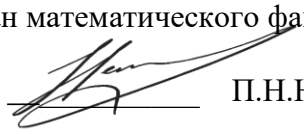
МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Ярославский государственный университет им. П.Г. Демидова

Кафедра компьютерной безопасности и математических методов обработки информации

УТВЕРЖДАЮ

Декан математического факультета


П.Н.Нестеров

«18» мая 2021 г.

Рабочая программа дисциплины
«Дискретные функции»

Направление подготовки
10.06.01 Информационная безопасность

Направленность (профиль)
«Методы и системы защиты информации,
информационная безопасность»

Форма обучения очная

Программа рассмотрена
на заседании кафедры компьютерной безопасности
и математических методов обработки информации
от «16» апреля 2021 года, протокол № 8

Ярославль

1. Цели освоения дисциплины

Дисциплина «Дискретные функции» обеспечивает приобретение фундаментальных и профессиональных знаний, умений и навыков, содействует дальнейшей фундаментализации образования, развитию логического мышления и формированию математического и общенаучного мировоззрения. Целью изучения дисциплины является овладение базовыми понятиями и методами теории дискретных функций, ознакомление с их применениями в области обеспечения информационной безопасности, ознакомление с базовыми подходами к оценке сложности задания и сложности вычисления дискретной функции.

2. Место дисциплины в структуре программы аспирантуры

Дисциплина «Дискретные функции» является факультативной дисциплиной вариативной части. Она играет важную роль для общематематической и общепрофессиональной подготовки специалиста. При ее изучении используются знания, полученные при изучении таких математических дисциплин, как “Алгебра”, "Теория чисел", "Дискретная математика", "Информатика" и "Математическая логика и теория алгоритмов".

3. Планируемые результаты обучения по дисциплине – знания, умения, навыки и (или) опыт деятельности, характеризующие этапы формирования компетенций и обеспечивающие достижение планируемых результатов освоения программы аспирантуры, и критерии их оценивания

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Общепрофессиональные компетенции:

- способностью формулировать научные задачи в области обеспечения информационной безопасности, применять для их решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность (ОПК-1);
- способностью разрабатывать частные методы исследования и применять их в самостоятельной научно-исследовательской деятельности для решения конкретных исследовательских задач в области обеспечения информационной безопасности (ОПК-2);

Результаты обучения выпускника формулируются в следующих категориях:
«знать» – означает способность выпускника воспроизводить учебный материал с требуемой степенью научной точности (формулировать определение, с достаточной полнотой описывать процесс и явление);
«уметь» – означает способность выпускника решать типовые (адаптированные) задачи на основе воспроизведения алгоритма решения и его применения в конкретных стандартных условиях;
«владеть» – означает способность выпускника решать усложненные, в том числе комплексные задачи. Задачи данного уровня решаются на основе ранее приобретенных знаний и умений, с их трансформацией и применением в новых нетиповых условиях.

Код	Планируемые результаты	Критерии оценивания результатов обучения		
		Пороговый	Продвинутый	Высокий

компетенции	обучения	уровень	уровень	Уровень
способностью формулировать научные задачи в области обеспечения информационной безопасности, применять для их решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность (ОПК-1)	**Знать:** - методологию научного познания в области физико-математических и технических наук (З-7.1); - научные подходы к обеспечению информационной безопасности и характеристику ее составляющих (З-7.2); - научную классификацию источников и угроз информационной безопасности (З-7.3). **Уметь:** - обоснованно классифицировать защищаемую информацию по видам тайны и степени конфиденциальности (У-7.1); - обоснованно классифицировать и оценивать угрозы информационной безопасности компьютерных систем (У-7.2). **Владеть:** - специальной профессиональной терминологией в области информационной безопасности (В-7.1); - научно обоснованными методами обеспечения	**Знает:** - методологию научного познания в области физико-математических и технических наук (З-7.1); - научные подходы к обеспечению информационной безопасности и характеристику ее составляющих (З-7.2); - научную классификацию источников и угроз информационной безопасности (З-7.3); - основные понятия, результаты и методы теории дискретных функций.	**Знает:** - методологию научного познания в области физико-математических и технических наук (З-7.1); - научные подходы к обеспечению информационной безопасности и характеристику ее составляющих (З-7.2); - научную классификацию источников и угроз информационной безопасности (З-7.3); - основные понятия, результаты и методы теории дискретных функций. **Умеет:** - обоснованно классифицировать защищаемую информацию по видам тайны и степени конфиденциальности (У-7.1); - обоснованно классифицировать и оценивать угрозы информационной безопасности компьютерных систем (У-7.2); - оценивать сложность задания и	**Знает:** - методологию научного познания в области физико-математических и технических наук (З-7.1); - научные подходы к обеспечению информационной безопасности и характеристику ее составляющих (З-7.2); - научную классификацию источников и угроз информационной безопасности (З-7.3). - основные понятия, результаты и методы теории дискретных функций. **Умеет:** - обоснованно классифицировать защищаемую информацию по видам тайны и степени конфиденциальности (У-7.1); - обоснованно классифицировать и оценивать угрозы информационной безопасности компьютерных систем (У-7.2); - оценивать сложность задания и вычисления дискретных функций.

	информационной безопасности и построения систем защиты информации от несанкционированного доступа (В-7.2).		вычисления дискретных функций.	**Владеет:** - специальной профессиональной терминологией в области информационной безопасности (В-7.1); - научно обоснованными методами обеспечения информационной безопасности и построения систем защиты информации от несанкционированного доступа (В-7.2).
способностью разрабатывать частные методы исследования и применять их в самостоятельной научно-исследовательской деятельности для решения конкретных исследовательских задач в области обеспечения информационной безопасности (ОПК-2)	**Знать:** - принципы и инструментарий научно-исследовательской деятельности в области обеспечения информационной безопасности (З-8.1); - средства и методы научного исследования (З-8.2); - математический аппарат и инструментарий обработки результатов исследований (З-8.3). **Уметь:** - применять философско-методологические принципы и установки для решения частных научных задач (У-8.1); - применять систему	**Знает:** - принципы и инструментарий научно-исследовательской деятельности в области обеспечения информационной безопасности (З-8.1); - средства и методы научного исследования (З-8.2); - математический аппарат и инструментарий обработки результатов исследований (З-8.3); основные понятия теории булевых функций и схем из функциональ	**Знает:** - принципы и инструментарий научно-исследовательской деятельности в области обеспечения информационной безопасности (З-8.1); - средства и методы научного исследования (З-8.2); - математический аппарат и инструментарий обработки результатов исследований (З-8.3); основные понятия теории булевых функций и схем из функциональных элементов. **Умеет:**	**Знает:** - принципы и инструментарий научно-исследовательской деятельности в области обеспечения информационной безопасности (З-8.1); - средства и методы научного исследования (З-8.2); - математический аппарат и инструментарий обработки результатов исследований (З-8.3); основные понятия теории булевых функций и схем из функциональных элементов. **Умеет:** - применять философско-методологически

	математических моделей и методов при осуществлении научно-исследовательской деятельности (У-8.2); - оценивать достоверность результатов, полученных в ходе исследований (У-8.3). **Владеть:** - методами проведения теоретических исследований (В-8.1); - методами планирования и проведения экспериментов (В-8.2); - методами использования средств обработки результатов исследований (В-8.3).	ных элементов.	- применять философско-методологические принципы и установки для решения частных научных задач (У-8.1); - применять систему математических моделей и методов при осуществлении научно-исследовательской деятельности (У-8.2); - оценивать достоверность результатов, полученных в ходе исследований (У-8.3).	е принципы и установки для решения частных научных задач (У-8.1); - применять систему математических моделей и методов при осуществлении научно-исследовательской деятельности (У-8.2); - оценивать достоверность результатов, полученных в ходе исследований (У-8.3). **Владеет:** - методами проведения теоретических исследований (В-8.1); - методами планирования и проведения экспериментов (В-8.2);- методами использования средств обработки результатов исследований (В-8.3).

4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 1 зачетная единица, 36 акад.часов

Дисциплина изучается в течение пятого семестра. Формой итоговой промежуточной аттестации по дисциплине является зачет.

№ п/п	Темы (разделы) дисциплины, их содержание	Семестр	Виды учебных занятий и их трудоемкость (в академических часах)	Формы текущего контроля успеваемости

			лекции	практические	лабораторные	консультации	самостоятельная работа	**Форма промежуточной аттестации** ***(по семестрам)***
		5						
1	Булевы функции.		1				4	
2	Функции к-значной логики.						4	
3	Схемы из функциональных элементов.						4	
4	Автоматные функции.		1				4	
5	Вычислимые по Тьюрингу функции.						4	
6	Частично рекурсивные функции.		1				4	
7	Универсальные функции.						4	
8	Функции, характеризующие сложность алгоритмов.		1				4	
		5						Зачет
	Всего		**4**				**32**	

Содержание разделов программы дисциплины
"Дискретные функции"

Тема № 1. Булевы функции.

Способы задания булевых функций. Существенные и несущественные переменные. Термы. Задание булевых функций термами. Элементарные функции и их свойства. Разложение функций по переменной.

Совершенные дизъюнктивная и конъюнктивная нормальные формы.

Полиномы Жегалкина. Представление булевых функций полиномами.

Замыкание произвольного класса булевых функций. Свойства операции замыкания. Замкнутые классы. Полные системы булевых функций.

Классы C_0 и C_1.

Линейные функции. Лемма о нелинейной функции.

Самодвойственные функции. Принцип двойственности. Лемма о несамодвойственной функции.

Монотонные функции. Лемма о немонотонной функции.

Теорема Поста о полноте систем булевых функций.

Предполные классы. Базисы, примеры базисов.

Дизъюнктивные нормальные формы (ДНФ). Тупиковая, минимальная и сокращенная ДНФ. Геометрическая интерпретация. Алгоритм нахождения всех минимальных ДНФ. Свойство сокращенной ДНФ для монотонных булевых функций. Методы построения сокращенной ДНФ: градиентный алгоритм, локальные алгоритмы.

Тема № 2. Функции к-значной логики.

Элементарные функции.

Полнота систем функций. Алгоритм распознавания полноты конечных систем функций в P_k.

Представление функций из P_k полиномами.

Особенности функций к-значной логики. Пример замкнутого класса в P_k, не имеющего базиса. Пример замкнутого класса в P_k, имеющего счетный базис. Пример континуального семейства замкнутых классов в P_k.

Теорема Кузнецова о функциональной полноте в P_k.

Существенные функции. Теорема Слупецкого.

Тема № 3. Схемы из функциональных элементов.

Сложность схем. Синтез схем из функциональных элементов для индивидуальных функций.

Схемы сложения и умножения n-разрядных чисел.

Простейшие универсальные методы синтеза. Метод Шеннона.

Мощностной метод получения оценок сложности.

Функция L (n). Порядок роста функции L (n).

Асимптотически наилучший метод синтеза схем из функциональных элементов в базисе {V, &, -- }. Асимптотика функции L (n).

Контактные схемы. Простейшие методы синтеза. Контактное дерево.

Универсальный многополюсник. Метод Шеннона для контактных схем.

Нижняя оценка сложности линейной функции в классе контактных схем (метод Кардо).

Тема № 4. Автоматные функции.

Конечные автоматы с выходом и без выхода. Входной, выходной и внутренний алфавиты. Функция переходов и выхода. Эквивалентность состояний автомата. Теорема об эквивалентности состояний конечного автомата. Эквивалентность автоматов. Построение автомата, эквивалентного данному, с минимальным числом состояний. Преобразование автоматными функциями периодических последовательностей.

. Операция суперпозиции. Отсутствие полных относительно операций суперпозиции конечных систем автоматных функций.

Схемы из логических элементов и элементов задержки. Реализация автоматных функций.

Регулярные выражения и регулярные языки. Теорема С. Клини.

Пример нерегулярного языка.

Тема № 5. Вычислимые по Тьюрингу функции.

Машины Тьюринга. Внешний и внутренний алфавиты, команды и программа машины Тьюринга. Различные варианты машин Тьюринга: многоленточные и одноленточные, с одномерной и многомерной лентой, с потенциально бесконечной в обе стороны лентой, с непродолжаемой влево лентой и т. д.

Словарные алгоритмы, реализуемые машинами Тьюринга. Вычислимые по Тьюрингу функции. Правильная вычислимость по Тьюрингу. Вычислимость по Тьюрингу элементарных теоретико-числовых функций.

Разрешимые и перечислимые множества слов.

Операции над машинами Тьюринга. Композиция машин Тьюринга. Разветвление. Зацикливание. Диаграммы машин Тьюринга. Циклический сдвиг, копирование.

Тезис Тьюринга. Замкнутость класса правильно вычислимых по Тьюрингу функций относительно операций суперпозиции, примитивной рекурсии и минимизации. Тезис А.Тьюринга.

Тема № 6. Частично рекурсивные функции.

Простейшие (исходные) функции. Операции суперпозиции, примитивной рекурсии и минимизации.

Примитивно рекурсивные функции. Примеры примитивно рекурсивных теоретико-числовых функций.

Частично рекурсивные и рекурсивные функции, примеры.

Операции над примитивными, рекурсивными и частично рекурсивными функциями. Тезис А. Черча.

Нумерация пар и n-ок натуральных чисел. Нумерационные функции.

Рекурсивные и рекурсивно перечислимые множества и предикаты. Теорема Э. Поста.

Теорема о графике функции.

Правильная вычислимость по Тьюрингу любой частично рекурсивной функции.

Тема 7. Универсальные функции.

Арифметизация теории машин Тьюринга. Геделева нумерация слов в конечных и счетных алфавитах.

Нумерация команд и программ машин Тьюринга. Нумерация конфигураций.

Построение примитивно рекурсивных функций, описывающих работу машин Тьюринга.

Частичная рекурсивность любой вычислимой по Тьюрингу функции.

Универсальные частично рекурсивные функции.

Неразрешимость проблем останова, самоприменимости и бессмертия для машин Тьюринга.

Нормальная форма С. Клини.

Универсальные машины Тьюринга.

Неразрешимые алгоритмические проблемы. Неразрешимость проблемы выводимости для полусистем Туэ.

Неразрешимость проблемы равенства для полугрупп и групп.

Теоремы А.А. Маркова и С.И. Адяна об алгоритмической неразрешимости проблем распознавания полугрупповых и групповых свойств. Неразрешимые проблемы в математической логике.

Тема № 8. Функции, характеризующие сложность алгоритмов.

Многоленточные машины Тьюринга: внешний и внутренний алфавиты, программы.

Сложностные характеристики работы машины Тьюринга: временная (число шагов) и емкостная (объем памяти), связь между ними.

Сложностные характеристики работы машины Тьюринга в худшем случае: временная и емкостная сигнализирующие функции (сложности, характеристики алгоритма), связь между ними.

Сложностные классы. Другие сложностные характеристики.

Сложность описания нормального алгорифма А.А.Маркова.

Сложность конечных объектов по А.Н.Колмогорову.

5. Образовательные технологии, используемые при осуществлении образовательного процесса по дисциплине

В процессе обучения используются следующие образовательные технологии:

Вводная лекция – дает первое целостное представление о дисциплине и ориентирует студента в системе изучения данной дисциплины. Студенты знакомятся с назначением и задачами курса, его ролью и местом в системе учебных дисциплин и в системе подготовки в целом. Дается краткий обзор курса, история развития науки и практики, достижения в этой сфере, имена известных ученых, излагаются перспективные направления исследований. На этой лекции высказываются методические и организационные особенности работы в рамках данной дисциплины, а также дается анализ рекомендуемой учебно-методической литературы.

Академическая лекция (или лекция общего курса) – последовательное изложение материала, осуществляемое преимущественно в виде монолога преподавателя. Требования к академической лекции: современный научный уровень и насыщенная информативность, убедительная аргументация, доступная и понятная речь, четкая структура и логика, наличие ярких примеров, научных доказательств, обоснований, фактов.

Практическое занятие – занятие, посвященное освоению конкретных умений и навыков и закреплению полученных на лекции знаний.

6. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения и информационных справочных систем (при необходимости).

В процессе осуществления образовательного процесса используются:

– для формирования текстов материалов для промежуточной и текущей аттестации – программы Microsoft Office, издательская система MikTex;

– для поиска учебной литературы библиотеки ЯрГУ – Автоматизированная библиотечная информационная система "БУКИ-NEXT" (АБИС "Буки-Next").

7. Перечень основной и дополнительной учебной литературы, необходимых для освоения дисциплины

а) основная литература

1. Ахо А., Хопкрофт Дж., Ульман Дж. Построение и анализ вычислительных алгоритмов. М.: Мир, 1983.
2. Гэри М., Джонсон Д. Вычислительные машины и труднорешаемые задачи.М.: Мир, 1979.
3. Дурнев, В. Г., Материалы по дисциплине "Теория алгоритмов и сложность вычислений" : метод. указания / В. Г. Дурнев ; Яросл. гос. ун-т, Ярославль, ЯрГУ, 2010, 40с
4. Дурнев, В. Г., Элементы теории алгоритмов : учеб. пособие для вузов / В. Г. Дурнев ; Яросл. гос. ун-т, Ярославль, ЯрГУ, 2008, 247с
5. Дурнев, В. Г., Элементы теории множеств и математической логики : учеб. пособие для вузов / В. Г. Дурнев ; Яросл. гос. ун-т, Ярославль, ЯрГУ, 2009, 411с
6. Кормен, Т., Алгоритмы : построение и анализ : учеб. пособие / Т. Кормен, Ч. Лейзерсон, Р. Ривест, М., МЦНМО, 2001, 955с
7. Мальцев, А.И. Алгоритмы и рекурсивные функции / А.И. Мальцев. М.: Наука, 1986.
8. Марков, А.А., Нагорный Н.М. Теория алгорифмов / А.А. Марков, М.: Наука, 1984.

9. Глухов М.М. Задачи и упражнения по математической логике, дискретным функциям и теории алгоритмов: учеб. пособие для вузов / М. М. Глухов, О. А. Козлитин, В. А. Шапошников, А. Б. Шишков. СПб., Лань, 2008, 111 с.
10. Лавров И.А. Задачи по теории множеств, математической логики и теории алгоритмов / И.А. Лавров, Л.Л. Максимова. М.: Наука. 1984. 287 с.

б) дополнительная литература

1. Адян С.И., Дурнев В.Г. Алгоритмические проблемы для групп и полугрупп //Успехи матем. наук. 2000. Том 55.С.3-94.
2. Булос Дж., Джеффри Р. Вычислимость и логика. М.: Мир, 1994.
3. Катленд Н. Вычислимость. Введение в теорию рекурсивных функций. М.: Мир, 1983.
4. Колмогоров А.Н., Успенский В.А. К определению понятия алгоритма //Успехи мат. наук. 1958. Т. 13. Вып. 4. С.3-28.
5. Манин Ю.И. Вычислимое и невычислимое. М.: Советское радио, 1979.
6. Марков А.А. Невозможность некоторых алгоритмов в теории ассоциативных систем // ДАН СССР. 1947. Том55. С.587-590.
7. Матиясевич Ю.В. Диофантовость перечислимых множеств //Докл. АН СССР. 1970. Т. 130. С.495-498.
8. Мендельсон Э. Введение в математическую логику. М.: Наука, 1976.
9. Трахтенброт Б.А. Алгоритмы и вычислительные автоматы. М.: Советское радио, 1974.
10. Эббинхауз Г.Д., Якобс К., Ман Ф.К., Хермес Г. Машины Тьюринга и рекурсивные функции. М.: Мир, 1972.
11. Post, E. Intoduction to a general theory of elementary propositions //Amer. J. Math. 1921. Vol.43.P.163-185.
12. Post E.L. Finite combinatory processes - formulation 1 //Journal of Symbolic Logic. 1936. Vol.1. P.103-105.
13. Post E.L. A variant of a recursively unsolvable problem //Bull. Amer. Math. Soc. 1946. Vol.52. P.264-268.
14. Post E.L. Recursive unsolvability of a problem of Thue //J. Symbol Log. 1947. Vol.12. P.1-11.
15. Rado T. On non-computable functions //Bell System Technical Journal. 1962. P.877-884.
16. Turing A.M. On computable numbers, with an application to the Entscheidugsproblem //Proceedings of London Mathematical Society. Ser. 2. 1936. Vol.42. P.230-265.

в) ресурсы сети «Интернет»

1.Электронные каталоги НБ ЯрГУ

(http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php) содержат библиографические записи всех видов документов, составляющих фонд библиотеки, на русском и иностранных языках.

2. Личный кабинет (http://lib.uniyar.ac.ru/opac/bk_login.php) возможность получения on-line доступа к списку выданной в автоматизированном режиме литературы, просмотра и копирования электронных версий изданий сотрудников университета (учеб. и метод. пособия, тексты лекций и т.д.) Для работы в «Личном кабинете» необходимо зайти на сайт Научной библиотеки ЯрГУ с любой точки, имеющей доступ в Internet, в пункт меню *«Электронный каталог»*; пройти процедуру авторизации, выбрав вкладку *«Авторизация»*, и заполнить представленные поля информации.

3.Электронная библиотека учебных материалов ЯрГУ

(http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php) содержит более 2500 полных текстов учебных и учебно-методических материалов по основным изучаемым дисциплинам, изданных в университете. Доступ в сети университета, либо по логину/паролю.

4.Электронный архив ЯрГУ

(http://elar.uniyar.ac.ru/jspui/community-list) представляет собой коллекцию полнотекстовых электронных публикаций в области научных исследований. База данных предназначена для использования в учебных и научных целях, облегчая доступ к информации о научных работах и их содержанию.

5. Электронная картотека «Книгообеспеченность»

(http://www.lib.uniyar.ac.ru/opac/bk_bookreq_find.php)

раскрывает учебный фонд научной библиотеки ЯрГУ, предоставляет оперативную информацию о состоянии книгообеспеченности дисциплин основной и дополнительной литературой, а также цикла дисциплин и специальностей. Электронная картотека «Книгообеспеченность» доступна в сети университета и через Личный кабинет.

Русскоязычные электронные ресурсы (внешние)

1. Научная электронная библиотека (НЭБ) (http://elibrary.ru) – это крупнейший российский информационный портал, содержащий рефераты и полные тексты более 12 млн. научных статей и публикаций. **ЯрГУ выписывает в электронном виде 66 журналов,** более 2 500 наименований журналов на английском и русском языках находятся в свободном доступе. Для работы с полными текстами необходимо зарегистрироваться. Доступ к полным текстам журналов в сети университета.

2. Электронная библиотека диссертаций Российской государственной библиотеки (http://diss.rsl.ru) содержит более 580 000 полных текстов диссертаций и авторефератов. Доступ осуществляется в сети университета.

8. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине включает в свой состав специальные помещения:

-учебные аудитории для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации;

-помещения для самостоятельной работы;

-помещения для хранения и профилактического обслуживания оборудования.

Специальные помещения укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления информации большой аудитории.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации.

Число посадочных мест в лекционной аудитории больше либо равно списочному составу потока, а в аудитории для практических занятий (семинаров) – списочному составу группы обучающихся.

Автор(ы) :

Зав. кафедрой компьютерной безопасности и математических методов обработки информации, д.ф.-м.н. Дурнев В.Г.

Приложение к №1 рабочей программе дисциплины
«Дискретные функции»

Оценочные средства
для проведения текущей и/или промежуточной аттестации аспирантов
по дисциплине

1. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Домашние задания по теме № 5 **Вычислимые по Тьюрингу функции."**

Задания для самостоятельного решения № 1 - 12 из параграфа 2 части III сборника задач Лавров И.А. Задачи по теории множеств, математической логики и теории алгоритмов / И.А. Лавров, Л.Л. Максимова. М.: Наука. 1984. 287 с.

Домашние задания по теме № 6 "**Частично рекурсивные функции."**

Задания для самостоятельного решения № 1 - 15 из параграфа 1 части III сборника задач Лавров И.А. Задачи по теории множеств, математической логики и теории алгоритмов / И.А. Лавров, Л.Л. Максимова. М.: Наука. 1984. 287 с.

Задания для самостоятельного решения № 16 - 30 из параграфа 1 части III сборника задач Лавров И.А. Задачи по теории множеств, математической логики и теории алгоритмов / И.А. Лавров, Л.Л. Максимова. М.: Наука. 1984. 287 с.

Домашние задания по теме № 8 "**Функции, характеризующие сложность "**

Задания для самостоятельного решения № 16.1 - 16.12 из параграфа 16 главы 3 сборника задач Глухов М.М. Задачи и упражнения по математической логике, дискретным функциям и теории алгоритмов: учеб. пособие для вузов / М. М. Глухов, О. А. Козлитин, В. А. Шапошников, А. Б. Шишков. СПб., Лань, 2008, 111 с.

Задания для самостоятельного решения № 9 - 25 из параграфа 2 части III сборника задач Лавров И.А. Задачи по теории множеств, математической логики и теории алгоритмов / И.А. Лавров, Л.Л. Максимова. М.: Наука. 1984. 287 с.

Задания для самостоятельного решения № 16.13 - 16.25 из параграфа 16 главы 3 сборника задач Глухов М.М. Задачи и упражнения по математической логике, дискретным функциям и теории алгоритмов: учеб. пособие для вузов / М. М. Глухов, О. А. Козлитин, В. А. Шапошников, А. Б. Шишков. СПб., Лань, 2008, 111 с.

Задания для самостоятельного решения № 16.1 - 16.26 из параграфа 16 главы 3 сборника задач Глухов М.М. Задачи и упражнения по математической логике, дискретным функциям и теории алгоритмов: учеб. пособие для вузов / М. М. Глухов, О. А. Козлитин, В. А. Шапошников, А. Б. Шишков. СПб., Лань, 2008, 111 с.

1.1 Список вопросов и (или) заданий для проведения промежуточной аттестации

Вопросы к зачету по дисциплине
"Дискретные функции "

(5 семестр)

Тема № 1. Булевы функции.

Способы задания булевых функций. Существенные и несущественные переменные. Термы. Задание булевых функций термами. Элементарные функции и их свойства. Разложение функций по переменной.

Совершенные дизъюнктивная и конъюнктивная нормальные формы.

Полиномы Жегалкина. Представление булевых функций полиномами.

Замыкание произвольного класса булевых функций. Свойства операции замыкания. Замкнутые классы. Полные системы булевых функций.

Классы C_0 и C_1.

Линейные функции. Лемма о нелинейной функции.

Самодвойственные функции. Принцип двойственности. Лемма о несамодвойственной функции.

Монотонные функции. Лемма о немонотонной функции.

Теорема Поста о полноте систем булевых функций.

Предполные классы. Базисы, примеры базисов.

Дизъюнктивные нормальные формы (ДНФ). Тупиковая, минимальная и сокращенная ДНФ. Геометрическая интерпретация. Алгоритм нахождения всех минимальных ДНФ. Свойство сокращенной ДНФ для монотонных булевых функций. Методы построения сокращенной ДНФ: градиентный алгоритм, локальные алгоритмы.

Тема № 2. Функции к-значной логики.

Элементарные функции.

Полнота систем функций. Алгоритм распознавания полноты конечных систем функций в P_k.

Представление функций из P_k полиномами.

Особенности функций к-значной логики. Пример замкнутого класса в P_k, не имеющего базиса. Пример замкнутого класса в P_k, имеющего счетный базис. Пример континуального семейства замкнутых классов в P_k.

Теорема Кузнецова о функциональной полноте в P_k.

Существенные функции. Теорема Слупецкого.

Тема № 3. Схемы из функциональных элементов.

Сложность схем. Синтез схем из функциональных элементов для индивидуальных функций.

Схемы сложения и умножения n-разрядных чисел.

Простейшие универсальные методы синтеза. Метод Шеннона.

Мощностной метод получения оценок сложности.

Функция L (n). Порядок роста функции L (n).

Асимптотически наилучший метод синтеза схем из функциональных элементов в базисе {V, &, -- }. Асимптотика функции L (n).

Контактные схемы. Простейшие методы синтеза. Контактное дерево.

Универсальный многополюсник. Метод Шеннона для контактных схем.

Нижняя оценка сложности линейной функции в классе контактных схем (метод Кардо).

Тема № 4. Автоматные функции.

Конечные автоматы с выходом и без выхода. Входной, выходной и внутренний

алфавиты. Функция переходов и выхода. Эквивалентность состояний автомата. Теорема об эквивалентности состояний конечного автомата. Эквивалентность автоматов. Построение автомата, эквивалентного данному, с минимальным числом состояний. Преобразование автоматными функциями периодических последовательностей.

. Операция суперпозиции. Отсутствие полных относительно операций суперпозиции конечных систем автоматных функций.

Схемы из логических элементов и элементов задержки. Реализация автоматных функций.

Регулярные выражения и регулярные языки. Теорема С. Клини.

Пример нерегулярного языка.

Тема № 5. Вычислимые по Тьюрингу функции.

Машины Тьюринга. Внешний и внутренний алфавиты, команды и программа машины Тьюринга. Различные варианты машин Тьюринга: многоленточные и одноленточные, с одномерной и многомерной лентой, с потенциально бесконечной в обе стороны лентой, с непродолжаемой влево лентой и т. д.

Словарные алгоритмы, реализуемые машинами Тьюринга. Вычислимые по Тьюрингу функции. Правильная вычислимость по Тьюрингу. Вычислимость по Тьюрингу элементарных теоретико-числовых функций.

Разрешимые и перечислимые множества слов.

Операции над машинами Тьюринга. Композиция машин Тьюринга. Разветвление. Зацикливание. Диаграммы машин Тьюринга. Циклический сдвиг, копирование.

Тезис Тьюринга. Замкнутость класса правильно вычислимых по Тьюрингу функций относительно операций суперпозиции, примитивной рекурсии и минимизации. Тезис А.Тьюринга.

Тема № 6. Частично рекурсивные функции.

Простейшие (исходные) функции. Операции суперпозиции, примитивной рекурсии и минимизации.

Примитивно рекурсивные функции. Примеры примитивно рекурсивных теоретико-числовых функций.

Частично рекурсивные и рекурсивные функции, примеры.

Операции над примитивными, рекурсивными и частично рекурсивными функциями. Тезис А. Черча.

Нумерация пар и n-ок натуральных чисел. Нумерационные функции.

Рекурсивные и рекурсивно перечислимые множества и предикаты. Теорема Э. Поста.

Теорема о графике функции.

Правильная вычислимость по Тьюрингу любой частично рекурсивной функции.

Тема 7. Универсальные функции.

Арифметизация теории машин Тьюринга. Геделева нумерация слов в конечных и счетных алфавитах.

Нумерация команд и программ машин Тьюринга. Нумерация конфигураций.

Построение примитивно рекурсивных функций, описывающих работу машин Тьюринга.

Частичная рекурсивность любой вычислимой по Тьюрингу функции.

Универсальные частично рекурсивные функции.

Неразрешимость проблем останова, самоприменимости и бессмертия для машин Тьюринга.

Нормальная форма С. Клини.

Универсальные машины Тьюринга.

Неразрешимые алгоритмические проблемы. Неразрешимость проблемы выводимости для полусистем Туэ.

Неразрешимость проблемы равенства для полугрупп и групп.

Теоремы А.А. Маркова и С.И. Адяна об алгоритмической неразрешимости проблем распознавания полугрупповых и групповых свойств. Неразрешимые проблемы в математической логике.

Тема № 8. Функции, характеризующие сложность алгоритмов.

Многоленточные машины Тьюринга: внешний и внутренний алфавиты, программы.

Сложностные характеристики работы машины Тьюринга: временная (число шагов) и емкостная (объем памяти), связь между ними.

Сложностные характеристики работы машины Тьюринга в худшем случае: временная и емкостная сигнализирующие функции (сложности, характеристики алгоритма), связь между ними.

Сложностные классы. Другие сложностные характеристики.

Сложность описания нормального алгорифма А.А.Маркова.

Сложность конечных объектов по А.Н.Колмогорову.

Приложение № 2 к рабочей программе дисциплины
«Дискретные функции»

Методические указания для аспирантов по освоению дисциплины

Для успешного освоения дисциплины важно самостоятельное изучение теоретического материала, решение достаточно большого набора хорошо подобранных задач, как в аудитории, так и самостоятельно в качестве домашних заданий. Примеры решения задач разбираются на практических занятиях, при необходимости по наиболее трудным темам проводятся дополнительные консультации. Основная цель решения задач – помочь усвоить фундаментальные понятия, методы и теоремы теории алгоритмов, научиться определять сложность вычислений. Для решения задач необходимо не только знать, но и понимать теоретический материал. Поэтому в процессе изучения дисциплины рекомендуется регулярная работа с рекомендованной литературой.

Большое внимание должно быть уделено выполнению домашней работы. В качестве заданий для самостоятельной работы дома аспирантам предлагаются задачи, аналогичные разобранным на практических занятиях или более сложные, которые являются результатом объединения нескольких базовых задач.

Для проверки и контроля усвоения теоретического материала, приобретенных практических навыков работы с основными понятиями в течение обучения проводятся мероприятия текущей аттестации в виде устного опроса на занятиях и консультациях и разбору некоторых заданий для самостоятельной работы.

Аспиранты сдают зачет во втором семестре. Зачет проводится на основании выполнения домашних заданий, контрольной работы и собеседования на основании списка вопросов к зачету, который охватывает полностью всю программу дисциплины.

Учебно-методическое обеспечение самостоятельной работы аспирантов по дисциплине

В качестве учебно-методического обеспечения рекомендуется использовать литературу, указанную в разделе № 7 данной рабочей программы