Дискретная математика, Коллоквиум 2

Балюк Игорь
@lodthe, GitHub

2019 — 2020

Материалы взяты из учебника Александра Рубцова.

Содержание

1 Определения **3**
1.1 Деление целых чисел с остатком. 3
1.2 Сравнения по модулю. Основные свойства. 3
1.3 Арифметика остатков (вычетов). Обратимые остатки (вычеты). 3
1.4 Малая теорема Ферма. 3
1.5 Функция Эйлера. Теорема Эйлера. 3
1.6 Наибольший общий делитель. Алгоритм Евклида. 4
1.7 Расширенный алгоритм Евклида нахождения решения линейного диофантова уравнения. 4
1.8 Простые числа, формулировка основной теоремы арифметики. 4
1.9 Равномощные множества. 4
1.10 Счётные множества. 4
1.11 Множества мощности континуум. 4
1.12 Основные определения элементарной теории вероятностей: исходы, события, вероятность события. 4
1.13 Формулировка формулы включений и исключений для вероятностей. 4
1.14 Условная вероятность. 4
1.15 Независимые события. Основные свойства независимых событий. 5
1.16 Формула полной вероятности. 5
1.17 Случайная величина и математическое ожидание. Линейность математического ожидания. 5
1.18 Формулировка неравенства Маркова. 5
1.19 Определение схемы в некотором функциональном базисе. Представление схем графами. . 5
1.20 Полный базис. Примеры полных и неполных базисов. 6
1.21 Полином Жегалкина (в стандартном виде). 6
1.22 Схемная сложность функции (размер схемы). 6

2 Вопросы на знание доказательств **6**
2.1 Сравнение $ax \equiv 1 \pmod N$ имеет решение тогда и только тогда, когда НОД$(a, N) = 1$. . . 6
2.2 Малая теорема Ферма. 6
2.3 Теорема Эйлера. 6
2.4 Корректность алгоритма Евклида и расширенного алгоритма Евклида. 6
2.5 Основная теорема арифметики. 6
2.6 Китайская теорема об остатках. 6
2.7 Мультипликативность функции Эйлера. Формула для функции Эйлера. 6
2.8 Формула Байеса. Формула полной вероятности. 6
2.9 Парадокс дней рождений (математическое ожидание числа людей с совпавшими днями рождений) 6
2.10 Неравенство Маркова. 6
2.11 Нижняя оценка на максимальное количество ребер в разрезе. 6
2.12 Любое бесконечное множество содержит счётное подмножество. Любое подмножество счётного множества конечно или счётно. 6
2.13 Конечное или счётное объединение конечных или счётных множеств конечно или счётно 6

2.14 Счётность декартова произведения счетных множеств. Счётность множества рациональных чисел. . . . 6
2.15 Равномощность отрезков, интервалов, лучей и прямых (явные биекции). . . . 6
2.16 Несчетность множества бесконечных двоичных последовательностей. . . . 7
2.17 Теорема Кантора-Бернштейна. . . . 7
2.18 Нижняя оценка на число монотонных булевых функций: монотонных булевых функций от $2n$ переменных не меньше $2^{\frac{2^n}{2n+1}}$ . . . 7
2.19 Существование и единственность полинома Жегалкина (в стандартном виде) для любой булевой функции. . . . 7
2.20 Разложение в ДНФ и КНФ булевой функции. . . . 7
2.21 Верхняя оценка $O(n2^n)$ схемной сложности булевой функции от n переменных. . . . 7
2.22 Булевы схемы для сложения и умножения n-битовых чисел. Оценка размера. . . . 7
2.23 Булева схема для задачи о связности графа. Оценка размера. . . . 7
2.24 Задача об угадывании числа. Верхняя и нижняя оценки. . . . 7
2.25 Задача о сортировке нижняя оценка. . . . 7
2.26 Задача о нахождении самой тяжелой монеты. Верхние и нижние оценки. . . . 7

1 Определения

Контрольный вопрос на понимание определений включает в себя формулировку одного определения из списка ниже и контрольный вопрос по этому определению. Пример: «Определение полного прообраза. Пусть $f(x) = x^2$ — функция из $\mathbb{Z}$ в $\mathbb{Z}$. Найдите полный прообраз множества $\{1, 2, 3, 4\}$.

1. Деление целых чисел с остатком.

Говорят, что целое число a делится на целое число b, если $a = bk$ для некоторого целого числа k. В этом случае говорят также «a кратно b», и «b является делителем числа a».

Теперь определим деление остатком. Пусть b — целое положительное число. Деля на b с остатком, мы связываем предметы в пачки по b в каждой, пока это возможно: количество полных пачек называется частным (говорят ещё «неполное частное», чтобы отличать от частного как дроби), и сколько-то предметов останется, их количество и называют остатком.

Формально: разделить целое a на целое положительное b означает найти такое целое q (*частное*) и такое r (*остаток*), что

$$a = b \cdot q + r; \quad 0 \leqslant r < b.$$

2. Сравнения по модулю. Основные свойства.

Если два числа a и b дают одинаковые остатки при делении на положительное число N, то говорят, что они *сравнимы* по модулю N, и пишут $a \equiv b \pmod N$.

Эквивалентное определение: a и b сравнимы по модулю N, если разность $a - b$ делится на N. В самом деле, если они дают одинаковый остаток r, то $a = k \cdot N + r$, $b = l \cdot N + r$, и $a - b = k \cdot N - l \cdot N = (k - l) \cdot N$. Наоборот, если $a - b = m \cdot N$, и b даёт остаток r, то $b = l \cdot N + r$ и $a = (a - b) + b = m \cdot N + l \cdot N + r = (m + l) \cdot N + r$, то есть a даёт тот же остаток r.

Можно сказать, что при данном N все целые числа разбиваются на N классов в зависимости от остатков по модулю N: два числа в одном классе сравнимы, а числа в разных классах — нет.

Важное свойство сравнений: чтобы узнать, в какой класс попадет сумма или произведение двух чисел, достаточно знать, в каком классе лежат слагаемые или сомножители: если одно из слагаемых (один из сомножителей) изменить на кратное N, то сумма (произведение) тоже изменится на кратное N.

В самом деле, если к одному из слагаемых прибавить $k \cdot N$, то к сумме тоже прибавится $k \cdot N$, аналогично для разности. С произведением: $(a + k \cdot N) \cdot b = a \cdot b + k \cdot b \cdot N \equiv a \cdot b \pmod N$.

Благодаря этому свойству в выражении, содержащем операции сложения и умножения (или возведение в целую степень, которое сводится к многократному умножению), можно заменять слагаемые или сомножители на сравнимые по модулю N — если результат нам важен лишь по модулю N.

Например, можно найти $2^{100} \bmod 7$ (остаток от деления 2^{100} на 7): поскольку $2^3 = 8 \equiv 1 \pmod 7$, то $2^{99} = (2^3)^{33} \equiv 1^{33} = 1 \pmod 7$, так что $2^{100} = 2^{99} \cdot 2 \equiv 1 \cdot 2 = 2 \pmod 7$.

3. Арифметика остатков (вычетов). Обратимые остатки (вычеты).

Остаток (вычет) по модулю N называется **обратимым**, если в произведении с каким-то другим остатком он даёт 1. Другими словами, a обратим, если уравнение $a \cdot x \equiv 1 \pmod N$ имеет решение.

4. Малая теорема Ферма.

Теорема. *Если p — простое число, то*

$$a^{p-1} \equiv 1 \pmod p$$

при любом a, не делящемся на p.

5. Функция Эйлера. Теорема Эйлера.

Теорема. *Пусть $N > 1$ — произвольное целое число, а $\varphi(N)$ равно количеству остатков среди $0, 1, \ldots, N - 1$, взаимно простых с N. Пусть a — один из этих остатков. Тогда*

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

Функцию φ называют **функцией Эйлера** и традиционно обозначают буквой φ. Если N простое, то $\varphi(N) = N - 1$, и теорема Эйлера превращается в малую теорему Ферма.

6. Наибольший общий делитель. Алгоритм Евклида.

Наибольшим общим делителем (НОД) для двух целых чисел m и n называется наибольший из их общих делителей. Пример: для чисел 54 и 24 наибольший общий делитель равен 6.

Алгоритм нахождения НОДа алгоритмом Евклида:

1. Большее число делим на меньшее.
2. Если делится без остатка, то меньшее число и есть НОД (следует выйти из цикла).
3. Если есть остаток, то большее число заменяем на остаток от деления.
4. Переходим к пункту 1.

7. Расширенный алгоритм Евклида нахождения решения линейного диофантова уравнения.

8. Простые числа, формулировка основной теоремы арифметики.

Целое число $p > 1$ называется простым, если оно не разлагается в произведение меньших чисел (то есть не имеет положительных делителей, кроме 1 и p).

Теорема. *Всякое целое положительное число, большее* 1*, разлагается на простые множители, причём единственным образом: любые два разложения отличаются только перестановкой сомножителей.*

9. Равномощные множества.

Множество A называется равномощным множеству B, если существует биекция множества A в множество B.

10. Счётные множества.

Множество называется счётным, если оно равномощно множеству натуральных чисел $\mathbb{N}$.

11. Множества мощности континуум.

Множество имеет мощность **континуум**, если оно равномощно $\mathbb{R}$.

12. Основные определения элементарной теории вероятностей: исходы, события, вероятность события.

Вероятностным пространством называется конечное множество U, его элементы называются **возможными исходами**. **Событием** называется произвольное подмножество $A \subseteq U$.

На вероятностном пространстве задана функция $Pr : U \to [0; 1]$, такая что $\sum\limits_{x \in U} Pr[x] = 1$. Функция Pr называется **вероятностным распределением**, а число $Pr[x]$ называется **вероятностью исхода** $x \in U$. Вероятностью события A называется число $Pr[A] = \sum\limits_{x \in A} Pr[x]$.

13. Формулировка формулы включений и исключений для вероятностей.

В равновозможной модели для произвольных множеств $A_1, \ldots, A_n \subseteq U$ верно

$$Pr[A_1 \cup A_2 \cup \cdots \cup A_n] = \sum_i Pr[A_i] - \sum_{i<j} Pr[A_i \cap A_j] + \cdots = \sum_{\varnothing \neq I \subseteq \{1,2,\ldots,n\}} (-1)^{|I|+1} Pr\left[\bigcap_{i \in I} A_i\right].$$

14. Условная вероятность.

Помимо вероятностей тех или иных событий бывает нужным говорить и о вероятностях одних событий при условии других. Неформально говоря, мы хотим определить вероятность выполнения события A в том случае, когда событие B выполняется.

В терминах вероятностного пространства определение этого понятия довольно естественное: нужно сузить вероятностное пространство на множество B. Так, для равновозможной модели мы получаем, что вероятность A при условии B есть просто $\dfrac{|A \cap B|}{|B|}$, то есть число благоприятных исходов поделенное на число всех исходов (после сужения всего вероятностного пространства до B).

В случае произвольного вероятностного пространства нужно учесть веса исходов, то есть нужно сложить вероятности исходов в $A \cap B$ и поделить на сумму вероятностей исходов в B.

Таким образом, мы приходим к формальному определению. **Условной вероятностью** события A при условии B называется число

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

15. Независимые события. Основные свойства независимых событий.

События A и B называются независимыми, если

$$Pr[A] = Pr[A \mid B].$$

Из определения условной вероятности мы сразу получаем эквивалентное определение независимостей событий. Событие A не зависит от события B, если

$$Pr[A \cap B] = Pr[A] \cdot Pr[B].$$

16. Формула полной вероятности.

Лемма. *Пусть $B_1, B_2, \ldots, B_n$ — разбиение вероятностного пространства, то есть $U = B_1 \cup B_2 \cup \cdots \cup B_n$, где $B_i \cap B_j = \varnothing$ при $i \neq j$. Пусть также $Pr[B_i] > 0$ для всякого i. Тогда для всякого события A*

$$Pr[A] = \sum_{i=1}^{n} Pr[A \mid B_i] \cdot Pr[B_i].$$

17. Случайная величина и математическое ожидание. Линейность математического ожидания.

Случайная величина — это числовая функция на вероятностном пространстве, то есть функция вида $\xi : U \to \mathbb{R}$. То есть, по сути, случайная величина — это обычная числовая функция, но теперь на её аргументах задано вероятностное распределение.

Математическим ожиданием случайной величины $\xi : U \to \mathbb{R}$ называется число

$$E[\xi] = \sum_{u \in U} \xi(u) \cdot Pr[u]$$

Лемма. *(линейность математического ожидания) Пусть $\xi : U \to \mathbb{R}$ и $g : U \to \mathbb{R}$ — две случайные величины на одном и том же вероятностном пространстве. Тогда*

$$E[f + g] = E[f] + E[g].$$

18. Формулировка неравенства Маркова.

Лемма. *Пусть ξ — случайная величина, принимающая только **неотрицательные** значения. Тогда для всякого $x > 0$ верно*

$$Pr[\xi \geqslant x] \leqslant \frac{E[\xi]}{x}.$$

То есть, вероятность того, что случайная величина ξ сильно больше своего математического ожидания, не слишком велика (заметим, что лемма становится содержательной, когда $x > E[\xi]$).

19. Определение схемы в некотором функциональном базисе. Представление схем графами.

Полным базисом называется набор связок, если через эти связки выражается любая булева функция.

Стандартным базисом назовём набор из операций конъюнкция (И), дизъюнкция (ИЛИ) и отрицание (НЕ).

Булевой схемой от переменных $x_1, \ldots, x_n$ мы будем называть последовательность булевых функций $g_1, \ldots, g_s$, в которой всякая g_i получается из предыдущих функций последовательности и переменных применением одной из логических операций из выбранного базиса для этой схемы.

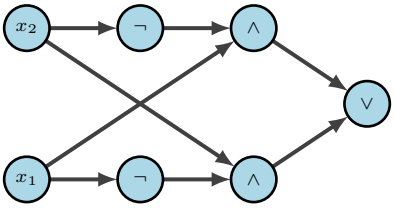
В булевой схеме задано некое число $m \geqslant 1$ и члены последовательности $g_{s-m+1}, \ldots, g_s$ называются **выходами схемы**. Число m называют числом выходов схемы.

Мы говорим, что схема вычисляет булеву функцию $f : \{0,1\}^n \to \{0,1\}^m$, если для всякого $x \in \{0,1\}^n$ верно $f(x) = (g_{s-m+1}(x), \ldots, g_s(x))$.

Размером схемы называют число s.

Рассмотрим представление схемы графом:

Рис. 1: Схема функции $x_1 \oplus x_2$



20. Полный базис. Примеры полных и неполных базисов.

21. Полином Жегалкина (в стандартном виде).

Многочленом Жегалкина называется формула вида

$$\bigoplus_{S \subseteq \{1,\ldots,n\}} a_S \bigwedge_{i \in S} x_i, \quad a_S \in \{0,1\}.$$

Примеры многочлена Жегалкина:

$$1 \oplus x_1 \oplus x_2 \oplus x_3 \oplus (x_1 \wedge x_2) \oplus (x_1 \wedge x_3) \oplus (x_2 \wedge x_3) \oplus (x_1 \wedge x_2 \wedge x_3);$$
$$x_3 \oplus (x_1 \wedge x_3) \oplus (x_2 \wedge x_3) \oplus (x_1 \wedge x_2 \wedge x_3).$$

Для простоты чтения $\wedge$ можно опускать:

$$1 \oplus x_1 \oplus x_2 \oplus x_3 \oplus x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_1x_2x_3;$$

22. Схемная сложность функции (размер схемы).

Схемная сложность булева отображения $f : \{0,1\}^n \to \{0,1\}^m$ (в частности, булевой функции) — это наименьший размер схемы, вычисляющей это выражение.

2 Вопросы на знание доказательств

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

2. Малая теорема Ферма.

3. Теорема Эйлера.

4. Корректность алгоритма Евклида и расширенного алгоритма Евклида.

5. Основная теорема арифметики.

6. Китайская теорема об остатках.

7. Мультипликативность функции Эйлера. Формула для функции Эйлера.

8. Формула Байеса. Формула полной вероятности.

9. Парадокс дней рождений (математическое ожидание числа людей с совпавшими днями рождений)

10. Неравенство Маркова.

11. Нижняя оценка на максимальное количество ребер в разрезе.

12. Любое бесконечное множество содержит счётное подмножество. Любое подмножество счётного множества конечно или счётно.

13. Конечное или счётное объединение конечных или счётных множеств конечно или счётно

14. Счётность декартова произведения счетных множеств. Счётность множества рациональных чисел.

15. Равномощность отрезков, интервалов, лучей и прямых (явные биекции).

16. **Несчетность множества бесконечных двоичных последовательностей.**

17. **Теорема Кантора-Бернштейна.**

18. **Нижняя оценка на число монотонных булевых функций: монотонных булевых функций от $2n$ переменных не меньше $2^{\frac{2^n}{2n+1}}$**

19. **Существование и единственность полинома Жегалкина (в стандартном виде) для любой булевой функции.**

20. **Разложение в ДНФ и КНФ булевой функции.**

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

22. **Булевы схемы для сложения и умножения n-битовых чисел. Оценка размера.**

23. **Булева схема для задачи о связности графа. Оценка размера.**

24. **Задача об угадывании числа. Верхняя и нижняя оценки.**

25. **Задача о сортировке нижняя оценка.**

26. **Задача о нахождении самой тяжелой монеты. Верхние и нижние оценки.**