

Лекции по дискретной математике

А. Шень М. Вялый В. Подольский А. Рубцов Д. Шварц

Черновой вариант от 7 сентября 2016 г.

Оглавление

Предисловие	7
I Начальные примеры	9
1 Математическая индукция	10
1.1 Задача о раскраске плоскости	10
1.2 Формулировка принципа математической индукции	12
1.3 Доказательство формул суммирования по индукции	14
1.4 Доказательство неравенств с помощью индукции	15
1.5 Пример из алгебры: существование решения однородной линейной системы уравнений	16
1.6 Коды Грея	18
1.7 Ханойская башня	21
1.8 Задачи для самостоятельного решения	23
2 Подсчёты	25
2.1 Правило суммы	25
2.2 Рекуррентное соотношение: пример	29
2.3 Рекуррентное соотношение: число путей	32
2.4 Слова и правило произведения	34
2.5 Выбор с ограничениями	37
2.6 Подсчёты с кратностью	39
2.7 Подмножества и числа сочетаний	41
2.8 Ещё о числах сочетаний	44
2.8.1 Симметрия	44
2.8.2 Сумма чисел в строке	45
2.8.3 Знакопеременная сумма	46
2.8.4 Слова о включениях и исключениях	47
2.8.5 Пути, подмножества, слова	48
2.8.6 Соседние числа в строке	49
2.8.7 Монеты и перегородки	51
2.9 Бином Ньютона и производящие функции	52

2.10	Числа Каталана	61
2.10.1	Правильные последовательности скобок	61
2.10.2	Рекуррентная формула	63
2.10.3	Вычисление с помощью отражений	65
2.10.4	Вычисление с производящей функцией	67
2.10.5	Вычисление с теорией вероятностей и поворотами	68
2.10.6	Доказательство по индукции с дробными параметрами	70
2.10.7	Неассоциативные произведения, триангуляции и стековый калькулятор	71
2.11	Что дальше?	75
3	Графы	76
3.1	Примеры	76
3.1.1	Граф авиарейсов	76
3.1.2	Перестановка коней	77
3.1.3	Эйлер и мосты в Кёнигсберге	78
3.1.4	Рукопожатия	80
3.1.5	Задачи и решения	81
3.1.6	Разбор контрольной*	82
3.1.7	Знакомые и незнакомые	84
3.2	Неориентированные графы	86
3.2.1	Определение	86
3.2.2	Соседи. Степени вершин	87
3.2.3	Связные компоненты	90
3.2.4	Расстояния. Простые пути.	97
3.2.5	Деревья	99
3.2.6	Полное бинарное берево	103
3.3	Ориентированные графы	103
3.3.1	Определение	103
3.3.2	Степени вершин	104
3.3.3	Пути и достижимость.	105
3.3.4	Достижимость и разрезы	105
3.3.5	Компоненты сильной связности и ациклические графы	107
3.3.6	Графы преобразований	109
3.4	Эйлеровы циклы	111
3.4.1	Определение	111
3.4.2	Критерий существования	111
3.4.3	Последовательности де Брёйна	113
3.4.4	Гамильтоновы циклы	113
3.5	Двудольные графы	114
3.5.1	Определение	114
3.5.2	Двудольные графы и раскраска в два цвета	115
3.5.3	Степени вершин	116

3.5.4	Паросочетания	116
3.6	Клики и независимые множества	118
4	Арифметика остатков	122
4.1	Чётные и нечётные числа	122
4.2	Деление на 3 и остатки	123
4.3	Деление с остатком	124
4.4	Сравнения по модулю	127
4.5	Таблицы сложения и умножения по модулю N	128
4.6	Обратимые элементы по модулю N	130
4.7	Обратимые элементы и диофантовы уравнения	133
4.8	Алгоритм Евклида	134
4.9	Алгоритм Евклида и диофантовы уравнения	136
4.10	Однозначность разложения на множители	139
4.11	Китайская теорема об остатках	141
4.12	Малая теорема Ферма	142
4.13	Функция Эйлера и теорема Эйлера	145
4.14	Что дальше?	146
II	Основные конструкции	148
5	Множества	149
5.1	Основные свойства множеств и операции с множествами	149
5.2	Теоретико-множественные тождества	154
6	Множества и логика	157
6.1	Логические переменные, логические связки	157
6.2	Наблюдения	160
6.3	Какие связки необходимы?	163
6.3.1	Полнота дизъюнкции, конъюнкции и отрицания	165
6.3.2	Полнота конъюнкции и отрицания	166
6.3.3	Алгебраическое доказательство теоремы 6.1	166
6.4	Формула включений-исключений	167
6.4.1	Первое доказательство	168
6.4.2	Второе доказательство	169
6.4.3	Формула для симметрической разности	170
7	Функции	171
7.1	Пример	172
7.2	Функции и связанные с ними понятия	172
7.2.1	Терминология и обозначения	173
7.2.2	Образ множества, полный прообраз	175
7.3	Декартово произведение множеств и графики функций	177

7.4	Инъекции, сюръекции и биекции	180
7.4.1	Определения	180
7.4.2	Биекции и сравнение множеств	183
7.5	Композиции функций	185
7.5.1	Определение	185
7.5.2	Ассоциативность	187
7.5.3	Обратная функция	187
7.5.4	Степени композиций	189
7.6	Подсчёты	190
7.7	Задачи для самостоятельного решения	192
8	Отношения и их графы	194
8.1	Отношения в естественном языке	194
8.2	Отношения с точки зрения математики	196
8.3	Свойства бинарных отношений	197
8.4	Графы, матрицы и бинарные отношения	199
8.5	Отношения эквивалентности	200
8.6	Композиция отношений	202
8.7	Отношения: что дальше?	205
8.8	Задачи для самостоятельного решения	206
9	Мощность множеств	207
9.1	Равномощные множества	207
9.1.1	Определение равномощности	207
9.1.2	Свойства равномощности	208
9.1.3	Примеры равномощных множеств	209
9.2	Счётные множества	211
9.2.1	Определение и простейшие примеры	211
9.2.2	Свойства счётных множеств	212
9.3	Несчётные множества	216
9.3.1	Интервал и отрезок равномощны	216
9.3.2	Добавление счётного множества	217
9.3.3	Числа и последовательности	218
9.3.4	Отрезок и квадрат	219
9.4	Диагональный аргумент Кантора и сравнение мощностей	220
9.4.1	Несчётность отрезка	220
9.4.2	Сравнение мощностей	222
9.5	Что дальше?	227
10	Упорядоченные множества	228
10.1	Отношения порядка	228
10.1.1	Отношения строгого частичного порядка	228
10.1.2	Строгие и нестрогие порядки	229
10.2	Примеры	230

10.3	Операции над частично упорядоченными множествами	233
10.4	Какие порядки считать «одинаковыми»?	235
10.5	Конечные линейные порядки	236
10.6	Порядки и индукция	237
10.7	Антицепи	239
11	Вероятность: первые шаги	241
11.1	Элементарная теория вероятностей: определения	242
11.2	Вероятность объединения событий	249
11.3	Вероятностный метод	252
11.4	Условные вероятности	253
11.5	Случайная величина, математическое ожидание	260
11.6	Частота орлов при подбрасывании монеты и биномиальные коэффициенты	267
11.7	Большие отклонения: неравенство Чернова	271
11.8	Подробности для любознательных	273
11.8.1	Ещё одна элементарная оценка отношения биномиальных коэффициентов	273
11.8.2	Другое доказательство неравенства Чернова	274
12	Комбинаторные игры	276
12.1	Позиции	276
12.2	Стратегии	279
12.3	Разбор с конца	281
12.4	Симметричные стратегии	285
12.5	Ним	289
12.6	Сумма игр и функция Шпрага–Гранди	292
III	Вычислимость	295
13	Разрешающие деревья	296
13.1	Задача об угадывании числа. Деление пополам. Мощностная нижняя оценка	296
13.2	Формализация модели	298
13.3	Угадывание числа, неадаптивный вариант задачи	299
13.4	Ограниченные модели деревьев разрешения. Сортировка, взвешивания, булевы функции	300
13.5	Рассуждение с противником	303
14	Булевы схемы и формулы	307
14.1	Булевы схемы	307
14.2	Формулы	315

15 Вычислимые функции. Перечислимые и разрешимые множества	320
15.1 Вычислимые функции	320
15.2 Универсальные вычислимые функции	323
15.3 Перечислимые и разрешимые множества	325
15.4 Перечислимые множества в терминах вычислимых функций	328
15.5 Проекция и графики	331
15.6 Перечислимые неразрешимые множества	332
15.7 Главные нумерации	334
15.8 Рекурсия и теорема о неподвижной точке	336
15.9 Теорема Успенского–Райса	339
16 Машины Тьюринга. Тезис Чёрча – Тьюринга	340
16.1 Машины Тьюринга	340
16.2 Тезис Чёрча – Тьюринга	343
16.3 Использование машин Тьюринга в доказательствах	344
16.4 Композиция функций, вычислимых МТ, и уборка мусора	346
16.5 Многоленточные машины Тьюринга	349
16.6 Моделирование многоленточной МТ на одноленточной	351
16.7 Универсальная машина Тьюринга	353
16.8 Универсальная 3-ленточная машина для 1-ленточных машин	355
16.9 Соответствие между абстрактной теорией алгоритмов и МТ	358
17 Примеры неразрешимых задач	361
17.1 Почему важна проблема остановки?	361
17.2 FRACTRAN	363
17.3 Язык программирования	364
17.4 Сведение проблемы остановки: от программ к пасьянсам	368
17.5 Задача достижимости на графе подстановок слов	370
17.6 Неразрешимость задачи достижимости для графа подстановок слов	372

Предисловие

Слова «дискретная математика», входящие в название этой книжки, употребляют в разных значениях. Иногда противопоставляют «дискретную» математику, говорящую о конечных или по крайней мере хорошо различимых объектах, и «непрерывную», где речь идёт о действительных числах, пределах, непрерывности, производных и т.п. Хотя это противопоставление условно и не всегда применимо (скажем, странно было бы разделять «дискретные» алгебраические кривые над конечным полем и «непрерывные» алгебраические кривые над полем комплексных чисел), некоторый смысл оно имеет.

Говоря о «советской школе дискретной математики», имеют в виду немного другое — прежде всего пионерские работы 1950-х и 1960-х годов (О.Б. Лупанов и его школа) по анализу булевых функций, их классов, обобщений на многозначную логику и др.

Наконец, «дискретная математика» как учебный предмет на младших курсах — это сборная солянка из разных понятий и результатов, которые являются частью базовой математической культуры и необходимы будущим математикам и программистам, но не входят в традиционно сложившиеся курсы начального математического цикла (анализ, алгебра, линейная алгебра).

Именно в этом смысле слова «дискретная математика» используются в названии этой книжки, представляющей собой расширенные записки лекций, читавшихся на факультете компьютерных наук Высшей школы экономики. Получилась она разнородной: некоторые темы (скажем, про математическую индукцию или про комбинаторику) — это то, что вполне могло бы изучаться в школе и даже когда-то изучалось.¹ В других случаях целью является освоение некоторого языка (скажем, что такое пересечение множеств или бинарное отношение). Или это может быть прологом к рассказу о некоторой математической теории, попыткой выделить какое-то минимальное содержательное начало, которое имело бы смысл рассказать даже тем, кто в дальнейшем с этим не столкнётся. Или просто какой-то красивый результат, который трудно найти доступно изложенным.

¹ «Гимназист бойко выводил какую-то формулу, со стуком ломая мел о доску, и все писал, несмотря на то, что профессор уже сказал ему: „Довольно“, — и велел нам взять билеты. „Ну что, ежели достанется теория сочетаний!“ — подумал я, доставая дрожащими пальцами билет из мягкой кипы нарезанных бумажек.» (Лев Толстой, *Юность* из цикла *Детство. Отрочество. Юность*, глава XI, *Экзамен математики*. Странно, но потом герой повести с успехом отвечает про бином Ньютона.)

В каждую «лекцию» (в реальности это могло быть несколько лекций) мы старались включить и достаточно трудный материал, чтобы студентам не было скучно. При этом мы не рассчитывали на то, что все это сразу поймут. Такие более трудные места можно и нужно пропускать, если они кажутся непонятными, и двигаться дальше.

Изложение сопровождается задачами; часть из них — это вопросы к слушателям для проверки понимания на лекциях, другие разбирались на семинарах и включались в домашние задания, третьи могут быть предметом самостоятельной работы для заинтересовавшихся студентов и указанием на возможное развитие темы. В общем, как говорил классик, *прими собрание пёстрых глав...*