Доклады семинара «Теория автоматов»

В 2022 году на научном семинаре «Теория автоматов» под руководством профессора Эльяра Эльдаровича Гасанова состоялось 14 докладов.

2 марта 2022 года

Асимптотически хорошие семейства классических и квантовых LDPC кодов

н.с. Пантелеев П. А., м.н.с. Калачев Г. В.

Классические LDPC коды являются важными компонентами современных систем хранения и передачи данных. Их квантовые аналоги (qLDPC коды) обещают значительную экономию ресурсов в протоколах для отказоустойчивых квантовых вычислений. Начиная с основополагающей работы Роберта Галлагера в начале 1960-х годов было известно, что существуют асимптотически хорошие семейства классических LDPC кодов, т.е. семейства, где размерность и минимальное расстояние растет линейно с ростом длины кода. Более того, 35 лет спустя Сипсер и Спилмен нашли эффективный способ построения таких кодов на основе графов расширителей (экспандерные коды). В то же время, вопрос о существовании асимптотически хороших квантовых LDPC кодов (qLDPC гипотеза) оставался открытым уже более двух десятилетий.

В докладе будет рассказано об аналоге экспандерных кодов Сипсера и Спилмена, позволяющем строить асимптотически хорошие семейства квантовых LDPC кодов на основе первых групп гомологий некоторого двумерного цепного комплекса, что доказывает qLDPC гипотезу. Более того, будет продемонстрировано как рассматривая вторые группы гомологий полученных цепных комплексов можно доказать существование классических локально тестируемых кодов с оптимальными асимптотическими параметрами, что в свою очередь решает другую важную открытую проблему, называемую c^3-гипотезой, ответ на которую также недавно независимо был получен в работе arXiv: 2111.04808.

В выступлении предполагается дать обзор конструкции и показать некоторые основные идеи, используемые в доказательстве, такие как понятие локальной минимальности, заимствованное из теории многомерных расширителей. Доклад основан на работе arXiv: 2111.03654.

9 марта 2022 года

Предикаты k-значной логики и задача удовлетворения ограничениям

с.н.с. Жук Д. Н.

В 1969 году была открыта удивительная связь между функциями и предикатами, а именно, было построено взаимно-однозначное соответствие между замкнутыми классами функций и замкнутыми классами предикатов. Несмотря на этот результат, многие годы именно функции были главным объектом исследований, а предикаты (отношения) оставались вспомогательным инструментом для описания предполных и замкнутых классов.

В докладе будет представлен обзор результатов, полученных с помощью подхода, в котором основным объектом являются предикаты, а функции играют лишь вспомогательную роль.

23 марта 2022 года

Оценки энергопотребления объёмных схем

м.н.с. Ефимов А. А.

Ещё в середине XX века в связи с интенсивным развитием вычислительной техники возникла задача синтеза схем, вычисляющих булевы функции и операторы. Одной из основных и наиболее подробно исследованных моделей схем является схема из функциональных элементов (СФЭ). В качестве характеристики оптимальности СФЭ можно рассматривать сложность — количество функциональных элементов, содержащихся в схеме. Таким образом, под сложностью булевой функции или оператора будем понимать минимальную сложность схемы, реализующую данную функцию или оператор.

Отметим, что в модели СФЭ не учитываются вполне естественные ограничения на размещение элементов схемы в плоскости или пространстве, способы их соединения, разводка проводов и т.п. В действительности, любая схема состоит из отдельных элементарных частей (функциональных элементов), которые имеют определенную длину, ширину и соединяются проводниками, размеры которых следует учитывать при оценке сложности реальных устройств.

В докладе рассматриваются объёмные схемы, являющиеся укладкой схем функциональных элементов в пространстве. Был рассмотрен класс объёмных схем, реализующих булевы операторы. Для этого класса получены верхняя и нижняя оценка потенциала — меры мощности, равной

количеству элементов схемы, выдающих единицу на данном входном наборе. Получен порядок функции Шеннона потенциала для класса всюду определенных операторов для объёмных схем без ограничений и схем с близкими выходами, а также нижняя оценка для частичных операторов.

30 марта 2022 года

Алгоритм, практически максимизирующий точность k-классификации на множестве представителей k классов эквивалентности

доц. Бернадотт А. К.

Идея данной работы родилась при решении задачи выбора словаря для разработки неинвазивного интерфейса мозг-компьютер с манипулятором для людей с ограниченными возможностями. При разработке устройства возникла необходимость подобрать словарь из слов-синонимов, объединенных в k классов эквивалентности по семантической близости. Задача состояла в том, чтобы найти такое множество представителей k классов эквивалентности, на котором k-точность классификации классификатором K удовлетворяет определенным критериям: (1) максимальная точность классификации, (2) максиминальная точность — точность классификации каждой пары распределений слов не ниже определенного значения. Идея заключалась в том, чтобы представить слова (множества), сгруппированные в k классов эквивалентности, в виде k-дольного взвешенного графа G и найти k-дольную клику, удовлетворяющую определенным критериям. Предложенный Алгоритм 1 позволял получить k-дольные клики с максимальной точностью классификации наихудшего случая; Алгоритм 2 обеспечивал k-дольные клики с максимальным суммарным весом. Задача поиска максимальной клики относится к классу NP-трудных. Однако представленные алгоритмы позволяют выбрать набор представителей оптимально с точки зрения практической максимизации точности классификации и времени выполнения. Алгоритмы увеличивают скорость подбора представителей на 5 порядков по сравнению с алгоритмом полного перебора с небольшой потерей точности.

13 апреля 2022 года

Вопросы выразимости в классах кусочно-линейных функций

инженер Кан А. Н.

Кусочно-линейные функции используются при проектировании искусственных нейронных сетей, к ним относятся суперпозиции из линейных функций и ReLU. Работа продолжает исследования В. С. Половникова по выразимости через суперпозиции в классах кусочно-линейных функций, содержащих линейные функции. При этом ограничении для класса кусочно-линейных функций найдены предполные классы. Одним из них является класс согласованных функций, который содержит единственный предполный подкласс, включающий линейные функции. Показано, что любая кусочно-линейная непрерывная функция двух переменных выражается через линейные функции и ReLU. Построена решетка одноместных следов замкнутых классов кусочно-линейных функций с рассматриваемым ограничением.

18 мая 2022 года

Асимптотика числа пороговых функций и асимптотика числа вырожденных ± 1-матриц

доц. Ирматов А. А.

В докладе будет рассказано о решении двух, ставших уже классическими, проблем дискретной математики, математической кибернетики и комбинаторики. Одной из этих проблем является нахождение асимптотики числа пороговых функций, которая в статье А.Д.Коршунова (см. А.Д.Коршунов, УМН, 2009, Т.64, В.5(389)) включена в список важных нерешенных проблем дискретной математики и математической кибернетики. В 19 веке L. Schläfli в эквивалентных терминах получил (около 1850 г.) верхнюю оценку для числа пороговых функций $P(2,n)$:

$$P(2,n) \leq 2\sum_{i=0}^{n}\binom{2^n-1}{i}.$$

С конца 50-х годов прошлого века вопрос о нахождении числа пороговых функций стал одним из центральных вопросов пороговой логики. В ряде статей были получены нижние оценки для $P(2,n)$, близкие по порядку логарифма к верхней оценке L. Schläfli. Наилучшая нижняя оценка в этой серии работ была получена автором в 1993 году:

$$P(2,n) \geq 2^{n^2\left(1-\frac{7}{\ln n}\right)} \cdot P\left(2, \left[\frac{7(n-1)}{\log_2(n-1)}\right]\right).$$

Проблема о распределении значений детерминанта ± 1-матрицы интенсивно изучается с 30-х годов 20-го века (см. A.M.Odlyzko, Journal of Comb.Theory, Ser.A 47, 124-133 (1988)). В 1963 году Komlós J. (опубликовано в 1967 году) доказал, что вероятность вырожденности случайной Бернуллиевой 0,1-матрицы M_n с ростом размерности стремится к нулю, что верно и для ± 1-матриц:

$$\mathbb{P}_n \stackrel{def}{=} \Pr\left(\det M_n = 0\right) = o_n(1).$$

В 1977 году он улучшил свой результат до верхней оценки

$$\mathbb{P}_n < O\left(\frac{1}{\sqrt{n}}\right).$$

В 1995 году Kahn J., Komlós J. и Szemerédi E. добились экспоненциального убывания верхней оценки: $(0.999 + o_n(1))^n$. В 2007 году Tao T. и Vu V. получили оценку $\left(\frac{3}{4} + o_n(1)\right)^n$, а в 2009 году Bourgain J., Vu V. H. и Wood P. M. улучшили ее до $\left(\frac{\sqrt{2}}{2} + o_n(1)\right)^n$. В 2018 году К. Тихомировым было показано, что

$$\mathbb{P}_n = \left(\frac{1}{2} + o_n(1)\right)^n.$$

В докладе будет исследовано представление числа пороговых функций в комбинаторно-топологических терминах, вытекающего из работ L. Schläfli, Zaslavsky T., Hall P. и Folkman J., и показана связь числа $P(2,n)$ с числом вырожденных ± 1-матриц, позволяющая установить следующие асимптотики.

Теорема 1. *Асимптотика вероятности $\mathbb{P}_n$ равна:*

$$\mathbb{P}_n \sim (n-1)^2\, 2^{1-n}, n \to \infty.$$

Теорема 2. *Асимптотика числа пороговых функций равна:*

$$P(2,n) \sim 2\binom{2^n - 1}{n}, n \to \infty.$$

Полное изложение результатов можно найти по адресу
https://arxiv.org/pdf/2004.03400v3.pdf

14 сентября 2022 года

Параметро-эффективная расшифровка булевых функций

м.н.с. Быстрыгова А. В.

Расшифровка функций (learning theory) — направление математики, которое началось развиваться практически полвека назад. Эта область остается актуальной и по сей день, поскольку связана с восстановлением оптимальным образом информации об исследуемом объекте на основе частичных сведений о нем. Более формально, под расшифровкой функции из заданного класса F понимают игру между "учеником" и "учителем", в которой учитель загадывает одну функцию из класса F, а ученик, зная этот класс F полностью, но не зная выбор учителя, задает учителю запросы разрешенного типа, получает ответы от учителя и на основе этих ответов восстанавливает какую-то информацию про выбранную функцию.

Чтобы оценить, насколько быстро можно расшифровать функции из того или иного класса, вводят понятие сложности расшифровки как максимальное число запросов, которое ученик должен задать учителю для расшифровки самой "плохой" функции. Иными словами, ученик выбирает "лучшую" стратегию восстановления функции. Затем проверяется, сколько запросов потребуется задать ученику, использующему эту стратегию, чтобы восстановить каждую функцию из класса. За сложность расшифровки принимают максимум среди этих значений.

В докладе будут представлены результаты сложности расшифровки булевых функций ограниченного веса для четырех типов запросов (запросы на значение, запросы на сравнение, запросы на ограниченную и расширенную эквивалентность), а также оценки сложности расшифровки всех замкнутых классов решетки Поста для двух типов запросов (запросы на значение, запросы на сравнение).

19 октября 2022 года

Булевы биюнктивные функции и порождаемые ими системы булевых уравнений

доц. Тарасов А. В.

Доклад посвящен результатам из области исследования булевых биюнктивных функций. Класс биюнктивных функций (функций, представимых в виде 2-КНФ) является одним из классов Шефера, порождающих полиномиально решаемые системы булевых уравнений.

Ряд задач, связанных с этими функциями, является труднорешаемыми. К таковым относится, в частности, задача нахождения веса функции по её 2-КНФ, известная как задача #2-SAT. Вместе с тем, 2-КНФ, представляющие биюнктивные функции, допускают компактное представление в виде ориентированных графов. В докладе обсуждаются методы эффективного оценивания веса биюнктивных функций. Данная задача фактически эквивалентна задаче оценки числа решений булевой двучленной системы уравнений.

Поскольку класс биюнктивных функций относится к классам Шефера, в докладе обсуждаются вопросы связи класса биюнктивных функций с другими классами Шефера. Центральным результатом здесь является описание групп преобразований n-мерного векторного пространства, стабилизирующих множество биюнктивных функций от n переменных и ряд его подмножеств.

Третья часть доклада посвящена изучению параметров метода максимального правдоподобия для решения систем булевых уравнений, порожденных дважды биюнктивными функциями, то есть такими биюнктивными функциями, отрицание которых также является биюнктивной функцией.

26 октября 2022 года

Цифровая подпись на основе кодов, определяющих изображения с точностью до аффинных преобразований

проф. Козлов В. Н.

Первый “допотопный” вариант защиты документа от подделки (используется, однако, и поныне) — это так называемая “живая” подпись (или факсимиле), и канцелярская печать. Но в наши дни документооборот большей частью электронный, и, зачастую, с очень большим числом документов (электронные торги, банковские платежные системы, сделки в криптовалютах, и пр.). Факсимиле в этом случае неудобно, а главное — крайне ненадежно. Здесь работает возникшая около тридцати лет назад цифровая подпись (или электронная цифровая подпись — ЭЦП). Как правило, сердцевиной этой конструкции, т.е. ЭЦП, является функция, у которой ее значение при заданном значении аргумента, вычисляется легко, а обратное, т.е. вычисление значения аргумента при известном значении функции, очень трудно. В докладе описывается аналог цифровой подписи на другой принципиальной основе — на использовании кодов, определяющих изображения с точностью до аффинных преобразований. Это способ защиты электронного изображения от подделки и проверки

подлинности полученной информации. Способ предназначен для работы с любыми изображениями (потенциально и с трехмерными), или с информацией, приводимой к изображениям (например, со звуком). В целом способ может быть использован для защиты канала связи между отправителем информации в виде изображения и получателем от попыток третьих сторон отправить получателю информацию под видом информации от отправителя, а также аутентификации полученного изображения или информации, приводимой к виду изображения.

9 ноября 2022 года

Об укладках схем из функциональных элементов на плоскости и в пространстве

м.н.с. Калачев Г. В.

В докладе будет рассказано о различных моделях схем, учитывающих ограничения на размещение элементов на плоскости или в пространстве. Первая часть доклада будет посвящена обзору различных результатов о сложности реализации булевых функций (и операторов) клеточными схемами, известные асимптотические оценки для клеточных схем. Во второй части доклада будет кратко рассказано о связи сложности клеточных схем со сложностью в других схожих моделях, таких как планарные схемы, клеточные схемы ограниченной ширины, трехмерные клеточные схемы, многослойные схемы. Рассматривается функция сложности преобразования схемы из одной модели в другую, и в терминах этой функции формулируются результаты о связи сложности в различных моделях. В связи с этим естественным образом возникает класс задач, где для данной пары моделей нужно оценить функцию сложности преобразования из одной модели в другую. Несмотря на то, что иногда эта функция оценивается с использованием уже известных результатов, для многих пар моделей вопрос остаётся открытым.

16 ноября 2022 года

Активность в различных моделях схем

м.н.с. Калачев Г. В.

В докладе речь пойдёт о различных мерах активности для схем из функциональных элементов и клеточных схем. Различные меры сложности схем моделируют различные характеристики чипов. Например, сложность схемы отражает площадь чипа, глубина схемы отражает задержку сингала на выходе, что в свою очередь определяет тактовую частоту устройства. Активность (также называемая мощностью) схемы

- мера сложности, отражающая энергопотребление физического устройства. Одним из наиболее естественных способов определить активность схемы — посчитать максимальное (или среднее) число единиц на выходах элементов, где максимум (или среднее) берётся по всевозможным входным наборам. Это наиболее исследованная мера активности схем, однако есть и другие способы определять активность, о которых будет рассказано в первой части доклада. Также будет дан обзор известных результатов об активности схем из функциональных элементов.

Во второй доклада части речь пойдёт об активности плоских и объёмных клеточных схем. Будут рассказаны результаты о связи мер сложности и активности, а также результаты о поведении функции Шеннона активности плоских и объёмных клеточных схем для класса частичных операторов. На примере класса всех булевых функций от n переменных будут проиллюстрированы несколько основных идей, используемых в доказательствах этих результатов.

23, 30 ноября 2022 года

О проблеме выполнимости булевых формул

доц. Боков Г. В.

Доклад посвящен проблеме выполнимости булевых формул и подходах к ее решению. Будет рассказано о различных моделях формальных систем, представляющих как общий, так и частные случаи проблемы выполнимости. В докладе рассматриваются ограничения на класс допустимых формул и перечень используемых тактик. Будет представлен сравнительных обзор известных результатов по этой теме.

7 декабря 2022 года

Тензорные сети для эффективной симуляции квантовых вычислений

н.с. Пантелеев П. А.

Тензорные сети являются важным инструментом, позволяющим в некоторых частных случаях значительно понижать сложность задач, для которых в общем случае не имеется эффективного алгоритма решения. Одним из многочисленных примеров подобных задач является задача симуляции квантовых схем маленькой глубины на классическом компьютере. В докладе предполагается рассказать об эффективных методах симуляции на основе тензорных сетей, а также о применении данных методов к случайным схемам, возникающим в экспериментах по демонстрации квантового превосходства.

14 декабря 2022 года

A-предпредполные классы в классе линейных автоматов

доц. Часовских А. А., асп. Бирюкова В. А.

В. А. Буевич ввел понятие аппроксимационного замыкания (A-замыкания) в классе конечных автоматов над двухэлементной логикой $P^2_{\text{о.д.}}$ что, по сравнению с замыканием по операциям композиции (K-замыкания), позволило увеличивать выразительные возможности его подмножеств. Вячеслав Александрович показал, что мощность множества A-предполных классов в $P^2_{\text{о.д.}}$ счетна, а не континуальна, как для оператора K-замыкания (В. Б. Кудрявцев). Несмотря на это, задача проверки A-полноты конечных подмножеств конечных автоматов, как и в случае K-замыкания, осталась алгоритмически неразрешимой (М. И. Кратко).

Для подкласса $L^2_{\text{о.д.}}$ класса $P^2_{\text{о.д.}}$, состоящего из линейных автоматов, количество K-предполных классов счетно, количество A-предполных классов конечно, задачи проверки K-полноты и A-полноты конечных подмножеств алгоритмически разрешимы. Эти же утверждения справедливы для классов линейных автоматов над конечными полями.

Доклад посвящен изучению A-предполных классов в $L^2_{\text{о.д.}}$. Для них построены A-базисы, найдены все их A-предполные подклассы. Таким образом, в решетке A-замкнутых классов $L^2_{\text{о.д.}}$ определены два слоя максимальных собственных подклассов. Несмотря на континуальность A-замкнутых подклассов в классе $L^2_{\text{о.д.}}$, количество A-предполных и A-предпредполных классов в нем конечно, что располагает к дальнейшим исследованиям задачи A-выразимости в $L^2_{\text{о.д.}}$.