливается, выводя n-й вывод алгоритма $\mathfrak{A}$ как результат своей работы.
Множество значений функции, которую вычисляет вышеописанный алгоритм, будет совпадать с множеством чисел, выводимых $\mathfrak{A}$, то есть с M.

[:|||:]

Теорема 20

Теорема. *Перечислимые множества являются множествами значений всюду определённых вычислимых функций.*

Доказательство. Пусть M — перечислимое множество. Тогда существует алгоритм $\mathfrak{A}$, выводящий все его элементы. Рассмотрим алгоритм, который принимает на вход натуральное число n, после чего запускает $\mathfrak{A}$ и считает его выводы. Дойдя до n-го по счёту (начиная с 0) вывода, алгоритм останавливается, выводя n-й вывод алгоритма $\mathfrak{A}$ как результат своей работы.
Множество значений функции f, которую вычисляет вышеописанный алгоритм, будет совпадать с множеством чисел, выводимых $\mathfrak{A}$, то есть с M. Если множество M бесконечно, то f также будет всюду определённой по построению. Если же M конечно, рассмотрим функцию

$f_1(x) = f(x \bmod (l+1))$, где l — номер вывода $\mathfrak{A}$, после которого количество различных выведенных $\mathfrak{A}$ элементов станет равно $[M]$. Значение l будет конечным, так как любой элемент M выводится $\mathfrak{A}$ за конечное число шагов. Данная функция будет всюду определённой, поскольку $\mathfrak{A}$ до своей остановки совершает не менее l шагов, и множество её значений будет совпадать с M, поскольку по построению в множестве её значений $[M]$ различных элементов, и все они являются результатом работы $\mathfrak{A}$.

[:|||:]

Теорема 21

Теорема. *Множества значений всюду определённых функций перечислимы.*

Доказательство. Пусть $M = f(\mathbb{N})$ — множество значений некоторой всюду определённой функции f. Рассмотрим алгоритм, последовательно выводящий для каждого натурального числа n, начиная с 0, значение $f(n)$. Он будет являться перечисляющий алгоритмом для M: для любого $m \in M$ верно, что $\exists x \in \mathbb{N} : f(x) = m$, следовательно, вышеописанный алгоритм выведет m на своём x-ом шаге. **[:|||:]**

Теорема 22

Теорема. *Множество значений всюду опрелённой вычислимой функции является областью определения вычислимой функции.*

Доказательство. Пусть f — всюду определённая вычислимая функция. Рассмотрим алгоритм, принимающий на вход натуральное число x, который последовательно вычисляет значения $f(n)$ для всех натуральных n, начиная с 0, и, если полученное в какой-то момент значение равно x, выводит 1. Если $x \in E(f)$, то $\exists m \in \mathbb{N} : f(m) = x$. Тогда вышеописанный алгоритм остановится за конечное число шагов: он завершит свою работу, вычислив значения $f(n)$ для всех $n \leqslant m$, а для этого требуется конечное число шагов, поскольку f вычислима и всюду определена. Если же $x \notin E(f)$, то данный алгоритм никогда не остановится, поскольку условие его остановки — существование такого $m \in \mathbb{N}$, что $f(m) = x$. Таким образом, функция, вычисляемая вышеопианным алгоритмом, определена в точности на $E(f)$. **[:|||:]**

Теорема 22

Теорема. *Область определения вычислимой функции является множеством значений вычислимой функции.*

Доказательство. Пусть S – область определения некоторой вычислимой функции f, а p – номер программы, вычисляющей f в нумерации U. Рассмотрим функцию g:

$$g(x,t) = \begin{cases} x & F(p,x,t) = 1 \\ - & F(p,x,t) = 0 \end{cases}$$

Если $x \in S$, то $x = g(x,t)$ для некоторого t. И обратно, если $x = g(x,t)$ для некоторого t, то $U(p,x)$ определена, а значит, определена и $f(x)$.

Мы представили S как множество значений функции от двух натуральных аргументов. Чтобы перейти к функциям одного аргумента, используем вычислимую биекцию $c : N \times N \to N$ и выразим S как $S = g \circ c^{-1}(N)$. **[:|||:]**