

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное учреждение
высшего профессионального образования
"Казанский (Приволжский) федеральный университет"
Институт вычислительной математики и информационных технологий



УТВЕРЖДАЮ

Проректор по образовательной деятельности КФУ

Проф. Тагорский Да



20__ г.

подписано электронно-цифровой подписью

Программа дисциплины

Вероятностные модели вычислений Б1.В.ДВ.4

Направление подготовки: 10.03.01 - Информационная безопасность

Профиль подготовки: Безопасность компьютерных систем

Квалификация выпускника: бакалавр

Форма обучения: очное

Язык обучения: русский

Автор(ы):

Гайнутдинова А.Ф.

Рецензент(ы):

Салимов Ф.И.

СОГЛАСОВАНО:

Заведующий(ая) кафедрой: Аблаев Ф. М.

Протокол заседания кафедры № ____ от "____" 201__ г

Учебно-методическая комиссия Института вычислительной математики и информационных технологий:

Протокол заседания УМК № ____ от "____" 201__ г

Регистрационный № 934717

Казань
2017

Содержание

1. Цели освоения дисциплины
2. Место дисциплины в структуре основной образовательной программы
3. Компетенции обучающегося, формируемые в результате освоения дисциплины /модуля
4. Структура и содержание дисциплины/ модуля
5. Образовательные технологии, включая интерактивные формы обучения
6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов
7. Литература
8. Интернет-ресурсы
9. Материально-техническое обеспечение дисциплины/модуля согласно утвержденному учебному плану

Программу дисциплины разработал(а)(и) доцент, к.н. Гайнутдинова А.Ф. кафедра теоретической кибернетики отделение фундаментальной информатики и информационных технологий , Aida.Gainutdinova@kpfu.ru

1. Цели освоения дисциплины

Данный курс предназначен для студентов-магистров первого года обучения. Целью данного курса является изучение различных детерминированных и вероятностных вычислительных моделей. Курс направлен на расширение и углубление образования студентов в области компьютерных наук, формирования у них системного мышления путем изучения подходов в проблематике построения дискретных и вероятностных вычислительных моделей, понимания проблем и современного состояния предметной области, умения анализировать и самостоятельно приобретать и применять новые знания и умения, формирование у студентов профессиональных компетенций.

Дискретные вычислительные модели могут быть классифицированы по объему используемой памяти как модели без памяти (схемы), модели с конечной памятью (автоматы), модели с потенциально бесконечной памятью (машины Тьюринга); по способу функционирования как детерминированные, недетерминированные, вероятностные модели.

Вычислительные модели также могут рассматриваться как формализация понятия алгоритм. Известно, что вычислительные задачи могут быть разбиты на классы в соответствии со сложностью их решения. Классы задач, которые могут быть решены на рассматриваемой вычислительной модели с определенными ограничениями на память и время составляют соответствующий класс сложности. Крайне важно понимать, каким образом соотносятся между собой основные сложностные классы, а также, какие вопросы в данной области на сегодняшний день пока не решены. Так, известно, что один из таких открытых вопросов о соотношении классов P и NP входит в список важнейших нерешенных проблем тысячелетия. Решение данной проблемы будет иметь важное значение для различных областей науки и практики.

В данном курсе рассматриваются такие вычислительные модели, как детерминированные, недетерминированные и вероятностные машины Тьюринга, автоматы и схемы из функциональных элементов. На основе моделей машин Тьюринга вводятся классы сложности, определяющие языки, распознаваемые с различными ограничениями на время и память. Рассматриваются соотношения между классами сложности и методы их доказательства. Приводятся примеры языков, принадлежащих рассматриваемым сложностным классам.

Для вероятностных вычислительных моделей рассматриваются классы сложности, определяемые различными критериями распознавания языков и соотношения между ними и детерминированными классами.

Также в курсе рассматривается понятие С-трудного и С-полного языка, признаки NP-полноты языков и методы доказательства NP-полноты. Рассматриваются однородные и неоднородные классы сложности, обсуждается разница между однородными и неоднородными вычислительными моделями.

Программа курса предусматривает лекции и практические занятия (28 часов). В самостоятельную работу студентов входит освоение теоретического материала, изучение основной литературы, знакомство с дополнительной литературой, выполнение домашних заданий и подготовка к экзамену.

Также в курсе рассматривается понятие С-трудного и С-полного языка, примеры NP-полноты языков и методы доказательства NP-полноты. Рассматриваются однородные и неоднородные классы сложности, обсуждается разница между однородными и неоднородными вычислительными моделями.

Программа курса предусматривает лекции. В самостоятельную работу студентов входит освоение теоретического материала, изучение основной литературы, знакомство с дополнительной литературой, выполнение домашних заданий и подготовка к зачету.

2. Место дисциплины в структуре основной образовательной программы высшего профессионального образования

Данная учебная дисциплина включена в раздел " Б1.В.ДВ.4 Дисциплины (модули)" основной образовательной программы 10.03.01 Информационная безопасность и относится к дисциплинам по выбору. Осваивается на 3 курсе, 6 семестр.

"Дискретные и вероятностные модели" входит в состав профессиональных дисциплин по выбору студента. Читается на 3 курсе, во 2 семестре.

Для освоения материала данного курса студент должен прослушать курсы "Дискретная математика", "Автоматы и грамматики", "Теория информации и кодирования", быть знаком с теорией сложности вычислений.

3. Компетенции обучающегося, формируемые в результате освоения дисциплины /модуля

В результате освоения дисциплины формируются следующие компетенции:

Шифр компетенции	Расшифровка приобретаемой компетенции
ОПК-2 (профессиональные компетенции)	способность применять соответствующий математический аппарат для решения профессиональных задач
ПК-10 (профессиональные компетенции)	способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности
ПК-2 (профессиональные компетенции)	способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач

В результате освоения дисциплины студент:

1. должен знать:

определения различных дискретных и вероятностных моделей вычислений (машин Тьюринга, автоматов, схем из функциональных элементов); то, каким образом производится обработка входных слов и распознавание языков в данных моделях; различия между классами рекурсивных и рекурсивно-перечислимых языков; определения основных сложностных классов для де-терминированных, недетерминированных и вероятностных машин Тьюринга (LSPACE, P, PSPACE, NP, EXPTIME, PP, BPP, RP, co-RP, ZPP); смысл понятий С-трудный и С-полный язык; различие между однородными и неоднородными вычислительными моделями;

2. должен уметь:

ориентироваться в области сложности вычислений, и в том, где применяются знания из этой области.

3. должен владеть:

приемами и методами доказательства принадлежности языков определенным классам сложности, методами доказательств соотношений между различными классами сложности, методами доказательства NP- полноты языков.

4. должен демонстрировать способность и готовность:

готовность и способность применять полученные знания на практике.

4. Структура и содержание дисциплины/ модуля

Общая трудоемкость дисциплины составляет 2 зачетных(ые) единиц(ы) 72 часа(ов).

Форма промежуточного контроля дисциплины зачет в 6 семестре.

Суммарно по дисциплине можно получить 100 баллов, из них текущая работа оценивается в 50 баллов, итоговая форма контроля - в 50 баллов. Минимальное количество для допуска к зачету 28 баллов.

86 баллов и более - "отлично" (отл.);

71-85 баллов - "хорошо" (хор.);

55-70 баллов - "удовлетворительно" (удов.);

54 балла и менее - "неудовлетворительно" (неуд.).

4.1 Структура и содержание аудиторной работы по дисциплине/ модулю

Тематический план дисциплины/модуля

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
1.	Тема 1. Алфавит, слова в алфавите, язык. Метод диагонализации. Вычислительные модели как формализация понятия алгоритм.	6	1	0	2	0	Письменное домашнее задание
2.	Тема 2. Детерминированная машина Тьюринга, распознавание слов, языков.	6	2	0	2	0	Письменное домашнее задание
3.	Тема 3. Тезис Черча. Классы сложности Time($f(n)$), Space($f(n)$). Теоремы о соотношении классов сложности Time($f(n)$) и Space($f(n)$).	6	3	0	2	0	Письменное домашнее задание
4.	Тема 4. Основные детерминированные классы сложности LSPACE, P, PSPACE, EXPTIME. Д	6	4	0	2	0	Письменная работа
5.	Тема 5. Определение конечного автомата. Теорема о соотношении классов сложности Reg и LSPACE.	6	5	0	2	0	Письменное домашнее задание

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
6.	Тема 6. Недетерминированные машины Тьюринга, представление слов, распознавание языков недетерминированной машиной Тьюринга.	6	6	0	2	0	Письменное домашнее задание
7.	Тема 7. Класс сложности NP.	6	7	0	2	0	Письменное домашнее задание
8.	Тема 8. Понятие полиномиальной сводимости языков. Свойства полиномиальной сводимости.	6	8	0	2	0	Письменная работа
9.	Тема 9. Понятие С-трудного и С-полного языка. NP-полный язык.	6	9	0	2	0	Письменное домашнее задание
10.	Тема 10. Доказательство NP-полноты.	6	10	0	2	0	Письменное домашнее задание
11.	Тема 11. Классы сложностей-дополнений.	6	11	0	2	0	Письменное домашнее задание
12.	Тема 12. Вероятностная машина Тьюринга. Принятие слов, критерии распознавания языков вероятностными машинами Тьюринга.	6	12	0	2	0	Письменное домашнее задание
13.	Тема 13. Распознавание языков с изолированной ошибкой.	6	13	0	2	0	Письменное домашнее задание
14.	Тема 14. Увеличение вероятности правильного результата для классов ВРР, РР.	6	14	0	2	0	Письменное домашнее задание

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
15.	Тема 15. Вероятностные классы сложности RP, co-RP. У	6	15	0	2	0	Письменная работа
16.	Тема 16. Вероятностный класс сложности ZPP. Соотношение с другими классами сложности.	6	16	0	2	0	Письменное домашнее задание
17.	Тема 17. Однородные и неоднородные вычислительные модели. Однородные и неоднородные классы сложности.	6	17	0	2	0	Письменное домашнее задание
18.	Тема 18. Теорема о включении класса BPP в класс P/poly.	6	18	0	2	0	Письменная работа
.	Тема . Итоговая форма контроля	6		0	0	0	Зачет
	Итого			0	36	0	

4.2 Содержание дисциплины

Тема 1. Алфавит, слова в алфавите, язык. Метод диагонализации. Вычислительные модели как формализация понятия алгоритм.

практическое занятие (2 часа(ов)):

Алфавит, слова в алфавите, язык. Свойства: множество всех слов счетно; множество всех языков несчетно. Метод диагонализации. Вычислительные модели как формализация понятия алгоритм. Вычислительные задачи как языки. Пространственная и временная сложность.

Тема 2. Детерминированная машина Тьюринга, распознавание слов, языков.

практическое занятие (2 часа(ов)):

Детерминированная машина Тьюринга, распознавание слов, языков. Рекурсивные и рекурсивно-перечислимые языки. Теорема о рекурсивности языка.

Тема 3. Тезис Черча. Классы сложности Time(f(n)), Space(f(n)). Теоремы о соотношении классов сложности Time(f(n)) и Space(f(n)).

практическое занятие (2 часа(ов)):

Тезис Черча. Классы сложности Time(f(n)), Space(f(n)). Теоремы о соотношении классов сложности Time(f(n)) и Space(f(n)).

Тема 4. Основные детерминированные классы сложности LSPACE, P, PSPACE, EXPTIME. Д

практическое занятие (2 часа(ов)):

Основные детерминированные классы сложности LSPACE, P, PSPACE, EXPTIME.

Доказательство соотношений между ними. Примеры языков, принадлежащих классам LSPACE, P, PSPACE, EXPTIME

Тема 5. Определение конечного автомата. Теорема о соотношении классов сложности Reg и LSPACE.

практическое занятие (2 часа(ов)):

Определение конечного автомата. Теорема о соотношении классов сложности Reg и LSPACE. Свойства: язык MULT (умножение) принадлежит P, язык SAT принадлежит PSPACE.

Тема 6. Недетерминированные машины Тьюринга, представление слов, распознавание языков недетерминированной машиной Тьюринга.

практическое занятие (2 часа(ов)):

Недетерминированные машины Тьюринга, представление слов, распознавание языков недетерминированной машиной Тьюринга. Соотношения детерминированных и недетерминированных классов сложности (по времени и памяти).

Тема 7. Класс сложности NP.

практическое занятие (2 часа(ов)):

Класс сложности NP. Свойство: SAT принадлежит NP. Соотношение классов P и NP. Теорема о вхождении класса NP в PSPACE.

Тема 8. Понятие полиномиальной сводимости языков. Свойства полиномиальной сводимости.

практическое занятие (2 часа(ов)):

Понятие полиномиальной сводимости языков. Свойства полиномиальной сводимости. Примеры полиномиальной сводимости: PALINDROM \leq_p SAT. Полиномиальная эквивалентность \equiv_p языков. Свойства полиномиальной эквивалентности.

Тема 9. Понятие С-трудного и С-полного языка. NP-полный язык.

практическое занятие (2 часа(ов)):

Понятие С-трудного и С-полного языка. NP-полный язык, Теорема: Пусть L принадлежит NPC. Тогда если L принадлежит P, то P=NP.

Тема 10. Доказательство NP-полноты.

практическое занятие (2 часа(ов)):

Доказательство NP-полноты. Теорема: язык K-NP-полный язык. Теорема: SAT - NP-полный язык.

Тема 11. Классы сложностей-дополнений.

практическое занятие (2 часа(ов)):

Классы сложностей-дополнений. Свойства Reg=co-Reg, LSPACE=co-LSPACE, PSPACE=co-PSPACE, P=co-P, EXTIME=co-EXPTIME. Соотношения недетерминированных классов и их дополнений.

Тема 12. Вероятностная машина Тьюринга. Принятие слов, критерии распознавания языков вероятностными машинами Тьюринга.

практическое занятие (2 часа(ов)):

Вероятностная машина Тьюринга. Принятие слов, критерии распознавания языков вероятностными машинами Тьюринга. Класс сложности RP. Теорема о соотношении классов сложности P, RP, PSPACE. Теорема о вхождении класса NP в RP.

Тема 13. Распознавание языков с изолированной ошибкой.

практическое занятие (2 часа(ов)):

Распознавание языков с изолированной ошибкой. Класс сложности BPP. Соотношение классов сложности P, RP, BPP.

Тема 14. Увеличение вероятности правильного результата для классов BPP, RP.

практическое занятие (2 часа(ов)):

Увеличение вероятности правильного результата для классов BPP, RP.

Тема 15. Вероятностные классы сложности RP, co-RP. У

практическое занятие (2 часа(ов)):

Вероятностные классы сложности RP, co-RP. Увеличение вероятности правильного результата для этих классов. Соотношения классов сложности RP, co-RP, BPP.

Тема 16. Вероятностный класс сложности ZPP. Соотношение с другими классами сложности.

практическое занятие (2 часа(ов)):

Вероятностный класс сложности ZPP. Соотношение с другими классами сложности.

Тема 17. Однородные и неоднородные вычислительные модели. Однородные и неоднородные классы сложности.

практическое занятие (2 часа(ов)):

Однородные и неоднородные вычислительные модели. Однородные и неоднородные классы сложности. Теорема о распознавании нерекурсивного языка.

Тема 18. Теорема о включении класса BPP в класс P/poly.

практическое занятие (2 часа(ов)):

Теорема о включении класса BPP в класс P/poly.

4.3 Структура и содержание самостоятельной работы дисциплины (модуля)

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
1.	Тема 1. Алфавит, слова в алфавите, язык. Метод диагонализации. Вычислительные модели как формализация понятия алгоритм.	6	1	подготовка домашнего задания	2	домашнее задание
2.	Тема 2. Детерминированная машина Тьюринга, распознавание слов, языков.	6	2	подготовка домашнего задания	2	домашнее задание
3.	Тема 3. Тезис Черча. Классы сложности Time($f(n)$), Space($f(n)$). Теоремы о соотношении классов сложности Time($f(n)$) и Space($f(n)$).	6	3	подготовка домашнего задания	2	домашнее задание
4.	Тема 4. Основные детерминированные классы сложности LSPACE, P, PSPACE, EXPTIME. Д	6	4	подготовка к письменной работе	2	письменная работа
5.	Тема 5. Определение конечного автомата. Теорема о соотношении классов сложности Reg и LSPACE.	6	5	подготовка домашнего задания	2	домашнее задание
6.	Тема 6. Недетерминированные машины Тьюринга, представление слов, распознавание языков недетерминированной машиной Тьюринга.	6	6	подготовка домашнего задания	2	домашнее задание

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
7.	Тема 7. Класс сложности NP.	6	7	подготовка домашнего задания	2	домашнее задание
8.	Тема 8. Понятие полиномиальной сводимости языков. Свойства полиномиальной сводимости.	6	8	подготовка к письменной работе	2	письменная работа
9.	Тема 9. Понятие C-трудного и C-полного языка. NP-полный язык.	6	9	подготовка домашнего задания	2	домашнее задание
10.	Тема 10. Доказательство NP-полноты.	6	10	подготовка домашнего задания	2	домашнее задание
11.	Тема 11. Классы сложностей-дополнений.	6	11	подготовка домашнего задания	2	домашнее задание
12.	Тема 12. Вероятностная машина Тьюринга. Принятие слов, критерии распознавания языков вероятностными машинами Тьюринга.	6	12	подготовка домашнего задания	2	домашнее задание
13.	Тема 13. Распознавание языков с изолированной ошибкой.	6	13	подготовка домашнего задания	2	домашнее задание
14.	Тема 14. Увеличение вероятности правильного результата для классов ВРР, РР.	6	14	подготовка домашнего задания	2	домашнее задание
15.	Тема 15. Вероятностные классы сложности RP, со-RP. У	6	15	подготовка к письменной работе	2	письменная работа
16.	Тема 16. Вероятностный класс сложности ZPP. Соотношение с другими классами сложности.	6	16	подготовка домашнего задания	2	домашнее задание

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
17.	Тема 17. Однородные и неоднородные вычислительные модели. Однородные и неоднородные классы сложности.	6	17	подготовка домашнего задания	2	домашнее задание
18.	Тема 18. Теорема о включении класса BPP в класс P/poly.	6	18	подготовка к письменной работе	2	письменная работа
	Итого				36	

5. Образовательные технологии, включая интерактивные формы обучения

Обучение происходит в форме лекционных и лабораторных занятий, а также самостоятельной работы студентов.

Теоретический материал излагается на лекциях. Причем конспект лекций, который остается у студента в результате прослушивания лекции не может заменить учебник. Его цель-формулировка основных утверждений и определений. Прослушав лекцию, полезно ознакомиться с более подробным изложением материала в учебнике. Список литературы разделен на две категории: необходимый для сдачи экзамена минимум и дополнительная литература.

Изучение курса подразумевает не только овладение теоретическим материалом, но и получение практических навыков для более глубокого понимания разделов на основе решения задач и упражнений, иллюстрирующих доказываемые теоретические положения, а также развитие абстрактного мышления и способности самостоятельно доказывать утверждения.

Самостоятельная работа предполагает выполнение домашних работ. Практические задания, выполненные в аудитории, предназначены для указания общих методов решения задач определенного типа. Закрепить навыки можно лишь в результате самостоятельной работы.

Кроме того, самостоятельная работа включает подготовку к экзамену. При подготовке к сдаче экзамена весь объем работы рекомендуется распределять равномерно по дням, отведенным для подготовки к экзамену, контролировать каждый день выполнения работы. Лучше, если можно перевыполнить план. Тогда будет резерв времени.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов

Тема 1. Алфавит, слова в алфавите, язык. Метод диагонализации. Вычислительные модели как формализация понятия алгоритм.

домашнее задание , примерные вопросы:

Пространственная и временная сложность решения задач. Метод диагонализации.

Тема 2. Детерминированная машина Тьюринга, распознавание слов, языков.

домашнее задание , примерные вопросы:

Доказательство Теоремы о рекурсивности языка.

Тема 3. Тезис Черча. Классы сложности Time(f(n)), Space(f(n)). Теоремы о соотношении классов сложности Time(f(n)) и Space(f(n)).

домашнее задание , примерные вопросы:

Обсуждение. Временные и пространственные классы сложности.

Тема 4. Основные детерминированные классы сложности LSPACE, P, PSPACE, EXPTIME.

Д

письменная работа , примерные вопросы:

Теоремы о соотношении классов сложности Time($f(n)$) и Space($f(n)$).

Тема 5. Определение конечного автомата. Теорема о соотношении классов сложности Reg и LSPACE.

домашнее задание , примерные вопросы:

Доказательство Теоремы о соотношении классов сложности Reg и LSPACE.

Тема 6. Недетерминированные машины Тьюринга, представление слов, распознавание языков недетерминированной машиной Тьюринга.

домашнее задание , примерные вопросы:

Примеры полиномиальной сводимости языков

Тема 7. Класс сложности NP.

домашнее задание , примерные вопросы:

Доказательство NP-полноты языков.

Тема 8. Понятие полиномиальной сводимости языков. Свойства полиномиальной сводимости.

письменная работа , примерные вопросы:

Примеры языков, принадлежащих классам LSPACE, P, PSPACE, EXPTIME с доказательством.

Тема 9. Понятие С-трудного и С-полного языка. NP-полный язык.

домашнее задание , примерные вопросы:

Доказательство утверждений о соотношении классов P, PP, PSPACE.

Тема 10. Доказательство NP-полноты.

домашнее задание , примерные вопросы:

Доказательство NP-полноты языка методом сведения на примере доказательства NP-полноты языка "Independent Set" (Независимое множество вершин в графе).

Тема 11. Классы сложностей-дополнений.

домашнее задание , примерные вопросы:

Доказать Свойство: Язык 3-SAT - NP-полный язык

Тема 12. Вероятностная машина Тьюринга. Принятие слов, критерии распознавания языков вероятностными машинами Тьюринга.

домашнее задание , примерные вопросы:

Теорема о вхождении класса NP в PP.

Тема 13. Распознавание языков с изолированной ошибкой.

домашнее задание , примерные вопросы:

Доказательство утверждения о соотношении классов NP и PP.

Тема 14. Увеличение вероятности правильного результата для классов BPP, PP.

домашнее задание , примерные вопросы:

Построение надежных вероятностных алгоритмов.

Тема 15. Вероятностные классы сложности RP, co-RP. У

письменная работа , примерные вопросы:

Детерминированный конечный автомат. Критерий регулярности языка. Свойство: Язык $L=\{0^*1^*\}$ принадлежит Reg.

Тема 16. Вероятностный класс сложности ZPP. Соотношение с другими классами сложности.

домашнее задание , примерные вопросы:

Увеличение вероятности правильного результата для классов \$BPP, PP, RP, co-RP\$.

Тема 17. Однородные и неоднородные вычислительные модели. Однородные и неоднородные классы сложности.

домашнее задание , примерные вопросы:

Доказательство Теоремы о распознавании нерекурсивного языка неоднородной моделью машины Тьюринга.

Тема 18. Теорема о включении класса BPP в класс P/poly.

письменная работа , примерные вопросы:

Квантовая машина Тьюринга. Сравнение с классическими машинами Тьюринга.

Тема . Итоговая форма контроля

Примерные вопросы к зачету:

Билет 1

1. Алфавит, слова в алфавите, язык. Свойства: множество всех слов счетно; множество всех языков несчетно. Метод диагонализации.

2. Примеры эффективных вероятностных алгоритмов: существование совершенного паросочетания в двудольном графе.

Билет 2

1. Вычислительные задачи как языки. Тезис Черча. Понятие временной и пространственной сложности. Классы сложности Time($f(n)$), Space($f(n)$). Теоремы о соотношении классов сложности Time($f(n)$) и Space($f(n)$).

2. Определение конечного недетерминированного автомата. Распознавание языков. Сравнение с моделью машины Тьюринга. Теорема: класс языков, распознаваемых недетерминированными конечными автоматами = Reg.

Билет 3

1. Теоремы Хартманиса о пространственной и временной иерархии детерминированных классов сложности. Доказательство Теоремы о пространственной иерархии.

2. Свойство: язык PALINDROM принадлежит LSPACE.

Билет 4

1. Детерминированная машина Тьюринга, распознавание слов, языков. Классы сложности Time($f(n)$), Space($f(n)$). Теоремы о соотношении классов сложности Time($f(n)$) и Space($f(n)$).

2. Доказательство NP-полноты языка методом сведения на примере доказательства NP-полноты языка "Independent Set" (Независимое множество вершин в графе).

Билет 5

1. Рекурсивные и рекурсивно-перечислимые языки. Теорема о рекурсивности языка.

2. Распознавание языка ZEROP (Равенства нулю полиномов) вероятностными и детерминированными машинами Тьюринга.

Билет 6

1. Различные критерии распознавания языков вероятностными машинами Тьюринга.

Соотношения детерминированных и вероятностных классов сложности. Распознавание языка ZEROP (Равенства нулю полиномов) вероятностными и детерминированными машинами Тьюринга.

2. Доказательство соотношений классов сложности NTIME($f(n)$) и TIME($f(n)$), NTIME($f(n)$) и SPACE($f(n)$).

Билет 7

1. Уменьшение вероятности ошибки для классов BPP, PP.

2. Примеры языков, принадлежащих классам LSPACE, P, PSPACE, EXPTIME с доказательством.

Билет 7

1. Основные детерминированные классы сложности LSPACE, P, PSPACE, EXPTIME. Доказательство соотношений между ними.

2. Свойство: SAT принадлежит NP.

Билет 8

1. Недетерминированные машины Тьюринга, представление слов, распознавание языков недетерминированной машиной Тьюринга. Классы сложности Time($f(n)$), Space($f(n)$). Теоремы о соотношении классов сложности Time($f(n)$) и Space($f(n)$). Класс сложности NP.

2. Методы доказательства NP-полноты. Примеры NP-полных языков.

Билет 9

1. Примеры эффективных вероятностных алгоритмов: существование совершенного паросочетания в двудольном графе.

2. Свойство: 3-SAT принадлежит NP.

Билет 10

1. Определение С-трудного и С-полного языка. Примеры. NP-полнота. Методы доказательства NP-полноты.

2. Доказательство соотношение классов P и NP, классов NP и PSPACE.

Билет 11

1. Полиномиальная сводимость языков и ее свойства. Примеры полиномиальной сводимости: PALINDROM \leq_p SAT. Полиномиальная эквивалентность \equiv языков. Свойства полиномиальной эквивалентности.

2. Доказательство соотношения классов сложности RP, co=RP, BPP.

Билет 12

1. Понятие пространственной и временной сложности. Классы сложности Time($f(n)$), Space($f(n)$). Теоремы о соотношении классов сложности Time($f(n)$) и Space($f(n)$).

2. Класс сложности Reg. Доказательство собственного включения класса Reg в класс LogSpace.

Билет 13

1. NP-полный язык. Теорема: Пусть L принадлежит NPC. Тогда если L принадлежит P, то P=NP.

2. Доказательство NP-полноты языка методом сведения на примере доказательства NP-полноты языка "Independent Set" (Независимое множество вершин в графе).

Билет 14

1. Классы сложностей-дополнений. Доказательство соотношений детерминированных классов и их дополнений. Соотношения недетерминированных классов и их дополнений.

2. Понятие NP-полного языка. Примеры NP-полных языков. Методы доказательства NP-полноты. Соотношение классов P и NP.

Билет 15

1. Определение вероятностной машины Тьюринга. Принятие слов, критерии распознавания языков вероятностными машинами Тьюринга. Вероятностные классы сложности, их различие.

2. Основные понятия квантовых вычислений. Квантовая машина Тьюринга. Сравнение с классическими машинами Тьюринга.

Билет 16

1. Класс сложности PP. Теорема о соотношении классов сложности P, PP, PSPACE. Увеличение вероятности правильного результата для языков из класса PP.

2. Свойство: Язык 3-SAT - NP-полный язык.

Билет 17

1. Недетерминированная машина Тьюринга. Распознавание языков недетерминированной машиной Тьюринга. Доказательство теоремы о вхождении класса NP в PP.

2. Определение детерминированного конечного автомата. Класс Reg. Свойство: Язык $L=\{0,1\}^*$ принадлежит Reg.

Билет 18

1. Распознавание языков с изолированной ошибкой. Класс сложности BPP. Соотношение классов сложности P, PP, BPP. Увеличение вероятности правильного результата для классов BPP, PP.

2. Свойства: язык SAT принадлежит PSPACE.

Билет 19

1. Язык-дополнение. Классы сложностей-дополнений. Соотношение классов сложностей и их дополнений в детерминированном и недетерминированном случаях.
2. Вероятностные вычисления с нулевой ошибкой. Класс сложности ZPP. Его соотношение с другими вероятностными классами сложности.

Билет 20

1. Вероятностные классы сложности RP, co-RP. Увеличение вероятности правильного результата для этих классов. Соотношение с вероятностными классами сложности.
2. Теорема о соотношении классов сложности Reg и LSPACE.

Билет 21

1. Определение детерминированной машины Тьюринга. Тезис Черча. Полиномиальный тезис Черча.
2. Детерминированный конечный автомат. Критерий регулярности языка. Свойство: Язык $L=\{0^*1^*\}$ принадлежит Reg.

Билет 22

1. Вероятностный класс сложности ZPP. Доказательство соотношение с другими классами сложности.
2. Определение конечного детерминированного автомата. Сравнение моделей конечного автомата и машины Тьюринга. Класс языков, распознаваемых конечным детерминированным автоматом. Критерий регулярности языка.

Билет 23

1. Определение конечного автомата. Теорема о соотношении классов сложности Reg и LogSPACE. Свойства: язык MULT (умножение) принадлежит P, язык SAT принадлежит PSPACE.
2. Вероятностная машина Тьюринга. Принятие слов, критерии распознавания языков вероятностными машинами Тьюринга. Класс сложности PP. Теорема о соотношении классов сложности P, PP, PSPACE. Теорема о вхождении класса NP в PP.

7.1. Основная литература:

- 1.Дуреева, Н. С. Роль моделей в теории познания [Электронный ресурс]: Учеб. пособие / Н. С. Дуреева, Р. Н. Галиахметов. - Красноярск : Сиб. федер. ун-т, 2011. - 192 с. . - Режим доступа: <http://www.znanium.com/bookread.php?book=443234>
2. Моделирование информационных ресурсов: теория и решение задач [Электронный ресурс]: учебное пособие / Г.Н. Исаев. - М.: Альфа-М: ИНФРА-М, 2010. - 224 с. - Режим доступа: <http://znanium.com/bookread.php?book=193771>

7.2. Дополнительная литература:

1. Математическая логика: Учебное пособие / В.И. Игошин. - М.: ИНФРА-М, 2012. - 399 с. URL: <http://znanium.com/bookread.php?book=242738>
2. Введение в логику: Учебник / В.А. Бочаров, В.И. Маркин. - 2-е изд., доп. и испр. - М.: ИД ФОРУМ: ИНФРА-М, 2011. - 560 с. URL: <http://znanium.com/bookread.php?book=264965>
3. Методы научного познания: Учебное пособие / С.А. Лебедев. - М.: Альфа-М: НИЦ ИНФРА-М, 2014. - 272 с. URL: <http://znanium.com/bookread.php?book=450183>

7.3. Интернет-ресурсы:

Интернет-портал образовательных ресурсов КФУ - <http://www.kfu-elearning.ru/>

Интернет-портал образовательных ресурсов по ИТ - <http://algolist.manual.ru/>

Интернет-портал ресурсов по математике - <http://www.allmath.com/>

Интернет-портал ресурсов по математическим наукам - <http://www.mathnet.ru>

Интернет-портал ресурсов по математическим наукам - [http://www.math.ru/](http://www.math.ru)

8. Материально-техническое обеспечение дисциплины(модуля)

Освоение дисциплины "Вероятностные модели вычислений" предполагает использование следующего материально-технического обеспечения:

Мультимедийная аудитория, вместимостью более 60 человек. Мультимедийная аудитория состоит из интегрированных инженерных систем с единой системой управления, оснащенная современными средствами воспроизведения и визуализации любой видео и аудио информации, получения и передачи электронных документов. Типовая комплектация мультимедийной аудитории состоит из: мультимедийного проектора, автоматизированного проекционного экрана, акустической системы, а также интерактивной трибуны преподавателя, включающей тач-скрин монитор с диагональю не менее 22 дюймов, персональный компьютер (с техническими характеристиками не ниже Intel Core i3-2100, DDR3 4096Mb, 500Gb), конференц-микрофон, беспроводной микрофон, блок управления оборудованием, интерфейсы подключения: USB, audio, HDMI. Интерактивная трибуна преподавателя является ключевым элементом управления, объединяющим все устройства в единую систему, и служит полноценным рабочим местом преподавателя. Преподаватель имеет возможность легко управлять всей системой, не отходя от трибуны, что позволяет проводить лекции, практические занятия, презентации, вебинары, конференции и другие виды аудиторной нагрузки обучающихся в удобной и доступной для них форме с применением современных интерактивных средств обучения, в том числе с использованием в процессе обучения всех корпоративных ресурсов. Мультимедийная аудитория также оснащена широкополосным доступом в сеть интернет. Компьютерное оборудование имеет соответствующее лицензионное программное обеспечение.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе "ZNANIUM.COM", доступ к которой предоставлен студентам. ЭБС "ZNANIUM.COM" содержит произведения крупнейших российских учёных, руководителей государственных органов, преподавателей ведущих вузов страны, высококвалифицированных специалистов в различных сферах бизнеса. Фонд библиотеки сформирован с учетом всех изменений образовательных стандартов и включает учебники, учебные пособия, УМК, монографии, авторефераты, диссертации, энциклопедии, словари и справочники, законодательно-нормативные документы, специальные периодические издания и издания, выпускаемые издательствами вузов. В настоящее время ЭБС ZNANIUM.COM соответствует всем требованиям федеральных государственных образовательных стандартов высшего профессионального образования (ФГОС ВПО) нового поколения.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе Издательства "Лань", доступ к которой предоставлен студентам. ЭБС Издательства "Лань" включает в себя электронные версии книг издательства "Лань" и других ведущих издательств учебной литературы, а также электронные версии периодических изданий по естественным, техническим и гуманитарным наукам. ЭБС Издательства "Лань" обеспечивает доступ к научной, учебной литературе и научным периодическим изданиям по максимальному количеству профильных направлений с соблюдением всех авторских и смежных прав.

лекции и лабораторные занятия по дисциплине проводятся в аудитории, оснащенной доской и мелом (маркером)

Программа составлена в соответствии с требованиями ФГОС ВПО и учебным планом по направлению 10.03.01 "Информационная безопасность" и профилю подготовки Безопасность компьютерных систем .

Автор(ы):

Гайнутдинова А.Ф. _____
"___" 201 ___ г.

Рецензент(ы):

Салимов Ф.И. _____
"___" 201 ___ г.