

**Федеральное государственное автономное образовательное
учреждение высшего образования
«Московский физико-технический институт
(национальный исследовательский университет)»**

УТВЕРЖДЕНО

**Директор физтех-школы
прикладной математики и
информатики
А.М. Райгородский**

	Рабочая программа дисциплины (модуля)
по дисциплине:	Дополнительные главы теории сложности
по направлению:	Прикладная математика и информатика
профиль подготовки:	Прикладная математика и информатика Физтех-школа Прикладной Математики и Информатики кафедра дискретной математики
курс:	1
квалификация:	магистр

Семестр, формы промежуточной аттестации: 2 (весенний) - Экзамен

Аудиторных часов: 30 всего, в том числе:

лекции: 30 час.

семинары: 0 час.

лабораторные занятия: 0 час.

Самостоятельная работа: 30 час.

Подготовка к экзамену: 30 час.

Всего часов: 90, всего зач. ед.: 2

Количество контрольных работ, заданий: 2

Программу составил: Д.В. Мусатов, канд. физ.-мат. наук

Программа обсуждена на заседании кафедры дискретной математики 01.03.2024

Аннотация

Дополнительные главы теории сложности изучает фундаментальные факты о том, какие ресурсы требуются для решения задач того или иного типа (например, знаменитый открытый вопрос о равенстве классов \mathbf{P} и \mathbf{NP} — одна из «проблем тысячелетия» — состоит в том, можно ли быстро найти решение всякой задачи, решения к которой можно быстро проверять). Изучаемые в ней понятия являются базовыми для любых рассуждений о вычислительной сложности — от эффективности работы алгоритмов до надёжности криптосистем.

Эта теория содержит массу открытых вопросов, однако есть в ней и множество красивых теорем и конструкций. Одно из немногих утверждений о равенстве сложностных классов — теорема Шамира для каждой задачи, решаемой с полиномиальной памятью, существует интерактивный протокол (всесильный $\text{emph{prover}}$ убеждает полиномиально ограниченного вероятностного $\text{emph{verifier}}$ а). Удивительно на первый взгляд и следующее утверждение (\mathbf{PCP} -теорема) решения любой \mathbf{NP} -задачи можно переписать таким образом, чтобы их можно было проверять, прочитав лишь константное число битов; эта теорема имеет разнообразные применения в теории (ограничения на приближенные алгоритмы) и на практике (blockchains).

1. Цели и задачи

Цель дисциплины

- формирование у студентов знаний об основных подходах к математическому уточнению интуитивного понятия алгоритм, их эквивалентности, о методах доказательства алгоритмической неразрешимости проблем, о способах оценки сложности выполнения алгоритмов, также изучение вопросов применения понятий и методов теории алгоритмов в математике и ее приложениях.

Задачи дисциплины

- обучение студентов современным принципам анализа алгоритмической сложности задач, выявление особенностей практических задач и их использование для нахождения эффективного алгоритмического решения;
- формирование подходов к выполнению исследований студентами в области анализа алгоритмической сложности задач в рамках выпускных работ на степень магистра.

2. Перечень формируемых компетенций

Освоение дисциплины направлено на формирование следующих компетенций:

Код и наименование компетенции	Индикаторы достижения компетенции
ОПК-1 Способен решать актуальные задачи фундаментальной и прикладной математики	ОПК-1.1 Знает и способен использовать в профессиональной деятельности фундаментальные научные знания и новые научные принципы и методы исследований в области прикладной математики и информатики
	ОПК-1.2 Способен обобщать и критически оценивать опыт и результаты научных исследований в области профессиональной деятельности
	ОПК-1.3 Понимает междисциплинарные связи в области прикладной математики и информатики и способен их применять при решении задач профессиональной деятельности
ПК-3 Владеет навыками участия в научных дискуссиях, выступления с сообщениями и докладами, устного, письменного и виртуального (размещение в информационных сетях) характера,	ПК-3.1 Знает основы ведения научной дискуссии и формы устного научного высказывания
	ПК-3.2 Умеет вести корректную дискуссию в области информационно-коммуникационных технологии и информационных систем, задавать вопросы и отвечать на поставленные вопросы по теме научной работы

представления материалов собственных исследований, проведения корректуры, редактирования, реферирования работ

ПК-3.3 Имеет практический опыт участия в научных студенческих конференциях, очных, виртуальных, заочных обсуждениях научных проблем в области информационных технологий

3. Перечень планируемых результатов обучения по дисциплине (модулю)

В результате освоения дисциплины обучающиеся должны

знать:

- основные определения, понятия и проблемы теории алгоритмов.

уметь:

- применять математический аппарат теории алгоритмов для решения профессиональных задач.

владеть:

- аппаратом теории алгоритмов и основными подходами к оценке сложности выполнения алгоритмов.

4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1. Разделы дисциплины (модуля) и трудоемкости по видам учебных занятий

№	Тема (раздел) дисциплины	Трудоемкость по видам учебных занятий, включая самостоятельную работу, час.			
		Лекции	Семинары	Лаборат. работы	Самост. работа
1	Теорема Разборова	2			3
2	Способы доказательства нижних оценок на размеры схем ограниченной глубины	2			3
3	Теорема Разборова-Смоленского	2			3
4	Естественные доказательства (NaturalProofs). Мотивация	2			3
5	PCP-теорема	4			3
6	Экстракторы	2			3
7	Дерандомизация вычислений	4			3
8	Псевдослучайный генератор	6			3
9	Теорема Вильямса	4			3
10	Деревья принятия решений	2			3
Итого часов		30			30
Подготовка к экзамену		30 час.			
Общая трудоёмкость		90 час., 2 зач.ед.			

4.2. Содержание дисциплины (модуля), структурированное по темам (разделам)

Семестр: 2 (Весенний)

1. Теорема Разборова

Теорема Разборова о квадратичном разрыве между недетерминированной и детерминированной сложностями

2. Способы доказательства нижних оценок на размеры схем ограниченной глубины

Общие идеи. Вводные определения. Лемма о переключении, доказательство через лемму Разборова. Доказательство леммы Разборова. Получение оценок

3. Теорема Разборова-Смоленского

Теорема Разборова-Смоленского. Нижние оценки в теории сложности доказательств: метод узкого места, интерполяция. Нижние оценки для деревьев принятия решения. Нижние оценки в коммуникационной сложности. Трудности доказательства нижних оценок: естественные доказательства.

4. Естественные доказательства (NaturalProofs). Мотивация

Естественные доказательства (NaturalProofs). Мотивация. Примеры. Теорема Разборова-Рудича. Превращение доказательства теоремы Разборова-Смоленского в естественное.

5. PCP-теорема

PCP-теорема. Увеличение зазора: сведения CSP-задач к хорошим CSP-задачам, увеличение зазора для хороших CSP-задач. Понижение алфавита.

6. Экстракторы

Экстракторы. Существование экстракторов, экстракторы из блуждания по экспандеру. Экстракторы из универсального семейства хеш-функций.

7. Дерандомизация вычислений

Дерандомизация вычислений с ограничениями по памяти.

Дерандомизация не проще нижних оценок для схем, дерандомизация PIT, дерандомизация promise-MA

8. Псевдослучайный генератор

Псевдослучайный генератор Нисана-Вигдерсона.

Экстрактор Тревисана (из псевдослучайного генератора).

Повышение трудности с помощью кодов.

9. Теорема Вильямса

Теорема Вильямса и ее доказательство

10. Деревья принятия решений

Деревья принятия решений. Примеры вычисления сложности. Сертификатная сложность. Вероятностные деревья принятия решений. Нижние оценки для вероятностных деревьев с помощью MINMAX-теоремы для матричных игр. Чувствительность и блочная чувствительность.

5. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

- проектор с возможностью подключения через HDMI и/или VGA);
- доска с мелом или whiteboard с фломастерами;
- компьютерный класс, оснащенные ПЭВМ.

6. Перечень рекомендуемой литературы

Основная литература

1. Эффективные алгоритмы и сложность вычислений [Текст] : учеб. пособие для вузов / Н. Н. Кузюрин, С. А. Фомин ; М-во образования и науки Рос. Федерации, Моск. физ.-техн. ин-т (гос. ун-т) .— М. : Изд-во МФТИ, 2007 .— 312 с.

Фонд литературы кафедры

2. Теория сложности вычислений. 5 [Текст] : сб. работ / под ред. Д. Ю. Григорьева ; Акад. наук СССР, Мат. ин-т В. А. Стеклова, Ленингр. отд. — Л. : Наука, 1991 .— 175 с. — (Записки науч. семинаров ЛОМИ ; Т. 192). - Библиогр. в конце ст. - 1000 экз.)

Дополнительная литература

1. Колмогоровская сложность и алгоритмическая случайность [Текст] : учеб. пособие для вузов / В. В. Вьюгин ; М-во образования и науки РФ, Моск. физ.-техн. ин-т (гос. ун-т), Ин-т проблем информации им. А. А. Харкевича .— М. : МФТИ, 2012 .— 140 с.

Фонд литературы кафедры

2. S. Arora, B. Barak, Computational Complexity: A Modern Approach. Cambridge University Press, 2009.

7. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)

A note on circuit lower bounds from derandomization // <https://eccc.weizmann.ac.il/report/2010/105/>

A note on exponential circuit lower bounds from derandomizing Arthur-Merlin games // <https://eccc.weizmann.ac.il/report/2010/174/>

Non-Uniform ACC Circuit Lower Bounds // <http://www.cs.cmu.edu/~ryanw/acc-lbs.pdf>

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

1. Scott Aaronson, Charles Fu, Greg Kuperberg, Christopher Granade, Complexity Zoo.

https://complexityzoo.uwaterloo.ca/Complexity_Zoo

2. Dick Lipton, Godel's Lost Letter and $P=NP$, <http://rjlipton.wordpress.com/>

3. Scott Aaronson, Shtetl-Optimized, <http://www.scottaaronson.com/blog/>

4. Computational Complexity Blog, <http://blog.computationalcomplexity.org/>

9. Методические указания для обучающихся по освоению дисциплины (модуля)

Студент, изучающий дисциплину, должен с одной стороны, овладеть общим понятийным аппаратом, а с другой стороны, должен научиться применять теоретические знания на практике. В результате изучения дисциплины студент должен знать основные определения, понятия, аксиомы.

Успешное освоение курса требует напряжённой самостоятельной работы студента. В программе курса приведено минимально необходимое время для работы студента над темой. Самостоятельная работа включает в себя:

- чтение и конспектирование рекомендованной литературы;
- проработку учебного материала (по конспектам лекций, учебной и научной литературе), подготовку ответов на вопросы, предназначенных для самостоятельного изучения, доказательство отдельных утверждений, свойств;
- подготовку к экзамену.

Руководство и контроль за самостоятельной работой студента осуществляется в форме индивидуальных консультаций.

Важно добиться понимания изучаемого материала, а не механического его запоминания. При затруднении изучения отдельных тем, вопросов, следует обращаться за консультациями к лектору.

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

по направлению: Прикладная математика и информатика
профиль подготовки: Прикладная математика и информатика
Физтех-школа Прикладной Математики и Информатики
кафедра дискретной математики
курс: 1
квалификация: магистр

Семестр, формы промежуточной аттестации: 2 (весенний) - Экзамен

Разработчик: Д.В. Мусатов, канд. физ.-мат. наук

1. Компетенции, формируемые в процессе изучения дисциплины

Код и наименование компетенции	Индикаторы достижения компетенции
ОПК-1 Способен решать актуальные задачи фундаментальной и прикладной математики	ОПК-1.1 Знает и способен использовать в профессиональной деятельности фундаментальные научные знания и новые научные принципы и методы исследований в области прикладной математики и информатики
	ОПК-1.2 Способен обобщать и критически оценивать опыт и результаты научных исследований в области профессиональной деятельности
	ОПК-1.3 Понимает междисциплинарные связи в области прикладной математики и информатики и способен их применять при решении задач профессиональной деятельности
ПК-3 Владеет навыками участия в научных дискуссиях, выступления с сообщениями и докладами, устного, письменного и виртуального (размещение в информационных сетях) характера, представления материалов собственных исследований, проведения корректуры, редактирования, реферирования работ	ПК-3.1 Знает основы ведения научной дискуссии и формы устного научного высказывания
	ПК-3.2 Умеет вести корректную дискуссию в области информационно-коммуникационных технологий и информационных систем, задавать вопросы и отвечать на поставленные вопросы по теме научной работы
	ПК-3.3 Имеет практический опыт участия в научных студенческих конференциях, очных, виртуальных, заочных обсуждениях научных проблем в области информационных технологий

2. Показатели оценивания компетенций

В результате изучения дисциплины «Дополнительные главы теории сложности» обучающийся должен:

знать:

- основные определения, понятия и проблемы теории алгоритмов.

уметь:

- применять математический аппарат теории алгоритмов для решения профессиональных задач.

владеть:

- аппаратом теории алгоритмов и основными подходами к оценке сложности выполнения алгоритмов.

3. Перечень типовых (примерных) вопросов, заданий, тем для подготовки к текущему контролю

С целью контроля освоения обучающимися учебного материала проводится устный опрос в начале занятия по теме прошлой лекции или в конце занятия по пройденной теме.

4. Перечень типовых (примерных) вопросов и тем для проведения промежуточной аттестации обучающихся

1. Теорема Разборова о квадратичном разрыве между недетерминированной и детерминированной сложностями;
2. Два способа доказательства нижних оценок на размеры схем ограниченной глубины: сокращение глубины с помощью леммы о переключении (Hastad's Switching Lemma) и аппроксимация схем полиномами маленькой степени;
3. Теорема Разборова-Смоленского. Нижние оценки в теории сложности доказательств: метод узкого места, интерполяция. Нижние оценки для деревьев принятия решения. Нижние оценки в коммуникационной сложности. Трудности доказательства нижних оценок: естественные доказательства;
4. Естественные доказательства (Natural Proofs);

5. РСР-теорема и приближённое решение NP-трудных задач;
6. Минимальная энтропия, экстракторы, существование экстракторов. Представление источника в виде выпуклой комбинации плоских. Построение экстрактора из усредняющего сэмплера. Экстрактор из случайного блуждания по экспандеру;
7. Дерандомизация вычислений с ограничениями по памяти;
8. Дерандомизация не проще нижних оценок для схем, дерандомизация PIT, дерандомизация promise-MA;
9. Псевдослучайный генератор Нисана-Вигдерсона;
10. Экстрактор Тревисана. XOR-лемма Яо;
11. Повышение трудности с помощью кодов;
12. Теорема Вильямса;
13. Использование деверев принятия решений в теории сложности.

Примеры билетов:

Билет №1

1. Теорема Разборова о квадратичном разрыве между недетерминированной и детерминированной сложностями;
2. Повышение трудности с помощью кодов.

Билет №2

1. Минимальная энтропия, экстракторы, существование экстракторов.
2. Псевдослучайный генератор Нисана-Вигдерсона.

Критерии оценивания

- оценка «отлично (10)» выставляется студенту, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины и умение уверенно применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений
- оценка «отлично (9)» выставляется студенту, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины и умение применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений
- оценка «отлично (8)» выставляется студенту, показавшему всесторонние систематизированные, глубокие знания учебной программы дисциплины и умение применять их на практике при решении конкретных задач, и правильное обоснование принятых решений
- оценка «хорошо (7)» выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности;
- оценка «хорошо (6)» выставляется студенту, если он знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности;
- оценка «хорошо (5)» выставляется студенту, если он знает материал, и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности;
- оценка «удовлетворительно (4)» выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, недостаточно правильные формулировки базовых понятий, нарушения логической последовательности в изложении программного материала, но при этом он владеет основными разделами учебной программы, необходимыми для дальнейшего обучения и может применять полученные знания по образцу в стандартной ситуации;
- оценка «удовлетворительно (3)» выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, недостаточно правильные формулировки базовых понятий, нарушения логической последовательности в изложении программного материала, но при этом он владеет фрагментарно основными разделами учебной программы, необходимыми для дальнейшего обучения и может применять полученные знания по образцу в стандартной ситуации;

- оценка «неудовлетворительно (2)» выставляется студенту, который не знает большей части основного содержания учебной программы дисциплины, допускает грубые ошибки в формулировках основных понятий дисциплины и не умеет использовать полученные знания при решении типовых практических задач
- оценка «неудовлетворительно (1)» выставляется студенту, который не знает формулировок основных понятий дисциплины.

5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Во время проведения экзамена обучающиеся могут пользоваться программой дисциплины.