**Программа учебной дисциплины «Сложность вычислений и логика в теоретической информатике»**

Утверждена

Академическим советом ООП

Протокол № от «\_\_»\_\_\_\_\_20\_\_ г.

|  |  |
| --- | --- |
| Автор  | **Н.К. Верещагин** nikolay.vereshchagin@gmail.com |
| Число кредитов  | 6 |
| Контактная работа (час.)  | 80 |
| Самостоятельная работа (час.)  | 110 |
| Курс  | 3 |
| Формат изучения дисциплины |  Очная, без использования онлайн курса |

1. **ЦЕЛЬ, РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ И ПРЕРЕКВИЗИТЫ**

Целями освоения дисциплины «Сложность вычислений и логика в теоретической информатике» являются овладение студентами основными концепциями и результатами сложности вычислений и математической логики, применяемыми в теоретической ифнорматике.

В результате освоения дисциплины студент должен:

**знать:**

- основные понятия и теоремы сложности вычислений;

- основные понятия и теоремы математической логики;

- методы доказательства разрешимости логических теорий;

- способы построения графов-экспандеров и их применения в сложности вычислений.

**уметь:**

- пользоваться основными методами построения экспандеров;

- пользоваться методами элиминации кванторов и игр Эренфойхта;

- пользоваться понятиями чуствительности и блочной чуствительности;

**владеть:**

- навыками доказательства нижних оценок в сложности вычислений;

- навыками доказательства верхних оценок в сложности вычислений;

- методом дерандомизации вероятностных алгоритмов с попощью графов-экспандеров.

Изучение дисциплины «Сложность вычислений и логика в теоретической информатике» базируется на следующих дисциплинах:

- линейная алгебра;

- дискретная математика 1;

- математический анализ .

Для освоения учебной дисциплины студенты должны владеть следующими знаниями и компетенциями:

* знать основные понятия дискретной математики, линейной алгебры и математического анализа.

Основные положения дисциплины должны быть использованы в дальнейшем при изучении следующих дисциплин:

1. **СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ**
* **Тема 1. Разрешимость логических теорий**

Язык логики предикатов: сигнатуры, термы, формулы.

Семантика логики предикатов: модели данной сигнатуры (алгебраические системы, интерпретации).

Формальные теории. Модели теорий, семантическое следование (истинность во всех моделях теории), нормальные модели.

Метод элиминации кванторов на примере элементарной теории упорядоченного множества действительных чисел.

Элементарная теория поля комплексных чисел, ее аксиоматизация и доказательство ее полноты.

Элементарная теория упорядоченного поля действительных чисел, ее аксиоматизация и доказательство ее полноты.

* **Тема 2. Графы-экспандеры и их применения.**

Определение комбинаторного однородного экспандера. Существование (вероятностное доказательство).

Реберное расширение и его связь с вершинным расширением.

Матрица графа и ее собственные числа.

Expander mixing lemma.

Связь второго собственного числа и рёберного расширения.

$L\_2$-расстояние до равномерного распределения при одном шаге случайного блуждания. Лапласиан графа.

Нижние оценки $\sqrt d$ и $2\sqrt{d-1}-o(1)$ на второе собственное числа $d$-регулярного графа.

Вероятностное доказательство существования спектрального экспандера.

Тензорное произведение графов и возведение графа в степень. Собственные числа получающихся графов.

Зигзаг-произведение графов, первая спектральная оценка для зигзаг-произведения.

Зигзаг-произведение графов: вторая спектральная оценка для зигзаг-произведения.

Построение спектрального экспандера с использованием первой спектральной оценки для зигзаг-произведения.

Уменьшение вероятности ошибки рандомизованного алгоритма с помощью экспандеров без использования дополнительной случайности.

Уменьшение вероятности ошибки рандомизованного алгоритма

с помощью экспандеров с использованием дополнительных случайных битов.

Алгоритм Рейнголда.

Экспандер Маргулиса.

Двудольные экспандеры: необходимое и достаточное условие существования.

Экспандер Варди-Парвареша.

Экспандерные коды: последовательный алгоритм декодирования.

Экспандерные коды: параллельный алгоритм декодирования.

* **Тема 3. Сложность разрешающих деревьев**

**Детерминированные деревья разрешения.**

**Метод противника для доказательства нижних оценок детерминированной сложности.**

**Сертификаты, чувствительность и блочная чувствительность булевых функций. Связь сертификатной сложности c представлением функции в виде ДНФ и КНФ.**

**Верхняя оценка детерминированной сложности в терминах сертификатной сложности (квадрат сертификатной сложности) и в терминах сертификатной сложности и блочной чувствительности**

**(их произведение).**

**Верхняя оценка сертификатной сложности**

**через блочную чувствительность и обычную чувствительность.**

* **Тема 4. Нижние оценки схемной сложности**

**Случайные ограничения и Hastad Switching Lemma.**

**Теорема Разборова о нижней оценки схемной сложноси функции клики для монотонных схем.**

**Теорема Разборова---Смоленского о нижней оценке cхемной сложности функции**

**MOD$\_2$ для схем глубины $d$ из элементов MOD$\_3$, $\lor$, $\land$, $\lnot$.**

1. **ОЦЕНИВАНИЕ**

Оцениваются 4 домашних задания, коллоквиум и экзамен.

Оценка за каждое домашнее задание равна доле решенных задач, умноженной на 10. Общая оценка за домашние задания равна среднему арифметическому оценок за решение каждого из заданий. На решение каждого ДЗ дается 14 дней, решение ДЗ нужно сдавать семинаристу до начала семинара. Сдача домашних заданий после их срока невозможна.

Каждое ДЗ будет проверено в течение 10 дней после дедлайна. Домашнее задание должно быть защищено в течение 3 недель после дедлайна. Для защиты студент должен прийти на консультацию и убедить преподавателя, что он понимает, что у него написано, и тем самым работа не списана.

Коллоквиум (устный) и экзамен (письменный) оцениваются по десятибалльной системе. На коллоквиуме не разрешается пользоваться никакими записями. На экзамене можно пользоваться любыми бумажными источниками и нельзя никакими электронными.

Сумма оценки за коллоквиум и оценки за домашние задания с коэффициентами 2/3 и 1/3, соответственно, составляют накопленную оценку. Накопленная оценка и оценка за экзамен с коэффициентами 3/5 и 2/5 дают итоговую оценку. Таким образом, оценки за коллоквиум и экзамен входят в итоговую оценку с коэффициентами 0.4, а оценка за домашние задания - с коэффициентом 0.2.

Те, кто не смог прийти на экзамен и коллоквиум по болезни, могут его сдать отдельно. Не набравшие в конце второго модуля нужное количество баллов (4) могут пересдать экзамен, а если и это не поможет, то сдавать экзамен комиссии. В последнем случае накопленная оценка аннулируется и оценка, полученная на экзамене, и является окончательной.

Для прохождения контроля студент должен продемонстрировать понимание основных определений, знание теорем и методов, умение применять изученные методы для решения задач.

За домашнее задание, коллоквиум или экзамен допускается оценка 0 в тех случаях, когда студент решил ни одной задачи в работе или ничего не рассказал на коллоквиуме. Оценка 0 также ставится в случаях доказанного списывания на экзамене.

По домашним заданиям проводится защита (устная беседа), цель которой состоит в проверке самостоятельности выполнения домашних заданий. В случае если студент не может ответить на ключевые вопросы по решению задачи или сформулировать используемые при решении задач теоремы и определения, преподаватель обнуляет либо оценку за одну задачу, либо оценку за всё задание, в зависимости от степени неудовлетворительности ответа студента на вопросы. Комиссия проходит в форме устного экзамена, накопленная оценка не учитывается.

1. **ПРИМЕРЫ ОЦЕНОЧНЫХ СРЕДСТВ**

# Оценочные средства для текущего контроля студента

# Четыре домашних задания. Примеры задач:

# Рассмотрим граф $K\_{3,2} (полный двудольный граф, у которого в левой доле 3 вершины,а в правой доле 2 вершины).

# Нарисовать график функции $\min\{|\Gamma(A)|/|A|: |A|=k\}$, как функции $k$.

# Рассмотрим граф $K\_{3,3}$. Нарисовать график функции $\min\{|E(A,\bar A))|/|A|: |A|=k\}$, как функции $k$. Верно ли, что для любого графа эта функция не возрастает?

# Рассмотрим бесконечное дерево со степенью каждой вершины равной 3 (у корня 3 сына, у всех других вершин 2 сына и один отец). Чему в таком дереве равен инфимум $|\Gamma(A)|/|A|$ по всем конечным множествам $A$?

# Пусть в графе $G$ на $n$ вершинах для любого множества вершин $|S|$ размера не превосходящего $n/2$ выполнено $|\Gamma'(S)| \ge |S|/100$. Тогда диаметр такого графа есть $O(\log n)$.

# Пусть в \emph{связном} графе $G$ на $n$ вершинах для любого множества вершин $|S|$ размера не превосходящего $n/100$ выполнено $|\Gamma'(S)| \ge |S|/100$. Тогда диаметр такого графа есть $O(\log n)$. Зачем нужно условие связности?

# Для любого $d$ для всех достаточно больших $n$ верно следующее. В любом $d$-регулярном графе на $2n$ вершинах найдется множество $S$ из $n$ вершин такое, что $|E(S, \bar{S})| \le \frac{dn}{2}$ (то есть не больше половины всех ребер). Почему это неверно для всех $d, n$?

# Рассмотрим булев куб $\{0,1\}^{2019}$ (вершинами графа являются двоичные слова длины 2019, а ребра соединяют слова, которые отличаются ровно в одной позиции, то есть, расстояние Хэмминга равно 1). Найти любое множество $A$ из $2^{2018}$ вершин, для которого $|Gamma'(A)|\le \binom{2019}{1010}$.

Докажите, что для следующих задач есть детерминированные алгоритмы, работающие на логарифмической памяти (можно пользоваться алгоритмом Рейнгольда без доказательства):задача выполнимости формулы вида

$$(x\_{i\_1} \oplus x\_{j\_1}) \land (x\_{i\_2} \oplus x\_{j\_2}) \land \ldots \land (x\_{i\_k} \oplus x\_{j\_k})$$

проверка того, что в заданном неориентированном графе есть цикл, проходящий через данное ребро.

Рассмотрим следующую задачу: дан граф $G = (V, E)$ и функция $\rho: V\to \mathbb{N}$. Требуется проверить, что на любом простом пути, соединяющем две различные вершины $u, v$ такие,что $\rho(u) = \rho(v)$, есть вершина $w$ такая, что $\rho(w) > \rho(u)$. Докажите, что из существования детерминированного алгоритма на логарифмической памяти для этой задачи вытекает существование детерминированного алгоритма на логарифмической памяти для задачи проверки связности графа (в этой задаче алгоритмом Рейнгольда без доказательства пользоваться нельзя).

Рассмотрим правильный $2n$-угольник и соединим ребрами пары противоположных вершин. Найдется ли $\varepsilon > 0$ такой, что все такие графы начиная с какого-то $n$ являются комбинаторными $(n, 3, \varepsilon)$-экспандерами?

Докажите, что для любого $d \ge 3$ для всех достаточно больших $n$ в любом $d$-регулярном графе на $n$ вершинах найдется множество вершин $S$ размера $|S| \le \sqrt{n}$ такое, что $|\Gamma(S)| \le (d - 1/2) \cdot |S|$.

Постройте (или докажите, что существует) спектральный $(46875, 50, 0.85)$-экспандер.

Пусть $0 = \lambda\_1 \le \lambda\_2 \le \lambda\_3 \le \ldots \le \lambda\_n$ --- собственные числа лапласиана цикла на $n$ вершинах. Докажите, что $\lambda\_2 = O\left(\frac{1}{n} \right)$.

Пусть граф $G$ является спектральным $(n, d, \gamma)$-экспандером, целое число $k \le \frac{1}{\gamma}$ является делителем $n$, при этом вершины графа раскрашены в $k$ цветов так, что каждый цвет использован ровно $n/k$ раз. Докажите, что в $G$ найдется вершина, среди соседей которой встречаются все $k$ цветов.

Пусть $\mathbb{F}$ --- конечное поле из $q$ элементов. Рассмотрим двудольный граф $G = (\mathbb{F}^2, \mathbb{F}^2, E\subset \mathbb{F}^2 \times \mathbb{F}^2$), у которого вершина $(x, y)\in\mathbb{F}^2$ из левой доли соединяется с вершиной $(a, b) \in\mathbb{F}^2$ из правой доли тогда и только тогда, когда $ax + b = y$. Докажите, что для любого множества левых вершин $S$ размера не больше $q$ выполнено $|\Gamma(S)| \ge \frac{q + 1}{2} \cdot |S|$.

Оценочные средства для промежуточной аттестации: устный коллоквиум. Вопросы коллоквиума: Определение комбинаторного однородного экспандера. Существование (вероятностное доказательство).

Реберное расширение и его связь с вершинным расширением. Матрица графа и ее собственные числа. Expander mixing lemma. Связь второго собственного числа и рёберного расширения. $L\_2$-расстояние до равномерного распределения при одном шаге случайного блуждания. Лапласиан графа. Нижние оценки $\sqrt d$ и $2\sqrt{d-1}-o(1)$ на второе собственное числа $d$-регулярного графа. Вероятностное доказательство существования спектрального экспандера. Тензорное произведение графов и возведение графа в степень. Собственные числа получающихся графов. Зигзаг-произведение графов, первая спектральная оценка для зигзаг-произведения. Зигзаг-произведение графов: вторая спектральная оценка для зигзаг-произведения. Построение спектрального экспандера с использованием первой спектральной оценки для зигзаг-произведения. Уменьшение вероятности ошибки рандомизованного алгоритма с помощью экспандеров без использования дополнительной случайности. Уменьшение вероятности ошибки рандомизованного алгоритма с помощью экспандеров с использованием дополнительных случайных битов. Алгоритм Рейнголда. Экспандер Маргулиса. Двудольные экспандеры: необходимое и достаточное условие существования. Экспандер Варди-Парвареша. Экспандерные коды: последовательный алгоритм декодирования. Экспандерные коды: параллельный алгоритм декодирования.

1. **РЕСУРСЫ**
	1. **Основная литература**
	2. Н. К. Верещагин, А. Шень. Языки и исчисления. 4-е изд., испр., М.: МЦНМО, 2012, 240 с.<http://www.mccme.ru/free-books/shen/shen-logic-part2-2.pdf> (свободно распостраняемое издание)
	3. **Дополнительная литература**
2. [А.Е. Ромащенко. Экспандеры: конструкции и приложения.](https://www.mccme.ru/~anromash/courses/expanders-notes-2014.pdf) (свободно распостраняемый текст)

2. [Moser R.A., Tardos G., A constructive proof of the general Lovasz Local Lemma,Journal of the ACM, 2010, 57(2), 11.1–11.15.](https://arxiv.org/abs/0903.0544) (свободно распостраняемый текст из arxiv.org)

3 N. Nisan, CREW PRAM's an d decision trees, STOC 1989, pages 327-335.

* 1. **Программное обеспечение**

|  |  |  |
| --- | --- | --- |
| **№ п/п** |  |  |
|   1. |  |  |
|  |  |  |

* 1. **Профессиональные базы данных, информационные справочные системы,
	интернет-ресурсы (электронные образовательные ресурсы)**

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |
|  |  |  |
|  |  |  |
|  |  |
|  |  |  |

* 1. **Материально-техническое обеспечение дисциплины**

Учебные аудитории для лекционных занятий по дисциплине обеспечивают использование и демонстрацию тематических иллюстраций, соответствующих программе дисциплины в составе:

ПЭВМ с доступом в Интернет (операционная система, офисные программы, антивирусные программы);

мультимедийный проектор с дистанционным управлением.