

Министерство науки и высшего образования  
Российской Федерации

---

Федеральное государственное бюджетное  
образовательное учреждение высшего образования  
«Тверской государственный университет»

Обсуждено на заседании  
Учёного совета ТвГУ  
протокол № 8  
от «29» марта 2023 г.



«УТВЕРЖДАЮ»

Врио ректора ТвГУ

С. Н. Смирнов

«29» марта 2023 г.

## ПРОГРАММА

кандидатского экзамена  
по специальной дисциплине

1.1.5 Математическая логика, алгебра,  
теория чисел и дискретная математика

---

Программа разработана на основе паспорта научной специальности 1.1.5 Математическая логика, алгебра, теория чисел и дискретная математика.

## Теория алгоритмов

- Общее понятие алгоритма и его формализации. Машины Тьюринга, счётчиковые машины, частично рекурсивные функции. Эквивалентность моделей. Тезис Чёрча – Тьюринга.
- Универсальные частично рекурсивные функции. Нумерации частично рекурсивных функций. Гёделевы нумерации. Теорема об эффективной подстановке (s-n-m-теорема). Теоремы Роджерса о неподвижной точке. Невозможность полной нумерации общерекурсивных функций. Частично рекурсивные функции, не дополняемые до общерекурсивных. Теорема Райса – Успенского об алгоритмической неразрешимости нетривиальных свойств вычислимых функций.
- Алгоритмические проблемы. Рекурсивно перечислимые и рекурсивные множества. Критерии рекурсивной перечислимости. Алгоритмическая m-сводимость. m-трудность и m-полнота. m-полнота проблем самоприменимости и остановки. m-трудность и неперечислимость проблемы тотальности. Теорема Поста о рекурсивных множествах.
- Минимальные номера. Невозможность перечисления минимальных номеров. Колмогоровская сложность слов и бесконечных последовательностей. Оптимальные интерпретаторы. Алгоритмическая невозможность оптимального сжатия. Случайные последовательности.

- Исчисления, линейные выводы и выводы в виде дерева. Рекурсивная перечислимость множества выводимых слов. Исчисления Туэ и ассоциативные исчисления. Построение ассоциативного исчисления с  $m$ -полной проблемой выводимости.
- $\lambda$ -исчисление. Представление вычислимых функций в  $\lambda$ -исчислении.  $m$ -полнота проблемы выводимости в  $\lambda$ -исчислении.
- Сложность вычислений. Аксиомы Блюма. Невозможность мажорирования мер сложности общерекурсивными функциями. Эквивалентность мер сложности. Диагональ Рабина и диагональ Блюма.
- Эквивалентность времени решения задачи на детерминированных устройствах с точностью до полинома. Недетерминированные вычисления. Теорема Сэвича о равенстве PSPACE и NPSPACE. Классы сложности P, NP, PSPACE. Сводимость за полиномиальное время. NP-полные задачи. Теорема Кука–Левина об NP-полноте задачи выполнимости для логики высказываний. Другие примеры NP-полных задач. Квантифицированные булевы формулы, PSPACE-полнота задачи об их истинности.

## Математическая логика

- Логика высказываний. Формулы логики высказываний, интерпретации в логике высказываний. Следование и эквивалентность. Представимость булевых функций формулами логики высказываний. Конъюнктивные и дизъюнктивные нормальные формы. Интерполяционная теорема Крейга для логики высказываний.

- 
- Исчисление высказываний. Допустимые аксиомы и правила вывода исчисления высказываний. Полнота и непротиворечивость исчисления высказываний. Независимость аксиом и правил вывода.
  - Логика предикатов. Формулы логики предикатов, интерпретации в логике предикатов. Приведение формул логики предикатов к предварённой форме.
  - Исчисление предикатов. Независимость аксиом и правил вывода. Допустимые аксиомы и правила вывода исчисления предикатов. Непротиворечивость исчисления предикатов. Теорема о дедукции для исчисления предикатов.
  - Полнота исчисления предикатов. Формально непротиворечивые, совместные и локально совместные множества. Лемма Генкина о совместности непротиворечивых множеств. Теорема Линденбаума о расширении непротиворечивой теории до полной. Теорема компактности. Неаксиоматизируемость конечности. Теоремы Лёвенгейма – Скулема о повышении и понижении мощности.
  - Теории, формализация теорий. Рекурсивная аксиоматизируемость и разрешимость теорий. Методы установления разрешимости, элиминация кванторов, автоматные системы, интерпретации. Теория плотного линейного порядка и её разрешимость. Теорема Чёрча о неразрешимости проблемы выводимости для логики предикатов. Теорема Трахтенброта о неразрешимости проблемы существования конечных моделей.
  - Элементарные теории классов алгебраических систем. Кате-

---

горичные в данной мощности теории. Теорема Лося – Воота о категоричности и полноте.

- Формальная арифметика. Аксиомы Пеано. Представимость вычислимых функций в формальной арифметике. Теорема Гёделя о неполноте формальной арифметики. Алгоритмическая неразрешимость проблемы выводимости для арифметики. Теорема Тарского о невыразимости арифметической истинности в арифметике. Предикаты выводимости в арифметике Пеано. Теорема Лёба. Теорема Гёделя о недоказуемости непротиворечивости.
- Аксиоматическая теория множеств ZFC. Частичные и линейные порядки. Аксиома выбора и её эквиваленты: теорема Хаусдорфа о максимальном элементе, лемма Цорна. Вполне упорядоченные множества, теорема Цермело о полном упорядочении. Трансфинитная индукция. Ординалы. Мощность множеств, кардиналы.
- Решётки и булевы алгебры. Фильтры булевых алгебр, ультрафильтры. Теорема Стоуна о булевых алгебрах. Фильтрованные произведения алгебраических систем, ультрапроизведения, теорема Лося об ультрапроизведениях.

## **Алгебра и теория чисел**

- Универсальные алгебры. Свободные алгебры. Подалгебры, гомоморфизмы, прямые произведения. Конгруэнтности. Основная теорема о гомоморфизмах. Многообразия алгебр. Теорема Биркгофа о замкнутости многообразий.

- 
- Полугруппы, моноиды, сократимые и обратимые элементы. Теорема Гротендика о вложении коммутативной полугруппы с сокращением в абелеву группу.
  - Группы, подгруппы, смежные классы. Порядок группы и её элемента, индекс подгруппы. Теорема Лагранжа о порядках групп и подгрупп. Теорема о строении конечно порождённых абелевых групп.
  - Теоремы о гомоморфизме групп. Свободные группы и определяющие соотношения. Центр и коммутант группы. Действие группы на множестве. Формулы орбит. Теоремы Силова о  $p$ -подгруппах. Простота знакопеременной группы  $\mathfrak{A}_n$ ,  $n \geq 5$ .
  - Кольца, тела и поля. Делители нуля. Целостные и евклидовы кольца. Поле частных. Гомоморфизмы колец, идеалы. Кольца главных идеалов и факториальность. Нётеровы кольца и модули. Теорема Гильберта о базисе.
  - Артиновы кольца. Модули над кольцом. Радикал кольца. Простые и полупростые кольца. Теорема Артина – Веддербёрна о строении простых и полупростых артиновых колец.
  - Конечные поля, их подполя и автоморфизмы. Строение мультипликативной группы конечного поля. Теорема Веддербёрна о коммутативности конечных тел.
  - Алгебраические расширения полей. Теорема о примитивном элементе для конечных расширений полей. Поле разложения многочлена. Группа Галуа. Основная теорема теории Галуа.
  - Алгебры над полем действительных чисел. Алгебраическая замкнутость поля комплексных чисел. Кватернионы. Теорема

---

Фробениуса.

- Алгебры Ли. Теорема Пуанкаре – Биркгофа – Витта об универсальной обёртывающей алгебре.
- Квадратичный закон взаимности.
- Первообразные корни и индексы.
- Неравенства Чебышёва для функции  $\Psi(x)$ . Асимптотический закон распределения простых чисел.
- Приближение вещественных чисел рациональными дробями. Теорема Лиувилля о приближении алгебраических чисел рациональными дробями. Примеры трансцендентных чисел. Трансцендентность чисел  $e$  и  $\pi$ .

## Дискретная математика

- Формальные языки. Задание языков грамматиками. Классы языков и грамматик. Иерархия Хомского.
- Конечные автоматы, автоматные грамматики, регулярные выражения. Эквивалентность перечисленных способов задания языков. Лемма о разрастании для автоматных языков. Детерминированные и недетерминированные автоматы. Детерминизация конечных автоматов.
- Контекстно-свободные грамматики и языки. Автоматы с магазинной памятью. Связь автоматов с магазинной памятью и контекстно-свободных грамматик. Лемма Огдена о разрастании для контекстно-свободных языков. Иерархии контекстно-свободных грамматик: LR- и LL-грамматики. Детерминированные контекстно-свободные языки.

- 
- Булевы функции. Представление булевых функций при помощи КНФ, ДНФ и многочленов Жегалкина. Сокращённые ДНФ. Проблема полноты множества булевых функций. Замкнутые классы булевых функций. Классы сохраняющих ноль и единицу, самодвойственных, линейных и монотонных функций. Теорема Поста о полноте множества булевых функций.
  - Эйлеровы и полуэйлеровы графы. Плоские и планарные графы. Развёртка многогранника в плоский граф. Формула Эйлера для плоских графов. Теорема Понтрягина – Куратовского о планарных графах. Хроматическое число графа. Двудольные графы. Раскраска плоских графов. Теорема Рамсея для конечных и бесконечных графов. NP-полные задачи для графов: гамильтонов цикл, раскраска, клика.
  - Алфавитное кодирование. Критерий Маркова однозначности декодирования. Неравенство Крафта – Макмиллана для длин кодовых слов. Оптимальное кодирование. Построение оптимальных кодов.
  - Коды, исправляющие ошибки. Граница упаковки, критерии количества обнаруженных и исправленных ошибок. Коды Хемминга, исправляющие единичную ошибку. Групповые и линейные коды. NP-полнота задач декодирования в общем случае. Полиномиальные коды. Коды Боуза – Чоудхури – Хоквингема.



---

## Литература

- [1] Бахтурин Ю. А. Основные структуры современной алгебры / Бахтурин Юрий Александрович. — Москва : Наука, 1990. — 318 с. ; 22 см. — Библиогр.: с. 307–309. — Указ. обозначений, предм.: с. 310–318. — ISBN 5-02-014290-5 (в пер.) : 3.90.
- [2] Берлекэмп Э. Алгебраическая теория кодирования / Пер. с англ. И. И. Грушко ; Под ред. С. Д. Бермана. — Москва : Мир, 1971. — 477 с. : черт.; 22 см.
- [3] Булос Дж. Вычислимость и логика / Дж. Булос, Р. Джеффри ; пер. с англ. В. А. Душского, Е. Ю. Ногиной ; под ред. С. Н. Артемова. — Москва : Мир, 1994. — 396 с. — Указ. имен. и предм.: с. 388–394. — ISBN 5-03-003067-0 : 7 500-00.
- [4] Бухштаб А. А. Теория чисел : учебное пособие для вузов. — 5-е изд., стер. — Санкт-Петербург : Лань, 2020. — 384 с. — ISBN 978-5-8114-5836-3.
- [5] Ван-дер-Варден Б. Л. Алгебра / Ван-дер-Варден Бартел Лендерт; пер. с нем. А. А. Бельского ; под ред. Ю. И. Мерзлякова. — 2-е изд. — Москва : Наука, 1979. — 623, [1] с. — Предм. указ.: с. 608–623. — 3.00.
- [6] Галочкин А. И. Введение в теорию чисел : Учеб. пособие / Галочкин Александр Иванович, Нестеренко Юрий Валентинович, Шидловский Андрей Борисович; Под ред. А. Б. Шидловского. — 2-е изд. — Москва : Изд-во Моск. ун-та, 1995. — 158, [1] с. : ил. — Библиогр.: с. 159. — ISBN 5-211-03075-3 : 7000.

- 
- [7] Гэри М. Вычислительные машины и труднорешаемые задачи / Гэри Майкл, Джонсон Дэвид; пер. с англ. Е. В. Левнера, М. А. Фрумкина. — Москва : Мир, 1982. — 416 с. : ил. ; 22 см.
- [8] Дехтярь М. И. Лекции по дискретной математике : Учебник / М. И. Дехтярь, С. М. Дудаков, Б. Н. Карлов. — 3-е издание, исправленное и дополненное. — Тверь : Тверской государственный университет, 2021. — 528 с. — EDN SEOZYF.
- [9] Дудаков С. М. Основы теории моделей : Учебник / С. М. Дудаков. — Тверь : Тверской государственный университет, 2013. — 480 с. — EDN QKEQSM.
- [10] Ленг С. Алгебра / Ленг Серж; пер. с англ. Е. С. Голода ; под ред. А. И. Кострикина. — Москва : Мир, 1968. — 564 с. — Библиогр.: с. 14 (14 назв.). — Указ.: с. 553–560. — 7500.00.
- [11] Столбоушкин А. П. Математические основания информатики / Столбоушкин Алексей Петрович, Тайцлин Михаил Александрович; ФГБОУ ВПО «Твер. гос. ун-т». — Тверь : Тверской государственный университет, 2013.