**Правительство Российской Федерации**

**Санкт-Петербургский государственный университет**

**РАБ О Ч А Я П Р О Г Р А М М А**

**УЧЕБНОЙ ДИСЦИПЛИНЫ**

Автоматическое доказательство теорем

Automatic Theorem Proving

**Язык(и) обучения**

русский

Трудоемкость в зачетных единицах: 3

Регистрационный номер рабочей программы: 002229

Санкт-Петербург

2020

**Раздел 1. Характеристики учебных занятий**

* 1. **Цели и задачи учебных занятий**

Семинар посвящен вопросам обширной области Автоматического Доказательства Теорем и, более широко, Automated Reasoning. В 1954 году М. Дэвис написал программу, реализующую алгоритм элиминации кванторов, построенный М. Пресбургером в 1929 году для арифметики со сложением. Значительно позже (в 1983 году), после периода интенсивного развития теории алгоритмической сложности, Дэвис отметил следующее:

“Since it is now known that Presburger’s procedure has worse than exponential complexity, it is not surprising that this program did not perform very well. Its great triumph was to prove that the sum of two even numbers is even.”

В данном курсе будут рассмотрены алгоритмы элиминации кванторов и вопросы разрешимости и сложности для арифметических теорий. Эти вопросы, находившиеся у истоков автоматического доказательства теорем, остаются весьма актуальными, содержат множество открытых проблем, таких как гипотеза Тарского об экспоненте и алгоритмическая сложность экзистенциальной арифметики со сложением и делимостью. С другой стороны, уже известные результаты позволяют ответить на различные вопросы Automated Reasoning, такие как разрешимость и сложность для вопросов одновременной жесткой *E*-унификации.

На семинаре сначала будет рассмотрен ряд классических теорем, а затем будут изучены результаты недавних работ. Основной целью курса является формирование у обучающихся некоторого представления о современном состоянии исследований в рассматриваемой области и умение разобраться в ключевых результатах современных работ, таких как, например, 3.4.2-6)-11).

**1.2. Требования подготовленности обучающегося к освоению содержания учебных занятий (пререквизиты)**

Дисциплина изучается в 5-м семестре бакалавриата. Обучающиеся должны обладать математической культурой, обычно приобретаемой к данному этапу обучения, и освоить программу общего курса «Математическая логика».

**1.3. Перечень результатов обучения (learningoutcomes)**

После освоения курса, обучающиеся должны знать основные понятия, методы исследования вопросов разрешимости и сложности арифметических теорий. Уметь применить результаты о разрешимости/сложности арифметических теорий для изучения аналогичных вопросов в различных областях automated reasoning, таких как, например, проблема достижимости для параметрических временных автоматов с различными ограничениями.

Уметь расширить и углубить свои знания по специализированной литературе (например, из списка дополнительной литературы 3.4.2), а также иметь возможность приступить к активному изучению современных работ, пытаться понимать их проблематику и суметь оценить излагаемые в этих работах результаты.

Компетенции, формируемые в результате освоения основной образовательной программы

|  |  |
| --- | --- |
| Код компетенции | Наименование и (или) описание компетенции |
| ОПК-1 | Способен применять фундаментальные знания, полученные в области математических и (или) естественных наук, и использовать их в профессиональной деятельности |
| ОПК-3 | Способен применять современные информационные технологии, в том числе отечественные, при создании программных продуктов и программных комплексов различного назначения |
| ОПК-4 | Способен участвовать в разработке технической документации программных продуктов и программных комплексов |
| ОПК-5 | Способен инсталлировать и сопровождать программное обеспечение для информационных систем и баз данных, в том числе отечественного производства |
| ПКА-1 | Способен демонстрировать базовые знания математических и естественных наук, программирования и информационных технологий |
| ПКП-2 | Способен решать задачи в области развития науки, техники и технологии с учетом нормативного правового регулирования в сфере интеллектуальной собственности |
| ПКП-4 | Способен применять современные информационные технологии при проектировании, реализации, оценке качества и анализа эффективности программного обеспечения для решения задач в различных предметных областях |
| ПКП-5 | Способен использовать основные методы и средства автоматизации проектирования, реализации, испытаний и оценки качества при создании конкурентоспособного программного продукта и программных комплексов, а также способен использовать методы и средства автоматизации, связанные с сопровождением, администрированием и модернизацией программных продуктов и программных комплексов |
| ПКП-6 | Способен использовать знания направлений развития компьютеров с традиционной (нетрадиционной) архитектурой; современных системных программных средств: операционных систем, операционных и сетевых оболочек, сервисных программ; тенденции развития функций и архитектур проблемно-ориентированных программных систем и комплексов в профессиональной деятельности |
| ПКП-8 | Способен использовать современные методы разработки и реализации конкретных алгоритмов математических моделей на базе языков программирования и пакетов прикладных программ моделирования |
| УКБ-3 | Способен понимать сущность и значение информации в развитии общества, использовать основные методы получения и работы с информацией с учетом современных технологий цифровой экономики и информационной безопасности |

**1.4. Перечень и объём активных и интерактивных форм учебных занятий**

Аудиторная учебная работа: семинары в объеме 2 часа в неделю в 5-м учебном семестре.

Самостоятельная работа:

а) под руководством преподавателя: выбор темы и подготовка докладов для семинара;

б) в присутствии преподавателя: доклады на семинаре;

в) без участия преподавателя: индивидуальная работа с доступными текстами по алгоритмам для арифметических теорий и приложениям в вопросах автоматического доказательства и формальной верификации.

**Раздел 2. Организация, структура и содержание учебных занятий**

**2.1. Организация учебных занятий**

**2.1.1 Основной курс**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Трудоёмкость, объёмы учебной работы и наполняемость групп обучающихся | | | | | | | | | | | | | | | | | | |
| Код модуля в составе дисциплины,  практики и т.п. | Контактная работа обучающихся с преподавателем | | | | | | | | | | | | Самостоятельная работа | | | | Объём активных и интерактивных  форм учебных занятий | Трудоёмкость |
| лекции | семинары | консультации | практические  занятия | лабораторныеработы | контрольныеработы | коллоквиумы | текущий контроль | промежуточная  аттестация | итоговая аттестация | под руководством преподавателя | в присутствии  преподавателя | сам. раб. с использованием  методических материалов | текущий контроль (сам.раб.) | промежуточная аттестация (сам.раб.) | итоговая аттестация  (сам.раб.) |
| ОСНОВНАЯ ТРАЕКТОРИЯ | | | | | | | | | | | | | | | | | | |
| Форма обучения: очная | | | | | | | | | | | | | | | | | | |
| Семестр 3 | 0 | 30 | 0 | 0 | 0 | 0 | 0 | 0 | 2 |  | 0 | 0 | 73 | 0 | 3 | 0 | 30 | 3 |
|  |  | 2-100 |  |  |  |  |  |  | 2-100 |  |  |  | 1-1 |  | 1-1 |  |  |  |
| ИТОГО | 0 | 30 | 0 | 0 | 0 | 0 | 0 | 0 | 2 |  | 0 | 0 | 73 | 0 | 3 | 0 | 30 | 3 |

|  |  |  |  |
| --- | --- | --- | --- |
| Формы текущего контроля успеваемости, виды промежуточной и итоговой аттестации | | | |
| Период обучения (модуль) | Формы текущего контроля успеваемости | Виды промежуточной аттестации | Виды итоговой аттестации  (только для программ итоговой аттестации и дополнительных образовательных программ) |
| ОСНОВНАЯ ТРАЕКТОРИЯ | | | |
| очная форма обучения | | | |
| Семестр 5 |  | Зачёт |  |

**2.2. Структура и содержание учебных занятий**

Период обучения (модуль): Семестр 5

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Наименование темы (раздела, части) | Вид учебных занятий | Количество часов |
| I. | Основные алгоритмические результаты об арифметиках: элиминация кванторов, разрешимость, сложность | семинары | 10 |
| по методическим материалам | 43 |
| II. | Доклады об алгоритмических вопросах для арифметик. | семинары | 10 |
| по методическим материалам | 15 |
| III. | Доклады о приложениях к вопросам разрешимости и сложности. | семинары | 10 |
| по методическим материалам | 15 |
| IV. | Промежуточная аттестация | самостоятельная работа | 3 |
| зачёт | 2 |
| **Итого** | | | **108** |

Курс будет состоять из трёх основных частей. В первой части будут рассмотрены следующие темы:

1. Элиминация кванторов в Арифметике Пресбургера.
2. Обобщение Виспфеннинга на задачу смешанного вещественно-целочисленного линейного программирования.
3. Арифметика Бюхи и результаты А. Л. Семёнова об обобщении элиминации кванторов.
4. Результаты об алгоритмической сложности фрагментов Арифметики Пресбургера.
5. Разрешимость и сложность экзистенциальной арифметики со сложением и делимостью.
6. Разрешимость арифметики Сколема.
7. Разрешимые экзистенциальные арифметики с умножением. Алгоритм Террье.
8. Вещественная арифметика: алгоритм Тарского.
9. Сложность алгоритма Тарского и алгоритм Коллинза.
10. Линейная вещественная арифметика и виртуальная подстановка.
11. Элиминация кванторов в линейной *p*-адической арифметике.
12. Неразрешимость 10-й проблемы Гильберта.
13. Неразрешимость экзистенциальной арифметики со сложением, делимостью и предикатом степенного роста.

Некоторые результаты будут доказаны полностью (1,2,8), для некоторых возможно изложить лишь набросок доказательства (5,6,12).

Указанные темы формируют основное направление курса и должны быть расширены докладами во второй части курса. Например, к теме 2) примыкает статья 3.4.2-8, к темам 3) и 11) работа 3.4.2-6, а к теме 5) -- 3.4.2-7. Преподаватель предлагает несколько статей (обзоров) для докладов, и обучающиеся могут выбрать одну из предложенных тем.

Третья часть курса посвящена приложениям рассмотренных вопросов. Примерами статей, по которым может быть сделан доклад, являются работы 3.4.2-9,10,11.

Каждая из указанных тринадцати тем могла бы быть темой отдельного семинара. Некоторые из вопросов могут оказаться незатронутыми, если обучающимися будут выбраны доклады, близкие к одной группе вопросов, например, вопросам обобщения линейной целочисленной арифметики (1-4) или алгоритмической сложности (4,5,9).

Список итоговых вопросов для тех обучающихся, кто не набрал 50 баллов за работу на семинаре, будет формироваться в соответствии с выбранными темами докладов.

**Раздел 3. Обеспечение учебных занятий**

**3.1. Методическое обеспечение**

**3.1.1 Методические указания по освоению дисциплины**

Уровень и глубина освоения курса, как обычно, зависит от активной систематической работы обучающихся. В первой части курса необходимо освоить ряд классических понятий и теорем, для чего желательно (но не обязательно) решить предлагаемые преподавателем задач. Задачи служат закреплению и расширению теоретического материала лекций.

Наиболее важной частью работы является доклад-сообщение о результатах выбранной обучающимся совместно с преподавателем работы. Для успешного освоения дисциплины необходимо также участвовать в обсуждении рассматриваемых вопросов.

**3.1.2 Методическое обеспечение самостоятельной работы**

При самостоятельном изучении теоретического материала и выполнении практических заданий можно использовать рекомендованную основную и дополнительную литературу, работ, предложенных преподавателем во время работы семинара либо найденных обучающимся самостоятельно.

**3.1.3 Методика проведения текущего контроля успеваемости и промежуточной аттестации и критерии оценивания**

Текущий контроль не предусмотрен.

Для получения зачёта обучающийся должен получить больше 50 баллов. За один доклад (в зависимости от сложности темы и качества доклада) можно получить 20-40-60 баллов. Также баллы можно получить за активное участие в работе семинара. Преподаватель на последнем занятии может предложить участникам семинара оценить участие кого-либо из участников 10 или 20 или 30 дополнительными баллами. Если среди присутствующих на этом занятии обучающихся будет не более одного голоса «против», баллы будут засчитаны.

К зачёту допускаются все записанные на курс обучающиеся. Если к моменту проведения зачёта обучающийся имеет больше 50 баллов, он получает зачёт. Иначе необходимо ответить на 2 вопроса. Ответ на каждый вопрос оценивается в 0-20-40 баллов. На подготовку ответа даётся не менее одного академического часа (без каких-либо ограничений на используемые источники информации).

|  |  |  |  |
| --- | --- | --- | --- |
| Итоговый процент  выполнения, % | Оценка СПбГУ при  проведении зачёта | Оценка  ECTS | Оценка СПбГУ при  проведении экзамена |
| 90-100 | Зачтено | A | отлично |
| 80-89 | Зачтено | B | хорошо |
| 71-79 | Зачтено | C | хорошо |
| 60-70 | Зачтено | D | удовлетворительно |
| 50-59 | Зачтено | E | удовлетворительно |
| менее 50 | не зачтено | F | неудовлетворительно |

**3.1.4 Методические материалы для проведения текущего контроля успеваемости и промежуточной аттестации (контрольно-измерительные материалы, оценочные средства)**

Обучающимся требуется сделать доклады по актуальным на момент реализации дисциплины научным работам, указанным преподавателем, по следующим темам:

1. Элиминация кванторов в Арифметике Пресбургера.
2. Обобщение Виспфеннинга на задачу смешанного вещественно-целочисленного линейного программирования.
3. Арифметика Бюхи и результаты А. Л. Семёнова об обобщении элиминации кванторов.
4. Результаты об алгоритмической сложности фрагментов Арифметики Пресбургера.
5. Разрешимость и сложность экзистенциальной арифметики со сложением и делимостью.
6. Разрешимость арифметики Сколема.
7. Разрешимые экзистенциальные арифметики с умножением. Алгоритм Террье.
8. Вещественная арифметика: алгоритм Тарского.
9. Сложность алгоритма Тарского и алгоритм Коллинза.
10. Линейная вещественная арифметика и виртуальная подстановка.
11. Элиминация кванторов в линейной *p*-адической арифметике.
12. Неразрешимость 10-й проблемы Гильберта.
13. Неразрешимость экзистенциальной арифметики со сложением, делимостью и предикатом степенного роста

**3.1.5 Методические материалы для оценки обучающимися содержания и качества учебного процесса**

Для оценки обучающимися содержания и качества учебного процесса применяется анкетирование в соответствии с методикой и графиком, утвержденными в установленном порядке.

**3.2. Кадровое обеспечение**

**3.2.1 Образование и (или) квалификация штатных преподавателей и иных лиц, допущенных к проведению учебных занятий**

К проведению лекционных занятий должны привлекаться преподаватели, имеющие диплом о высшем образовании по соответствующему направлению.

**3.2.2 Обеспечение учебно-вспомогательным и (или) иным персоналом**

Не требуется.

**3.3. Материально-техническое обеспечение**

**3.3.1 Характеристики аудиторий (помещений, мест) для проведения занятий**

Требуется стандартная лекционная аудитория с меловыми или маркерными досками.

**3.3.2 Характеристики аудиторного оборудования, в том числе неспециализированного компьютерного оборудования и программного обеспечения общего пользования**

Не требуется.

**3.3.3 Характеристики специализированного оборудования**

Не требуется.

**3.3.4 Характеристики специализированного программного обеспечения**

Не требуется.

**3.3.5 Перечень и объёмы требуемых расходных материалов**

Мел, маркеры, тряпки для стирания мела, губки для стирания маркерной записи.

**3.4. Информационное обеспечение**

**3.4.1 Список обязательной литературы.**

1. Верещагин Н.К., Шень А. Лекции по математической логике и теории алгоритмов. Часть 2. Языки и исчисления. М.: МЦНМО, 2002.
2. Клини С.К. Математическая логика. М.: Мир, 1973.
3. Чень Ч., Ли Р. Математическая логика и автоматическое доказательство теорем. М.: Наука, 1983.
   * 1. **Список дополнительной литературы**
4. А. Л. Семёнов, Логические теории одноместных функций на натуральном ряде, Изв. АН СССР. Сер. матем., 1983, том 47, выпуск 3, 623–658
5. Handbook of Automated Reasoning. Editors A. Robinson and A. Voronkov. Elsevier Science, 2001. (Chapter 1 & Chapter 12)
6. Haase, C. A Survival Guide to Presburger Arithmetic // ACM SIGLOG News. vol. 8, no. 3 (2018), pp. 67-82.
7. Thomas Sturm. Thirty Years of Virtual Substitution. ISSAC 2018 - 43rd International Symposium on Symbolic and Algebraic Computation, Jul 2018, New York, United States.
8. Nipkow, T. Linear Quantifier Elimination // J Autom Reasoning. 2010. Vol. 45, P. 189–212.
9. Gu´epin F., Haase, C., Worrell, J. On the Existential Theories of B¨uchi Arithmetic and Linear p-adic Fields // 30th Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2019, pp. 1-10.
10. Lechner, A., Ouaknine J., Worrell J. On the Complexity of Linear Arithmetic with Divisibility // 30th Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2015, pp. 667-676.
11. [Bès](https://arxiv.org/search/cs?searchtype=author&query=B%C3%A8s%2C+A) A., [Choffrut](https://arxiv.org/search/cs?searchtype=author&query=Choffrut%2C+C) C. Theories of real addition with and without a predicate for integers // arXiv:2002.04282 [cs.LO], Feb. 2020.
12. Daniel Bundala, Joël Ouaknine:On parametric timed automata and one-counter machines. Inf. Comput. 253: 272-303 (2017)
13. Backeman, Peter et al. “Bit-Vector Interpolation and Quantifier Elimination by Lazy Reduction.” 2018 Formal Methods in Computer Aided Design (FMCAD) (2018): 1-10.
14. P´erez G. A. and Raha R. Revisiting Synthesis for One-Counter Automata // arXiv:2005.01071 [cs.LO], Oct. 2020.

**3.4.3 Перечень иных информационных источников**

Не предусмотрены.

**Раздел 4. Разработчики программы**

Старчак Михаил Романович, ассистент кафедры информатики, <mikhstark@gmail.com>.