Московский физико-технический институт (ГУ)
Факультет инноваций и высоких технологий
Математическая логика и теория алгоритмов, весна 2016/17 уч.г.
Программа курса

Все материалы по курсу выкладываются на сайте

`ru.discrete-mathematics.org`.

Основные цели и задачи курса:

- Научиться рассуждать о бесконечных множествах.
- Освоить различные абстрактные модели вычислений и научиться рассуждать о них.
- Понять, что не всё можно вычислить и не всё можно доказать.

Основные темы курса:

1. **Трансфинитная индукция.** Фундированные и вполне упорядоченные множества. Начальные отрезки вполне упорядоченного множества. Сравнимость любых вполне упорядоченных множеств. Арифметические операции над вполне упорядоченными множествами. Понятие ординала. Аксиома выбора. Теорема Цермело. Сравнимость мощностей любых двух множеств. Мощности декартова произведения и объединения бесконечных множеств. Лемма Цорна. Равномощность бесконечного множества и его декартова квадрата. Базис Гамеля. Существование аддитивной функции действительного аргумента, отличной от умножения на константу.
2. **Разрешимость и неразрешимость.** Понятие алгоритма. Формальные модели вычислений. Вычислимые функции. Разрешимые множества. Перечислимые множества и свойства, эквивалентные перечислимости. Теорема Поста (множество разрешимо тогда и только тогда, когда перечислимы и оно, и его дополнение). Универсальные вычислимые функции. Неразрешимость проблем самоприменимости и остановки. Понятие m-сводимости. Примеры множеств, которые одновременно не перечислимы и не коперечислимы. Главные универсальные вычислимые функции. Теорема Райса–Успенского. Построение неглавной универсальной вычислимой функции. Теорема Клини о неподвижной точке и её приложения. Вычисления с оракулом. Сводимость по Тьюрингу. Теорема о представимости множеств, вычислимых с оракулом $\mathbf{0}'$. Арифметическая иерархия, её несхлопываемость. Множества, являющиеся m-полными на уровнях арифметической иерархии.
3. **Формальная арифметика и доказуемость.** Выразимость предикатов в формальной арифметике при помощи β-функции Гёделя. Представление в формальной арифметике множеств из арифметической иерархии. Аксиоматика Пеано. Теорема Тарского. Первая теорема Гёделя о неполноте формальной арифметики. Построение арифметической формулы, выражающей непротиворечивость системы аксиом. Теорема Лёба. Вторая теорема Гёделя о неполноте. Теорема Чёрча о неразрешимости множества общезначимых формул (б/д).

4. **Лямбда-исчисление.** Построение лямбда-термов. Процедуры α-конверсии и β-редукции. Эквивалентность лямбда-термов. Нормальная форма. Теорема Чёрча–Россера (б/д). Представление данных и операций с ними в лямбда-исчислении: нумералы и простейшие арифметические операции, логические значения и операции, работа с парами. Трюк Клини: представление вычитание. Комбинатор неподвижной точки и рекурсивное программирование: представление деления. Представимость функций в лямбда-исчислении. Непредставимость проверки наличия нормальной формы.

План по лекциям и контрольным

Лекции будут проходить по вторникам в 10:45 в 117 ГК и по средам в 9:00 в 113 ГК. Так же по средам в то же время будут проходить мини-контрольные. В этом календаре планируемые даты лекций помечены синим, контрольных — красным.

February

		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28					

March

		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

April

					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

May

1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

Лекция 1, 7 февраля 2017 г. Фундированные и вполне упорядоченные множества. Частично и линейно упорядоченные множества. Три определения свойства фундированности и их эквивалентность. Вполне упорядоченные множества. Примеры. Сложение и умножение фундированных и вполне упорядоченных множеств.

Лекция 2, 8 февраля 2017 г. Начальные отрезки вполне упорядоченных множеств. Теорема: строго монотонная функция на вполне упорядоченном множестве всегда не меньше тождественной. Определение и простые свойства начальных отрезков вполне упорядоченного множества. Начальные отрезки вида $[0, a)$ и $[0, a]$. Теорема: любой начальный отрезок имеет вид $[0, a)$ или совпадает со всем множеством. Теорема о трансфинитной рекурсии. Сравнимость любых двух вполне упорядоченных множеств.

Лекция 3, 15 февраля 2017 г. Ординальная арифметика и аксиома выбора. Понятие ординала. Вычитание и деление с остатком для ординалов. Возведение ординалов в степень. Аксиома выбора: неформальное утверждение и формализация. Теорема Цермело: любое множество можно вполне упорядочить.

Лекция 4, 21 февраля 2017 г. Приложения аксиомы выбора. Сравнимость по мощности любых двух множеств. Декартово произведение бесконечного множества A и счётного множества B равномощно A. Цепи в упорядоченных множествах. Верхние и нижние грани подмножеств упорядоченного множества. Минимальные и максимальые

элементы упорядоченного множества. Лемма Цорна: если любая цепь упорядоченного множества имеет верхнюю грань, то само множество имеет максимальный элемент. Базис Гамеля: определение, теорема существования. Базис Гамеля для множества $\mathbb{R}$, рассматриваемого как векторное пространство над $\mathbb{Q}$. Изоморфизм упорядоченных множеств $\langle \mathbb{R}, + \rangle$ и $\langle \mathbb{R}^2, + \rangle$. Существование аддитивной функции из $\mathbb{R}$ в $\mathbb{R}$, отличной от умножения на константу.

Лекция 5, 22 февраля 2017 г. Разрешимые и перечислимые множества. Понятие алгоритма. Основные черты алгоритма: конечное описание, получение входа, пошаговое выполнение, остановка, получение выхода. Способы формализации понятия алгоритма и кодирования данных. Машина Тьюринга. Тезис Чёрча. Определение вычислимой функции. Вывод существования невычислимых функций из соображений мощности. Определение разрешимого множества. Эквивалентность разрешимости множества и вычислимости его характеристической функции. Замкнутость класса разрешимых множеств относительно операций объединения, пересечения, дополнения. Перечисляющие алгоритмы и перечислимые множества. Свойства, эквивалентные перечислимости: вычислимость полухарактеристической функции, область определения вычислимой функции, область значений вычислимой функции, пустота или облать значений всюду определённой вычислимой функции, проекция разрешимого множества. Замкнутость класса перечислимых множеств относительно операций объединения и пересечения. Теорема Поста: множество разрешимо тогда и только тогда, когда оно само и его дополнение разрешимы.

Лекция 6, 28 февраля 2017 г. Неразрешимость проблем самоприменимости и остановки. Универсальная вычислимая функция и её построение через универсальную машину Тьюринга. Диагональная функция. Доказательство невозможности существования универсальной тотальной вычислимой функции. Существование вычислимой функции, совпадающей с любой другой вычислимой функцией хотя бы на одном входе. Продолжения вычислимых функций. Непродолжаемость диагональной функции. Неразрешимость проблемы самоприменимости. Неразрешимость проблемы остановки. Существование перечислимого неразрешимого множества. Существование перечислимых неотделимых множеств. Понятие m-сводимости и его основные свойства.

Мини-контрольная 1, 1 марта 2017 г.: Вполне упорядоченные множества и ординальная арифметика.

Лекция 7, 14 марта 2017 г. Теорема Райса–Успенского. Универсальные вычислимые функции. Главные универсальные вычислимые функции: определение и пример (универсальная машина Тьюринга). Свойства машин Тьюринга. Свойства вычислимых функций. Теорема Райса–Успенского: множество машин Тьюринга, вычисляющих функции с нетривиальным свойством, не разрешимо. Построение неглавной универсальной вычислимой функции.

Мини-контрольная 2, 15 марта 2017 г.: Задачи на трансфинитную индукцию.

Лекция 8, 21 марта 2017 г. Теорема Клини. Преобразования вычислимых функций. Теорема Клини о неподвижной точке: для любой всюду определённой вычислимой функции h и главной универсальной вычислимой функции U существует n, такое что при всех x верно $U(n, x) = U(h(n), x)$. Программа, печатающая собственный текст. Вывод теоремы Райса–Успенского из теоремы Клини. Рекурсивное программирование для произвольной главной универсальной функции.

Лекция 9, 22 марта 2017 г. Арифметическая иерархия. Классы Σ_n и Π_n: определения через кванторы и через чередование операций проекции и дополнения.

Объединение Σ_n и Π_n вложено в пересечение Σ_{n+1} и Π_{n+1}. Объединение и пересечение множеств из Σ_n лежит в Σ_n. Объединение и пересечение множеств из Π_n лежит в Π_n. Универсальные множества для классов Σ_n и Π_n: определение и конструкция. Универсальное множество для класса Σ_n не лежит в Π_n. Каждое из множеств Σ_n и Π_n является собственным подмножеством каждого из множеств Σ_{n+1} и Π_{n+1}.

Лекция 10, 28 марта 2017 г. Вычисления с оракулами. Понятие m-полного множества. m-полнота проблемы остановки в классе перечислимых множеств и проблемы всюду определённости в классе Π_2. Машины Тьюринга с оракулами. Оракул $\mathbf{0}'$, примеры множеств, разрешимых с этим оракулом. Теорема о характеризации любой $\mathbf{0}'$-вычислимой функции как предела всюду определённой функции двух аргументов.

Мини-контрольная 3, 29 марта 2017 г.: Разрешимые и перечислимые множества.

Лекция 11, 4 апреля 2017 г. Выразимость и выводмость в арифметике. Арифметика как интерпретация $\langle \mathbb{N}, =, +, \cdot \rangle$. Арифметичность предикатов (подмножеств $\mathbb{N}^k$). Арифметичность простейших предикатов: константы, сравнение, делимость, простота, НОД, НОК и т.д. Арифметичность предикатов «n — степень двойки» и «n — степень четвёрки». Построение β-функции Гёделя и доказательство её основного свойства: для любой последовательности $(x_1, \ldots, x_k)$ существуют a и b, такие что $x_i = \beta(a, b, i)$ при всех i. Арифметичность предикатов «n — степень шестёрки», «$n = 2^k$», «n — совершенное число» и т.д. Кодирование слов натуральными числами и арифметичность операций над словами. Арифметичность графиков вычислимых функций. Список аксиом Пеано и их мотивировка. Примеры выводов различных утверждений: арифметических равенств, простейших свойств арифметических действий. Кодирование формул и доказательств натуральными числами. Разрешимость множества корректных доказательств и перечислимость множества всех теорем в арифметике Пеано. Запись предиката доказуемости арифметической формулой.

Лекция 12, 5 апреля 2017 г. Теорема Гёделя о неполноте. Теорема Гёделя о неполноте: при любом выборе разрешимой системы аксиом арифметики множества истинных и доказуемых формул не совпадают. Лемма: любое арифметическое множество m-сводится к множеству всех арифметических истин. Теорема Тарского: множество истинных арифметических формул не арифметично. Непосредственное доказательство теоремы Гёделя о неполноте: построение формулы «Эту формулу невозможно доказать». Непосредственное доказательство теоремы Тарского.

Лекция 13, 11 апреля 2017 г. Вокруг теоремы Гёделя. Лемма о диагонализации: для любой формулы ψ с одной свободной переменной существует замкнутая формула ϕ, такая что $\phi \leftrightarrow \psi(\langle \phi \rangle)$. Построение арифметической формулы, выражающей непротиворечивость системы аксиом. «Доказательство» существования единорогов. Теорема Лёба. Вторая теорема Гёделя о неполноте. Теорема Чёрча о неразрешимости множества общезначимых формул: формулировка и идея доказательства. Построение программы, про которую нельзя в формальной арифметике доказать отличие ни от какой другой программы.

Мини-контрольная 4, 12 апреля 2017 г.: Теоремы Райса–Успенского и Клини.

Лекция 14, 18 апреля 2017 г. Синтаксис лямбда-исчисления. Философские основания: почему удобно любой объект рассматривать как функцию. Идеология функционального программирования. Алфавит лямбда-исчисления. Построение лямбда-термов. Соглашения о сокращённой записи. Операции α-конверсии и β-редукции. Примеры. Понятие равенства лямбда-термов. Понятие лямбда-терма в нормальной форме. Теорема

Чёрча-Россера (б/д). Пример лямбда-терма, не имеющего нормальной формы.

Лекция 15, 19 апреля 2017 г. Программирование в лямбда-исчислении. Кодирование различных структур данных в лямбда-исчислении. Понятие комбинатора. Комбинаторы, представляющие логические константы и логические операции. Нумералы Чёрча и представление простейших арифметических операций: сложения, умножения, возведения в степень. Кодирование пар. Трюк Клини и операция вычитания. Комбинаторы неподвижной точки и рекурсивное программирование. Комбинатор, вычисляющий операции деления и взятия остатка. Представление функции нескольких натуральных аргументов в лямбда-исчислении. Теорема о представимости любой вычислимой функции (б/д). Непредставимость проверки существования нормальной формы.

Мини-контрольная 5, 10 мая 2017 г.: Арифметическая иерархия и формальная арифметика.

Мини-контрольная 6, 17 мая 2017 г.: Лямбда-исчисление.

Выставление оценок

На каждой мини-контрольной будет даваться 3 тестовых вопроса и 2–4 задачи. Каждый тестовый вопрос приносит 0.6 балла в случае верного ответа, задача — 1 балл в случае полностью верного решения. Если задача не решена, то задача на ту же тему появится на следующей контрольной и принесёт 0.8 балла в случае решения. Если и второй раз задача не решена, то похожая задача выдаётся на дом и приносит 0.5 балла в случае решения. Также на дом могут выдаваться более сложные задачи на 1.5 балла (но их будет меньше, чем в первом семестре). В конце семестра будут объявлены пороги для получения 1, 2 или 3 баллов за семестр, после чего ещё можно будет дорешать небольшое число задач. Устный экзамен будет оцениваться исходя из 7 баллов. Студенты, набравшие меньше 2 баллов за семестр, должны будут писать специальный тест для допуска к экзамену. В билете будет по одному вопросу по каждой из 3 больших тем: множества, логика и алгоритмы. Ещё 2 балла будет ставиться за опрос по определениям и простым утверждениям, а ещё 2 балла — за изучение дополнительных, более трудных вопросов. К набранным баллам будет добавляться оценка за семестр, что даст оценку по 10-балльной шкале.

Литература:

1. Верещагин Н.К., Шень А. Лекции по математической логике. Часть I. Начала теории множеств. М.: МЦНМО, 2002. (Электронная версия доступна на странице `http://www.mccme.ru/free-books`)

2. Верещагин Н.К., Шень А. Лекции по математической логике. Часть II. Языки и исчисления. М.: МЦНМО, 2002. (Электронная версия доступна на странице `http://www.mccme.ru/free-books`)

3. Верещагин Н.К., Шень А. Лекции по математической логике. Часть III. Вычислимые функции. М.: МЦНМО, 2002. (Электронная версия доступна на странице `http://www.mccme.ru/free-books`)

4. Мендельсон Э. Введение в математическую логику. М.: Наука, 1984.

5. Булос Дж., Джеффри Р. Вычислимость и логика. М.: Мир, 1994.

6. Успенский В.А., Верещагин Н.К., Плиско В.Е. Вводный курс математической логики. М.: Физматлит, 2004

7. Лавров И.А., Максимова Л.Л. Задачи по теории множеств, математической логике и теории алгоритмов. М.: Физматлит, 2002.

8. Пентус А.Е., Пентус М.Р., Математическая теория формальных языков, М.: Интернет-университет информационных технологий; БИНОМ. Лаборатория знаний, 2006.

9. Пентус М.Р. Введение в математическую логику. Конспект лекций на механико-математическом факультете МГУ, весна 2006.
`http://lpcs.math.msu.su/~pentus/ftp/mehmat/vmlk06le.pdf`

10. Плиско В.Е. Математическая логика. Конспект.
`http://lpcs.math.msu.su/~plisko/matlog.pdf`

11. Bilaniuk, S., A Problem Course in Mathematical Logic.
`http://euclid.trentu.ca/math/sb/pcml`

Дополнительная литература:

14. Клини С.К. Математическая логика. М.: Мир, 1973.

15. Смаллиан Р. Как же называется эта книга? М.: Мир, 1981.

16. Линдон Р. Заметки по логике. М.: Мир, 1968.

17. Манин Ю.И. Доказуемое и недоказуемое. М.: Советское радио, 1979.

18. Манин Ю.И. Вычислимое и невычислимое. М.: Советское радио, 1980.

19. Хофштадтер Д. Гёдель, Эшер, Бах: эта бесконечная гирлянда. Самара: Бахрах-М, 2001.