

Оглавление

1. Математика	2
1.1. Математический анализ	2
1.2. Дискретная математика и математическая логика	3
1.3. Алгебра и теория чисел	4
1.4. Теория вероятностей	10
2. Алгоритмы и структуры данных	13
2.1. Оценка алгоритмов	13
2.2. Простейшие алгоритмы	13
2.3. Простейшие структуры данных	14
3. Программирование	15

1. Математика

1.1. Математический анализ

Предел

1

Обозначения $O()$ и $o()$

1

Доказательство и применение асимптотических оценок, при необходимости переформулировка в «терминах эпсилон и дельта»

1

Непрерывность

1

Производная

1

Первообразная

1

Дифференциал

1

Нахождение экстремума функции от одной и от многих переменных

1

Формула Тейлора

1

1.2. Дискретная математика и математическая логика

Отображения и отношения и их свойства

1

Транзитивное замыкание отношения

1

Эквивалентность

1

Отношения порядка

1

Логика высказываний

1

Кванторы

1

Метод математической индукции

1

Основные понятия теории графов

1

Лемма о рукопожатиях

1

Критерий двудольности

1

Оценки числа ребер

1

Характеризация деревьев

1

1.3. Алгебра и теория чисел

Группы

Непустое множество G с заданной на нём бинарной операцией $*$: $G \times G \rightarrow G$ называется группой $(G, *)$, если выполнены следующие аксиомы:

1. ассоциативность:

$$\forall(a, b, c \in G): (a * b) * c = a * (b * c);$$

2. наличие нейтрального элемента:

$$\exists e \in G \quad \forall a \in G: (e * a = a * e = a);$$

3. наличие обратного элемента:

$$\forall a \in G \quad \exists a^{-1} \in G: (a * a^{-1} = a^{-1} * a = e).$$

Поля

Множество F с введёнными на нём алгебраическими операциями сложения $+$ и умножения $*$ ($+: F \times F \rightarrow F$, $*$: $F \times F \rightarrow F$, т. е. $\forall a, b \in F \quad (a + b) \in F$, $a * b \in F$) называется полем $\langle F, +, * \rangle$, если выполнены следующие аксиомы:

1. Коммутативность сложения:

$$\forall a, b \in F \quad a + b = b + a.$$

2. Ассоциативность сложения:

$$\forall a, b, c \in F \quad (a + b) + c = a + (b + c).$$

3. Существование нулевого элемента:

$$\exists 0 \in F: \forall a \in F \quad a + 0 = 0 + a = a.$$

4. Существование противоположного элемента:

$$\forall a \in F \exists (-a) \in F: a + (-a) = 0.$$

5. Коммутативность умножения:

$$\forall a, b \in F \quad a * b = b * a.$$

6. Ассоциативность умножения:

$$\forall a, b, c \in F \quad (a * b) * c = a * (b * c).$$

7. Существование единичного элемента:

$$\exists e \in F \setminus \{0\}: \forall a \in F \quad a * e = a.$$

8. Существование обратного элемента для ненулевых элементов:

$$\forall a \in F: a \neq 0) \exists a^{-1} \in F: a * a^{-1} = e.$$

9. Дистрибутивность умножения относительно сложения:

$$\forall a, b, c \in F \quad (a + b) * c = (a * c) + (b * c).$$

Кольца

Множество R , на котором заданы две бинарные операции: $+$ и $*$ (называемые сложение и умножение), со следующими свойствами, выполняющимися для любых $a, b, c \in R$:

1. Коммутативность сложения:

$$a + b = b + a.$$

2. Ассоциативность сложения:

$$(a + b) + c = a + (b + c).$$

3. Существование нулевого элемента:

$$\exists 0 \in R: a + 0 = 0 + a = a.$$

4. Существование противоположного элемента:

$$\forall a \in R \exists (-a) \in R: a + (-a) = 0.$$

5. Ассоциативность умножения:

$$(a * b) * c = a * (b * c).$$

6. Дистрибутивность:

$$a * (b + c) = (a * b) + (a * c)$$

$$(b + c) * a = (b * a) + (c * a).$$

Факторизация

Факторизацией натурального числа называется его разложение в произведение простых множителей. Может быть выполнена, например, **перебором возможных делителей**. Способ заключается в том, чтобы последовательно делить факторизуемое число n на натуральные числа от 1 до $\lfloor \sqrt{n} \rfloor$. Формально достаточно делить только на простые числа в этом интервале, однако, для этого необходимо знать их множество. На практике составляется таблица простых чисел и производится проверка небольших чисел (например, до 2^{16}). Для очень больших чисел алгоритм не используется в силу низкой скорости работы.

Идеал

Для кольца R идеалом называется подкольцо, замкнутое относительно умножения на элементы из R .

Идеалом кольца R называется такое подкольцо (подкольцо кольца $(K, +, *)$ рассматривается как подмножество $R \subset K$, замкнутое относительно операций $+$ и $*$ из основного кольца) I кольца R , что

1. $\forall i \in I \forall r \in R$ произведение $ir \in I$ (условие на правые идеалы);
2. $\forall i \in I \forall r \in R$ произведение $ri \in I$ (условие на левые идеалы);

Сравнения

Если два целых числа a и b при делении на m дают одинаковые остатки, то они называются сравнимыми (или равноостаточными) по модулю числа m .

Сравнимость чисел a и b записывается в виде формулы (сравнения):

$$a \equiv b \pmod{m}$$

. Число m называется модулем сравнения.

Алгоритм Евклида

Алгоритм Евклида – эффективный алгоритм для нахождения наибольшего общего делителя двух целых чисел.

Пусть a и b — целые числа, не равные одновременно нулю, и последовательность чисел $a > b > r_1 > r_2 > r_3 > r_4 > \dots > r_n$ определена тем, что каждое r_k — это остаток от деления предпредыдущего числа на предыдущее, а предпоследнее делится на последнее нацело, то есть:

$$a = bq_0 + r_1,$$

$$b = r_1q_1 + r_2,$$

$$r_1 = r_2q_2 + r_3,$$

...

$$r_{k-2} = r_{k-1}q_{k-1} + r_k,$$

...

$$r_{n-2} = r_{n-1}q_{n-1} + r_n,$$

$$r_{n-1} = r_nq_n.$$

Тогда НОД(a, b), наибольший общий делитель a и b , равен r_n , последнему ненулевому члену этой последовательности.

Теоремы Эйлера и Ферма

Теорема Эйлера: если a и m взаимно просты, то $a^{\varphi(m)} \equiv 1 \pmod{m}$, где $\varphi(m)$ — функция Эйлера (количество натуральных чисел, меньших m и взаимно простых с ним).

Малая теорема Ферма: если a не делится на простое число p , то $a^{p-1} \equiv 1 \pmod{p}$.

Кольцо многочленов

Многочлен от x с коэффициентами в поле k — это выражение вида $p = p_mx^m + p_{m-1}x^{m-1} + \dots + p_1x + p_0$, где p_0, \dots, p_m — элементы k , коэффициенты p, a, x, x^2, \dots — формальные символы («степени x »). Такие выражения можно складывать и перемножать по обычным правилам действий с алгебраическими выражениями (коммутативность сложения, дистрибутивность, приведение подобных членов и т. д.). Члены p_kx^k с нулевым коэффициентом

p_k при записи обычно опускаются. Используя символ суммы, многочлены записывают в более компактном виде:

$$p = p_m x^m + p_{m-1} x^{m-1} + \dots + p_1 x + p_0 = \sum_{k=0}^m p_k x^k.$$

Множество всех многочленов с коэффициентами в k образует коммутативное кольцо, обозначаемое $k[x]$ и называемое **кольцом многочленов** над k .

Число корней многочлена

Корень многочлена (не равного тождественно нулю) $a_0 + a_1 x + \dots + a_n x^n$ над полем K — это элемент $c \in K$ (либо элемент расширения поля K), такой, что выполняются два следующих равносильных условия:

- данный многочлен делится на многочлен $x - c$;
- подстановка элемента c вместо x обращает уравнение $a_0 + a_1 x + \dots + a_n x^n = 0$ в тождество.

Число корней многочлена степени n не превышает n даже в том случае, если кратные корни учитывать кратное количество раз.

Линейные пространства и операторы

Линейное пространство $V(F)$ над полем F — это упорядоченная четвёрка $(V, F, +, \cdot)$, где

- V — непустое множество элементов произвольной природы, которые называются векторами;
- F — поле, элементы которого называются скалярами;
- Определена операция сложения векторов $V \times V \rightarrow V$, сопоставляющая каждой паре элементов \mathbf{x}, \mathbf{y} множества V единственный элемент множества V , называемый их суммой и обозначаемый $\mathbf{x} + \mathbf{y}$;
- Определена операция умножения векторов на скаляры $F \times V \rightarrow V$, сопоставляющая каждому элементу λ поля F и каждому элементу \mathbf{x} множества V единственный элемент множества V , обозначаемый $\lambda \cdot \mathbf{x}$ или $\lambda \mathbf{x}$;

причём заданные операции удовлетворяют следующим аксиомам — аксиомам линейного (векторного) пространства:

- $\mathbf{x} + \mathbf{y} = \mathbf{y} + \mathbf{x}$, для любых $\mathbf{x}, \mathbf{y} \in V$ (коммутативность сложения);
- $\mathbf{x} + (\mathbf{y} + \mathbf{z}) = (\mathbf{x} + \mathbf{y}) + \mathbf{z}$, для любых $\mathbf{x}, \mathbf{y}, \mathbf{z} \in V$ (ассоциативность сложения);
- существует такой элемент $\mathbf{0} \in V$, что $\mathbf{x} + \mathbf{0} = \mathbf{0} + \mathbf{x} = \mathbf{x}$ для любого $\mathbf{x} \in V$ (существование нейтрального элемента относительно сложения), называемый нулевым вектором или просто нулём пространства V ;
- для любого $\mathbf{x} \in V$ существует такой элемент $-\mathbf{x} \in V$, что $\mathbf{x} + (-\mathbf{x}) = \mathbf{0}$, называемый вектором, противоположным вектору \mathbf{x} ;
- $\alpha(\beta\mathbf{x}) = (\alpha\beta)\mathbf{x}$ (ассоциативность умножения на скаляр);
- $1 \cdot \mathbf{x} = \mathbf{x}$ (унитарность: умножение на нейтральный (по умножению) элемент поля F сохраняет вектор).
- $(\alpha + \beta)\mathbf{x} = \alpha\mathbf{x} + \beta\mathbf{x}$ (дистрибутивность умножения вектора на скаляр относительно сложения скаляров);
- $\alpha(\mathbf{x} + \mathbf{y}) = \alpha\mathbf{x} + \alpha\mathbf{y}$ (дистрибутивность умножения вектора на скаляр относительно сложения векторов).

Линейным отображением (оператором) векторного пространства L_K над полем K в векторное пространство M_K над тем же полем K (линейным оператором из L_K в M_K) называется отображение $f: L_K \rightarrow M_K$, удовлетворяющее условию линейности:

- $f(x + y) = f(x) + f(y)$,
- $f(\alpha x) = \alpha f(x)$.

для всех $x, y \in L_K$ и $\alpha \in K$.

Базис, размерность, ранг

Рангом системы строк (столбцов) матрицы A с m строк и n столбцов называется максимальное число линейно независимых строк.

Число столбцов и строк задают **размерность** матрицы.

Векторы $\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_n$ называются линейно зависимыми, если существует их нетривиальная линейная комбинация, значение которой равно нулю; то есть $\alpha_1\mathbf{x}_1 + \alpha_2\mathbf{x}_2 + \dots + \alpha_n\mathbf{x}_n = \mathbf{0}$ при некоторых коэффициентах $\alpha_1, \alpha_2, \dots, \alpha_n \in F$, причём хотя бы один из коэффициентов α_i отличен от нуля.

В противном случае эти векторы называются линейно независимыми.

Число элементов (мощность) максимального линейно независимого множества элементов векторного пространства не зависит от выбора этого множества. Данное число называется **рангом**, или **размерностью**, пространства, а само это множество — **базисом**. Элементы базиса именуют **базисными векторами**. Размерность пространства чаще всего обозначается символом \dim .

Собственные числа и собственные векторы

Пусть L — линейное пространство над полем K , $A: L \rightarrow L$ — линейное преобразование.

Собственным вектором линейного преобразования A называется такой ненулевой вектор $x \in L$, что для некоторого $\lambda \in K$ $Ax = \lambda x$.

Собственным значением (собственным числом) линейного преобразования A называется такое число $\lambda \in K$, для которого существует собственный вектор, то есть уравнение $Ax = \lambda x$ имеет ненулевое решение $x \in L$.

Упрощённо говоря, собственный вектор — любой ненулевой вектор x , который отображается в коллинеарный ему вектор λx оператором A , а соответствующий скаляр λ называется собственным значением оператора.

Характеристический многочлен

Для данной матрицы A , $\chi(\lambda) = \det(A - \lambda E)$, где E — единичная матрица, является многочленом от λ , который называется характеристическим многочленом матрицы A .

1.4. Теория вероятностей

Зависимые и независимые события

Два события называются **независимыми**, если появление одного из них не изменяет вероятность появления другого. Например, если в цехе работают две автоматические линии, по условиям производства не взаимосвязанные, то остановки этих линий являются независимыми событиями.

События называются **зависимыми**, если одно из них влияет на вероятность появления другого. Например, две производственные установки связаны единым технологическим циклом. Тогда вероятность выхода из строя одной из них зависит от того, в каком состоянии находится другая.

Условные вероятности

Вероятность одного события B , вычисленная в предположении осуществления другого события A , называется условной вероятностью события B и обозначается $P\{B|A\}$.

Формула полной вероятности

Если событие A наступает только при условии появления одного из событий B_1, B_2, \dots, B_n , образующих полную группу несовместных событий, то вероятность события A равна сумме произведений вероятностей каждого из событий B_1, B_2, \dots, B_n на соответствующую условную вероятность события B_1, B_2, \dots, B_n : $P\{A\} = \sum_{i=1}^n P\{B_i\}P\{A|B_i\}$.

При этом события B_i , $i = 1, \dots, n$ называются гипотезами, а вероятности $P\{B_i\}$ — априорными.

Математическое ожидание

Математическое ожидание дискретной случайной величины X вычисляется как сумма произведений значений x_i , которые принимает случайная величина X , на соответствующие вероятности p_i : $M[X] = \sum_{i=1}^{\infty} x_i p_i$.

Задание. Вероятность попадания в цель при одном выстреле равна 0,8 и уменьшается с каждым выстрелом на 0,1. Составить закон распределения числа попаданий в цель, если сделано три выстрела. Найти математическое ожидание, этой случайной величины.

Решение. Введем дискретную случайную величину X = (Число попаданий в цель). X может принимать значения 0, 1, 2 и 3. Найдем соответствующие вероятности. Вероятность не попасть 3 раза: $0,2 * 0,3 * 0,4$. Вероятность не попасть 2 раза: $0,2 * 0,3 * 0,6 + 0,2 * 0,7 * 0,4 + 0,8 * 0,3 * 0,4$. И т.д. Мат.

ожидание будет $0*0,2*0,3*0,4+1*0,2*0,3*0,6+0,2*0,7*0,4+0,8*0,3*0,4$ и т.д.

Второй момент

Начальным моментом s -го порядка прерывной случайной величины называется сумма вида: $\alpha_s[X] = \sum_{i=1}^{\infty} x_i^s p_i$.

Математическое ожидание – первый начальный момент случайной величины.

Неравенства Маркова и Чебышёва

Неравенство Маркова дает вероятностную оценку того, что значение неотрицательной случайной величины превзойдет некоторую константу через известное математическое ожидание. Когда никаких других данных о распределении нет, неравенство дает некоторую информацию, хотя зачастую оценка груба или тривиальна.

Пусть X - случайная величина, принимающая неотрицательные значения, $M(X)$ - ее конечное математическое ожидание, то для любых $a > 0$ выполняется: $P(X \geq a) \leq \frac{M(X)}{a}$.

Задача: Среднее количество вызовов, поступающих на коммутатор завода в течение часа, равно 300. Оценить вероятность того, что в течение следующего часа число вызовов на коммутатор превысит 400. **Решение:** По условию $M(X) = 300$. Воспользуемся формулой (неравенством Маркова): $P(X \geq 400) \leq \frac{300}{400} = 0,75$, т.е. вероятность того, что число вызовов превысит 400, будет не более 0,75.

Неравенство Чебышева показывает, что случайная величина принимает значения близкие к среднему (математическому ожиданию) и дает оценку вероятности больших отклонений.

$$P(|X - M(X)| \geq a) \leq \frac{D(X)}{a^2}, a > 0$$

2. Алгоритмы и структуры данных

Нужно уметь написать код для перечисленных ниже элементарных алгоритмов.

2.1. Оценка алгоритмов

Мы рассчитываем, что вы понимаете, какое количество операций и объём дополнительной памяти необходимы для обсуждаемых алгоритмов и из каких соображений это получается.

2.2. Простейшие алгоритмы

Поиск заданного элемента

Пои

Поиск наибольшего элемента

1

Сортировка вставкой

1

Сортировка пузырьком

1

Быстрая сортировка

1

Иерархические сортировки

1

2.3. Простейшие структуры данных

Массив

1

Список

1

Стек

1

Очередь

1

3. Программирование

Нужно знать базовые принципы одного из «традиционных» (C, C++, Java, Python и др.) языков программирования.

Основы синтаксиса

Переменные

Условные выражения

Циклы

Массивы

Функции

Рекурсия

Динамическая память

Стек