

**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:	Сложность вычислений
по направлению:	Прикладная математика и информатика
профиль подготовки:	Информатика Физтех-школа Прикладной Математики и Информатики кафедра дискретной математики
курс:	2
квалификация:	бакалавр

Семестр, формы промежуточной аттестации: 4 (весенний) - Экзамен

Аудиторных часов: 60 всего, в том числе:

лекции: 30 час.

семинары: 30 час.

лабораторные занятия: 0 час.

Самостоятельная работа: 45 час.

Подготовка к экзамену: 30 час.

Всего часов: 135, всего зач. ед.: 3

Количество контрольных работ, заданий: 1

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

Программа обсуждена на заседании кафедры дискретной математики 05.03.2020

Аннотация

Полугодовой курс закладывает основы теории сложности вычислений, которые далее при желании можно развивать в различных направлениях. Основные вопросы курса: какие бывают вычислительные ресурсы, как подсчитывать их необходимое количество для решения данной алгоритмической задачи и как отличить решаемые на практике задачи от нерешаемых. Много внимания уделяется изучению различных сложностных классов, связей между ними и классификации конкретных задач.

1. Цели и задачи

Цель дисциплины

освоение понятия сложных вычислений.

Задачи дисциплины

- ☐ Научиться оценивать сложность алгоритмической задачи в терминах вычислительных ресурсов.
- ☐ Научиться отделять практически решаемые задачи от нерешаемых.
- ☐ Изучить «зоопарк» сложностных классов и начать в нём ориентироваться.
- ☐ Изучить набор открытых гипотез о соотношении сложностей задач и связи между этими гипотезами.

2. Перечень формируемых компетенций

Освоение дисциплины направлено на формирование следующих компетенций:

Код и наименование компетенции	Индикаторы достижения компетенции
ОПК-2 Способен использовать современные информационные технологии и программные средства при решении задач профессиональной деятельности, соблюдая требования информационной безопасности	ОПК-2.1 Способен применять современные вычислительную технику и сервисы сети Интернет в области (сфере) профессиональной деятельности
ПК-1 Способен ставить, формализовывать и решать задачи, в том числе разрабатывать и исследовать математические модели изучаемых явлений и процессов, системно анализировать научные проблемы, получать новые научные результаты	ПК-1.2 Способен выдвигать гипотезы, строить математические модели для описания изучаемых явлений и процессов, оценивать качество разработанной модели
ПК-2 Способен самостоятельно или в качестве члена (руководителя) малого коллектива организовывать и проводить научные исследования и их апробацию	ПК-2.1 Знает принципы построения научной работы, методы сбора и анализа полученного материала, способы аргументации

3. Перечень планируемых результатов обучения по дисциплине (модулю)

В результате освоения дисциплины обучающиеся должны

знать:

- ☐ фундаментальные понятия, законы, теории сложных вычислений;
- ☐ современные проблемы соответствующих разделов сложных вычислений;
- ☐ понятия, аксиомы, методы доказательств и доказательства основных теорем в разделах, входящих в базовую часть цикла;
- ☐ основные свойства соответствующих математических объектов;
- ☐ аналитические и численные подходы и методы для решения типовых прикладных задач сложных вычислений.

уметь:

- ☐ понять поставленную задачу;
- ☐ использовать свои знания для решения фундаментальных и прикладных задач ЭК;
- ☐ оценивать корректность постановок задач;
- ☐ строго доказывать или опровергать утверждение;
- ☐ самостоятельно находить алгоритмы решения задач, в том числе и нестандартных, и проводить их анализ;
- ☐ самостоятельно видеть следствия полученных результатов;
- ☐ точно представить математические знания в области сложных вычислений в устной и письменной форме.

владеть:

- ☐ навыками освоения большого объема информации и решения задач (в том числе, сложных);
- ☐ навыками самостоятельной работы и освоения новых дисциплин;
- ☐ культурой постановки, анализа и решения математических и прикладных задач, требующих для своего решения использования математических подходов и методов ЭК;
- ☐ предметным языком сложных вычислений и навыками грамотного описания решения задач и представления полученных результатов.

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	Понятие сложности	6	6		
2	Временная сложность	6	6		
3	Метод диагонализации.	6	6		
4	Схемная сложность	6	6		
5	Дерандомизация	6	6		45
Итого часов		30	30		45
Подготовка к экзамену		30 час.			
Общая трудоёмкость		135 час., 3 зач.ед.			

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

Семестр: 4 (Весенний)

1. Понятие сложности

Измерение сложности алгоритма и задачи. Тезис Чёрча-Тьюринга в сильной форме.

2. Временная сложность

Классы P и NP. Теория NP-полноты

3. Метод диагонализации.

Метод диагонализации. Полиномиальная иерархия. Пространственная сложность

4. Схемная сложность

Вероятностные алгоритмы и сложностные классы. Сложность задач подсчёта.

5. Дерандомизация

Сложность в среднем. Основания криптографии.

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

Стандартная учебная аудитория.

6.Перечень рекомендуемой литературы

Основная литература

1. Колмогоровская сложность и алгоритмическая случайность [Текст] / Н. К. З. Верещагин, В. А. Успенский, А. Шень .— [Научное изд.] .— М. : МЦНМО, 2013 .— 576 с. + pdf-версия. - Библиогр.: с. 546-558. - Предм. указ.: с. 559-567. - Указ. имен: с. 568-570. - 400 экз. - ISBN 978-5-4439-0212-8 (в пер.) .— Полный текст (Доступ из сети МФТИ / Удаленный доступ).

Дополнительная литература

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

<http://dm.fizteh.ru/>

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

учебная аудитория, экран и проектор.

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

1. Рекомендуется успешно сдавать контрольные работы, так как это упрощает итоговую аттестацию по предмету.
2. Для подготовки к итоговой аттестации по предмету лучше всего пользоваться материалами лекций.

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

по направлению: Прикладная математика и информатика
профиль подготовки: Информатика
Физтех-школа Прикладной Математики и Информатики
кафедра дискретной математики
курс: 2
квалификация: бакалавр

Семестр, формы промежуточной аттестации: 4 (весенний) - Экзамен

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

1. Компетенции, формируемые в процессе изучения дисциплины

Код и наименование компетенции	Индикаторы достижения компетенции
ОПК-2 Способен использовать современные информационные технологии и программные средства при решении задач профессиональной деятельности, соблюдая требования информационной безопасности	ОПК-2.1 Способен применять современные вычислительную технику и сервисы сети Интернет в области (сфере) профессиональной деятельности
ПК-1 Способен ставить, формализовывать и решать задачи, в том числе разрабатывать и исследовать математические модели изучаемых явлений и процессов, системно анализировать научные проблемы, получать новые научные результаты	ПК-1.2 Способен выдвигать гипотезы, строить математические модели для описания изучаемых явлений и процессов, оценивать качество разработанной модели
ПК-2 Способен самостоятельно или в качестве члена (руководителя) малого коллектива организовывать и проводить научные исследования и их апробацию	ПК-2.1 Знает принципы построения научной работы, методы сбора и анализа полученного материала, способы аргументации

2. Показатели оценивания компетенций

В результате изучения дисциплины «Сложность вычислений» обучающийся должен:

знать:

- ☐ фундаментальные понятия, законы, теории сложных вычислений;
- ☐ современные проблемы соответствующих разделов сложных вычислений;
- ☐ понятия, аксиомы, методы доказательств и доказательства основных теорем в разделах, входящих в базовую часть цикла;
- ☐ основные свойства соответствующих математических объектов;
- ☐ аналитические и численные подходы и методы для решения типовых прикладных задач сложных вычислений.

уметь:

- ☐ понять поставленную задачу;
- ☐ использовать свои знания для решения фундаментальных и прикладных задач ЭК;
- ☐ оценивать корректность постановок задач;
- ☐ строго доказывать или опровергать утверждение;
- ☐ самостоятельно находить алгоритмы решения задач, в том числе и нестандартных, и проводить их анализ;
- ☐ самостоятельно видеть следствия полученных результатов;
- ☐ точно представить математические знания в области сложных вычислений в устной и письменной форме.

владеть:

- ☐ навыками освоения большого объема информации и решения задач (в том числе, сложных);
- ☐ навыками самостоятельной работы и освоения новых дисциплин;
- ☐ культурой постановки, анализа и решения математических и прикладных задач, требующих для своего решения использования математических подходов и методов ЭК;
- ☐ предметным языком сложных вычислений и навыками грамотного описания решения задач и представления полученных результатов.

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

Оценка за курс складывается из трёх компонентов: решения задач на контрольных (оценка С от 0 до 15 с шагом 0.1), индивидуального проекта (оценка Р от 0 до 12 с шагом 1) и устного экзамена (оценка Е от 2 до 10 с шагом 1). Итоговая оценка выставляется по формуле $0.3 \cdot C + 0.2 \cdot P + 0.5 \cdot E$ с округлением вниз. Ограничения: для оценки 8 и выше должен быть обязательно сдан проект ($P \geq 5$), для любой положительной оценки должен быть сдан экзамен ($E > 2$), для оценки 10 экзамен должен быть сдан на «отлично» ($E \geq 8$).

Примеры задач из самостоятельных

1. Дайте формальное определение многоленточной машины Тьюринга, которой запрещено изменять содержимое первой ленты (достаточно указать отличия от обычного определения). Докажите, что на машине такого вида можно смоделировать классическую многоленточную машину Тьюринга с не более чем полиномиальным замедлением.
2. Пусть $A, B \in \text{coNP}$. Докажите, что $A \cup B \in \text{coNP}$.
3. Рассмотрим язык $\text{LASTBIT-MAJ} = \{x \in \{0,1\}^{2n} \mid x_{2n} \text{ совпадает с наиболее частым значением из } x_1, \dots, x_{(2n-1)}\}$. Докажите, что он лежит в L .
4. Придумайте бесконечный язык $A \in \text{P/poly}$, такой что для любого $B \subseteq A$ выполнено $B \in \text{P/poly}$.

Примеры задач из контрольных

1. Придумайте NP-полные языки A и B , такие что $A \cap B \in P$.
2. Докажите PSPACE-полноту языка $\text{LOOPING} = \{(M, 1^n, k) \mid \text{детерминированная машина Тьюринга } M \text{ закикливается на пустом входе, заняв не больше } n \text{ ячеек и сделав не больше } k \text{ ходов}\}$.
3. Докажите, что язык $\text{DOUBLEDSTRING} = \{(x, y) \mid x \sqsubseteq y\}$ лежит в AC^0 .
4. Докажите, что задача $\text{DNFSAT} = \{\phi \mid \phi - \text{выполнимая формула в ДНФ}\}$ лежит в P , но задача подсчёта выполняющих наборов для ДНФ является NP-трудной.

Примеры тем для проектов/курсовых

1. Обзорные проекты по теории:
 - a. Задача об изоморфизме графов: класс GI и полные задачи в нём.
 - b. Сложность поиска неподвижных точек (класс FIXP и др).
2. Изложение доказательства некоторой теоремы:
 - a. Теорема Импаляццо--Вигдерсона: если в классе E есть язык, не распознаваемый схемами субэкспоненциального размера, то $P=BPP$.
 - b. Теорема Разборова--Смоленского: $\text{mod}_p \# \text{ACC}^0(q)$ для различных простых p и q .
3. Обзоры сложности задач в некоторой области математики. Для заданной области нужно составить выборку задач и классифицировать их насколько возможно по различным сложностным классам: P , NP , PH , $PSPACE$ и т.д. Хотя бы для одной из задач нужно доказать полноту в соответствующем классе.
4. Исследовательские проекты.
 - a. Нужно найти ошибку в одном из опубликованных доказательств или опровержений $P=NP$.
 - b. Нужно проанализировать сложность какой-то компьютерной или настольной игры.
5. Алгоритмические проекты. Требуется описать некоторый алгоритм, доказать его корректность и имплементировать его (возможно, в частном случае) на любом языке программирования. Текст отчёта должен включать в себя описание алгоритма, его анализ и результаты тестовых запусков. В частности, нужно описать, в каких случаях алгоритм работает хорошо, а в каких – плохо. Оценивается прежде всего текст отчёта, а не текст программы.

Примеры задач:

- a. Поиск дерева Штейнера.
- b. Решение метрической задачи коммивояжёра.
- c. Поиск раскраски графа в 3 цвета (за экспоненциальное время с малым основанием экспоненты).

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

Примеры вопросов к экзамену:

1. Модели вычислений: одноленточные и многоленточные машины Тьюринга. Тезис Тьюринга в сильной форме.
2. Измерение времени работы алгоритма. Класс P и примеры задач из него.
3. Класс NP : два определения и их эквивалентность. Класс coNP . Полиномиальная сводимость по Карпу и её свойства. NP-трудные и NP-полные задачи. Теоремы об иерархии.
4. Теорема Ладнера о существовании NP-промежуточных задач. Измерение зоны работы алгоритма. Класс $PSPACE$. Теорема Сэвича. $PSPACE$ -полные задачи.

5. Классы L, NL и coNL. NL-полнота. $NL = coNL$.
 6. Вероятностные алгоритмы. Классы BPP и RP. Вероятностные алгоритмы проверки простоты. Интерактивные доказательства и класс IP.
 7. Интерактивные доказательства с общими случайными битами и класс AM.
 8. $IP = PSPACE$.
 9. Основные понятия криптографии: односторонние функции и псевдослучайные генераторы.
 10. Доказательства с нулевым разглашением.
 11. Приближённое нахождение оптимума: полиномиальные алгоритмы для отдельных задач и PCP-теорема.
 12. Введение в теорию колмогоровской сложности.
 13. Введение в теорию квантовых вычислений.
- Примеры экзаменационных билетов

Билет №1

1. Классы L, NL и coNL. NL-полнота. $NL = coNL$.
2. Введение в теорию квантовых вычислений.

Билет №2

1. Измерение времени работы алгоритма. Класс P и примеры задач из него.
2. Доказательства с нулевым разглашением.

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.