Дискретная математика. Коллоквиум весна 2017. Определения

Орлов Никита, Тимофей Гутор, Данила Усачёв, Иван Петровский, Андрей Ткачев

12 марта 2017 г.

1. Пространством элементарных исходов $\mathbf{\Omega}$ («омега») называется конечное множество, содержащее все возможные результаты данного случайного эксперимента, из которых в эксперименте происходит ровно один. Элементы этого множества называют элементарными исходами и обозначают буквой ω («омега») с индексами или без.

   Событиями мы будем называть подмножества множества $\mathbf{\Omega}$. Говорят, что в результате эксперимента произошло событие $A \subseteq \mathbf{\Omega}$, если в эксперименте произошел один из элементарных исходов, входящих в множество A.

   Поставим каждому элементарному исходу $\omega_i \in \mathbf{\Omega}$ в соответствие число $p(\omega_i) \in [0,1]$ так, что

   $$\sum_{\omega_i \in \mathbf{\Omega}} p(\omega_i) = 1.$$

   Назовем число $p(\omega_i)$ вероятностью элементарного исхода ω_i. Вероятностью события $A \subseteq \mathbf{\Omega}$ называется число

   $$\mathsf{P}(A) = \sum_{\omega_i \in A} p(\omega_i),$$

   равное сумме вероятностей элементарных исходов, входящих в множество A.

2. Случайный граф на n вершинах — элемент вероятностного пространства Ω, состоящего из всевозможных графов на n вершинах, каждому из которых приписана некоторая вероятность. В терминологии данного курса, граф не содержит петель и кратных ребер, поэтому всего графов на n вершинах $2^{\binom{n}{2}} \Rightarrow |\Omega| = 2^{\binom{n}{2}}$. Понятно, что случайным будет множество ребер графа.

   Пример конструкции — каждому графу Ω присвоена одинаковая вероятность, т.е. все графы равно вероятны (т.е. для любого графа $G = (V, E) \in \Omega$, для каждой пары вершин $u, v \in V$, $Pr[(u, v) \in E] = \frac{1}{2}$).

   Случайные графы используются для изучения каких-то свойств графов. Например, нестрогая постановка вопроса при работе со случайными графами: велика ли вероятность того, что граф обладает данным свойством? Более конкретный пример использования: доказательство того, что при достаточно большом числе вершин, случайный граф (в равновозможной модели) будет почти всегда связен. Формально: Ω_n — вероятностное пространство состоящее из графов на n вершинах, все графы равновозможны, событие A_n — случайный граф на n вершинах связен; доказать $\lim_{n\to\infty} Pr[A_n] = 1$.

3. Условная вероятность — вероятность наступления одного события при условии, что другое событие уже произошло.

$$P(A|B) = \frac{P(A \cap B)}{P(B)}$$

$P(A|B)$ – условная вероятность итога A;

$P(A \cap B)$ – вероятность совместного появления событий A и B;

$P(B)$ – вероятность события B.

4. События A и B называются независимыми, если вероятность композиции событий $P(AB)$ равна произведению вероятностей $P(A) \cdot P(B)$

   Свойства независимых событий:

   (a) Если $p(B) \neq 0$, то условная вероятности $p(A \cap B)$ равна вероятности события $p(A)$.

   (b) Если события A и B независимы, то события $\overline{A}$ и B, A и $\overline{B}$ и $\overline{A}$ и $\overline{B}$ также независимы.

5. *Случайная величина* – функция $f : U \to \mathbb{R}$ из вероятностного пространства U.

   Матожидание случайной величины – произведение значений случайной величины на соответствующие вероятности. Говоря простым языком, это среднееожидаемое значение при многократном повторении испытаний. Пусть случайная величина X принимает значения $x_1, x_2 ... x_n$ с вероятностями $p_1, p_2 \dots p_n$ соответственно. Тогда математическое ожидание данной случайной величины равно сумме произведений всех её значений на соответствующие вероятности:

$$\mathbb{E}(x) = \sum_{i=1}^{n} x_i p_i$$

6. Множества называются *равномощными*, если между ними существует *биекция*, или взаимооднозначное соответствие. Равномощность множеств обозначают значком $\sim$.

   Свойства равномощности:

   (a) *Симметричтность:* $A \sim B \Rightarrow B \sim A$.

   (b) *Рефлексивность:* $\forall A : \ A \sim A$

   (c) *Транзитивность:* $A \sim B, \ B \sim C \Rightarrow A \sim C$

7. Бесконечное множество называется *счетным*, если оно равномощно множеству $\mathbb{N}$.

   Примеры:

   (a) Натуральные числа

   (b) Целые числа

   (c) Рациональные числа

   Примером несчетных множеств могут являться следующие множества:

   (a) Вещественные числа

   (b) Комплексные числа

8. Счетные множества обладают некоторыми свойствами:

   (a) Всякое подмножество счетного множества конечно или счетно

(b) Конечное либо счетное объединение конечных либо счетных множеств конечно либо счетно.

(c) Объединение счетных множеств счетно

(d) Всякое бесконечное множество содержит счетное подмножество

(e) Множество $\mathbb{Q}$ рациональных чисел счетно

(f) Декартово произведение счетных множеств $A \times B$ счетно.

(g) Число слов в конечном или счетном алфавите счетно.

9. Континуум - мощность множества [0,1]. Примеры:

   (a) Множество бесконечных последовательностей нулей и единиц

   (b) Множество вещественных чисел

   (c) Квадрат [0,1]x[0,1].

10. Свойства континуума:

    (a) В любом континуальном множестве есть счетное подмножество.

    (b) Мощность объединения не более чем континуального семейства множеств, каждое из которых не более чем континуально, не превосходит континуума.

    (c) Если континуальное множество представимо в виде счетного объединения его подмножеств, то по крайней мере одно подмножество должно быть континуальнм.

11. Булева функция от n аргументов - отображение из B^n в B, где B - {0,1}. Количество всех n-арных булевых функций равно 2^{2^n}. Булеву функцию можно задать таблицей истинности.

12. Полный базис - это такой набор, который для реализации любой сколь угодно сложной логической функции не потребует использования каких-либо других операций, не входящих в этот набор. Примеры полных базисов:

    (a) Конъюнкция, дизъюнкция, отрицание.

    (b) Конъюнкция, отрицание.

    (c) Конъюнкция, сложение по модулю два, константа один - базис Жегалкина.

    (d) Штрих Шеффера (таблица истинности - 0111).

13. *Разложением Шеннона* функции $f : \{0,1\}^n \to \{0,1\}$ по переменной x_i называется представление фукнции f в виде:

$$f(x_n, \ldots, x_i, \ldots, x_1) = \overline{x_i} \cdot f(x_n, \ldots, 0, \ldots x_1) \vee x_i \cdot f(x_n, \ldots, 1, \ldots, x_1)$$

    Разложением Рида называется следующее представление функции:

$$f(x_n, \ldots, x_i, \ldots, x_1) = g_0 \oplus (g_0 \oplus g_1) \cdot x_i),$$

$$g_0 = f(x_n, \ldots, 0, \ldots x_1)$$

$$g_1 = f(x_n, \ldots, 1, \ldots, x_1)$$

14. ДНФ, СДНФ и СКНФ. *Необходимое определение.* Простой конъюнкцией называется конъюнкция одной или нескольких переменных или их отрицаний, причём каждая переменная встречается не более одного раза.

    Простая конъюнкция

- **полная**, если в неё каждая переменная (или её отрицание) входит ровно 1 раз;
- **монотонная**, если она не содержит отрицаний переменных.

Дизъюнктивная нормальная форма, она же ДНФ – нормальная форма, в которой булева функция имеет вид дизъюнкции нескольких *простых* конъюнктов.

Пример ДНФ: $f(x,y,z) = (x \wedge y) \vee (y \wedge \neg z)$.

Совершенная дизъюнктивная нормальная форма, СДНФ – ДНФ, удовлетворяющая условиям:

- в ней нет одинаковых простых конъюнкций,
- каждая простая конъюнкция полная.

Пример СДНФ: $f(x,y,z) = (x \wedge \neg y \wedge z) \vee (x \wedge y \wedge \neg z)$.

Конъюктивная нормальная форма и Совершенная конъюктивная нормальная форма определяются аналогично:

- Конъюктивная нормальная форма – конъюнкция простых дизъюнктов
- СКНФ – КНФ, в которой каждый дизъюнкт — полный.

15. *Полином Жегалкина* — полином с коэффициентами вида 0 и 1, где в качестве произведения берётся конъюнкция, а в качестве сложения исключающее или. Каждая булева функция единственным образом представляется в виде полинома Жегалкина.

16. *Булевой схемой* от n переменных $x_1, \ldots, x_n$ называется последовательность булевых функций $g_1, \ldots, g_s$, в которой всякая g_i или равна одной из переменных, или получается из предыдущих применением одной из логических операций из *базиса схемы*. Также в булевой схеме задано некоторое число $m \geq 1$ и члены последовательности $g_{s-m+1}, \ldots, g_s$ называются выходами схемы. Число m называют числом выходов. Число s называют размером схемы.

17. *Схемная сложность* функции f относительно базиса B — это минимальное количество функциональных элементов из набора B, необходимое для реализации функции f в базисе B.

18. Свойства вычислимой функции:

    (a) Если функция f вычислима, то её область определения $D(f)$ является перечислимым множеством.

    (b) Если функция f вычислима, то её область значений $E(f)$ является перечислимым множеством.

    (c) Если функция f вычислима, то для любого перечислимого множества X его образ $f(X)$ является перечислимым множеством.

    (d) Если функция f вычислима, то для любого перечислимого множества X его прообраз $f^{-1}(X)$ является перечислимым множеством.

    (e) Композиция вычислимых функция также является вычислимой

19. Множество называется *разрешимым*, если для него существует разрешающий алгоритм, который на любом входе останавливается за конечное число шагов (*разрешающий алгоритм для множества — алгоритм, получающий на вход натуральное число и определяющий, принадлежит ли оно данному множеству*). Говорят, что такой алгоритм вычисляет *характеристическую функцию*

20. Счетное множество называется *перечислимым*, если все его элементы могут быть получены с помощью некоторого алгоритма.

21. Свойства перечислимых множеств:

    (a) Если множества A и B перечислимы, то их объединение $A \cup B$ и пересечение $A \cap B$ также перечислимы (*отсюда следует, что объединение или пересечение конечного числа перечислимых множеств перечислимо*).

    (b) Если множество A перечислимо, то оно является областью значений некоторой вычислимой функции (*это также является достаточным условием перечислимости*).

    (c) Если множество A перечислимо, то оно является областью определения некоторой вычислимой функции (*это также является достаточным условием перечислимости*).

22. Функция $U : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ называется универсальной, если для любой функции $f : \mathbb{N} \to \mathbb{N}$ существует такое p, что $U(p, x) = f(x)$ для любых x (*равенство здесь понимается в том смысле, что при любом x обе функции либо принимают одинаковое значение, либо не определены*).

23. Определение отладочной функции

    Пусть $U(p, x)$ – универсальная вычислимая функция. Для данной у.в.ф. существует функция $F : \mathbb{N} \times \mathbb{N} \times \mathbb{N} \to \{0, 1\}$, называемая отладочной, для которой выполняются следущие свойства:

    - $F(p, x, t)$ не убывает по t (Т.е. $\forall x, p \in N : t_0 < t_1 \Leftrightarrow F(p, x, t_0) \leq F(p, x, t_1)$)
    - $U(p, x)$ не определена $\Leftrightarrow \forall t \in N : F(p, x) = 0$

    Неформально говоря, значение функции $F(p, x, t)$ равно 0 тогда и только тогда, когда программа p на входе x не закончила работу за количество шагов t. В противном случае значение функции $F(p, x, t)$ равно 1.

24. Универсальную вычислимую функцию $U(p, x)$ называют *главной*, если для любой вычислимой функции $V(q, y)$ существует *транслятор* – вычислимая тотальная функция, такая что
$$\forall q, y : \ V(q, y) = U(s(q), y)$$
    Такие функции также называются *главными нумерациями*.

25. Пусть $F = \{f \mid f : \mathbb{N} \to \mathbb{N}\}$ - множество вычислимых функций. Пусть $A \subseteq F$ - подмножество функций. Говорят, что функция удовлетворяет некому *свойству*, если она лежит в A. Пусть $U(p, x)$ – универсальная функция. Пусть $P_a = \{p \mid U(p, x) \in A\}$. Утверждается, что если A – нетривиально (т.е $A \neq \oslash, \overline{A} \neq \oslash$), то множество P_a неразрешимо.

26. Пусть $U(p, x)$ – главная нумерация. Тогда для любой тотальной вычислимой функции $p(t)$ $\exists t : \ U(p(t), x) = U(t, x)$. Это утверждение называется теоремой о неподвижной точке.

27. *Машиной Тьюринга (МТ)* называется модель вычислений, состоящая из

    (a) бесконечной в обе стороны *ленты*, в которой могут быть записаны символы *конечного алфавита* A;

    (b) *головки*, которая может двигаться по ленте и которая может работать в один момент времени только с одной ячейкой;

(c) *множества состояний* Q;

(d) *таблицы переходов*, которая задает функцию

$$\delta : \ A \times Q \to A \times Q \times \{-1, 0, +1\}$$

МТ может быть *многолентоточной*, тогда число головок будет соответствовать числу лент, и наша функция δ на МТ с n лент примет вид

$$\delta : \ A^n \times Q \to A^n \times Q \times \{-1, 0, +1\}^n$$

28. Функция $f : B* \to B$, где B – подмножество алфавита машины без пустого символа, вычислима на МТ, если для любого x из области определения функции результат работы МТ равен $f(w)$, иначе МТ не останавливается. Иными словами, фукнция вычислима на МТ, если для любого входа, на котором функция определена, МТ останавливается и выдает правильный ответ, иначе она не останавливается.