

Доклады семинара «Теория автоматов»

В первом полугодии 2025 года на научном семинаре «Теория автоматов» под руководством профессора Эльяра Эльдаровича Гасанова состоялось 14 докладов.

19 февраля 2025 года

Задачи машинного обучения в электронной торговле и транспортных технологиях

м. н. с. А. П. Соколов

В докладе будут рассмотрены некоторые сервисы электронной торговли и транспортных технологий, в которых применяются методы машинного обучения. Будут рассмотрены актуальные постановки задач, по которым проводятся исследования в рамках службы развития ML технологий Яндекса, подходы к решению этих задач и ближайшие планы.

26 февраля 2025 года

Классы линейных 2-адических автоматов с сумматором

асп. М. Э. Калашников

Для линейных автоматов известны результаты о выразимости линейных автоматных функций через системы, содержащие сумматор. Также известен критерий вхождения сумматора в замкнутый класс линейных функций.

В докладе будет рассказано о линейных 2-адических автоматах и некоторых предполных классах в них. Докладчиком получены критерий выразимости произвольных линейных 2-адических функций в системах с сумматором и критерий вхождения сумматора в произвольный замкнутый класс. Также будет описана критериальная система предполных классов в T_0 , множестве линейных 2-адических автоматов, сохраняющих 0 в начальный момент времени.

5 марта 2025 года

Лабиринты и автоматные системы

ст. н. с. Н. Ю. Волков

В докладе даётся обзор и критический разбор некоторых моделей взаимодействия систем автоматов в лабиринтах. Предложена формализация модели системы автоматов в лабиринте через автоматную систему. Такая формализация является весьма универсальной и даёт необходимую строгость. Введён класс классических лабиринтов.

Автоматная система S — это множество параметров X с функцией обзора $\beta : X \rightarrow A$ ($|A| < \infty$), конечное множество преобразований множества X , параметризованное функцией-преобразователем $\gamma : B \rightarrow C(X)$ ($|B| < \infty$, здесь $C(X)$ — частичные отображения X в себя) и конечный автомат \mathcal{A} с входным алфавитом A и выходным алфавитом B . Таким образом, $S = (\mathcal{A}, X, \beta, \gamma)$. Модель автоматной системы является наиболее универсальным вычислителем. Множество автоматных систем, имеющих разные автоматы \mathcal{A} , но одни и те же X, A, B, β, γ , называется типом автоматных систем. Тип автоматных систем задаётся вычислительным пространством $\mathcal{X} = (X, A, B, \beta, \gamma)$. Таким образом, $S = (\mathcal{A}, \mathcal{X})$.

Очевидно, что любая система автоматов в лабиринтах может быть смоделирована автоматной системой. Оказалось верно и обратное: любая автоматная система моделируется одним автоматом в классическом лабиринте, или в семействе классических лабиринтов. Таким образом, модель автомата в классическом лабиринте является ведущим частным случаем максимально универсальной модели автоматной системы. При этом, каждый классический лабиринт задаёт вычислительное пространство.

Определяется понятие класса алгоритмов над лабиринтом L (или, что то же самое, над вычислительным пространством X). Каждый алгоритм над лабиринтом L задаётся автоматом, способным перемещаться в этом лабиринте. Два алгоритма эквивалентны, если поведения задающих их автоматов в лабиринте L совпадают при любой точке старта. Этот подход равносильен заданию алгоритма как класса сильно-эквивалентных друг другу автоматных систем над фиксированным вычислительным пространством. Такое определение алгоритма позволяет изучать намного более широкие классы алгоритмов, чем Тьюринговы алгоритмы. В отличие от описания сверхтьюринговых алгоритмов при помощи модели *вычислений с оракулом*, которая есть лишь искусственная надстройка над Тьюринговыми алгоритмами, наш подход позволяет изложить теорию алгоритмов более системно и с общих позиций.

12 марта 2025 года

Проблема полноты в классе линейных дефинитных автоматов

асп. И. В. Молдованов

Проблема проверки полноты конечных подмножеств играет важную роль при исследовании функциональных систем. В классе конечных автоматов с операциями композиции задача проверки полноты конечных подмножеств является алгоритмически неразрешимой, тогда как класс конечных автоматов с операциями суперпозиции не содержит конечных полных систем. Подкласс дефинитных автоматов характеризуется наличием конечных полных систем относительно операций суперпозиции, однако задача проверки полноты конечных подмножеств в данном случае также оказывается алгоритмически неразрешимой.

Ранее был рассмотрен класс линейных автоматов с операциями композиции. Для данного класса был получен алгоритм определения полноты конечных подмножеств. В то же время для линейных автоматов с операциями суперпозиции было установлено отсутствие конечных полных систем. Интерес представляет рассмотрение данной задачи применительно к классу дефинитных линейных автоматов с операциями суперпозиции. В рамках доклада будет освещена критериальная система для класса одноместных линейных дефинитных автоматов, сохраняющих нулевую последовательность, а также представлен алгоритм проверки полноты конечных содержащих константу ноль подмножеств в классе линейных дефинитных автоматов.

19 марта 2025 года

Решение арифметических задач клеточными автоматами с локаторами

проф. Э. Э. Гасанов

В докладе будет введено понятие клеточного автомата с локаторами. С помощью этих автоматов будут решены следующие задачи: перевод натурального числа из унарного представления в бинарное, перевод натурального числа из бинарного представления в унарное, сложение, умножение и деление натуральных чисел, вычисление суммы большого числа натуральных чисел.

26 марта 2025 года

Универсальные алгоритмы для решения задачи удовлетворения ограничениям

ст. н. с. Д. Н. Жук

Универсальным алгоритмом для задачи удовлетворения ограничениям мы называем алгоритм, который на вход получает экземпляр задачи и за полиномиальное время выдает ответ (иногда правильный, иногда нет) и при этом никак не привязан к языку ограничений и другим параметрам задачи. Обычно такие алгоритмы либо пытаются вывести какое-то противоречие локально, либо сводят задачу к задаче линейного программирования и пытаются получить противоречие там. Если же противоречие получить не удастся, алгоритм просто возвращает «Да». Чтобы усилить такие алгоритмы, мы можем сначала зафиксировать какую-то переменную каким-то значением, а потом запустить алгоритм, и если он вернет «Нет», удалить это значение из области значений соответствующей переменной.

Мне удалось придумать универсальную конструкцию, которая позволила для каждого из универсальных алгоритмов описать когда его усиленная версия корректно решает задачу. Кроме этого, удалось показать, что самый сильный из этих алгоритмов решает задачу удовлетворения ограничениям на любом языке ограничений на 7-элементном множестве, но уже на 8-элементном множестве есть язык ограничений, который не решается никакой комбинацией известных универсальных алгоритмов.

2 апреля 2025 года

Использование контрольной суммы для улучшения восстанавливающей способности многоуровневых кодов

доц. Д. В. Алексеев, м. н. с. Д. В. Ронжин

В рамках доклада будет представлено краткое введение в схемы, использующиеся для помехоустойчивого кодирования в СХД (системах хранения данных), и методы оценки надежности этих схем. Будет описан метод для улучшения корректирующей способности многоуровневых кодовых схем, предложенный авторами. Метод основан на использовании дополнительной избыточности данных (CRC) и итерационном декодировании с локализацией ошибок.

О новой системе шифрования с открытым ключом рюкзачного типа

доц. А. А. Ирматов, асп. А. И. Болотников

Задача о чередующемся взвешенном пути возникла при изучении разбиений пространства функций весов уравнениями конфигурации паросочетаний. Для данной задачи была доказана NP-полнота. В докладе будет представлена построенная на её основе новая система шифрования Болотникова—Ирматова с открытым ключом рюкзачного типа.

О сложности задачи существования в нейронной сети предельного цикла заданной длины

доц. Г. В. Боков, асп. А. С. Дробышев

В докладе будет рассказано о модели нейронной сети, представляющей собой ориентированный граф, вершинам которого приписаны пороговые булевы функции. Вершины такого графа называются нейронами, а входящие ребра определяют связь нейрона с соседними нейронами так, что между входящими ребрами и существенными переменными пороговой функции нейрона устанавливается взаимно однозначная связь. Нейронная сеть функционирует в дискретные моменты времени и каждый такт пересчитывает состояние каждого нейрона. Состояние всех нейронов называется конфигурацией сети. Представляет интерес исследовать поведение конфигурации нейронной сети с точки зрения длины предельного цикла, которому она может принадлежать. В докладе будет представлен ряд результатов, связанных с оценкой сложности задачи существования в нейронной сети предельного цикла заданной длины.

9 апреля 2025 года

О модификации диаграммы Мура функцией отрицания

студ. Д. О. Маслеников

В докладе вводится понятие результата применения функции $f : B \rightarrow B$ к инициальному автомату. После того, как автомат совершает переход из состояния в состояние, происходит изменение его диаграммы: если был выведен символ b , он заменяется на данном переходе на $f(b)$. Полученную словарную функцию называем результатом применения правила f к автомату.

Можно показать, что данная словарная функция является ограниченно-детерминированной с не более чем $n \cdot |B|^{n \cdot |A|}$ остаточных функций, где n — число состояний, поэтому далее рассматриваем её как инициальный автомат приведённого вида.

Для результата применения функции отрицания к сильно связному автомату с входным и выходным алфавитом $\{0, 1\}$ получены верхняя и нижняя оценки числа его состояний: $n \cdot 2^{n+1}$ и 2^{n+1} соответственно.

Вводятся понятие остова — неинициального автомата без функции выхода — и результата применения к нему функции — неинициального аналога результата применения функции к автомату. Рассматриваются две серии примеров применения отрицания к остову. Как следствие, показана неулучшаемость оценок приведённых выше — верхней в общем случае, и нижней для нечётных n .

16 апреля 2025 года

Предикатное задание минимальных клонов трехзначной логики

студ. А. И. Зданович

Минимальные клоны являются нижними элементами решетки замкнутых классов, содержащих тождественную функцию. По аналогии с существованием не конечно порожденного предполного класса, можно задать «двойственный» вопрос о существовании не предикатно описуемого минимального клона. В данном докладе мы обсудим предикатное задание минимальных клонов трехзначной логики, а также приведем не предикатно описуемый минимальный клон для произвольной значности.

Об отношениях на конечном множестве, обладающих внутренней симметрией

студ. А. Е. Жариков

Из соответствия Галуа между клонами и замкнутыми множествами предикатов мы знаем, что любой клон можно задать как класс сохранения какого-то множества предикатов. При этом можно показать, что для этого не требуются все предикаты, а достаточно использовать только существенные предикаты или, ещё точнее, только ключевые предикаты. В данном докладе будет дан ответ на вопрос, какую долю составляют существенные предикаты от числа всех предикатов при различных k . Для $k > 2$ описать все ключевые предикаты достаточно сложно, поэтому будут введены подклассы ключевых предикатов, обладающих дополнительными свойствами, усиливающими их симметрию: абсолютно ключевые и биективно ключевые предикаты. Для случая $k = 3$ будет дано описание биективно ключевых предикатов.

23 апреля 2025 года

Полиномиальная полнота и полнота n -квазигрупп: критерии и методы обеспечения

студ. С. С. Чаплыгина

Доклад посвящен исследованию ряда свойств квазигрупп и n -квазигрупп с точки зрения их применения в задачах криптографии. Рассматриваемые алгебраические структуры представляют интерес для создания различных криптоалгоритмов, таких как шифры, хэш-функции, протоколы аутентификации и другие. Для обеспечения стойкости важно требовать от квазигрупп выполнения особых свойств. В. А. Артамоновым было предложено рассматривать полиномиально полные квазигруппы без собственных подквазигрупп. Следствием результата Й. Хагеманна и К. Херрманна о полиномиальной полноте алгебры, содержащей мальцевскую операцию, а также работы В. А. Артамонова является критерий полиномиальной полноты квазигруппы как алгебры с тремя операциями. В докладе предлагается критерий полиномиальной полноты n -квазигрупп как алгебр с одной операцией (квазигрупповой), а также критерий полноты n -квазигрупп. Вторым результатом, представленным в докладе, являются алгоритмы, которые с помощью изотопных преобразований усиливают криптографические свойства. В случае квазигрупп удается добиться полиномиальной полноты, простоты, неафинности, отсутствия подквазигрупп и тривиальности группы автоморфизмов. В случае n -квазигрупп при $n = 3$ на выходе алгоритма гарантируется либо полиномиальная полнота, либо отсутствие собственных подквазигрупп. При $n > 3$ удается добиться одновременного выполнения обоих свойств. Предложенный алгоритм является обобщением и усилением известного результата Т. Кепки.

14 мая 2025 года

О восстановлении последовательностей машины Тьюринга

асп. В. В. Ушакова

Доклад посвящён изучению машин Тьюринга. Вводятся и рассматриваются последовательности машины Тьюринга: последовательность входных символов, последовательность выходных символов, последовательность состояний, а также последовательность перемещений.

Пусть некоторые из рассматриваемых четырёх последовательностей машины Тьюринга неизвестны. Рассматривается возможность восстановления неизвестных последовательностей по известным. Рассматрива-

ются разные случаи, когда программа и вход машины Тьюринга заданы и не заданы.