Московский физико-технический институт (ГУ)
Факультет инноваций и высоких технологий
Математическая логика и теория алгоритмов, весна 2021
Программа экзамена

Никто и никогда не понуждает знать. Знать просто следует, вот и всё. Даже если рискуешь понять неправильно.

У. Эко, *Имя розы*

Экзамен будет проходить в 3 дня: 14, 15 и 16 июня. Распределение по дням в целом соответствует заявленному расписанию, но возможны переносы по просьбам студентов. Удовлетворение просьб не гарантируется, но причины переноса принимаются во внимание. Студенты будут приглашаться небольшими группами с интервалом в 30-40 минут, точное расписание будет объявлено накануне экзамена.

На экзамене можно получить от 0 до 7 баллов, к которым будет добавлено от 0 до 3 баллов за семестр. Билет на экзамене будет содержать три вопроса из данного списка, по одному на каждую тему (множества, логика и вычислимость) и по одному каждого уровня сложности (3, 4 и 5). Каждый вопрос строится вокруг одного или нескольких связанных утверждений, которое(-ые) нужно сформулировать и доказать. Попутно нужно сформулировать все необходимые определения и используемые вспомогательные утверждения. Экзаменатор также может задавать вопросы по определениям, простым утверждениям и формулировкам теорем, не связанным с исходными вопросами. Знать определение — значит не только уметь его воспроизвести, но и привести примеры как объектов, соответствующих определению, так и объектов, ему не соответствующих. Простые утверждения нужно уметь не только формулировать, но и доказывать. Количество таких вопросов заранее не регламентируется. За эту часть экзамена может быть поставлено до 5 баллов (по 1 баллу за каждый из вопросов билета и до 2 баллов за прочее). Большее число баллов можно получить, ответив на дополнительные вопросы. Некоторые из дополнительных вопросов могли не быть освещены на лекциях и семинарах, или освещены кратко.

Дополнительные вопросы выдаются лишь в случае, когда студент получил хотя бы 4 балла из 5. Рядом с каждым вопросом написан максимальный балл, который за него можно получить (7, 6 или 5). Если набрано 4 балла, то ответ на вопрос с пометкой 5 или 6 приносит 5 баллов, с пометкой 7 — 6 баллов. Если набрано 5 баллов, то вопросы с пометкой 5 не задаются, вопросы с пометками 6 и 7 приносят 6 и 7 баллов соответственно. Вначале студент выбирает, на какую оценку он хочет получить вопрос. Затем экзаменатор назначает одну из трёх тем. После этого студент выбирает три возможных вопроса на эту оценку и эту тему, а экзаменатор указывает на один из них. В случае успешной сдачи вопроса с пометкой 6 можно с разрешения экзаменатора попытаться рассказать вопрос с пометкой 7. В случае неуспешной сдачи вопроса с пометкой 7 брать вопрос с пометкой 6 нельзя.

Независимо от баллов в семестре, для оценки «удовлетворительно» и выше необходимо продемонстрировать знание основных определений и простых утверждений и полностью ответить хотя бы на один из вопросов билета. В частности, за ответ на экзамене нужно набрать хотя бы 2 балла (1 балл за вопрос из билета, 1 из 2 баллов за опрос).

При подготовке ответа можно пользоваться любыми материалами, в том числе электронными, но нельзя пользоваться интернетом и общаться. При этом отвечать следует «с чистого листа», записывая необходимые формулы и фразы в процессе ответа. При ответе допускается время от времени с разрешения экзаменатора подглядывать в записи, но не читать написанное, в том числе написанное уже на экзамене. На вопросы по определениям, простым утверждениям и формулировкам следует отвечать сразу или почти сразу. Над дополнительными вопросами можно размышлять, но уже без использования материалов.

1 Логика и арифметика

1.1 Определения

1) Булевы функции, примеры. Двойственность.
2) Классы булевых функций: сохраняющие 0 и 1, монотонные, самодвойственные, линейные.
3) Пропозициональные формулы. Тавтологии. Конъюнктивные и дизъюнктивные нормальные формы.
4) Многочлены Жегалкина.
5) Аксиомы исчисления высказываний, modus ponens.
6) Логические выводы и выводимые формулы.
7) Резолюции.
8) Языки первого порядка: индивидные переменные, логические связки, кванторы, функциональные и предикатные символы, термы, атомарные формулы, формулы общего вида.
9) Интерпретация языка первого порядка. Оценка переменных. Общезначимые формулы.
10) Свободные и связанные вхождения переменных. Параметры формулы.
11) Выразимость предиката или функции в данной интерпретации.
12) Аксиомы исчисления предикатов, правила Бернайса, правило обобщения.
13) Аксиомы равенства.
14) Теории, модели, нормальные модели.
15) Аксиомы арифметики Пеано.
16) Совместность, непротиворечивость, полнота теории.

1.2 Простые утверждения

1) Любую булеву функцию можно выразить формулой в КНФ или формулой в ДНФ.
2) Замкнутость классов Поста относительно композиции.
3) Вывод формулы вида $A \to A$ в исчислении высказываний.
4) Теорема о корректности исчисления высказываний.
5) Сведение задачи о выполнимости произвольной формулы к задаче о выполнимости 3-КНФ.

6) Представление задачи о раскраске графа и задачи о расстановке ферзей на шахматной доске как задачи о выполнимости КНФ.
7) Теорема о корректности метода резолюций: из выполнимой КНФ нельзя вывести $\perp$.
8) Значение терма (формулы) первого порядка зависит только от значений его (её) параметров.
9) Выразимость свойств «равняться нулю», «равняться единице», «делиться нацело», «быть простым числом», «равняться наибольшему общему делителю», «равняться наименьшему общему кратному» в интерпретации $\langle \mathbb{N}, \cdot, = \rangle$.
10) Любую формулу первого порядка можно привести к предварённой нормальной форме.
11) Вывод правила обобщения в исчислении предикатов.
12) Вывод формулы вида $\exists x \forall y \varphi \to \forall y \exists x \varphi$ в исчислении предикатов.
13) Любое совместное множество формул первого порядка непротиворечиво.
14) Из теоремы Гёделя о полноте исчисления предикатов в сильной форме (любая непротиворечивая теория имеет модель) следует теорема в слабой форме (любая общезначимая формула выводима в исчислении предикатов).
15) Выразимость в арифметике свойства «быть степенью двойки».
16) Множество предложений, выводимых в арифметике Пеано, перечислимо.

1.3 Вопросы из билетов

1) (3) Теорема об однозначном представлении булевой функции многочленом Жегалкина.
2) (3) Теорема о дедукции для исчисления высказываний.
3) (3) Теорема о полноте исчисления высказываний.
4) (4) Теорема о полноте метода резолюций: из невыполнимой КНФ всегда можно вывести $\perp$.
5) (3) Устойчивость выразимых предикатов при автоморфизмах интерпретаций.
6) (4) Теорема Гёделя о полноте исчисления предикатов: расширение любого непротиворечивого множества до полного и экзистенциально полного.
7) (4) Теорема Гёделя о полноте исчисления предикатов: построение модели из замкнутых термов у любого непротиворечивого, полного и экзистенциально полного множества.
8) (5) Представимость конечных последовательностей в арифметике при помощи β-функции Гёделя.
9) (4) Арифметичность предикатов «n — степень шестёрки» и «$n = 2^k$».
10) (5) Вывод коммутативности сложения в арифметике Пеано.
11) (5) Множество замкнутых формул, истинных в $\mathbb{N}$, неперечислимо. Первая теорема Гёделя о неполноте.
12) (5) Теорема Тарского о неарифметичности множества истинных арифметических формул.

1.4 Дополнительные вопросы

1) (5) Теорема об однозначности синтаксического разбора пропозициональных формул.
2) (6) Базис класса монотонных функций.
3) (5) Теорема о компактности для исчисления высказываний.
4) (6) Если сколь угодно большой квадрат можно правильно замостить данным конечным набором раскрашенных квадратиков, то и всю плоскость можно ими замостить.
5) (7) Эквивалентность теоремы о компактности для исчисления высказываний в случае счётного числа переменных и леммы Кёнига (для любого конечного ветвления).
6) (6) Элиминация кванторов на примере $\langle \mathbb{Q}, <, = \rangle$.
7) (7) Элементарная эквивалентность упорядоченных множеств $\mathbb{Z}$ и $\mathbb{Z}+\mathbb{Z}$ (если используется игра Эренфойхта, нужно доказать теорему в нужную сторону).
8) (6) Следствия из теоремы Гёделя о полноте исчисления предикатов: теорема о компактности и эквивалентность выводимости и семантического следования.
9) (7) Несуществование формулы первого порядка, выражающей связность графа (в сигнатуре из равенства и соседства по ребру). Если используется игра Эренфойхта или игра Эренфойхта–Фраиссе, нужно доказать теорему в нужную сторону
10) (6) Несуществование аксиоматики конечных полей.
11) (6) Существование нормальной модели у любой непротиворечивой теории с равенством и теорема о компактности для нормальных моделей.
12) (5) Пример формулы, истинной в любой конечной интерпретации, но необщезначимой.
13) (7) Существование нестандартных моделей арифметики. Теорема о порядке на галактиках в этих моделях (он корректно определён, линеен, всюду плотен, не имеет наибольшего, имеет наименьший элемент).
14) (7) Представимость конечных множеств в арифметике при помощи кодирования Смаллиана.
15) (6) Арифметичность свойства «x — совершенное число».
16) (5) Лемма о диагонализации: для любой формулы ψ с одной свободной переменной существует замкнутая формула φ, эквивалентная $\psi(\langle\varphi\rangle)$.
17) (7) Теорема Лёба и вывод из неё второй теоремы Гёделя о неполноте.
18) (7) Построение программы, отличие которой ни от какой другой нельзя доказать в арифметике Пеано.
19) (7) Теорема Чёрча о неразрешимости множества общезначимых формул.

2 Теория множеств

Некоторые определения и простые утверждения повторяют те, которые были в курсе ОКТЧ. Разумеется, их нужно знать для успешной сдачи экзамена.

2.1 Определения

1) Множество, основные теоретико-множественные операции, декартово произведение.
2) Отображения и соответствия. Образ и прообраз. Инъекции, сюръекции, биекции. Композиция отображений. Возведение множества в степень множества.
3) Равномощность. Счётные и континуальные множества.
4) Бинарные отношения. Рефлексивность, транзитивность, (анти-)симметричность и т.д. Отношения эквивалентности и отношения порядка.
5) Упорядоченное множество, линейно упорядоченное множество, фундированное множество, вполне упорядоченное множество.
6) Цепи в упорядоченных множествах. Верхние и нижние грани, максимальные и минимальные, наибольшие и наименьшие элементы.
7) Гомоморфизмы и изоморфизмы упорядоченных множеств.
8) Сложение и умножение упорядоченных множеств.
9) Начальные отрезки вполне упорядоченных множеств.
10) Предельные элементы вполне упорядоченных множеств.
11) Порядковые типы ω, ω^k, ω^ω, ε_0.
12) Аксиома выбора.
13) Базис Гамеля.

2.2 Простые утверждения

1) Основные тождества про теоретико-множественные операции, декартово произведение, возведение множества в степень множества.
2) Равномощность — отношение эквивалентности.
3) Объединение и декартово произведение счётных множеств счётны.
4) В любом бесконечном множестве найдётся счётное подмножество.
5) Несчётность множества точек на отрезке.
6) Нефундированность прямого лексикографического порядка на конечных словах.
7) Любой начальный отрезок вполне упорядоченного множества, отличный от всего множества, представляется в виде $[0, a)$.
8) Вполне упорядоченное множество неизоморфно своему начальному отрезку вида $[0, a)$ (вывод из леммы о монотонной функции).
9) Сумма и произведение фундированных множеств фундированы, вполне упорядоченных — вполне упорядочены.
10) Свойства сложения и умножения вполне упорядоченных множеств.
11) Сравнимость любых двух множеств по мощности (вывод из теоремы Цермело и свойств вполне упорядоченных множеств).

2.3 Вопросы из билетов

1) (3) Эквивалентность фундированности, отсутствия бесконечно убывающей последовательности элементов и принципа трансфинитной индукции.
2) (3) Лемма о монотонной функции из вполне упорядоченного множества в себя.
3) (3) Теорема о структуре вполне упорядоченного множество: оно представляется как $\omega \cdot L + F$, где L — множество предельных элементов (кроме, возможно, наибольшего), F — конечное множество.
4) (3) Теорема о трансфинитной рекурсии.
5) (4) Сравнимость любых двух вполне упорядоченных множеств.
6) (4) Теорема о вычитании вполне упорядоченных множеств.
7) (4) Теорема о делении с остатком вполне упорядоченных множеств.
8) (5) Теорема Цермело.
9) (5) Лемма Цорна.
10) (4) Любой частичный порядок можно дополнить до линейного.
11) (5) Объединение двух бесконечных множеств равномощно одному из них.
12) (5) Декартов квадрат бесконечного множества равномощен ему.

2.4 Дополнительные вопросы

1) (6) Парадокс Бурали-Форти: не существует множества, содержащего по одному представителю для каждого порядкового типа.
2) (7) Возведение вполне упорядоченных множеств в степень: определение и свойства. Счётный ординал в счётной степени счётен.
3) (6) Представление любого ординала меньше ε_0 в виде суммы (итерированных) степеней ω.
4) (6) Точная верхняя грань счётного множества счётных ординалов счётна
5) (5) Существование множества на плоскости, пересекающегося с любой прямой ровно по двум точкам.
6) (7) Теорема Гудстейна о сходимости к нулю последовательности чисел, полученных чередованием вычитания единицы и замены основания в полном разложении в сумму степеней с коэффициентами.
7) (7) Теорема об отделимости любых двух выпуклых множеств на плоскости.
8) (6) Вывод аксиомы выбора из теоремы Цермело или из леммы Цорна.
9) (5) Существование базиса Гамеля в $\mathbb{R}$ над $\mathbb{Q}$.
10) (7) Существование нелинейной аддитивной функции, т.е. такой функции f, что $f(x+y) = f(x) + f(y)$ при всех $x, y \in \mathbb{R}$, но $f(x)$ не является умножением на константу.
11) (7) Любое счётное вполне упорядоченное множество изоморфно некоторому подмножеству $\mathbb{R}$.
12) (5) Декартово произведение двух бесконечных множеств равномощно одному из них.
13) (5) Для бесконечного множества A выполнено $2^A \cong A^A$.
14) (6) Построение неизмеримого множества на окружности.

15) (7) Теорема Банаха–Тарского: равносоставленность сферы и пары сфер.
16) (6) Вывод из теоремы Банаха–Тарского равносоставленности любых двух ограниченных фигур в $\mathbb{R}^3$, имеющих внутренние точки.

3 Вычислимость

3.1 Определения

1) Машина Тьюринга.
2) Вычислимая функция.
3) Разрешимое множество.
4) Перечислимое множество.
5) Универсальная машина Тьюринга.
6) Универсальная вычислимая функция.
7) Главная универсальная вычислимая функция.
8) m-сводимость.
9) Классы арифметической иерархии.
10) λ-термы, α-конверсии, β-редукции, нормальная форма.
11) Нумералы Чёрча.
12) Комбинатор неподвижной точки.

3.2 Простые утверждения

1) Композиция вычислимых функций вычислима.
2) Существование невычислимых функций, неразрешимых и неперечислимых множеств.
3) Перечислимость любого разрешимого множества.
4) Разрешимость любого конечного множества.
5) Замкнутость классов разрешимых и перечислимых множеств относительно пересечения и объединения, класса разрешимых относительно дополнения.
6) Существование вычислимой в обе стороны биекции между $\mathbb{N}^2$ и $\mathbb{N}$.
7) Подмножество разрешимого (перечислимого) множества не обязательно разрешимо (перечислимо), и наоборот.
8) Свойства m-сводимости: транзитивность, сводимость дополнений, разрешимость множества, m-сводимого к разрешимому, перечислимость множества, m-сводимого к перечислимому.
9) Вложенность классов в арифметической иерархии.
10) Замкнутость классов арифметической иерархии относительно объединения и пересечения.
11) Пример λ-терма, к которому можно применить β-редукцию только после α-конверсии.
12) Пример λ-терма, не имеющего нормальной формы.
13) Построение комбинаторов сложения и умножения для нумералов Чёрча (с доказательством корректности).

3.3 Вопросы из билетов

1) (4) Моделирование машины Тьюринга с несколькими лентами на машине Тьюринга с одной лентой.
2) (3) Эквивалентность следующих утверждений: множество перечислимо, полухарактеристическая функция множества вычислима, множество является областью определения вычислимой функции, множество является проекцией разрешимого множества пар.
3) (3) Теорема Поста: критерий разрешимости в терминах перечислимости множества и его дополнения.
4) (3) Неразрешимость проблем самоприменимости и остановки.
5) (4) Несуществование универсальной тотально вычислимой функции.
6) (5) Неперечислимость и некоперечислимость множества всюду определённых программ.
7) (4) Существование главной универсальной вычислимой функции.
8) (5) Теорема Райса–Успенского о неразрешимости нетривиальных свойств вычислимых функций.
9) (5) Теорема Клини о неподвижной точке. Построение программы, на любом входе печатающей некоторый собственный номер.
10) (5) Теорема об арифметической иерархии: $\Sigma_n \neq \Sigma_{n+1}$, $\Sigma_n \neq \Pi_n$.
11) (3) Теорема Чёрча–Россера (б/д). Единственность нормальной формы.
12) (4) Построение комбинаторов логических значений, булевых функций, операций с парами, проверки на ноль для нумералов Чёрча (с доказательством корректности).

3.4 Дополнительные вопросы

1) (5) Образ и прообраз перечислимого множества относительно вычислимой функции перечислимы.
2) (6) Существование универсального перечислимого множества.
3) (6) Существование вычислимой функции, не имеющей всюду определённого вычислимого продолжения.
4) (7) Существование непересекающихся перечислимых множеств, не отделимых никаким разрешимым.
5) (6) Неперечислимость и некоперечислимость множества программ, определённых в нуле и не определённых в единице.
6) (5) Несуществование универсального разрешимого множества.
7) (5) Вывод теоремы Райса–Успенского из теоремы Клини.
8) (7) Построение неглавной универсальной вычислимой функции.
9) (6) Существование бесконечного множества, любое бесконечное подмножество которого неразрешимо.
10) (7) Бесконечность множества неподвижных точек в теореме Клини.
11) (7) Главность универсальной вычислимой функции эквивалентна тому, что по номерам двух функций можно вычислить номер их композиции.
12) (6) Теорема о m-полноте проблемы остановки в классе перечислимых множеств.

13) (7) Построение перечислимого неразрешимого множества, не являющегося m-полным в классе перечислимых.
14) (7) Теорема о характеризации $0'$-вычислимых функций как пределов вычислимых функций двух аргументов.
15) (6) Построение комбинатора возведения в степень для нумералов Чёрча (с полным доказательством корректности).
16) (6) Построение комбинаторов взятия предыдущего и вычитания для нумералов Чёрча в λ-исчислении (с доказательством корректности).
17) (6) Рекурсия в λ-исчислении. Построение комбинаторов неполного частного и остатка.
18) (7) Построение комбинатора, возвращающего n-е простое число (для нумералов Чёрча).
19) (7) Невыразимость в λ-исчислении предиката существования нормальной формы у λ-терма (с деталями конструкции).